

<u>WSTĘP</u>	6
--------------------	---

<u>CZEŚĆ I. PROBLEMATYKA PRZETWARZANIA DANYCH</u> <u>OSOBOWYCH PRZEZ PODMIOTY PUBLICZNE</u> <u>I PRYWATNE</u>	9
---	---

<u>A. ZAGADNIENIA OGÓLNE</u>	9
------------------------------------	---

<u>I. Definicja danych osobowych</u>	9
<u>II. Pojęcie administratora danych</u>	10
<u>III. Zbiory danych osobowych</u>	12
<u>IV. Przekazywanie danych osobowych za granicę</u>	12
<u>V. Ustawa o ochronie danych osobowych a przepisy Kodeksu postępowania</u> <u>administracyjnego</u>	13
<u>VI. Umowa powierzenia</u>	15

<u>B. SPRAWY Z ZAKRESU ADMINISTRACJI PUBLICZNEJ</u>	17
---	----

<u>I. Przetwarzanie danych osobowych przez organy administracji samorządowej</u>	17
<u>I.1 Sprawy z zakresu komunikacji</u>	17
<u>I.2 Urzędy Stanu Cywilnego</u>	18
<u>I.3 Oświata</u>	20
<u>I.4 Straż Miejska</u>	22
<u>I.5 Pomoc społeczna</u>	24
<u>I.6 Inne sprawy związane z problematyką przetwarzania danych przez samorządy</u>	28
<u>II. Przetwarzanie danych przez organy administracji rządowej</u>	38
<u>III. Przetwarzanie danych osobowych przez inne organy</u>	42
<u>IV. Inne sprawy</u>	45

<u>C. PRZETWARZANIE DANYCH OSOBOWYCH PRZEZ</u> <u>FUNKCJONARIUSZY SŁUŻB PUBLICZNYCH</u>	47
--	----

<u>I. Przetwarzanie danych osobowych przez Policję</u>	47
--	----

<u>II. Przetwarzanie danych osobowych przez Służbę Więzienną</u>	52
<u>III. Przetwarzanie danych osobowych przez Wojskowe Komendy Uzupelnień</u>	53
<u>D. ORGANY WYMIARU SPRAWIEDLIWOŚCI</u>	54
<u>I. Zakres i podstawy przetwarzania danych osobowych przez sądy</u>	56
<u>II. Przetwarzanie danych osobowych przez prokuraturę</u>	71
<u>III. Problematyka przetwarzania danych osobowych przez komorników sądowych</u>	80
<u>E. PRZETWARZANIE DANYCH OSOBOWYCH W ZAKRESIE</u>	
<u>OCHRONY ZDROWIA</u>	84
<u>I. Przetwarzanie danych osobowych przez Kasy Chorych</u>	85
<u>II. Udostępnianie danych medycznych przez podmioty opieki zdrowotnej</u>	96
<u>III. Inne sprawy</u>	116
<u>F. PRZETWARZANIE DANYCH OSOBOWYCH PRZEZ</u>	
<u>SPÓŁDZIELNIE I WSPÓLNOTY MIESZKANIOWE</u>	116
<u>G. STOSUNKI PRACY</u>	127
<u>H. PRZETWARZANIE DANYCH OSOBOWYCH W SEKTORZE</u>	
<u>TELEKOMUNIKACJI</u>	147
<u>I. PRZETWARZANIE DANYCH OSOBOWYCH PRZEZ BANKI,</u>	
<u>ZWIĄZEK BANKÓW POLSKICH I INSTYTUCJE</u>	
<u>WSPÓŁPRACYJĄCE Z BANKAMI</u>	160
<u>J. DZIAŁALNOŚĆ MARKETINGOWA</u>	175
<u>K. PRZETWARZANIE DANYCH OSOBOWYCH PRZEZ ZAKŁADY</u>	
<u>UBEZPIECZENIOWE I FUNDUSZE EMERYTALNE</u>	186

CZEŚĆ II. KONTROLE.....198

<u>I. Ocena zabezpieczeń organizacyjnych i technicznych systemów informatycznych przez administratorów danych osobowych</u>.....	199
<u>I.1 Warunki techniczne i organizacyjne w jakich przetwarzane były dane osobowe w dużych i średnich jednostkach organizacyjnych</u>	200
<u>I.2 Polityka bezpieczeństwa, techniczne warunki przetwarzania</u>	200
<u>I.3 Instrukcje i procedury</u>	202
<u>I.4 Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych</u>	205
<u>I.5 Warunki techniczne i organizacyjne w jakich przetwarzane były dane osobowe w małych jednostkach organizacyjnych</u>	206
<u>I.6 Uchybienia w zakresie wymagań funkcjonalnych stawianych systemom informatycznym przetwarzającym dane osobowe</u>	208
<u>II. Omówienie zakresu kontroli w poszczególnych jednostkach organizacyjnych</u>....	209

CZEŚĆ III. REJESTRACJA ZBIORÓW DANYCH OSOBOWYCH.....259

<u>I. Zagadnienia wstępne dotyczące procesu rejestracyjnego</u>.....	259
<u>II. Zawiadomienia o zwolnieniach i zgłoszeniach przez podmioty nieuprawnione</u>...	262
<u>II.1 Zwolnienia z obowiązku zgłoszenia zbioru danych osobowych do rejestracji</u>	262
<u>1) Zbiory danych osobowych przetwarzanych przez właściwe organy dla potrzeb postępowania sądowego (art. 43 ust. 1 pkt 2)</u>	263
<u>2) Zbiory danych osobowych dotyczących osób zatrudnionych, zrzeszonych lub uczących się (art. 43 ust. 1 pkt 4)</u>	263
<u>3) Zbiory danych osobowych dotyczące osób korzystających z usług medycznych, obsługi notarialnej, adwokackiej lub rady prawnego (art. 43 ust. 1 pkt 5)</u>	265
<u>4) Zbiory danych osobowych tworzonych na podstawie ordynacji wyborczych do Sejmu, Senatu, rad gmin, rad powiatów i sejmików województw, ustawy o wyborze Prezydenta Rzeczypospolitej Polskiej oraz ustaw o referendum gminnym (art. 43 ust. 1 pkt 6)</u>	266
<u>5) Zbiory danych osobowych przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub sprawozdawczości finansowej (art. 43 ust. 1 pkt 8)</u>	266
<u>6) Zbiory danych osobowych powszechnie dostępnych (art. 43 ust. 1 pkt 9)</u>	267
<u>7) Zbiory danych osobowych przetwarzanych w zakresie drobnych bieżących spraw życia codziennego (art. 43 ust. 1 pkt 11)</u>	268

<u>II.2 Zgłoszenia zbiorów danych osobowych do rejestracji dokonane przez podmioty nieuprawnione</u>	268
<u>III. Postępowania wyjaśniające</u>	269
<u>III.1 Postępowania wyjaśniające zakończone rejestracją zbioru danych osobowych</u>	269
<u>III.2 Postępowania wyjaśniające zakończone wydaniem decyzji odmawiającej rejestracji</u>	272
<u>IV. Zaświadczenia</u>	277
<u>V. Wnioski</u>	277
 <u>CZEŚĆ IV. ZAWIADOMIENIA O POPEŁNIENIU PRZESTĘPSTWA</u>	283
 <u>CZEŚĆ V. WYSTĄPIENIA GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH</u>	298
 <u>CZEŚĆ VI. PROPAGOWANIE IDEI OCHRONY DANYCH OSOBOWYCH</u>	351
 <u>WNIOSKI KOŃCOWE</u>	356
 <u>ZAŁĄCZNIKI</u>	368
<u>Załącznik nr 1</u>	368
<u>Załącznik nr 2</u>	372
<u>Załącznik nr 3</u>	380
<u>Załącznik nr 4</u>	381
<u>Załącznik nr 5</u>	386
<u>Załącznik nr 6</u>	387
<u>Załącznik nr 7</u>	388
<u>Załącznik nr 8</u>	392

GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

**SPRAWOZDANIE
Z DZIAŁALNOŚCI GENERALNEGO INSPEKTORA
OCHRONY DANYCH OSOBOWYCH**

ZA OKRES

01.01.2000 r. – 31.12.2000 r.

Wstęp

Sprawozdanie Generalnego Inspektora Ochrony Danych Osobowych, składane na podstawie art. 20 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.), obejmuje okres od 1 stycznia do 31 grudnia 2000 r.¹

W roku 2000 do Generalnego Inspektora wpłynęły 5 652 sprawy, w tym: 761 skarg na administratorów danych osobowych, 1628 pytań i wniosków o interpretację ustawy o ochronie danych osobowych oraz relację ustawy do innych aktów normatywnych, 462 wnioski o zaopiniowanie projektów aktów prawnych z punktu widzenia zgodności z ustawą o ochronie danych osobowych i 2801 zgłoszeń do zarejestrowania zbiorów danych osobowych.

W porównaniu z rokiem 1999 wzrosła liczba skarg na działania administratorów danych osobowych (w 1999 r. – 479) oraz liczba aktów prawnych skierowanych do zaopiniowania (w 1999 r. – 262), zmniejszyła się natomiast liczba pytań o interpretację przepisów ustawy (w 1999 r. – 1902) oraz – znacząco – liczba zgłoszeń do zarejestrowania zbiorów danych osobowych (w 1999 r. – 69 974).²

Podobnie, jak w roku 1999, także w 2000 r., sprawy związane z rejestracją zbiorów danych osobowych stanowiły znaczącą część działalności Generalnego Inspektora. W roku sprawozdawczym zarejestrowanych zostało 35 675 zbiorów danych osobowych, natomiast w 4031 wypadkach zostało wszczęte postępowanie administracyjne wskutek nieprawidłowego zgłoszenia zbioru danych do zarejestrowania, a w 62 sprawach wydane zostały decyzje odmawiające rejestracji. Wydanych zostało także 1890 zaświadczeń o zarejestrowaniu zbioru.

¹ Generalny Inspektor Ochrony Danych Osobowych działa na podstawie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.) oraz przepisów wykonawczych do ustawy: rozporządzenia Prezydenta Rzeczypospolitej Polskiej z dnia 29 maja 1998 r. w sprawie nadania statutu Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. Nr 73, poz. 464 z późn. zm.), rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 80, poz. 521), rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia wzorów wniosku o udostępnienie danych osobowych, zgłoszenia zbioru danych do rejestracji oraz imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. Nr 80, poz. 522 z późn. zm.).

² Znaczna liczba zgłoszeń do zarejestrowania zbiorów danych osobowych w 1999 r. wynikała z upływu z dniem 30 października 1999 r. ustawowego terminu zgłaszania do zarejestrowania zbiorów prowadzonych w systemach informatycznych w chwili wejścia w życie ustawy o ochronie danych (art. 61).

W związku z prowadzonymi postępowaniami administracyjnymi, jak też w ramach planu kontroli, w roku sprawozdawczym przeprowadzonych zostało 127 kontroli (w tym 102 kontrole całościowe i 25 czynności kontrolnych obejmujących kontrole częściowe, związane z wyjaśnianiem skarg lub sprawdzaniem wykonania decyzji).

Problematyka kontroli dotyczyła podstaw prawnych przetwarzania danych osobowych, w szczególności istnienia podstaw prawnych przetwarzania danych szczególnie chronionych, źródeł pozyskiwania danych, wykonywania obowiązku informacyjnego wobec osób, których dane przetwarzane były w zbiorach kontrolowanych administratorów danych, realizowania obowiązków określonych w art. 32 zwłaszcza dotyczących załatwiania sprzeciwów o których mowa w ust. 7 i 8, dopełnienia obowiązków organizacyjnych i technicznych określonych w ustawie o ochronie danych osobowych i przepisach wykonawczych, w tym zabezpieczenia zbiorów danych. Z ogólnej liczby 102 dokonanych kontroli całościowych, 19 przeprowadzono w spółkach marketingowych, 9 - w bankach i innych podmiotach finansowych, 7 - w towarzystwach ubezpieczeniowych i agencjach pośrednictwa ubezpieczeniowego, 6 - w centralnych i terenowych organach administracji publicznej, 6 - w jednostkach administracji samorządowej, 6 - w placówkach medycznych i 6 - w Kasach Chorych, 5 - w agencjach obrotu nieruchomościami, 4 - w wydawnictwach, 2 - w spółkach telefonii komórkowej i 2 w jednostkach TP S.A. oraz 32 w innych podmiotach (np. Komitet Ochrony Praw Dziecka, PKP, aeroklub, spółdzielnie, spółki telewizyjne, spółka konsultingowa). W związku z wynikami przeprowadzonych kontroli Generalny Inspektor wydał 22 decyzje nakazujące przywrócenie stanu zgodnego z prawem, skierował 3 zawiadomienia do prokuratury oraz 3 wnioski o wszczęcie postępowania dyscyplinarnego wobec osób odpowiedzialnych za przetwarzanie danych osobowych w kontrolowanej jednostce. W 17 przypadkach wyniki kontroli przekazane zostały do innych departamentów Biura GODO (Departamentu Rejestracji Zbiorów Danych i Departamentu Prawnego) do wykorzystania w sprawach prowadzonych przez te departamenty. W pozostałych przypadkach, wyniki kontroli nie dawały podstaw do wszczęcia postępowania administracyjnego, ponieważ uchybienia usunięte zostały jeszcze w toku kontroli lub materiał zebrany w sprawie nie dawał jeszcze podstaw do wydania decyzji.

Ponadto Generalny Inspektor w 46 przypadkach skierował do organów ścigania zawiadomienia o popełnieniu przestępstw związanych z naruszeniem praw przysługujących osobom na podstawie ustawy o ochronie danych osobowych lub z niedopełnieniem obowiązków nałożonych ustawą na administratorów danych. Generalny Inspektor również

skierował do centralnych organów państwa i innych jednostek organizacyjnych 56 pism o charakterze ogólnym, wskazujących na niespójność systemu prawa lub luki w prawie, jak też na nieprawidłowości w toku stosowania prawa .

W dalszym ciągu pracownicy Generalnego Inspektora zarówno w formie pisemnej (także z wykorzystaniem fax i e-mail), jak i telefonicznie, udzielali odpowiedzi na pytania związane ze stosowaniem ustawy o ochronie danych osobowych (około 13 tys. rozmów telefonicznych). Pytania w szczególności dotyczyły dopełniania obowiązku rejestracyjnego, obowiązku informacyjnego, zakresu ochrony przysługującej na podstawie ustawy o ochronie danych, uprawnień osób, których dane dotyczą, zwłaszcza prawa do zgłoszenia sprzeciwu przeciwko przetwarzaniu danych w celach marketingowych oraz możliwości uzyskania odszkodowania za naruszenie praw wynikających z ustawy.

Osoby zainteresowane korzystały także często z informacji zawartych na stronie internetowej GIODO (<http://www.giodo.gov.pl>), zawierającej zarówno akty prawne dotyczące ochrony danych osobowych, jak i przykłady rozstrzygnięć i interpretacji przepisów ustawy; w 2000 r. ze strony internetowej korzystano 29 472 razy.

Część I. PROBLEMATYKA PRZETWARZANIA DANYCH OSOBOWYCH PRZEZ PODMIOTY PUBLICZNE I PRYWATNE

A. ZAGADNIENIA OGÓLNE

I. Definicja danych osobowych

Zgodnie z art. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.) ustawa określa zasady przetwarzania danych osobowych oraz prawa osób fizycznych, których dane są lub mogą być przetwarzane w zbiorach danych.

Na gruncie ustawy o ochronie danych osobowych zasadnicze znaczenie ma definicja danych osobowych. W myśl art. 6 ustawy za dane osobowe należy uznać każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby. Ta jednoznaczna wydawałoby się definicja, sprawia jednak w praktyce wiele trudności, o czym świadczą pytania kierowane do Generalnego Inspektora Ochrony Danych Osobowych.

W odpowiedzi na jedno z zadanych pytań prawnych Generalny Inspektor stwierdził, iż nie podlega przepisom ustawy gromadzenie informacji wyłącznie o liczbie, wieku i płci osób niepełnosprawnych, rodzaju i stopnia ich niepełnosprawności, oraz posiadania lub braku pracy. Bez dodania do tych informacji imion i nazwisk, adresów lub innych danych identyfikujących poszczególne osoby, nie są one danymi osobowymi w rozumieniu ustawy.³ Urząd miasta gromadząc i opracowując takie informacje nie narusza ustawy o ochronie danych osobowych.⁴

W skardze złożonej na działania Urzędu Mieszkalnictwa i Rozwoju Miast stwierdzono, że odbiorcy zamawiający dostarczanie komunikatów Urzędu nie są chronieni w należyty sposób przed udostępnieniem ich danych osobom trzecim, a na *adresy e-mailowe* przesyłane są materiały od osób nieznanych i wcześniej nie zamawiane.⁵ Generalny Inspektor zauważył, że nie każda informacja dotycząca osoby fizycznej wskazuje jednocześnie na jej tożsamość. Ustawa chroni jedynie informacje, które same w sobie pozwalają na identyfikację osoby fizycznej, a więc wyodrębnienie tej osoby z określonej grupy społecznej i wskazanie w

³ Również Dyrektywa WE 95/46/EC Parlamentu Europejskiego i Rady stanowi w pkt 24 Preambuły, że postanowienia Dyrektywy nie dotyczą ustawodawstwa o ochronie osób prawnych w odniesieniu do przetwarzania danych osobowych. Zgodnie z art. 2 tej Dyrektywy pojęcie „dane osobowe” oznacza wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

⁴ GI-DP-625/00

sposób nie budzący wątpliwości, że chodzi właśnie o nią. Tylko wówczas, jeżeli za pomocą adresu e-mail można ustalić tożsamość osoby, to informację o takim adresie można uznać za dane osobowe. Musiałby on, np. zawierać informację o imieniu i nazwisku właściciela konta lub inne podobne informacje.

II. Pojęcie administratora danych

Kolejnym kluczowym terminem ustawy o ochronie danych osobowych jest „administrator danych”. Ustalenie tego podmiotu jest niezwykle istotne, bowiem z osobą administratora danych wiąże się szereg obowiązków przewidzianych ustawą, których niewypełnianie zagrożone jest sankcją karną.

W związku ze zgłaszaniem przez zarządy dzielnic zbiorów danych osobowych do rejestracji, Generalny Inspektor rozpatrywał kwestię, *czy dzielnice działające w ramach struktury organizacyjnej gminy posiadają status administratora danych w rozumieniu art. 7 ust. 4 ustawy o ochronie danych osobowych*. Generalny Inspektor stwierdził, że na podstawie art. 23 ustawy z dnia 25 marca 1994 r. o ustroju miasta stołecznego Warszawy (Dz. U. Nr 48, poz. 195 z późn. zm.), w związku z art. 5 ustawy z dnia 8 marca 1990 r., o samorządzie gminnym (Dz. U. 1996 r., Nr 13, poz. 74), rada gminy może w drodze uchwały tworzyć dzielnice, jako jednostki pomocnicze gminy. Art. 24 ustawy o ustroju miasta stołecznego Warszawy stanowi, że gminy warszawskie tworząc dzielnice, przekazują im określone zadania i kompetencje należące do właściwości gminy, dotyczące:

- 1) udzielenia wskazań i wydawania decyzji lokalizacyjnych,
- 2) utrzymywania i eksploatacji komunalnych zasobów mieszkaniowych i handlowo usługowych,
- 3) utrzymywania i eksploatacji placówek oświaty i wychowania, kultury, ochrony zdrowia, pomocy społecznej, rekreacji, sportu i turystyki,
- 4) utrzymywania zieleni i cmentarzy,
- 5) utrzymywania i eksploatacji dzielnicowych obiektów administracyjnych,
- 6) sprawowania nadzoru nad jednostkami niższego rzędu utworzonymi na obszarze dzielnicy.

Dzielnicom mogą być również przekazywane inne zadania i kompetencje należące do właściwości gminy.

⁵ GI-DP-024/1278/00

Zgodnie z art. 7 pkt 4 ustawy o ochronie danych osobowych, administratorem danych osobowych jest organ, instytucja, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych. Niezbędnym przymiotem administratora danych osobowych jest więc posiadanie kompetencji decyzyjnych (władztwo) w stosunku do danych podlegających przetwarzaniu (decydowanie o celach i środkach). W konsekwencji nie każdy podmiot dysponujący danymi osobowymi jest administratorem danych w rozumieniu ustawy.

W definicji ustawowej administratora danych użyte zostało wyrażenie "organ". W doktrynie wskazuje się na dwa podstawowe znaczenia tego pojęcia:

- 1) organy ustrojowe danego podmiotu,
- 2) organy właściwe w sprawie, czyli posiadające kompetencję administracyjną.

Ustawa o ochronie danych osobowych posługuje się pojęciem organu w drugim znaczeniu, chodzi więc o takie ciała, którym przypisana jest nie tyle ogólna władza organizacyjna w danej instytucji, ile kompetencja w określonej sprawie (lub dziedzinie). Organami ustrojowymi są w gminie rada i zarząd, ale na mocy art. 39 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 1996 r. Nr 13, poz. 74 z późn. zm.) decyzje w indywidualnych sprawach z zakresu administracji publicznej wydaje wójt lub burmistrz. Zgodnie z ust. 2 powołanego przepisu istnieje możliwość upoważnienia różnych osób do działania (wydawania decyzji administracyjnych) w imieniu wójta lub burmistrza. Kompetencje dyrektorów dzielnic i urzędników nie są oparte na przepisie ustawy, lecz na upoważnieniu, którego treść, w ramach wyznaczonych przez ustawę, określa uchwała rady gminy. Kompetencje gminy (burmistrza) wykonywane są w dzielnicach przez dyrektorów dzielnic, na podstawie przepisów statutowych dekoncentrujących uprawnienia i kompetencje gminne zarówno w indywidualnych sprawach z zakresu administracji publicznej (decyzje administracyjne), jak i w innych sprawach z zakresu zarządzania publicznego.

W myśl art. 30 ustawy o ustroju miasta stołecznego Warszawy, przy wydawaniu decyzji w indywidualnych sprawach z zakresu administracji publicznej organy dzielnic, którym przekazano takie uprawnienia działają z upoważnienia właściwego organu gminy.

Generalny Inspektor stwierdził, że uprawnienia gmin, jako administratorów danych podlegają dekoncentracji, w ślad za merytoryczną kompetencją, z którą związane jest przetwarzanie danych osobowych.⁶ Jednostki pomocnicze, jakimi są dzielnice działają na podstawie prawa miejscowego, ich organy wykonują funkcje administracji we własnym

imieniu, a ponadto zgodnie z art. 39 ust. 5 ustawy o samorządzie gminnym, od decyzji wydanych przez organ dzielniczy przysługuje odwołanie do samorządowego kolegium odwoławczego. To właśnie dzielnica jest administratorem danych przetwarzanych w związku z wykonywaniem przez nią ustawowych zadań.

III. Zbiory danych osobowych

Zgodnie z art. 7 pkt 1 ustawy o ochronie danych osobowych zbiorem danych jest każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

Generalnemu Inspektorowi sygnalizowano przypadki, gdy *organy samorządu terytorialnego zamierzały przy pomocy kamer monitorować główne ulice miasta*. Monitorowanie ulic polegać miałyoby na perspektywicznym zapisie obrazu przez kamery umieszczone na krańcach ulic. Szczegółowa analiza następować miałaby wyłącznie w przypadku popełnienia przestępstw lub wykroczeń.⁷ Generalny Inspektor uznał, że w tym przypadku ustawa o ochronie danych osobowych nie znajduje zastosowania. Zgodnie bowiem z art. 2 ust. 2 ustawę stosuje się wyłącznie do przetwarzania danych osobowych w systemach informatycznych oraz w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych. W przedstawionej do analizy sytuacji stwierdzono natomiast, że film video nie ma charakteru zbioru danych osobowych w rozumieniu art. 7 pkt 1 ustawy.⁸

IV. Przekazywanie danych osobowych za granicę

Ustawodawca polski, wzorem innych krajów, wprowadził ograniczenia w przekazywaniu danych osobowych za granicę. Podstawowe znaczenie dla omawianej problematyki ma zasada, zgodnie z którą przekazanie danych osobowych może nastąpić jedynie wtedy, gdy kraj docelowy daje gwarancje ochrony danym osobowym na swoim terytorium przynajmniej takie, jak obowiązujące na terytorium Rzeczypospolitej Polskiej.

⁶ Por. orzeczenie NSA w Łodzi z dnia 24 czerwca 1994 r. (S.A/Łd 1417/94 OSP 1996/5/101, orzeczenie NSA z dnia 9 lutego 1994 r. (S.A/Gd 2470/93 ONSA 1995/3/103)

⁷ GI-DP-476/00

⁸ Również Dyrektywa 95/46/WE Parlamentu Europejskiego oraz Rady z 24 października 1995 r. o ochronie osób w związku z przetwarzaniem danych osobowych oraz swobodnym obiegu tychże danych wskazuje, że nie podlega jej postanowieniom przetwarzanie danych dźwiękowych i obrazowych, np. w sytuacji inwigilacji/kontroli wizyjnej, jeśli jest wykonywane dla celów bezpieczeństwa publicznego, obronności, bezpieczeństwa państwowego, jako część działań państwa związanych z dziedziną prawa karnego lub innych czynności, które nie podlegają prawu Wspólnoty (pkt 16 Preambuły Dyrektywy).

Niezależnie jednak od poziomu ochrony jaką zapewnia inne państwo, dane osobowe można przekazywać za granicę, jeżeli wynika to z obowiązku nałożonego na administratora danych przepisami prawa lub postanowieniami ratyfikowanej umowy międzynarodowej. Ponadto przekazanie danych za granicę jest możliwe w razie spełnienia przesłanek określonych w art. 47 ust. 3 ustawy o ochronie danych osobowych. W związku z tą kwestią Generalny Inspektor zwracał uwagę, że przesłanki przekazywania danych osobowych za granicę określone w art. 47 ust. 3 pkt 1-6 ustawy o ochronie danych osobowych, powinny być traktowane alternatywnie, co oznacza, że spełnienie choćby jednej z nich umożliwia administratorowi danych przekazywanie tych danych za granicę.

Niektóre zakłady opieki zdrowotnej zwracały się do Generalnego Inspektora o wyrażenie zgody na przekazywanie danych o stanie zdrowia, w zakresie wyznaczonym realizacją danego programu, łączącego je z ośrodkiem zagranicznym, (np. znajdującym się w Niemczech).⁹ Generalny Inspektor poinformował, iż w odniesieniu do Niemiec, warunek, o którym mowa w art. 47 ust. 1 ww. ustawy, jest spełniony z uwagi na obowiązki ustawodawstwa w zakresie ochrony danych osobowych zarówno na szczeblu federalnym (Federalna ustawa o ochronie danych osobowych z dnia 20 grudnia 1990 r. – Bundesdatenschutzgesetz vom 20 Dezember 1990), jak i na szczeblu krajowym (Saksońska ustawa o ochronie danych osobowych z dnia 11 grudnia 1991 r. – Sächsisches Datenschutzgesetz vom 11 Dezember 1991). Spełnienie warunku zagwarantowania odpowiedniej ochrony danych osobowych w kraju docelowym sprawia, że nie jest wymagana zgoda Generalnego Inspektora na przekazywanie danych. Oprócz warunków formalnych administrator danych o stanie zdrowia zobowiązany jest do wykazania jednej z przesłanek określonych w art. 27 ust. 2 ustawy o ochronie danych osobowych. W sytuacji, gdy celem programu jest, np. przekazywanie diagnoz, konsultacja medyczna, spełniona jest tym samym przesłanka wskazana w art. 27 ust. 2 pkt 7 ww. ustawy.

V. Ustawa o ochronie danych osobowych a przepisy Kodeksu postępowania administracyjnego

Jednym z niezwykle często występujących nieporozumień wynikających z błędnej interpretacji przepisów ustawy o ochronie danych osobowych jest praktyka *żądania przez organy administracji wyrażenia przez petenta zgody na przetwarzanie jego danych*

⁹ GI-DP-555/00, GI/734/00

osobowych i to niejednokrotnie pod rygorem niezłatwienia sprawy.¹⁰ Stanowisko takie jest jednak niezasadne, bowiem dla organów administracji publicznej podstawę przetwarzania danych osobowych stanowią przepisy materialnego prawa administracyjnego oraz przepisy ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2000 r., Nr 98, poz. 1071). Generalny Inspektor wielokrotnie podkreślał, że przetwarzanie danych osobowych jest dopuszczalne w razie spełnienia którejkolwiek z przesłanek określonych w art. 23 ust. 1 ustawy o ochronie danych osobowych. W omawianym przypadku przesłanką taką jest przepis prawa, tj. art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych.

Pytano także, czy w świetle ustawy o ochronie danych osobowych zasadne jest *podawanie w piśmie urzędowym, w części „do wiadomości” wszystkich danych osoby prywatnej, będącej stroną postępowania administracyjnego, tj. jej imienia, nazwiska i adresu zamieszkania.*¹¹ Generalny Inspektor wskazywał, że wydaje się konieczne umieszczenie tylko takich danych osobowych, które umożliwią bezbłędne oznaczenie strony postępowania. Również i w tym przypadku znajduje zastosowanie art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych. Zgodnie z ustalonym orzecznictwem NSA, np. właściciele nieruchomości sąsiadujących bezpośrednio z działką, na której ma być wzniesiony obiekt budowlany mają przymiot strony w postępowaniu o wydanie pozwolenia na budowę (wyrok NSA z dnia 22 października 1987 r., IV SA 590/87, ONSA 1987, nr 2 poz. 71). Osoby te stają się stronami postępowania w takim zakresie, w jakim budowa ta może niekorzystnie oddziaływać na ich uzasadnione interesy (wyrok NSA z dnia 6 marca 1987 IV SA 1017/86). Stronami postępowania administracyjnego nie mogą być bliżej nieokreślone podmioty. Powinny one być ściśle oznaczone z imienia i nazwiska oraz adresu zamieszkania. Ponadto, decyzja administracyjna rozstrzyga w każdym wypadku o prawach lub obowiązkach stron, a nie osób, które tylko pośrednio są zainteresowane sposobem rozstrzygnięcia sprawy (por. wyrok NSA z dnia 27 maja 1989 r., II SA 437/89, nie publikowany).

W sprawie udostępnienia wierzycielowi - stronie postępowania - danych zawartych w aktach sprawy, w ocenie Generalnego Inspektora działanie takie pozostaje w zgodzie z przepisami ustawy o ochronie danych osobowych, ponieważ odbywa się na podstawie przesłanki określonej w art. 23 ust. 1 pkt 2. Podobnie jak w ubiegłym okresie sprawozdawczym, wskazywano np., że zgodnie z art. 18 ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. 1991 r., Nr 36, poz. 161 z późn. zm.), o ile ustawa ta nie stanowi inaczej, w postępowaniu egzekucyjnym mają zastosowanie przepisy

¹⁰ GI-DP-024/593/00

kodeksu postępowania administracyjnego.¹² W związku z art. 73 K.p.a. organ administracji jest zobowiązany umożliwić stronie przeglądanie akt sprawy oraz sporządzanie z nich odpisów i notatek. Przepis ten rozwija zasadę czynnego udziału strony wynikającą z art. 10 K.p.a. Także zdaniem Naczelnego Sądu Administracyjnego (wyrok z dnia 8 kwietnia 1998 r., I SA 1657/97), prawo wglądu do akt i sporządzania z nich odpisów obejmuje wszelkie pisma znajdujące się w aktach sprawy, bez względu na to, czy dotyczą merytorycznego rozstrzygnięcia, czy wprost do niego nie prowadzą. Skoro na mocy wyraźnego postanowienia art. 18 ustawy o postępowaniu egzekucyjnym w administracji, do tego postępowania odpowiednio stosuje się przepisy kodeksu postępowania administracyjnego, stwierdzić należy, że wierzyciel ma prawo wglądu do akt postępowania. Odmowa udostępnienia akt z powołaniem się na ustawę o ochronie danych osobowych stanowi więc nie tylko nadinterpretację ustawy o ochronie danych osobowych, ale także naruszenie podstawowych zasad postępowania administracyjnego.

VI. Umowa powierzenia

Do Generalnego Inspektora Ochrony Danych Osobowych wpływały pytania dotyczące interpretacji art. 31 ustawy o ochronie danych osobowych. Szczególnie wiele wątpliwości wywoływała kwestia określenia zakresu praw i obowiązków podmiotu, któremu administrator danych powierzył przetwarzanie danych osobowych na podstawie ww. przepisu. Pytano, np. czy na podmiocie, któremu powierzono przetwarzanie danych, *w celu związanym z działalnością marketingową* (np. wysyłka materiałów reklamowych), spoczywa obowiązek rejestracyjny.¹³ Generalny Inspektor informował, że zgodnie z art. 31 ustawy o ochronie danych osobowych, administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych osobowych. Cytowany przepis szczegółowo określił zasady przekazania danych osobowych innemu podmiotowi, który w imieniu i na rzecz administratora przetwarzałby dane osobowe. Administrator danych powinien także, zgodnie z treścią art. 26 ust. 1 ustawy, dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą. Powinien zatem dopilnować, aby podmiot, któremu dane powierza podjął środki zabezpieczające zbiór danych, o którym mowa w artykułach 36-39 ustawy. Jeżeli dane osobowe powierza do przetwarzania administrator

¹¹ GI-DP-358/00

¹² GI-DP-291/00, GI-DIS-192/00

¹³ GI-DP-024/1333/00

danych mający siedzibę za granicą podmiotowi mającemu siedzibę w Polsce, powyższe zasady również będą miały zastosowanie.¹⁴

¹⁴ Por. GI-DP-755/00/1226

B. SPRAWY Z ZAKRESU ADMINISTRACJI PUBLICZNEJ

W minionym okresie sprawozdawczym najwięcej spraw dotyczyło działalności organów administracji zarówno rządowej, jak i samorządowej, a także jednostek organizacyjnych, takich jak szkoły, przedszkola, biblioteki i innych (ok. 600 spraw).

I. Przetwarzanie danych osobowych przez organy administracji samorządowej

I.1 Sprawy z zakresu komunikacji

Do Generalnego Inspektora kierowane były pytania i prośby o interwencję oraz spowodowanie udzielenia informacji przez wydziały komunikacji urzędów gminy dotyczącej samochodów i numerów rejestracyjnych pojazdów należących do dłużników, w stosunku do których wydano klauzulę wykonalności. Zgodnie z treścią tej klauzuli „wszystkie osoby i urzędy, których to dotyczy są zobligowane do wykonania tytułu oraz gdy o to prawnie wezwane będą udzielały pomocy”.¹⁵ Generalny Inspektor nie jest jednakże uprawniony do nakazania udostępnienia danych o pojazdach należących do dłużników. Zarówno numer rejestracyjny, jak i marka oraz rok produkcji pojazdu nie pozwalają na określenie tożsamości właściciela pojazdu, więc i z tego powodu nie są danymi osobowymi w rozumieniu ustawy o ochronie danych osobowych.

Pytano także, czy rada gminy w uchwale dotyczącej opłat za parkowanie pojazdów może ustalić *obowiązek umieszczania za szybą identyfikatora* zawierającego oprócz danych dotyczących pojazdu (marka i numer rejestracyjny) dane osobowe właściciela tego pojazdu. Również i w tym przypadku ustawa o ochronie danych osobowych nie znajduje zastosowania, ponieważ umieszczanie identyfikatorów zawierających dane osobowe właściciela pojazdu za szybą tego pojazdu nie stanowi przetwarzania danych w zbiorze. Zgodnie z art. 13 ustawy z dnia 21 marca 1985 r. o drogach publicznych (Dz. U. z 2000 r., Nr 71, poz. 838 z późn. zm.), korzystanie z dróg publicznych może być uzależnione od wniesienia opłat. Zasady ustalania i pobierania tych opłat określone zostały w rozporządzeniu Rady Ministrów z dnia 27 czerwca 2000 r. w sprawie szczegółowych zasad wprowadzania opłat za parkowanie pojazdów samochodowych na drogach publicznych (Dz. U. z 2000 r., Nr 51, poz. 608). Na podstawie § 3 tego rozporządzenia opłaty wprowadza i ustala sposób ich pobierania rada gminy (miasta). W myśl tego przepisu rada gminy jest uprawniona do

określenia takiego wzoru identyfikatora, który umożliwi sprawowanie kontroli, czy z prawa bezpłatnego postoju korzysta osoba, której to prawo rzeczywiście przysługuje. Kwestia zgodności z prawem uchwały rady gminy podlega ocenie nie przez Generalnego Inspektora Ochrony Danych Osobowych, lecz przez właściwe organy nadzoru (wojewoda), podlega także kontroli sądowej dokonywanej przez NSA.

Ze skarg kierowanych do Generalnego Inspektora wynika, że przepisy obowiązujące lokalnie niejednokrotnie przewidują *obowiązek okazywania odcinków rent i emerytur podczas kontroli dokumentów* uprawniających do ulgowych lub bezpłatnych przejazdów w autobusach komunikacji miejskiej.¹⁶ Z uwagi jednak na to, że okazywanie takich dokumentów kontrolerom nie dotyczy danych osobowych zgromadzonych w zbiorze danych, ustawa o ochronie danych osobowych także w omawianym przypadku nie znajduje zastosowania. Generalny Inspektor uznając jednak, że praktyka ta stoi w sprzeczności z normami Konstytucji, w piśmie z dnia 24 maja 2000 r. zwrócił się do Rzecznika Praw Obywatelskich z prośbą o zbadanie tej kwestii w ramach uprawnień przyznanych mu ustawą z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich (Dz. U. z 2001 r. Nr 14, poz. 147). Generalny Inspektor wskazał w szczególności na przepisy art. 47 oraz art. 51 Konstytucji, które stanowią, że każdy ma prawo do ochrony prawnej życia prywatnego, a ponadto nikt nie może być zobowiązany inaczej, niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.¹⁷

I.2 Urzędy Stanu Cywilnego

Jest oczywiste, że krótki okres obowiązywania ustawy niejednokrotnie nie pozwala na zapoznanie się przez obywateli z przysługującymi im na podstawie ustawy prawami. Zdarzało się na przykład, że *urzędy stanu cywilnego odmawiały osobom uprawnionym wydania odpisów aktów stanu cywilnego* powołując się przy tym na przepisy ustawy o ochronie danych osobowych. Generalny Inspektor wskazywał jednakże, że ustawa o ochronie danych osobowych w art. 5 stanowi, iż jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują dalej idącą ich ochronę, niż wynika to z ustawy o ochronie danych osobowych, stosuje się przepisy tych ustaw. Zasady sporządzania aktów stanu cywilnego, ich prowadzenia i udostępniania uregulowane zostały w ustawie z dnia 29 września 1986 r. Prawo o aktach stanu cywilnego (Dz. U. Nr 36, poz. 180 ze zm.). W tym

¹⁵ GI-DP-024/1439/00, GI-DP-024/1467/00, GI-DP-024/1484/00,

¹⁶ GI-DP-024/1323/00

¹⁷ Wystąpienie Generalnego Inspektora Ochrony Danych Osobowych z dnia 24 maja 2000 r., sygn. GI-474/00

zakresie wyłączone zostaje zatem stosowanie przepisów ustawy o ochronie danych osobowych.

Krąg podmiotów uprawnionych do otrzymania skróconego odpisu aktu stanu cywilnego określony został w art. 83 ust. 1 i ust. 2 ustawy Prawo o aktach stanu cywilnego. Wyliczenie to nie ma charakteru wyczerpującego. Poza osobami wymienionymi w art. 83 ust. 1, odpis skróconego aktu stanu cywilnego otrzymać mogą także inne osoby, jeżeli wykażą w tym interes prawny (art. 83 ust. 2). Warunkiem uzyskania skróconego aktu urodzenia jest albo wykazanie istnienia jednej z przesłanek z art. 83 ust. 1, albo interesu prawnego. Generalny Inspektor podkreślał również, że odmienne stanowisko (przedstawiane czasem przez kierowników USC) stanowi nadinterpretację i nie znajduje oparcia w przepisach prawa. Informowano także o możliwości skierowania skargi na czynności kierownika urzędu do wojewody, który sprawuje nadzór nad działalnością gminy.¹⁸ W jednym z pism skarżono się na wydanie *skróconego odpisu aktu urodzenia osobie nieuprawnionej*. Jak ustalono odpis aktu urodzenia został wydany adwokatowi siostrzenicy skarżącego, w celu przedstawienia jako dowód w postępowaniu sądowym o stwierdzenie nabycia spadku po ojcu skarżącego. Należy zatem stwierdzić, że była to osoba uprawniona, bowiem wykazała interes prawny.¹⁹

Z kolei na pytanie urzędu gminy o *dopuszczalność udostępniania danych z ewidencji ludności samodzielnemu publicznemu zakładowi opieki zdrowotnej*,²⁰ Generalny Inspektor udzielił odpowiedzi, że przepisy nie upoważniają urzędu gminy do udostępnienia takich danych zakładom opieki zdrowotnej. Ustawa z dnia 6 lutego 1997 r. o powszechnym ubezpieczeniu zdrowotnym (Dz. U. Nr 28, poz. 153 z późn. zm.) oraz wydane na jej podstawie akty wykonawcze, w szczególności rozporządzenie Ministra Zdrowia i Opieki Społecznej z dnia 15 stycznia 1999 r. w sprawie ustalenia zakresu niezbędnych danych gromadzonych przez świadczeniodawców oraz w systemach informatycznych Kas Chorych, a także zakresu i procedury wymiany danych pomiędzy Kasami Chorych oraz Kasami Chorych a świadczeniodawcami, Urzędem Nadzoru Ubezpieczeń Zdrowotnych i Krajowym Związkiem Kas Chorych (Dz. U. Nr 7, poz. 66 z późn. zm.) nakładają obowiązek zbierania określonych danych osobowych na zakłady opieki zdrowotnej. Przepisy powyższe nie zobowiązują jednak gminy do udostępniania danych osobowych ZOZ-om. W tej sytuacji nie zostaje zatem spełniona przesłanka udostępnienia określona w art. 23 ust. 1 pkt 2 ustawy.

¹⁸ GI-DIS-222/00

¹⁹ GI-DIS-273/00

²⁰ GI-DP-666/00

Warto jednak wskazać, że przypadków takich w omawianym okresie sprawozdawczym było znacznie mniej niż w 1999 roku. Należy zatem uznać, iż działania Generalnego Inspektora Ochrony Danych Osobowych w zakresie informowania Urzędy Stanu Cywilnego o zakresie stosowania przepisów o ochronie danych osobowych przyniosły pozytywny skutek.

I.3 Oświata

Do Generalnego Inspektora Ochrony Danych Osobowych wpłynęła skarga na *udostępnienie właścicielce prywatnej szkoły podstawowej*, którą wykreślono z ewidencji działalności oświatowej ze względu na nie podjęcie działalności w terminie wskazanym w zgłoszeniu do ewidencji, *danych osobowych dzieci*, które w danym roku podlegały obowiązkowi szkolnemu oraz danych rodziców tych dzieci (dane wykorzystano do rozesłania oferty szkoły). Generalny Inspektor Ochrony Danych Osobowych stwierdził, iż szkoła była uprawniona do uzyskania przedmiotowych danych.²¹ Podstawę udostępnienia spornych danych przez Urząd Gminy i Miasta stanowiły przepisy ustawy o ochronie danych osobowych, a w szczególności art. 29 ust. 3 tej ustawy.²²

Zgodnie z art. 29 ust. 3 ustawy, dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie. Dyrektor prywatnej szkoły podstawowej złożył pisemny, umotywowany wniosek o udostępnienie danych osobowych, który zawierał informacje umożliwiające wyszukanie w zbiorze żądane dane osobowe, wskazywał ich zakres oraz przeznaczenie. W związku z powyższym spełnione zostały ustawowe wymogi dotyczące udostępniania danych osobowych w celach innych, niż włączenie danych osobowych do zbioru (art. 29 ust. 3 ustawy). Ponadto dyrektor spełnił wymogi określone w art. 29 ust. 4 ustawy. We wniosku o udostępnienie danych osobowych dyrektor prywatnej szkoły podstawowej wskazał, że przeznaczeniem dla udostępnionych danych jest „zawiadomienie rodziców o możliwości zapisania dziecka do szkoły”.²³ Postępowanie wyjaśniające

²¹ GI-DIS-191/00, zob. także GI-DEC-DP-89/00

²² Na podstawie art. 19 ust. 1 ustawy o systemie oświaty dyrektorzy publicznych szkół podstawowych i gimnazjów kontrolują spełnianie obowiązku szkolnego przez dzieci zamieszkujące w obwodach tych szkół, a gmina kontroluje spełnianie obowiązku szkolnego lub obowiązku nauki przez młodzież w wieku 16-18 lat, a także prowadzą ewidencję spełniania obowiązku szkolnego oraz obowiązku nauki. Na mocy zaś ust. 2 omawianego przepisu organ gminy prowadzący ewidencję ludności jest obowiązany w ramach zadań własnych przysyłać właściwym dyrektorom szkół informacje o aktualnym stanie i zmianach w ewidencji dzieci i młodzieży w wieku 3-18 lat.

²³ Zob. GI-DEC-DP-89/00

przeprowadzone w niniejszej sprawie nie wykazało, aby udostępnienie danych osobowych naruszyło prawa i wolności skarżącego, jak również, aby dane zostały wykorzystane w celu innym niż wskazany we wniosku o udostępnienie.

Jedna ze skarg dotyczyła *zakresu zbieranych danych przy rejestrowaniu szkoły niepublicznej* (wykraczającego poza określony przepisami ustawy o systemie oświaty) oraz kserowania wybranych stron dowodu osobistego.²⁴ W przedmiotowej sprawie wszczęto postępowanie administracyjne, w wyniku którego Generalny Inspektor Ochrony Danych Osobowych nakazał staroście powiatu przywrócenie stanu zgodnego z prawem poprzez usunięcie danych osób zamierzających prowadzić szkołę lub placówkę, innych niż imię (imiona) i nazwisko oraz adres zamieszkania, jako nieadekwatnych w stosunku do celu ich przetwarzania, stosownie do art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych oraz zaprzestanie kopiowania dokumentów potwierdzających tożsamość, jako prowadzącego do pozyskiwania nieadekwatnych, w stosunku do celu przetwarzania, danych osób zamierzających prowadzić szkołę lub placówkę oświatową, stosownie do art. 26 ust. 1 pkt 3 wskazanej ustawy.²⁵

Zgodnie z art. 82 ust. 2 ustawy z dnia 7 września 1991 r. o systemie oświaty (Dz. U. z 1996 r. Nr 67, poz. 329 ze zm.), zgłoszenie do ewidencji powinno zawierać: oznaczenie osoby zamierzającej prowadzić szkołę lub placówkę, jej miejsca zamieszkania lub siedziby, określenie typu szkoły lub placówki, oraz daty rozpoczęcia jej funkcjonowania, a w przypadku szkoły zawodowej także zawodów lub profili zawodowych, w jakich szkoła będzie kształcić, wskazanie miejsca prowadzenia szkoły lub placówki i warunków lokalowych zapewniających bezpieczne i higieniczne warunki osobom przebywającym na jej terenie, zgodnie z odrębnymi przepisami, statut szkoły lub placówki, dane dotyczące kwalifikacji pracowników pedagogicznych i dyrektora, przewidzianych do zatrudnienia w szkole lub placówce, zobowiązanie do przestrzegania wymagań określonych w art. 7 ust. 3 w przypadku szkoły podstawowej oraz gimnazjum, a także w przypadku szkoły ponadgimnazjalnej ubiegającej się o nadanie uprawnień szkoły publicznej z dniem rozpoczęcia działalności.

Wśród skarg nadchodzących do Generalnego Inspektora znajdowały się również skargi na nieuprawnione – zdaniem skarżących – *żądanie podawania szczegółowych danych ucznia i jego rodziców na pierwszej stronie dzienniczka ucznia*.²⁶ Generalny Inspektor

²⁴ GI-DIS-251/00

²⁵ GI-DEC-DP-54/00,

²⁶ GGI-024-1/00/942

wskazał, iż na podstawie § 3 rozporządzenia Ministra Edukacji Narodowej z dnia 19 kwietnia 1999 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. Nr 41, poz. 414) szkoły podstawowe i gimnazja prowadzą księgi ewidencji dzieci podlegających obowiązkowi szkolnemu, zamieszkałych w obwodzie szkoły. Do księgi ewidencji wpisuje się – według roku urodzenia - imię (imiona) i nazwisko oraz datę, miejsce urodzenia i adres zamieszkania dziecka, a także imiona i nazwiska rodziców (opiekunów prawnych) oraz adresy ich zamieszkania. Także, stosownie do § 6 wymienionego wyżej rozporządzenia, szkoła prowadzi dla każdego oddziału dziennik lekcyjny, w którym dokumentuje się przebieg nauczania w danym roku szkolnym. Do dziennika wpisuje się nazwiska i imiona uczniów, daty, miejsca urodzenia i adresy ich zamieszkania, imiona i nazwiska rodziców (prawnych opiekunów) oraz adresy ich zamieszkania. Informacje te, gromadzone przez szkoły, są - czy powinny być - odpowiednio zabezpieczone i udostępniane jedynie uprawnionym osobom .

Przepisy wyżej powołanego rozporządzenia oraz pozostałe przepisy wykonawcze do ustawy o systemie oświaty nie wskazują, jakie dane winien uczeń podać do dzienniczka ucznia.

W związku z powyższym, Generalny Inspektor zwrócił się o wskazanie podstawy prawnej żądania przez nauczycieli szkół podstawowych, średnich i ogólnokształcących tak szerokiego zakresu danych o uczniu oraz podstawy nakładania na uczniów obowiązku wypełniania pierwszej strony dzienniczka ucznia.²⁷ W odpowiedzi na powyższe Minister Edukacji Narodowej zobowiązał się do podjęcia działań mających na celu wyeliminowanie zasygnalizowanej przez Generalnego Inspektora praktyki i przywrócenia tym samym stanu zgodnego z prawem.²⁸

I.4 Straż Miejska

W omawianym okresie sprawozdawczym do Generalnego Inspektora Ochrony Danych Osobowych wielokrotnie napływały sygnały dotyczące odmowy udostępnienia Straży Miejskiej danych osobowych znajdujących się w zbiorach danych zarówno podmiotów prywatnych jak i organów administracji publicznej (np. gminy, operatorzy sieci telekomunikacyjnej użytku publicznego).²⁹ Odmowę udostępnienia wnioskowanych przez

²⁷ Ibidem

²⁸ Pismo z dnia 15 listopada 2000 r., znak: DKW-073-78/2000/EZ

²⁹ Np. w sprawach GI-DP-024/1723/00, GI-DIS-430/411/00

Straż Miejską danych uzasadniano brakiem właściwej podstawy prawnej i obowiązywaniem pracowników danego organu tajemnicy służbowej. Ponadto wskazano, iż wnioskodawca nie uzasadnił w sposób wiarygodny potrzeby posiadania danych, w związku z czym administrator danych będących przedmiotem sporu nie mógł dokonać wszechstronnej oceny, czy udostępnienie nie naruszy praw i wolności osób, których dane dotyczą.

W sprawach tych po przeprowadzeniu postępowania administracyjnego często okazywało się, iż odmowa udostępnienia wnioskowanych przez Straż Miejską danych osobowych była nieuzasadniona.

Zakres zadań straży miejskiej określony został w przepisach ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz. U. Nr 123, poz. 779). Zgodnie z art. 10 ust. 1 cytowanej ustawy straż wykonuje zadania w zakresie ochrony porządku publicznego wynikające z ustaw i aktów prawa miejscowego. W związku z wykonywaniem ustawowo określonych zadań strażnik ma prawo m.in. do dokonywania czynności sprawdzających, kierowania wniosków o ukaranie do kolegium do spraw wykroczeń, oskarżania przed kolegium do spraw wykroczeń i wnoszenia środków odwoławczych – w trybie przewidzianym przepisami o postępowaniu w sprawach o wykroczenia (art. 12 ust 1 pkt 5 ustawy o strażach gminnych). Warunkiem koniecznym dla złożenia wniosku, o którym mowa w art. 21 K.p.w. jest ustalenie tożsamości sprawcy wykroczenia.

Generalny Inspektor Ochrony Danych Osobowych zwrócił uwagę, iż przepisy ustawy o strażach gminnych i Kodeksu postępowania w sprawach o wykroczenia nie tylko uprawniają, ale jednocześnie zobowiązują Straż Miejską do pozyskania wszelkich niezbędnych danych w celu ustalenia sprawcy wykroczenia, a następnie skierowania do kolegium stosownego wniosku o ukaranie podmiotu w pełni zidentyfikowanego.

W ocenie Generalnego Inspektora zasadność udostępnienia żądanych przez Straż Miejską danych osobowych uzasadniają nie tylko przepisy prawa (a więc przesłanki, o której mowa w art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych), ale również przesłanka określona w art. 23 ust. 1 pkt 4 ustawy o ochronie danych osobowych, zgodnie z którym przetwarzanie danych jest dopuszczalne, gdy jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego. Do przedmiotowych działań niewątpliwie należy zaliczyć ściganie sprawców przestępstw i wykroczeń. Funkcjonariusz Straży Miejskiej wykonujący zadania w zakresie ochrony porządku publicznego wynikające z

ustaw i prawa miejscowego ma prawo do żądania niezbędnej pomocy od instytucji państwowych i samorządowych.³⁰

W konsekwencji Generalny Inspektor wydawał decyzje nakazujące administratorom udostępnienie danych Straży Miejskiej w zakresie określonym przepisami prawa.³¹

I.5 Pomoc społeczna

Ta grupa spraw dotyczy sfery szczególnie istotnej dla poszczególnych obywateli, bowiem niejednokrotnie już sam fakt korzystania z pomocy społecznej jest dla niektórych osób wstydlivy. Także zakres pozyskiwanych w celu udzielenia świadczenia z pomocy społecznej danych osobowych wymaga szczególnej dbałości w wykonywaniu nałożonych na administratorów danych obowiązków.

Podstawą prawną przetwarzania danych osób korzystających ze świadczeń pomocy społecznej są przepisy ustawy z dnia 29 sierpnia 1990 r. o pomocy społecznej (Dz. U. z 1998 r. Nr 64, poz. 414 z późn. zm.). W pismach kierowanych do Generalnego Inspektora Ochrony Danych Osobowych często pojawiało się pytanie o *konieczność uzyskiwania zgody małżonków na przeprowadzenie wywiadu środowiskowego oraz gromadzenie informacji o danej rodzinie*, której Miejski Ośrodek Pomocy Rodzinie udziela pomocy. Niejednokrotnie odmawiano przy tym osobom uprawnionym wglądu w akta sprawy.³² Generalny Inspektor odpowiadał, że na przeprowadzenie wywiadu środowiskowego nie jest konieczna zgoda, gdyż zgodnie z art. 43 ust. 3 cytowanej ustawy pracownik socjalny ma obowiązek przeprowadzić wywiad środowiskowy polegający na zbieraniu danych osoby ubiegającej się o świadczenie z pomocy społecznej, zgodnie z rozporządzeniem Ministra Pracy i Polityki Społecznej z dnia 24 lipca 1997 r. w sprawie wywiadu środowiskowego (rodzinnego), wzoru kwestionariusza wywiadu środowiskowego oraz oświadczenia o stanie majątkowym, rodzaju dokumentów wymaganych do przyznania renty socjalnej, a także wzoru legitymacji pracownika socjalnego (Dz. U. Nr 93, poz. 570 z późn. zm.).³³

Odpowiadając na pytanie o dopuszczalność przetwarzania przez ośrodki pomocy społecznej danych o pochodzeniu rasowym i etnicznym, o przekonaniach religijnych i przynależności wyznaniowej, przynależności związkowej oraz danych o życiu seksualnym danej osoby Generalny Inspektor Ochrony Danych Osobowych stwierdził, że w przypadku zbierania danych dla celów przyznania świadczenia z pomocy społecznej, przesłankę

³⁰ GI-DIS-430/411/00

³¹ GI-DEC-DS-38/01, GI-DEC-39/00

³² GI-DP-024/1433/00, por. także GI-DIS-69/00

legalności przetwarzania danych osobowych stanowią przepisy prawa, w szczególności ustawy o pomocy społecznej.

Do Generalnego Inspektora zwrócono się również z żądaniem nakazania sprostowania notatki służbowej sporządzonej przez pracownika socjalnego jako zawierającej dane niezgodne z prawdą.³⁴ W odpowiedzi poinformowano skarżącą, że Generalny Inspektor Ochrony Danych Osobowych nie ma kompetencji do dokonywania zmian w dokumentach zawartych w aktach postępowań prowadzonych przez inne organy administracji. Następnie, poinformowano o podstawie przetwarzania danych przez ośrodki pomocy społecznej, tj. wyjaśniono, że podstawą są przepisy ustawy o pomocy społecznej oraz, że notatka służbowa w zakresie zawartych w niej danych osobowych skarżącej, tj. imienia i nazwiska była zgodna z prawdą, inne zawarte w niej informacje nie były danymi osobowymi, a zatem nie podlegały ochronie wynikającej z przepisów o ochronie danych osobowych. Ponadto, powiadomiono skarżącą o możliwości wystąpienia z powództwem cywilnym w sytuacji naruszenia jej dóbr osobistych.

Podobnie jak w ubiegłym okresie sprawozdawczym, przedmiotem wielu pytań była kwestia, *czy w świetle przepisów ustawy o ochronie danych osobowych członkowie komisji rewizyjnej rady miasta mogą kontrolować bieżącą działalność miejskiego ośrodka pomocy społecznej w zakresie celowości i wysokości wypłacanych świadczeń*.³⁵ Generalny Inspektor stwierdził, że z uwagi na tajemnicę socjalną wyrażoną w art. 36 ustawy o pomocy społecznej, jak i na przesłanki przetwarzania danych szczególnie chronionych określone w art. 27 ustawy o ochronie danych osobowych, kontrolowanie konkretnych akt spraw z zakresu pomocy społecznej, musiałoby znaleźć podstawę ustawową wyrażającą się w konkretnym ustawowym upoważnieniu uprawniającym do przetwarzania danych szczególnie chronionych. Zgodnie z art. 18a ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 1996 r. Nr 13, poz. 74 z późn. zm.), rada gminy kontroluje działalność zarządu oraz gminnych jednostek organizacyjnych; w tym celu powołuje komisję rewizyjną. Przepis ten stanowi podstawę prawną działalności kontrolnej komisji rewizyjnej wobec gminnego ośrodka pomocy społecznej. Zawarta w nim regulacja, ze względu na jej ogólnikowy charakter może natomiast budzić uzasadnione wątpliwości co do zakresu uprawnień komisji rewizyjnej w ramach przeprowadzanej kontroli. W szczególności mogą one dotyczyć trudności w ustaleniu, czy komisja rewizyjna ma prawo wglądu w dane osobowe, a także jakiego rodzaju dane mogą

³³ Rozporządzenie powyższe zostało uchylone z dniem 1 stycznia 2001 r.

³⁴ GI-DIS-101/00

³⁵ GI-DP-024/1341/00

być udostępniane komisji. Komplikacje, jakie rodzi powyższy przepis, w sposób szczególnie uwidaczniają się w przypadku kontrolowania ośrodka pomocy społecznej. Działalność ośrodków pomocy społecznej związana jest bowiem często ze zbieraniem danych szczególnie chronionych, które dotyczą ściśle prywatnej sfery życia obywateli, np. danych o stanie zdrowia. Prawo wprowadza w związku z tym szereg zapisów, które w sposób rygorystyczny określają sytuacje, w jakich przetwarzanie przedmiotowych danych jest dopuszczalne.

Podstawowe znaczenie będzie tutaj miała ustawa o pomocy społecznej, której zapisy wprowadzają tajemnicę socjalną. Znajduje ona wyraz w przepisie art. 36 ust. 2 tej ustawy, zgodnie z którym, w postępowaniu w sprawie świadczeń pomocy społecznej należy kierować się przede wszystkim dobrem osób korzystających z pomocy społecznej i ochroną ich dóbr osobistych. W szczególności nie należy podawać do wiadomości nazwisk osób korzystających z pomocy społecznej oraz rodzaju i zakresu przyznanego świadczenia. Regulacja ta stanowi wyraz szczególnej troski ustawodawcy mającej na celu zapewnienie maksymalnego stopnia ochrony informacjom uzyskanym w związku z postępowaniem o przyznanie pomocy społecznej. Wynika z niej wyraźny zakaz udostępniania danych osób korzystających z pomocy społecznej. Ustawodawca uznał zatem, iż prawo jednostki do ochrony prywatności jest wartością, która ma prymat nad interesem publicznym, który w tym wypadku nie uzasadnia dostatecznie ingerencji w sferę praw i wolności obywatelskich. Wobec takiego ujęcia przez przepisy omawianego problemu, uzasadnienie dla ingerencji przez komisję rewizyjną w dane osobowe objęte tajemnicą socjalną, powinno wynikać z normy zawartej w ustawie, która w sposób równie kategoryczny i wyraźny zawierałaby ograniczenie praw jednostki określonych przez tajemnicę socjalną. Ponadto, jednostka kontrolna nie powinna występować o udostępnienie danych ponad te, które są niezbędne dla prawidłowego przeprowadzenia opartej na przepisach prawa kontroli.

Niejednokrotnie akta dotyczące postępowania w sprawie przyznania pomocy zawierają także dane dotyczące skazań czy też orzeczeń o ukaraniu, których przetwarzanie może mieć miejsce wyłącznie na podstawie ustawy. Zgodnie bowiem z art. 28 ust. 1 ustawy o ochronie danych osobowych przetwarzanie danych dotyczących skazań, orzeczeń o ukaraniu, mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym można prowadzić wyłącznie na podstawie ustawy. Przepisy ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. Nr 13, poz. 74 z późn. zm.) takiego upoważnienia dla komisji rewizyjnej nie przewidują.

Należy ponadto zauważyć, że kierownik OPS, może w każdym stadium postępowania udostępniać akta sprawy, ale tylko stronie. Komisja rewizyjna nie jest stroną w

myśl przepisów Kodeksu postępowania administracyjnego. Decyzje w sprawach pomocy społecznej wydaje kierownik ośrodka pomocy społecznej. Decyzja ta podlega kontroli instancyjnej realizowanej przez właściwe organy, ostatecznie kontroli tej dokonuje NSA. Legalność i zasadność podejmowanych rozstrzygnięć w sprawach pomocy społecznej należy zatem do organów, które w tym celu zostały powołane.

Nie jest też dopuszczalne udostępnianie informacji, czy dana osoba będąca klientem ośrodka pomocy społecznej pobierała lub pobiera zasiłek lub korzysta z innej formy pomocy społecznej bankom.³⁶

Inaczej natomiast przedstawia się kwestia przekazywania danych zawartych w aktach sprawy organowi wyższej instancji.³⁷ Generalny Inspektor wskazywał, że przekazanie zebranych informacji i akt wojewodzie oraz Naczelnemu Sądowi Administracyjnemu wskutek wniesienia odwołania i skargi podlega przepisom procedury administracyjnej, która jako *lex specialis* reguluje postępowanie w tym zakresie.

Generalny Inspektor zajmował się kwestią, czy *osoby kierowane do ośrodka pomocy społecznej w ramach uczniowskich lub studenckich praktyk zawodowych mogą po podpisaniu zobowiązania o zachowaniu tajemnicy mieć wgląd w dane osobowe gromadzone w zbiorach ośrodka*.³⁸ W sprawie tej stwierdzono, że nie ma podstaw do udostępnienia studentom i uczniom kierowanym na praktyki zawodowe danych osobowych na potrzeby udzielania świadczeń z pomocy społecznej. Zgodnie z przepisem § 8 ust. 1 pkt 2 rozporządzenia Rady Ministrów z dnia 12 sierpnia 1991 r. w sprawie studenckich praktyk zawodowych (Dz. U. Nr 73, poz. 323 z późn. zm.) wydanego na podstawie art. 146 ust. 2 ustawy z dnia 12 września 1990 r. o szkolnictwie wyższym (Dz. U. Nr 65, poz. 385 z późn. zm.) zakład pracy, w tym miejski ośrodek pomocy społecznej, jest obowiązany do zapoznania studentów z zakładowym regulaminem pracy, przepisami o bezpieczeństwie i higienie pracy oraz o ochronie tajemnicy państwowej i służbowej. Wprawdzie ustawa o pomocy społecznej nie normuje zagadnień tajemnicy służbowej, jednakże przepis art. 36 ust. 2 wskazanej ustawy, w myśl którego w postępowaniu w sprawie świadczeń pomocy społecznej należy kierować się przede wszystkim dobrem osób korzystających z pomocy społecznej i ochroną ich dóbr osobistych, w szczególności nie należy podawać do wiadomości nazwisk osób korzystających z pomocy społecznej i zakresu przyznanego świadczenia - określa tajemnicę socjalną.

³⁶ GI-DP-988/00

³⁷ DEC/GI/DIS/1/2000

³⁸ GI-DP-024/1551/00

1.6 Inne sprawy związane z problematyką przetwarzania danych przez samorządy

Generalny Inspektor rozpatrywał skargę dotyczącą *konieczności podania nazwiska byłej żony przy dopełnianiu obowiązku meldunkowego*.³⁹ Skargę uznano za uzasadnioną. Przepis § 7 ust. 1 pkt 4 rozporządzenia Ministra Spraw Wewnętrznych z dnia 28 czerwca 1984 r. w sprawie wykonywania obowiązku meldunkowego i prowadzenia ewidencji ludności (Dz. U. Nr 32, poz. 176 z późn. zm.), wskazuje na obowiązek podania stanu cywilnego, pod tym pojęciem jednakże należy rozumieć tylko informację, czy dana osoba jest stanu wolnego, czy też pozostaje w związku małżeńskim. Generalny Inspektor Ochrony Danych Osobowych wystąpił do Ministra Spraw Wewnętrznych i Administracji o wyjaśnienie zasadności i ewentualnej zmiany zapisu określonego w § 7 ust. 1 pkt 10 i 11 ww. rozporządzenia Ministra Spraw Wewnętrznych, obligującego osoby fizyczne - w ramach obowiązku meldunkowego - do zgłoszenia danych o wykształceniu i zawodzie wyuczonym, miejscu pracy i zawodzie wykonywanym, imion i nazwisk rodowych rodziców, jak również nazwisk z poprzedniego małżeństwa oraz stosowną zmianę treści dotychczas obowiązujących druków meldunkowych. W obecnym stanie prawnym została uwzględniona jedynie sugestia Generalnego Inspektora w zakresie zbędności podawania danych byłych małżonków.⁴⁰

Jedna z gmin zgłosiła do rejestracji zbiór o nazwie „ewidencja ludności i dowody osobiste”, w którym znajdowały się m.in. *informacje o karalności* obywateli.⁴¹ Po zbadaniu sprawy okazało się, że administrator danych za podstawę przetwarzania danych o skazaniach podał przepisy ustawy z dnia 6 czerwca 1997 r. Kodeks karny wykonawczy (Dz. U. Nr 90, poz. 557 z późn. zm.). Przepisy ww. ustawy stanowią, że w razie orzeczenia pozbawienia praw publicznych sąd zawiadamia właściwy dla miejsca ostatniego zamieszkania lub pobytu skazanego odpowiedni organ administracji publicznej (art. 179 pkt 1 K.k.w.). Przepisy K.k.w. dają właściwym organom administracji umocowanie także do przetwarzania danych o wymierzeniu środka karnego w postaci zakazu prowadzenia określonej działalności

³⁹ GI-DIS-292/00

⁴⁰ W dniu 27 maja 2001 r. weszła w życie ustawa z dnia 11 kwietnia 2001 r. o zmianie ustawy o ewidencji ludności i dowodach osobistych oraz o zmianie niektórych innych ustaw (Dz. U. z 2001 r. Nr 43, poz. 476). Na podstawie art. 1 pkt 4 tej ustawy art. 11 ust. 1 rozporządzenia Ministra Spraw Wewnętrznych z dnia 28 czerwca 1984 r. w sprawie wykonywania obowiązku meldunkowego i prowadzenia ewidencji ludności (Dz. U. Nr 32, poz. 176 z późn. zm.) otrzymał brzmienie: „Osoba zobowiązana do zameldowania na pobyt stały przedstawia organowi gminy właściwemu ze względu na nowe miejsce jej pobytu stałego zaświadczenie o wymeldowaniu się z poprzedniego miejsca pobytu oraz zgłasza następujące dane osobowe: nazwisko i imiona, nazwisko rodowe, nazwiska i imiona poprzednie, imiona rodziców, stan cywilny, imię i nazwisko małżonka oraz jego nazwisko rodowe, płeć, datę i miejsce urodzenia, obywatelstwo, numer PESEL, dotyczące obowiązku wojskowego (...), adres poprzedniego miejsca pobytu stałego, rodzaj, serię i numer dokumentu tożsamości, informacje o wykształceniu.”

⁴¹ GI-DP-108/00

gospodarczej, czy zakazu prowadzenia pojazdów. Stanowi to w świetle art. 28 ust. 1 ustawy o ochronie danych osobowych wystarczającą przesłankę przetwarzania danych osobowych.

Generalny Inspektor uznał także, że art. 7b ust. 1 pkt 4 ustawy z dnia 17 maja 1989 r. – Prawo geodezyjne i kartograficzne (Dz. U. z 2000 r. Nr 100, poz. 1086 z późn. zm.) stanowi wystarczającą *podstawę ewidencjonowania lokalnych systemów informacji o terenie oraz o przechowywania kopii zabezpieczających baz danych*, w tym w szczególności baz danych ewidencji gruntów i budynków.⁴² Wojewódzki inspektor, jako podmiot prowadzący ewidencję nadzoru geodezyjnego i kartograficznego nie jest obowiązany każdorazowo występować do marszałka i starosty z pisemnym umotywowanym wnioskiem o udostępnienie danych ponieważ prowadzi zbiór, którym jest ewidencja. Przepisy ustawy - Prawo geodezyjne i kartograficzne nie upoważniają wprawdzie *expressis verbis* wojewódzkiego inspektora do występowania do marszałka i starosty o udostępnienie danych, jednak zgodnie z art. 40 ust. 3 ww. ustawy gromadzenie i prowadzenie państwowego zasobu geodezyjnego i kartograficznego, kontrola opracowań przyjmowanych do zasobu oraz udostępnianie tego zasobu zainteresowanym jednostkom oraz osobom prawnym i fizycznym należy do marszałków województw w zakresie zasobów wojewódzkich, a do starostów w zakresie zasobów powiatowych. Ponadto, zgodnie z ust. 3a powołanego artykułu, nadzór nad prowadzeniem państwowego zasobu geodezyjnego i kartograficznego w zakresie zasobów powiatowych i wojewódzkich należy do wojewódzkich inspektorów nadzoru geodezyjnego i kartograficznego.

Generalny Inspektor rozpatrywał także skargę na *odmowę przekazania danych osobowych z ewidencji gruntów burmistrzowi*.⁴³ W przedmiotowej sprawie wszczęto postępowanie administracyjne, w wyniku którego Generalny Inspektor Ochrony Danych Osobowych nakazał staroście powiatu udostępnienie burmistrzowi danych ze zbioru ewidencji gruntów i budynków bez prawa ich udostępniania osobom trzecim. W uzasadnieniu podniesiono, że burmistrz jest uprawniony do pozyskania danych z ewidencji gruntów i budynków na podstawie przepisów prawa, tj. art. 24 ust. 4 ustawy Prawo geodezyjne i kartograficzne. Zgodnie z treścią tego przepisu, starosta zapewnia nieodpłatnie gminom dostęp do całej bazy danych ewidencji gruntów i budynków, a więc do wszystkich zawartych w niej informacji. Udostępnienie danych z ewidencji gruntów i budynków gminie (burmistrzowi) znajduje zatem uzasadnienie w art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych.

⁴² GI-DP-705/00

W omawianym okresie sprawozdawczym zajmowano się również problematyką *udostępniania prasie informacji o działalności organów administracji* na zasadach określonych w ustawie z dnia 26 stycznia 1984 r. Prawo prasowe (Dz. U. Nr 5, poz. 24 z późn. zm.). Jak podkreślał Generalny Inspektor, szczególne znaczenie ma tutaj orzeczenie Sądu Najwyższego z dnia 11 stycznia 1996 r. (III ARN 57/95 OSNAP 1996/13/179), w którym Sąd stwierdził że „określone w art. 4 ust. 1 ustawy prawo prasowe uprawnienie prasy do uzyskania informacji o działalności organu samorządu terytorialnego, nie wyłącza wglądu do akt organu zobowiązanego do udzielenia informacji o ile nie sprzeciwiają się temu przepisy prawa, z których wynika niedopuszczalność ich udostępnienia, w szczególności ze względu na ochronę tajemnicy państwowej i innej tajemnicy chronionej ustawą oraz dóbr osobistych zaliczanych do sfery prywatności, nie wiążącej się z działalnością publiczną”.⁴⁴

Pytano także, czy *wystosowanie przez zarząd gminy odpowiedzi na list otwarty radnego skierowany do mieszkańców gminy, z użyciem imienia, nazwiska oraz adresu zamieszkania tego radnego* narusza przepisy ustawy o ochronie danych osobowych.⁴⁵ Generalny Inspektor w przedstawionym mu przypadku nie stwierdził naruszenia przepisów ustawy o ochronie danych osobowych i zauważył, że dane osobowe radnych nie są objęte taką ochroną, jak osób nie korzystających z biernego prawa wyborczego. Ustawa z dnia 16 lipca 1998 r. Ordynacja wyborcza do rad gmin, rad powiatów i sejmików województw (Dz. U. Nr 95, poz. 602 z późn. zm.) stanowi w art. 99 ust. 1 pkt 3, że w zgłoszeniu listy kandydatów podaje się nazwiska, imiona, wiek oraz miejsce zamieszkania kandydatów. W art. 109 ust. 5 ustawa ta stanowi, że komisja wyborcza zarządza wydrukowanie obwieszczenia o zarejestrowanych listach kandydatów, zawierającego ich numery, dane o kandydatach umieszczone w zgłoszeniach list wraz z ewentualnymi oznaczeniami kandydatów i list. Wynika z powyższego, że dane radnych (imiona, nazwiska, wiek oraz miejsce zamieszkania) są jawne. Jawność danych osobowych radnych w zakresie ich funkcji publicznych wynika też z samej Konstytucji RP. Fakt zamieszkania w danej gminie jest elementem niezbędnym do oceny zdolności radnego do pełnienia mandatu. Nie można więc utajniać faktu zamieszkania radnego w innej gminie. Art. 9 cytowanej ordynacji wyborczej do rad gmin stanowi, że przy ustalaniu faktu stałego zamieszkania dla potrzeb ordynacji stosuje się przepisy Kodeksu cywilnego z dnia 23 kwietnia 1964 r. (Dz. U. Nr 16 poz. 93 z późn. zm.). Fakt umieszczenia w spisie wyborców na podstawie ordynacji wyborczej do Sejmu, nie jest

⁴³ GI-DIS-242/00

⁴⁴ GI-DP-314/00

⁴⁵ GI-DP-331/00

więc wystarczający do dokonania oceny faktu zamieszkania w gminie. Radny jest funkcjonariuszem publicznym, który odpowiada przed swoimi wyborcami.

W praktyce organów administracji szczególnie częste były przypadki, gdy *gmina kontrolująca swoje jednostki organizacyjne żądała wglądu np. w akta osobowe pracowników zatrudnionych w tych jednostkach*. Przypadki te występowały także w poprzednim okresie sprawozdawczym i były szczególnie częstą przyczyną nieporozumień, a nawet konfliktów pomiędzy zainteresowanymi stronami. Generalny Inspektor w tego rodzaju sprawach wielokrotnie podkreślał jednakże, że dostęp do akt osobowych pracowników może mieć jedynie pracodawca, a odmowa udostępnienia kontrolerom gminnym umów o pracę oraz informacji o wynagrodzeniu pracowników tych jednostek jest uzasadniona.⁴⁶ W niektórych przypadkach administratorem danych jest dyrektor domu kultury, w innych np. kierownik ośrodka pomocy społecznej. Żaden z przepisów ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 1998 r. Nr 21, poz. 94 z późn. zm.) oraz rozporządzenia Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt pracowniczych (Dz. U. Nr 62, poz. 286), nie przewiduje możliwości udostępnienia akt pracowniczych innemu podmiotowi.

Uprawnienia dla organów kontrolnych gminy do wglądu w akta pracownicze nie dają również przepisy ustawy z dnia 25 października 1991 r. o organizowaniu i prowadzeniu działalności kulturalnej (Dz. U. z 1997 r. Nr 110, poz. 721 z późn. zm.), interpretowane w związku z przepisami ustawy o samorządzie gminnym. Fakt, iż gmina – na podstawie przepisu art. 10 w zw. z art. 9 ustawy o organizowaniu i prowadzeniu działalności kulturalnej – jest organizatorem danej instytucji kultury, nie upoważnia jej do kontrolowania zgodności zatrudnienia pracowników tejże instytucji z przepisami prawa pracy. W uchwale z dnia 16 lipca 1993 r. Sąd Najwyższy orzekł, iż ujawnienie przez pracodawcę, bez zgody pracownika, wysokości jego wynagrodzenia za pracę może stanowić naruszenie dobra osobistego w rozumieniu art. 23 i 24 Kodeksu cywilnego (OSNC 1994/1/2). W związku z przepisem art. 7 Konstytucji Rzeczypospolitej Polskiej stanowiącym, iż organy władzy publicznej działają na podstawie i w granicach prawa, podkreślenia wymaga, że kompetencje tych organów nie mogą być domniemywane, lecz winny wynikać wprost ze szczególnego przepisu prawa. Z uwagi na powyższe Generalny Inspektor stwierdzał, że gmina nie ma prawa kontrolowania zgodności zatrudnienia pracowników w innej, podległej jej jednostce organizacyjnej z

⁴⁶ GI-DP-1108/00

przepisami prawa pracy. Nie ma bowiem szczególnego uregulowania, które przyznawałoby organom kontrolnym gminy prawo wglądu do akt pracowników rzeczonoj instytucji.

Pytano także o dopuszczalność *udostępniania gminie informacji o osobach korzystających z poradni rodzinnych*. Poradnie takie udzielają często wsparcia zamieszkałym na terenie gminy rodzinom poprzez różnego rodzaju pomoc psychologiczną, poradnictwo prawne, terapie indywidualne i grupowe oraz grupy wsparcia dla dorosłych i dzieci. Jednostki te swoją opieką obejmują także ubogie rodziny wielodzietne. Udostępnienie informacji polegać miało na przekazaniu imienia i nazwiska osoby korzystającej z poradni oraz jej adresu, bez określenia, z pomocy którego pracownika dana osoba korzystała.⁴⁷ W odpowiedzi Generalny Inspektor stwierdził, że przepis art. 23 ust. 1 pkt 2, znajdujący zastosowanie w sytuacji, gdy przetwarzane są dane osobowe tzw. zwykłe (tj. inne niż określone w art. 27 i 28 ustawy o ochronie danych osobowych), należy rozumieć w ten sposób, że przetwarzanie danych osobowych jest dopuszczalne tylko wtedy, gdy zezwalają na to przepisy prawa. Zgodnie z art. 6 ustawy o samorządzie gminnym do zadań własnych gminy należy zaspokajanie zbiorowych potrzeb wspólnoty. Przykłady tych zadań zawiera art. 7 ust. 1 ustawy o samorządzie gminnym. Z mocy art. 1 ust. 1 ustawy o samorządzie gminnym mieszkańcy gminy stanowią wspólnotę samorządową. W celu wykonywania zadań określonych w art. 7 ust. 1, gmina może tworzyć i kontrolować za pomocą komisji rewizyjnej jej jednostki organizacyjne. W myśl art. 18a ust. 1 ustawy o samorządzie gminnym rada gminy kontroluje działalność zarządu oraz gminnych jednostek organizacyjnych za pomocą komisji rewizyjnej. Przepisy prawa ustanawiają zatem kompetencję dla rady gminy do sprawowania kontroli nad realizacją przez gminne jednostki organizacyjne wyznaczonych im zadań, jednostki te zobowiązane są do przekazywania niezbędnych do realizacji celu kontroli danych, w tym danych osobowych (nie dotyczy to jednak danych tzw. szczególnie chronionych, do udostępniania których stosuje się przepisy art. 27 ust. 2 ustawy o ochronie danych osobowych). Uprawnienie rady gminy do uzyskiwania określonych danych nie oznacza jednak prawa komisji rewizyjnej do uzyskania dostępu do pełnej dokumentacji zawierającej różnego rodzaju dane osób korzystających z poradni (niejednokrotnie także dane szczególnie chronione, jak np. informacje o stanie zdrowia). Ustawodawca w art. 26 ust. 1 pkt 3 wymaga bowiem od administratorów danych zapewnienia, aby dane były adekwatne w stosunku do celów, w jakich są przetwarzane. Rada gminy wykonuje zadania na obszarze swej właściwości (z pewnymi wyjątkami). Jest zatem uprawniona do kontrolowania, czy

⁴⁷ GI-DP-024/1289/00

pomoc świadczona przez jej jednostki organizacyjne jest udzielana rzeczywiście osobom należącym do wspólnoty samorządowej.

Generalny Inspektor Ochrony Danych Osobowych zajmował się również *zakresem danych przetwarzanych przez gminną komisję rozwiązywania problemów alkoholowych*. W ocenie skarżących przetwarzanie ich danych osobowych w postaci informacji o nałogach (*alkoholizm, narkomania*) przez ww. komisję było *pozbawione podstaw prawnych*.⁴⁸ Generalny Inspektor zwrócił uwagę na treść art. 27 ust. 2 pkt. 2 ustawy o ochronie danych osobowych, zgodnie z którym przetwarzanie danych o nałogach jest dopuszczalne, jeżeli przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą i stwarza pełne gwarancje ich ochrony. Przepisy takie zawarte są m.in. w ustawie z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi (Dz. U. Nr 35, poz. 230 z późn. zm.). Na podstawie przepisów art. 24 i 25 wskazanej ustawy osoby, które w związku z nadużywaniem alkoholu powodują rozkład życia rodzinnego, demoralizację małoletnich, uchylają się od pracy albo systematycznie zakłócają porządek publiczny kierowane są przez gminną komisję rozwiązywania problemów alkoholowych – na wniosek osoby nadużywającej alkoholu lub z inicjatywy gminnej komisji rozwiązywania problemów alkoholowych – na badanie przez biegłego w celu wydania opinii w przedmiocie uzależnienia od alkoholu i wskazania rodzaju zakładu leczniczego. W tej sytuacji zarówno działania komisji, jak i lekarzy wydających opinię w przedmiocie stopnia zaawansowania choroby alkoholowej, jeżeli znajdują oparcie w przepisie prawa, nie mogą być uznane za niezgodne z ustawą o ochronie danych osobowych.⁴⁹ W sytuacji, gdy zadawane pytania dotyczą, np. skazań oraz innych orzeczeń sądowych i administracyjnych wydanych wobec pacjenta, przetwarzanie takich danych powinno się odbywać na podstawie zezwolenia ustawowego.⁵⁰

Wskazane wyżej przepisy ustawy o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi, w ocenie Generalnego Inspektora Ochrony Danych Osobowych, nie mogą natomiast stanowić podstawy prawnej uprawniającej gminy do uzyskania informacji zawierających dane osobowe pacjentów izb wytrzeźwień.⁵¹ Nie można wyjść z założenia, iż pobyt określonej osoby w izbie wytrzeźwień wiąże się z tym, że nałogiem danej osoby jest

⁴⁸ Np. GI-DP-322/00

⁴⁹ Por. GI-DP-98/00/531

⁵⁰ Zgodnie z art. 28 ust. 1 ustawy o ochronie danych osobowych przetwarzanie danych o skazaniach, orzeczeniach o ukaraniu, mandatach karnych i innych orzeczeniach wydanych w postępowaniu administracyjnym można prowadzić wyłącznie na podstawie innej ustawy.

⁵¹ GI-DP-024/1340

alkoholizm. Udostępnienie przedmiotowych danych powinno być zatem rozpatrywane w kontekście przesłanek wskazanych w przepisie art. 23 ust. 1, nie zaś, jak twierdzili niektórzy zapytujący, w świetle art. 27 ust. 2 ustawy o ochronie danych osobowych.

Do Biura GIODO kierowano ponadto liczne pytania związane z przetwarzaniem informacji o podatkach. W związku z tematyką podatkową pytano w szczególności, *czy na wniosek członka komisji rewizyjnej skarbnik gminy lub pracownik referatu podatkowego może udzielić informacji komu i w jakiej wysokości umorzony został podatek rolny*, oraz czy członek komisji rewizyjnej może wystąpić do rady gminy o przeprowadzenie przez komisję rewizyjną kontroli umorzeń podatkowych w indywidualnych sprawach.⁵² W odpowiedzi Generalny Inspektor poinformował, że komisja rewizyjna nie może mieć wglądu do informacji o podatnikach. Zgodnie z artykułem 18a ust. 1 ustawy o samorządzie gminnym, uprawnienia kontrolne komisji rewizyjnej obejmują jedynie sprawy zastrzeżone do jej kompetencji, a więc wykonanie budżetu gminy oraz inne zadania zlecone przez radę gminy w zakresie kontroli, np. kwestię wykonywania uchwał rady. Do bezpośredniej ingerencji w działalność wójta jako organu podatkowego i urzędu gminy wykonującego zadania z tego zakresu niezbędny byłby szczególny przepis prawa. Takiego przepisu brak, a jedynym właściwym organem do spraw podatkowych jest przewodniczący zarządu gminy, gdyż to on jest w myśl art. 13 § 1 pkt 1 ustawy Ordynacja podatkowa organem podatkowym I instancji. Prawdliwość podejmowanych przez niego decyzji podlega kontroli w trybie odwoławczym przez samorządowe kolegium odwoławcze. Komisja rewizyjna takowych uprawnień nie posiada. Organ podatkowy, zgodnie z art. 178 § 1 Ordynacji podatkowej, owszem może w każdym stadium postępowania udostępniać akta sprawy, ale tylko stronie. Komisja rewizyjna nie jest stroną w myśl art. 133 tejże ustawy i przez to także nie może mieć prawa wglądu do informacji zawartych w aktach sprawy indywidualnych podatników.

W jednym z pism zwrócono się do Generalnego Inspektora Ochrony Danych Osobowych z pytaniem, czy jest zgodne z ustawą *żądanie urzędu gminy od weterynarzy rejestru właścicieli psów*. Wskazywano przy tym, że takie informacje są niezbędne w celu egzekucji podatku, a ich uzyskanie z innych źródeł jest praktycznie niemożliwe.⁵³ Generalny Inspektor wskazał jednakże, że żądanie udostępnienia danych przez weterynarzy nie znajduje oparcia w przepisach. Obowiązującym prawem na terenie gminy będzie również przepis prawa miejscowego. Treść uchwały regulującej przedstawiony problem i kwestia jej legalności nie należy jednak do zakresu kompetencji Generalnego Inspektora. W świetle

⁵² GI-DP-33/00, GI-DP-451/00, GI-DP-604/00

uregulowań Konstytucji RP zawartych w art. 171, działalność samorządu terytorialnego podlega nadzorowi z punktu widzenia legalności. Organami nadzoru nad działalnością jednostek samorządu terytorialnego są Prezes Rady Ministrów i wojewodowie. Zgodnie z art. 91 ust. 1 ustawy o samorządzie gminnym uchwała rady gminy sprzeczna z prawem jest nieważna. Organem uprawnionym do stwierdzenia tego faktu jest jednak organ nadzoru, a więc Prezes Rady Ministrów i wojewoda.

Niemniej należy stwierdzić, że stosowne regulacje dotyczące podatku od posiadania psów zawiera ustawa z dnia 12 stycznia 1991 r. o podatkach i opłatach lokalnych (Dz. U. Nr 9, poz. 31 z późn. zm.). Zgodnie z art. 14 pkt 2 tej ustawy rada gminy określa zasady ustalania i poboru oraz terminy płatności tego podatku. Przepis ten stanowi więc podstawę do wydania przez gminę uchwały regulującej kwestie będące przedmiotem niniejszego upoważnienia. Gmina ustalając przepisy miejscowe musi jednak działać w granicach obowiązującego prawa, w tym także przy podejmowaniu uchwał w sprawie podatków i opłat lokalnych (art. 40 ust. 1 ustawy o samorządzie gminnym). Z delegacji zawartej w art. 14 pkt. 2 ustawy o podatkach i opłatach lokalnych oraz przepisów art. 13 ustawy o samorządzie gminnym wynika, że gmina jest uprawniona do przetwarzania danych posiadaczy psów w związku z ciążącym na nich obowiązkiem podatkowym. Delegacja zawarta w art. 14 powyższej ustawy nie zawiera wyraźnego upoważnienia do ustalania osób zobowiązanych do płacenia przedmiotowego podatku poprzez zebranie takich informacji od weterynarzy. Sama ustawa decyduje w tym przypadku, kto jest podatnikiem podatku od posiadania psów.

Liczna grupa skarg i zapytań prawnych dotyczyła prawidłowości realizacji przez administratorów danych organy samorządu terytorialnego – obowiązków nałożonych przez ustawę o ochronie danych osobowych, m.in. *obowiązku właściwego zabezpieczenia danych*. W jednej ze spraw Generalny Inspektor stwierdził, że *przekazywanie pism urzędowych* w taki sposób, że mają do nich dostęp osoby nieuprawnione stanowi uchybienie obowiązkowi określonemu w art. 36 ustawy o ochronie danych osobowych, zgodnie z którym administrator danych jest obowiązany do właściwego zabezpieczenia danych.⁵⁴ Jak zauważył Sąd Apelacyjny w Łodzi w wyroku z dnia 7 listopada 1995 r., I ACr 529/95, OSA 1995, nr 11-12, poz. 70, adresat przesyłki o charakterze urzędowym ma prawo oczekiwać, że korespondencja ta zostanie przesłana w sposób zabezpieczający przed możliwością zapoznania się z treścią przesyłki przez osoby obce. Powinnością osoby kierującej przesyłką jest zastosowanie takiej formy przesłania, by odpowiednio chroniła jej treść. Jeżeli dokonano przesyłki w sposób

⁵³ GI-DP-767/00

umożliwiający zapoznanie się z jej treścią przez inne niż adresat osoby, to stanowi to naruszenie dobra osobistego adresata, w postaci tajemnicy korespondencji.

Pojawiały się również *pytania, czy prezydent miasta może odmówić ujawnienia danych osób, którym przyznał mieszkania komunalne* w trybie wyjątkowym, czy przesłanką odmowy mogą być przepisy ustawy o ochronie danych osobowych. Według postanowień uchwały rady miasta, w przypadkach szczególnych, uzasadnionych ważnymi względami społecznymi Prezydent może, po zasięgnięciu opinii właściwej komisji odstąpić od uregulowań zawartych w uchwale. Prezydent wedle postanowień tej uchwały składa radzie informacje o podjętych wyjątkach wraz z uzasadnieniem.⁵⁵ Generalny Inspektor stwierdził, że powoływanie się na przepisy ustawy o ochronie danych osobowych przy odmowie ujawnienia nazwisk osób, którym przyznano mieszkania z gminnego zasobu mieszkaniowego, jest nieuzasadnione, ponieważ dopuszczalność przetwarzania wynika z przepisów prawa. Ustawa z dnia 2 lipca 1994 r. o najmie lokali i dodatkach mieszkaniowych (Dz. U. z 1998 r. Nr 120, poz. 787 z późn. zm.)⁵⁶ stanowi, iż gmina jest obowiązana do tworzenia i do racjonalnej gospodarki pozostającym w jej dyspozycji zasobem mieszkaniowym oraz utrzymywania go na poziomie umożliwiającym zaspokajanie potrzeb rodzin o niskich dochodach. Przepis art. 5 ust 3 powołanej ustawy stanowi, że zasady gospodarowania mieszkaniowym zasobem gminy oraz kryteria wyboru osób, z którymi umowy najmu powinny być zawierane w pierwszej kolejności, określa rada gminy. Cytowany przepis nie określa wprawdzie prawnej formy działania rady gminy w tym przedmiocie, jednakże nie ulega wątpliwości, że określenie wspomnianych kryteriów następuje w drodze uchwały rady gminy. Uchwała taka należy do kategorii tzw. uchwał wykonawczych, o których mowa w art. 40 ust. 1 ustawy o samorządzie gminnym, zawiera bowiem przepisy gminne powszechnie obowiązujące na obszarze gminy. Zatem określenie w uchwale rady gminy kryteriów, o których mowa w art. 5 ust. 3 ustawy o najmie lokali i dodatkach mieszkaniowych, zobowiązuje właściwy organ gminy do ich przestrzegania przy procedurze zawierania umów najmu lokali mieszkalnych należących do zasobu mieszkaniowego gminy. Tak też orzekł Sąd Najwyższy w uchwale z dnia 5 listopada 1997 r. o sygn. ZP 37/97 (OSNAP 1998/7/200). Powołany przepis art. 5 ust. 3 nakłada ponadto na gminy obowiązek zapewnienia społecznej kontroli zasad gospodarowania gminnym zasobem mieszkaniowym. Istotne jest, że pojęcie „społecznej kontroli”, o którym w

⁵⁴ GI-DP-375/00

⁵⁵ GI-DP-024/1550/00

⁵⁶ Zmieniona ustawą z dnia 21 czerwca 2001 r. o ochronie praw lokatorów, mieszkaniowym zasobie gminy i o zmianie Kodeksu cywilnego (Dz. U. Nr 71, poz. 739).

przepisie tym mowa, nie może być ograniczone jedynie do kontroli sprawowanej przez organizacje społeczne, stowarzyszenia i inne podobne podmioty. Sformułowanie to oznacza w rzeczywistości kontrolę sprawowaną przez wszystkie podmioty, w szczególności przez mieszkańców danej gminy, tworzących z mocy prawa samorządową wspólnotę gminną. Gminy winny zatem realizować ten postulat podając do publicznej wiadomości dane osób, z którymi w pierwszej kolejności mają być zawarte umowy najmu.

Podobnie jak w ubiegłym okresie sprawozdawczym, pytano wielokrotnie, w jaki sposób spełnić obowiązek informacyjny względem mieszkańców, których dane osobowe znajdują się w zbiorach danych. Pytano także, czy wystarczające jest *podanie w prasie lokalnej informacji o nazwach zbiorów prowadzonych przez urząd* z jednoczesną informacją o uprawnieniach osób, których dane znajdują się w zbiorach.⁵⁷ W odpowiedzi wskazywano, że ustawa o ochronie danych osobowych w art. 24 nakłada na administratora danych obowiązek udzielenia informacji osobom, których dane przetwarza. Podmiot zbierający dane powinien podać swą pełną nazwę i adres siedziby, cel zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych. W celu prawidłowej realizacji obowiązku informacyjnego podmiot taki powinien ponadto poinformować osobę, której dane zbiera o przysługującym jej prawie wglądu do swoich danych oraz ich poprawiania, a także zamieścić informację o dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej. Podanie w prasie lokalnej informacji o nazwach zbiorów prowadzonych przez urząd, z jednoczesną informacją o uprawnieniach osób, których dane znajdują się w tych zbiorach, nie można uznać za wywiązanie się z powyższego obowiązku. Powyższy obowiązek odnosi się jednakże wyłącznie do danych zbieranych po dniu wejścia w życie ustawy. W związku z tym od dnia 30 kwietnia 1998 r. administratorzy danych mają obowiązek informowania osób, których dane zbierają. Należy jednak podkreślić, że obowiązek informacyjny dotyczy osób, których dane są *zbierane*, a nie *przetwarzane*. Tym samym liczba osób, które powinny zostać poinformowane przez administratora danych jest mniejsza, ponieważ obowiązek informacyjny nie obejmuje osób, których dane zostały zebrane przed dniem wejścia w życie ustawy, a po tym dniu są przechowywane (np. osoby, których dane figurowały przed 30 kwietnia 1998 r. w księgach meldunkowych), natomiast po wejściu w życie ustawy obowiązek informacyjny powinien być dokonywany w momencie zbierania danych.

⁵⁷ GI-DP-189/00

II. Przetwarzanie danych przez organy administracji rządowej

W jednym z pism pytano, czy jest zgodna z prawem praktyka ujawniania numeru identyfikacji podatkowej NIP na wystawianym przez urząd miasta nakazie płatniczym za użytkowanie terenu.⁵⁸ Generalny Inspektor wskazywał zatem, że żądanie umieszczenia NIP na dowodach wpłaty jest zasadne. Zgodnie bowiem z art. 11 ustawy z dnia 13 października 1995 r. o zasadach ewidencji i identyfikacji podatników i płatników (Dz. U. Nr 142, poz. 702 z późn. zm.), podatnicy podają NIP na wszelkich dokumentach związanych z wykonywaniem zobowiązań podatkowych, oraz niepodatkowych należności budżetowych, do których poboru obowiązane są organy podatkowe lub celne.

Do Generalnego Inspektora Ochrony Danych Osobowych zwrócił się urząd skarbowy z pytaniem o możliwość udostępniania numerów rachunków bankowych podatników innym organom takim, jak np. urzędy celne, zakład ubezpieczeń społecznych, urzędy pracy.⁵⁹ W odpowiedzi wskazano, że przepis art. 299 § 1 i 3 ustawy z dnia 29 sierpnia 1997 r. Ordynacja podatkowa (Dz. U. Nr 137, poz. 926 z późn. zm.) zobowiązuje organy podatkowe do udostępniania innym organom podatkowym, organom kontroli skarbowej i Ministrowi Finansów, organom celnym, rejonowym urządowi pracy i jednostkom organizacyjnym Zakładu Ubezpieczeń Społecznych informacji wynikających z akt spraw podatkowych, z wyłączeniem informacji wskazanych w art. 182 Ordynacji podatkowej, w tym informacji dotyczących m.in. rachunków bankowych. Do uzyskania informacji o numerach rachunków bankowych – stosownie do przepisu art. 299 § 4 Ordynacji podatkowej – upoważnione są jedynie jednostki organizacyjne Zakładu Ubezpieczeń Społecznych.

Jednocześnie przepis art. 299 § 2 Ordynacji podatkowej stanowi, iż w zakresie i na zasadach określonych w odrębnych przepisach organy podatkowe obowiązane są udostępnić informacje wynikające z akt spraw podatkowych. Stosownie do art. 36 § 1 ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 1991 r. Nr 36 poz. 161 z późn. zm.) organ egzekucyjny może żądać od uczestników postępowania złożenia wyjaśnień oraz zasięgać od organów administracji publicznej i instytucji informacji niezbędnych do prowadzenia egzekucji.

Analiza przytoczonych powyżej przepisów wskazuje na istniejącą niespójność w regulacji prawnej dotyczącej udostępniania przez urzędy skarbowe innym podmiotom

⁵⁸ GI-DP-282/00

informacji objętych tajemnicą skarbową. Niespójność ta zachodzi jednakże między przepisami ustawy o postępowaniu egzekucyjnym w administracji a przepisami ordynacji podatkowej i istniała jeszcze przed uchwaleniem ustawy o ochronie danych osobowych. Jej wejście w życie nie wprowadziło w omawianym zakresie żadnych zmian. Generalny Inspektor wskazywał jednakże, że interpretacja przepisów powołanych wyżej ustaw nie mieści się w zakresie jego kompetencji.

Jedna ze skarg dotyczyła udostępnienia, w związku z prowadzonym postępowaniem egzekucyjnym, danych i wysokości zaległości podatkowych skarżących bankom i biuru maklerskiemu. Organ egzekucyjny dokonał zajęć we wszystkich bankach jednocześnie, dzięki czemu uzyskał informację, gdzie znajdują się rachunki dłużników.⁶⁰ Po dokonaniu czynności wyjaśniających skarga została uznana za niezasadną, ponieważ art. 182 § 1 i art. 183 ustawy Ordynacja podatkowa dają urzędowi skarbowemu upoważnienie do udostępniania bankom danych stron postępowania podatkowego w celu uzyskania informacji od tych banków. Udzielając odpowiedzi skarżącemu powołano się również na art. 36 § 1 ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (tekst jednolity Dz. U. z 1991 r., Nr 36, poz. 161 z późn. zm.), zgodnie z którym organ egzekucyjny może żądać od uczestników postępowania złożenia wyjaśnień oraz zasięgać od organów administracji publicznej i instytucji informacji niezbędnych do prowadzenia egzekucji. Zdaniem Generalnego Inspektora organ egzekucyjny mając uprawnienie do żądania informacji, miał również prawo do udostępniania bankom danych niezbędnych do udzielenia takich informacji. Tym samym krąg podmiotów, do których organ egzekucyjny może się zwrócić o udzielenie ww. informacji jest szeroki. Ponadto, skarżących poinformowano o uprawnieniach dotyczących wnoszenia środków odwoławczych w postępowaniu egzekucyjnym.

Generalny Inspektor nie dopatrzył się natomiast naruszenia przepisów ustawy o ochronie danych osobowych w sprawie *udostępnienia danych osobowych inspektorom kontroli skarbowej*, wyłącznie na podstawie ustnego wezwania przez uprawnione osoby.⁶¹ Tryb postępowania inspektorów kontroli skarbowej wynika z przepisów o kontroli skarbowej. Zgodnie z art. 23 ust. 1 pkt 2 ustawy przetwarzanie danych, w tym zgodnie z art. 7 pkt 2 tej ustawy, ich udostępnianie jest dopuszczalne, jeżeli zezwala na to przepis prawa. Uprawnienia inspektora kontroli skarbowej określone zostały w ustawie z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. 1999 r. Nr 54, poz. 572 z późn. zm.).

⁵⁹ GI-DP-1176/00

⁶⁰ GI-DIS-44/2000

⁶¹ GI-DP-024/1353/00

W związku z powyższym stwierdzić należy, że udostępnienie żądanych przez urząd kontroli skarbowej informacji znajduje podstawę w przepisach prawa. Udostępnienie danych w zakresie niezbędnym do przeprowadzenia kontroli skarbowej (i tylko w tym zakresie) nie narusza ustawy o ochronie danych osobowych.

Inne stanowisko Generalny Inspektor Ochrony Danych Osobowych zajął w przedmiocie dopuszczalności przetwarzania danych przez inspektorów Urzędu Kontroli Skarbowej przeprowadzających kontrolę dokumentacji medycznej pacjentów, którym wykonano wyspecjalizowane zabiegi medyczne (przeszczepy narządów, wszczepy endoprotez, itp.).⁶² Inspektorzy Kontroli Skarbowej twierdzili, iż posiadając upoważnienie do prowadzenia badania celowości i zgodności z prawem gospodarowania środkami budżetowymi posiadają tym samym prawo wglądu w dokumentację medyczną „celem sprawdzenia rzetelności danych w rozliczeniach merytorycznych i finansowych składanych do Ministerstwa Zdrowia”.

Zgodnie z art. 2 ust. 1 ustawy o kontroli skarbowej do zakresu kontroli skarbowej należy m.in. kontrola celowości i zgodności z prawem gospodarowania środkami pochodzącymi z budżetu państwa, środkami państwowych jednostek budżetowych i państwowych jednostek gospodarki pozabudżetowej oraz środkami państwowych funduszy celowych, zarówno u przekazujących, jak i otrzymujących te środki. Kontrolowany, w myśl art. 17 ust. 1 ww. ustawy, jest obowiązany umożliwić inspektorowi dokonanie czynności kontrolnych, a w szczególności zapewnić wgląd w dokumentację i prowadzone ewidencje objęte zakresem kontroli. Przepisy ustawy o kontroli skarbowej w żadnym miejscu nie wskazują, iż w związku z przeprowadzoną kontrolą inspektor ma prawo dostępu również do dokumentacji medycznej pacjenta. Również ustawa o zakładach opieki zdrowotnej w art. 18 ust. 3 nie wymienia urzędów kontroli skarbowej, jako podmiotów uprawnionych do pozyskania danych zawartych w dokumentacji medycznej. Z kolei w świetle art. 40 ust. 1 ustawy o zawodzie lekarza, lekarz ma obowiązek zachowania tajemnicy lekarskiej. Przepisu tego nie stosuje się w sytuacjach enumeratywnie wymienionych w ustępie drugim tego artykułu. Jednakże wśród osób i podmiotów wymienionych w tym przepisie brak jest urzędów kontroli skarbowej.⁶³

Podobnie jak w roku 1999, w omawianym okresie sprawozdawczym Generalnemu Inspektorowi sygnalizowano *kwestię dostępu inspektorów Najwyższej Izby Kontroli do danych o pacjentach cierpiących na choroby płuc*. Jako przesłankę dopuszczalności

⁶² GI-DP-815/001140

przetwarzania danych szczególnie chronionych ustawa o ochronie danych osobowych wymienia zezwolenie przepisu szczególnego innej ustawy na przetwarzanie takich danych bez zgody osoby, której dane dotyczą (art. 27 ust. 2 pkt 2). Oznacza to, że inna ustawa musi wyraźnie zezwalać na przetwarzanie danych o stanie zdrowia, czyli na udostępnianie danych określonym podmiotom, bądź na zbieranie i wykorzystywanie danych przez określone podmioty. W ocenie Generalnego Inspektora upoważnienia inspektorów NIK do przetwarzania tak szczególnej kategorii danych, jakimi są dane o stanie zdrowia, nie można wywodzić z ogólnych przepisów ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 1995 r. Nr 13, poz. 59 z późn. zm.). Tym samym brak jest podstaw do przekazywania danych konkretnych pacjentów w trakcie kontroli prowadzonej przez inspektorów NIK.⁶⁴

W wielu pismach wyrażano także wątpliwość, czy nie narusza ustawy o ochronie danych osobowych *podawanie do publicznej wiadomości wykazów pracodawców i osób fizycznych, którym udzielono pożyczki z Funduszu Pracy*.⁶⁵ W odpowiedzi informowano, że działanie takie nie narusza ustawy o ochronie danych osobowych, ponieważ wykazy pracodawców i osób, którym udzielono pożyczki, podawane są do wiadomości publicznej w powiatowym urzędzie pracy na podstawie przepisu art. 18 ust. 6 ustawy z dnia 14 grudnia 1994 r. o zatrudnieniu i przeciwdziałaniu bezrobociu (Dz. U. z 1995 r. Nr 1, poz. 1 z późn. zm.). Zgodnie z art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych spełniona jest więc przesłanka dopuszczalności przetwarzania danych zawartych w publikowanych wykazach na podstawie przepisów prawa. Informacje podawane w wykazie do publicznej wiadomości nie są wykorzystywane do niezgodnych z prawem celów, a jedynie dla wypełnienia obowiązku nałożonego na urząd. Generalny Inspektor zauważył także, iż zgodnie z art. 52 ustawy o zatrudnieniu i przeciwdziałaniu bezrobociu Fundusz Pracy jest państwowym funduszem celowym, a więc pożyczki udzielane są ze środków publicznych. Norma wynikająca z przywołanego wyżej przepisu art. 18 ust. 6 ustawy o zatrudnieniu i przeciwdziałaniu bezrobociu została skonstruowana w celu zapewnienia kontroli wykorzystania środków publicznych, ponieważ pieniądze przydzielane na pożyczki udzielane z Funduszu Pracy pochodzą m.in. ze środków budżetu państwa. Ponadto zgodnie z art. 55 ww. ustawy dochodami Funduszu są także obowiązkowe składki wpłacane przez m.in. pracodawców i osoby podlegające ubezpieczeniu społecznemu.

⁶³ Ibidem

⁶⁴ Szerzej w wystąpieniu Generalnego Inspektora do Prezesa NIK z dnia 3 stycznia 2000 r., sygn. GI/3/2000

⁶⁵ GI-DP-762/00

Ważne jest, aby pracodawcy i osoby, którym udzielono pożyczki, a także inni zainteresowani informowani byli jak wykorzystywane są środki, o których przydzieleniu (w formie pożyczki) decyduje powiatowy urząd pracy. Środki te, pochodzące z budżetu państwa, powinny być bowiem wykorzystywane dla uzasadnionych prawem celów. Celem takim jest właśnie realizacja zadań państwa w zakresie zatrudniania, przeciwdziałania bezrobociu i łagodzenia jego skutków. Organy zatrudniania, a w szczególności powiatowy urząd pracy, na podstawie przepisu art. 14 pkt 4 ustawy o zatrudnieniu i przeciwdziałaniu bezrobociu, w celu ograniczenia bezrobocia, w razie braku możliwości zapewnienia bezrobotnym odpowiedniego zatrudnienia, udziela pożyczek z Funduszu Pracy na podjęcie działalności na własny rachunek. Przedmiotowy wykaz jest formą informowania wszystkich zainteresowanych w jaki sposób środki pochodzące z Funduszu wykorzystywane są na udzielenie pożyczek.

III. Przetwarzanie danych osobowych przez inne organy

W sprawie dotyczącej *zbierania informacji o przynależności członków zarządu mediów publicznych do partii politycznych* przeprowadzone przez Generalnego Inspektora Ochrony Danych Osobowych postępowanie administracyjne wykazało, że Krajowa Rada Radiofonii i Telewizji (KRRiT) stworzyła zbiór danych osobowych członków zarządów mediów publicznych, w którym przetwarzane były dane o przynależności partyjnej. Jako podstawę prawną powoływano przy tym art. 23 ust. 1 pkt 4 ustawy, który stanowi, że przetwarzanie danych jest dopuszczalne wtedy, gdy jest to niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego. Odnosząc się do tej opinii Generalny Inspektor podkreślił, że przepis art. 23 ust. 1 ustawy statuuje przesłanki przetwarzania „zwykłych” danych osobowych. Jednakże dane, o których mowa w art. 27 ust. 1 ustawy (m.in. dane ujawniające poglądy polityczne oraz przynależność partyjną) stanowią szczególną kategorię danych osobowych, bowiem ujawniają informacje wyjątkowo ważne dla prywatności osoby, której dane dotyczą. W związku z powyższym, ustawa zabroniła przetwarzania danych wrażliwych, dopuszczając jednakże ich przetwarzanie wyłącznie w okolicznościach, określonych w art. 27 ust. 2 ustawy. Podkreślono także, że przesłanki przetwarzania danych wymienione w przepisie art. 23 ust. 1 ustawy znajdują zastosowanie w odniesieniu do wszystkich danych osobowych, z wyjątkiem danych wrażliwych (art. 27) oraz danych, o których mowa w art. 28 ustawy.

W konsekwencji, wobec braku stosownych przepisów szczególnych innej ustawy zezwalających KRRiT na przetwarzanie danych o przynależności partyjnej członków zarządów mediów publicznych bez ich zgody, Krajowa Rada, aby legalnie przetwarzać

powyższe dane musiałyby się legitymować spełnieniem co najmniej jednego z warunków wymienionych w art. 27 ust. 2 ustawy. W aktualnym stanie prawnym przetwarzanie tych danych byłoby więc dopuszczalne, jeżeli członkowie zarządów mediów publicznych wyraziliby odpowiednią zgodę na piśmie, albo jeżeli przetwarzanie dotyczyłoby danych, które zostały podane przez nich do publicznej wiadomości.

Generalny Inspektor nakazał zatem Krajowej Radzie Radiofonii i Telewizji usunięcie danych ujawniających przynależność partyjną członków zarządów mediów publicznych zebranych bez spełnienia co najmniej jednej z przesłanek przetwarzania danych wymienionych w art. 27 ust. 2 ustawy o ochronie danych osobowych.⁶⁶

Do Biura GIODO wpłynęło pismo powiatowego rzecznika konsumentów, który pytał o to, czy ustawa o ochronie danych osobowych nie stoi na przeszkodzie do uzyskiwania przez niego, do celów związanych z wypełnianiem obowiązków ustawowych, danych osobowych konsumentów. Z docierających do Generalnego Inspektora sygnałów wynikało, że organy gmin często reprezentują stanowisko, że rzecznik nie jest uprawniony do uzyskiwania tych danych, a same dane dostępne są wyłącznie dla organów ścigania i wymiaru sprawiedliwości.⁶⁷ Taka interpretacja przepisów ustawy niejednokrotnie paraliżuje pracę rzeczników konsumentów. Generalny Inspektor poinformował, że uzyskiwanie takich informacji nie stoi w żadnej mierze w sprzeczności z przepisami ustawy o ochronie danych osobowych. Do realizacji zadań, do których pełnienia został powołany powiatowy rzecznik konsumentów niezbędne jest posiadanie danych osobowych, a kierowanie spraw do sądu, lub zawiadomienie właściwych organów o popełnieniu przestępstwa nie odbywa się bez wiedzy poszkodowanego. To właśnie skargi poszkodowanych inicjują to postępowanie. Oni też bezpośrednio przekazują swoje dane, bez których postępowanie nie może dojść do skutku. Nie ma zatem takiej potrzeby, by dodatkowo sięgać do informacji zawartych w ewidencji ludności.

Liczna grupa skarg i pytań prawnych odnosiła się do przetwarzania danych osobowych przez Zakład Ubezpieczeń Społecznych. Przedmiotem wielu skarg była zasadność udostępniania organom ZUS oryginałów druku zwolnienia lekarskiego, na których umieszczony zostaje numer choroby, tym samym w ocenie wielu skarżących z danymi dotyczącymi ich stanu zdrowia mogą się zapoznać osoby nieuprawnione. Generalny Inspektor nie podzielił zarzutów skarżących i poinformował, iż zgodnie z art. 58 ustawy z dnia 25 czerwca 1999 r. o świadczeniach pieniężnych z tytułu ubezpieczenia społecznego w razie

⁶⁶ GI-DEC-DP-53/00

choroby i macierzyństwa (Dz. U. Nr 60, poz. 636 z późn. zm.) zaświadczenie lekarskie wystawia się z dwiema kopiami. Oryginał zaświadczenia przesyłany jest przez wystawiającego zaświadczenie do Zakładu Ubezpieczeń Społecznych. Pierwszą kopię zaświadczenia otrzymuje ubezpieczony, natomiast drugą kopię, wystawiający zaświadczenie przechowuje przez okres trzech lat. Zgodnie z ust. 2 powołanego przepisu numery statystyczne choroby ustalone według Międzynarodowej Statystycznej Klasyfikacji Chorób i Problemów Zdrowotnych, wpisuje się tylko na oryginale i na drugiej kopii. Przepisy powyższej ustawy w sposób wyczerpujący regulują kwestię wystawiania i przesyłania zaświadczeń lekarskich ZUS-owi.⁶⁸

W związku z przeprowadzanym programem naukowym badania Polskich Stulatków „PolSto99” organizatorzy programu w celu jego realizacji zwracali się do ZUS o udostępnienie im aktualnych danych wszystkich Polaków, którzy ukończyli 100 lat życia. Organy ZUS odmawiały udostępnienia przedmiotowych danych, powołując się na treść art. 26 ust. 2 ustawy o ochronie danych osobowych. Generalny Inspektor nie podzielił powyższego stanowiska.⁶⁹ W myśl art. 23 ust. 1 pkt 5 ustawy o ochronie danych osobowych, przetwarzanie danych jest dopuszczalne, jeżeli jest niezbędne do wypełnienia usprawiedliwionych celów administratorów danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą. Uregulowanie takie jest zgodne z Dyrektywą 95/46/EC Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych. W preambule tego aktu w punkcie 29 stwierdzono, że przetwarzanie danych osobowych dla celów naukowych nie jest na ogół uważane za niezgodne z celami, dla których dane były pierwotnie gromadzone, pod warunkiem zapewnienia odpowiednich zabezpieczeń prawnych. Aby przetwarzanie danych osobowych do celów naukowych było zgodne z prawem, nie mogą one być wykorzystywane w innym celu. Zgodnie z art. 6 Dyrektywy przetwarzanie danych w celach naukowych zasadniczo jest zgodne z przepisami prawa, pod warunkiem wprowadzenia odpowiednich zabezpieczeń przez dane państwo. Generalny Inspektor uznał, iż w przedstawionym przez organizatorów stanie faktycznym prowadzenie badań naukowych stanowi usprawiedliwiony cel administratora danych, zbieranie danych jest niezbędne do realizacji zadania badawczego, a realizacja celu nie narusza praw i wolności

⁶⁷ GI-DP-161/00

⁶⁸ Zob. w sprawie GI-DP-164/00/324

⁶⁹ GI-DP-734/00/1506

osób, których dane są zbierane. Ustawa o ochronie danych osobowych nie stoi zatem na przeszkodzie udostępnieniu tego rodzaju danych przez ZUS.

Wielu pytających zwracało się również do Generalnego Inspektora o ocenę *stanowiska ZUS w przedmiocie odmowy udostępnienia im informacji o zmarłych członkach ich rodzin, ubezpieczonych w ZUS.*⁷⁰ Generalny Inspektor nie dopatrywał się w tej sytuacji naruszenia ustawy o ochronie danych osobowych. Zgodnie z art. 123 ustawy o systemie ubezpieczeń społecznych zarówno tryb jak i formę udostępnienia lub odmowy udostępnienia wnioskowanych danych regulują unormowania zawarte w ustawie Kodeks postępowania administracyjnego. W przypadku, gdy przedmiotowe dane zostały uzyskane przez dany oddział ZUS od ubezpieczonych płatników składek, w myśl art. 79 ustawy o systemie ubezpieczeń społecznych, objęte zostały tajemnicą służbową ZUS.

IV. Inne sprawy

Generalny Inspektor zajmował się sprawą *udostępnienia przez wójta gminy danych osób (Grupy Inicjatywnej) popierających przeprowadzenie referendum w sprawie odwołania rady gminy*, adwokatowi reprezentującemu wójta w postępowaniu cywilnym i karnym. Wójt w wyjaśnieniach potwierdził fakt udostępnienia danych osobowych członków Grupy Inicjatywnej swojemu pełnomocnikowi i w związku z tym, Generalny Inspektor Ochrony Danych Osobowych, zawiadomił Prokuraturę Rejonową w Kielcach (zaw. 24/00) o popełnieniu przestępstwa określonego w art. 51 ustawy o ochronie danych osobowych. Z

Prokuratury Rejonowej w Skarżysku-Kamiennej wpłynęło zawiadomienie o wszczęciu śledztwa w przedmiotowej sprawie.⁷¹ Sprawa jest w toku.

W odpowiedzi na jedno z pytań prawnych Generalny Inspektor uznał, iż *biblioteki przetwarzają dane o czytelnikach na podstawie przesłanki określonej w art. 23 ust. 1 pkt 2 ustawy*. Na gromadzenie tych informacji zezwalają bowiem przepisy ustawy z dnia 27 czerwca 1997 r. o bibliotekach (Dz. U. Nr 85, poz. 539).⁷²

Nie tylko jednak przepis prawa stanowi przesłankę legalności przetwarzania danych osobowych. *Zapewnianie porządku i czystości* oraz tworzenie warunków do ich utrzymania, zgodnie z art. 3 ust. 1 ustawy z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach (Dz. U. Nr 132, poz. 622 z późn. zm.), należy do obowiązkowych zadań gminy. Zdaniem Generalnego Inspektora należy przyjąć, że utrzymywanie porządku i czystości w

⁷⁰ GI-DP-872/00/1092

⁷¹ GI-DIS-169/00

⁷² GI-DP-137/00

gminie stanowi prawem określone działanie realizowane dla dobra publicznego, o którym mówi art. 23 ust. 1 pkt 4 ustawy o ochronie danych osobowych. Z uwagi na to, udostępnienie danych osobowych podmiotom działającym na rzecz utrzymania czystości, upoważnionym do tego na mocy przepisów prawa (zarówno ustawowych jak i stanowionych przez gminę, na obszarze jej właściwości), w zakresie rzeczywiście niezbędnym dla prowadzenia tej działalności, nie narusza przepisów o ochronie danych osobowych.⁷³

Komisja zakładowa związku zwróciła się do Generalnego Inspektora Ochrony Danych Osobowych z prośbą o interwencję wobec odmowy udostępnienia przez marszałka województwa *informacji dotyczącej przewoźnika prowadzącego usługi regularnego transportu osobowego zawartej w wydanej decyzji*.⁷⁴

Generalny Inspektor uznał, że udzielenie informacji o przewoźnikach w zakresie żądanym, nie narusza przepisów ustawy o ochronie danych osobowych. Zgodnie z art. 2 pkt 1 ustawy z dnia 29 sierpnia 1997 r. o warunkach wykonywania krajowego drogowego przewozu osób (Dz. U. Nr 141, poz. 942 z późn. zm.) przewóz zarobkowy jest działalnością gospodarczą polegającą na odpłatnym przewozie osób pojazdami samochodowymi. Dane przewoźników nie są danymi osobowymi w rozumieniu ustawy o ochronie danych osobowych, lecz informacjami o podmiotach występujących w obrocie gospodarczym. W takim zakresie, w jakim dane te identyfikują podmiot w związku z prowadzoną działalnością zawodową, nie podlegają ochronie przewidzianej przepisami ustawy o ochronie danych osobowych, także wówczas, gdy zakres ich pokrywa się z zakresem danych osoby fizycznej.

W sprawie dotyczącej udostępnienia osobie nieupoważnionej danych o osobach posiadających rzadkie imiona, w wyniku przeprowadzonych czynności wyjaśniających ustalono, że o *udostępnienie danych ww. osób na potrzeby badań socjologicznych* zwrócił się Uniwersytet Warszawski (dane były niezbędne studentce piszącej pracę magisterską na temat osób posiadających rzadkie imiona).⁷⁵ W związku z tym, że dane zostały udostępnione w oparciu o art. 26 ust. 2 ustawy o ochronie danych osobowych nie stwierdzono naruszenia przepisów o ochronie danych osobowych. Skarżącą poinformowano ponadto o możliwości

⁷³ GI-DP-024/1475/00

⁷⁴ GI-DP-430/1463/00

⁷⁵ GI-DIS-213/00

wniesienia pisemnego, umotywowanego żądania zaprzestania udostępniania danych ze względu na szczególną sytuację.

C. PRZETWARZANIE DANYCH OSOBOWYCH PRZEZ FUNKCJONARIUSZY SŁUŻB PUBLICZNYCH

I. Przetwarzanie danych osobowych przez Policję

Wśród zadawanych pytań najczęściej pojawiała się kwestia, czy policjanci mogą, nie naruszając przy tym ustawy o ochronie danych osobowych, podawać do wiadomości osoby poszkodowanej imię, nazwisko, adres zamieszkania, kategorię i numer prawa jazdy, adres zamieszkania właściciela pojazdu (niejednokrotnie kierujący pojazdem sprawca kolizji nie jest właścicielem tego pojazdu) i inne dane niezbędne poszkodowanemu do uzyskania odszkodowania z ubezpieczenia.⁷⁶ Odpowiadając Generalny Inspektor Ochrony Danych Osobowych wskazywał, że odmowa podania danych, o których mowa w art. 44 ust. 1 pkt 4 ustawy Prawo o ruchu drogowym, z powołaniem się na ustawę o ochronie danych osobowych wynika z niezrozumienia tej ustawy. Przesłanką legalności przetwarzania danych osobowych, o której mowa jest w art. 23 ust. 1 pkt 2 jest przepis art. 44 ust. 1 pkt 4 ustawy z dnia 20 czerwca 1997 r. Prawo o ruchu drogowym (Dz. U. Nr 98, poz. 602 z późn. zm.). Stanowi on, że kierujący pojazdem w razie uczestniczenia w wypadku drogowym jest obowiązany podać swoje dane personalne, dane personalne właściciela lub posiadacza pojazdu oraz dane dotyczące zakładu ubezpieczeń, z którym zawarta jest umowa obowiązkowego ubezpieczenia odpowiedzialności cywilnej, na żądanie osoby uczestniczącej w wypadku. W niektórych przypadkach sprawcy kolizji argumentują, że nie można mówić o wypadku, gdy doszło jedynie do kolizji. Generalny Inspektor wskazywał jednakże, że pojęcie wypadku drogowego występuje w prawie o ruchu drogowym w bardzo szerokim znaczeniu. Pod pojęciem tym ustawa ujmuje wszystkie zdarzenia związane z ruchem drogowym, które zaistniały na drodze publicznej, spowodowały uszkodzenie ciała, rozstrój zdrowia, śmierć albo jakkolwiek szkodę w mieniu oraz zostały spowodowane przez jakiekolwiek działanie lub zaniechanie sprawcy (kierującego, pieszego lub innego uczestnika ruchu drogowego).

Do Generalnego Inspektora Ochrony Danych Osobowych zwrócił się Wojewoda Zachodniopomorski z pytaniem o dopuszczalność zawarcia porozumienia z Komendantem Wojewódzkim Policji, na mocy którego do komendy wojewódzkiej Policji przekazywane

⁷⁶ GI-DP-367/00/387

byłyby *dane osób ukaranych mandatami kredytowymi*, a które uchylają się od ich opłacania.⁷⁷ W ocenie Generalnego Inspektora, na mocy przepisów prawa, tj. art. 15 § 2 ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego oraz art. 20 ustawy dnia 6 kwietnia 1990 r. o Policji (Dz. U. Nr 30, poz. 179 z późn. zm.) Policja może zwracać się do Urzędu Wojewódzkiego o udostępnienie danych osobowych wskazanych osób, np. w związku z prowadzeniem czynności operacyjno – rozpoznawczych, dochodzeniowo – śledczych i administracyjno – porządkowych podejmowanych w celu wykrywania przestępstw lub podczas prowadzonego postępowania karnego, nie jest jednak uprawniona do prowadzenia ewidencji danych osób ukaranych mandatami karnymi kredytowanymi w celu usprawnienia procedury egzekwowania stosownych należności. Generalny Inspektor wskazał na przepis § 3 rozporządzenia Rady Ministrów z dnia 9 grudnia 1994 r. w sprawie sposobu dokumentacji i ewidencji grzywien za wykroczenia, ściąganych w postępowaniu mandatowym, oraz organów właściwych w sprawach rozprowadzania i rozliczania bloczków mandatowych (Dz. U. Nr 131, poz. 663), wydanego na podstawie art. 8 ustawy z dnia 23 lutego 1992 r. o zmianie niektórych przepisów prawa karnego, prawa o wykroczeniach i o postępowaniu w sprawach nieletnich (Dz. U. Nr 24, poz. 101), który stanowi, że właściwymi w sprawach ewidencjonowania wpływów i należności z tytułu grzywien nałożonych w drodze mandatu karnego, zgodnie z przepisami o zasadach prowadzenia rachunkowości są urzędy wojewódzkie.

W jednym z pism komenda miejska Policji wystąpiła z pytaniem, *jakie dane sprawcy wypadku drogowego Policja może udostępnić osobie poszkodowanej w tym wypadku*. Wydział ruchu drogowego komendy miejskiej uznał, że zgodnie z art. 44 ust. 1 pkt 4 ustawy Prawo o ruchu drogowym uczestnicy zdarzenia mają prawo znać dane personalne osób uczestniczących w zdarzeniu drogowym i w toczących się postępowaniach odszkodowawczych, administracyjnych lub karnych przysługują im bowiem, jako stronom postępowania uprawnienia w postaci, np. prawa przeglądania akt oraz dokonywania z nich odpisów. W tym celu opracowano wzór dokumentu, zwany Notatką Informacyjną zawierający szereg informacji, których zakres wykracza poza krąg określony przez ustawodawcę.⁷⁸ Zastrzeżenia Generalnego Inspektora budził przede wszystkim zamieszczony w notatce zapis o ukaraniu sprawcy. W myśl art. 28 ust. 1 ustawy o ochronie danych osobowych przetwarzanie danych dotyczących skazań, orzeczeń o ukaraniu, mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym

⁷⁷ GI-DP-1030/00

można prowadzić wyłącznie na podstawie ustawy. Powołany przepis Prawa o ruchu drogowym nie przewiduje podawania tego rodzaju informacji, wobec czego brak jest ustawowej podstawy do ich udostępniania innym podmiotom. Generalny Inspektor zwrócił uwagę, że postępowanie mandatowe zostało uregulowane w dziale V Kodeksu postępowania w sprawach o wykroczenia. Przepisy te nie stanowią jednak o sporządzaniu przez Policję żadnej dokumentacji o charakterze procesowym. Jedynym dokumentem wydawanym w ramach tego postępowania jest mandat karny, który określa osobę i zarzucane jej wykroczenie. Jeżeli sprawca wykroczenia godzi się na wymierzenie grzywny w postaci mandatu karnego, nie jest kierowany wniosek o ukaranie do kolegium ds. wykroczeń. Ustawa o ochronie danych osobowych nie przewiduje sposobu rozporządzania dokumentami zawierającymi dane osobowe, a powstającymi w ramach wewnętrznych procedur poszczególnych podmiotów. Jednakże w odniesieniu do danych wymienionych w art. 28 ust. 1 ustawy o ochronie danych osobowych, ich przetwarzanie dopuszczalne jest jedynie na podstawie przepisu rangi ustawowej. Udostępnianie takich informacji bez spełnienia określonej przesłanki legalności przetwarzania stanowi naruszenie przepisów ustawy. Udostępnienie innych informacji zawartych w Notatce powinno mieć umocowanie w przesłance określonej w art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych.

W jednym z pism zwrócono się do Generalnego Inspektora Ochrony Danych Osobowych z pytaniem o zasadność *odmowy udostępnienia przez Policję danych określonej, uciążliwej dla otoczenia osoby*. Policja nie udostępniła żądanych danych motywując ten fakt potrzebą przestrzegania przepisów o ochronie danych osobowych.⁷⁹ Generalny Inspektor zwrócił uwagę, że ustawa o ochronie danych osobowych wprowadziła instytucję udostępnienia danych osobowych w celu innym, niż włączenie do zbioru. Zgodnie z przepisem art. 29 ust. 2 ustawy o ochronie danych osobowych, Policja winna po otrzymaniu wniosku uzasadnionego potrzebą dochodzenia praw przed sądem udostępnić dane osoby, która zdaniem wnioskodawcy dopuściła się czynu zabronionego. Nie mogą to być jednakże akta konkretnej sprawy.

Policja *nie udostępniła danych również osobie, która została pomówiona o uszkodzenie pojazdu*. Po umorzeniu postępowania przygotowawczego osoba ta zdecydowała się na wystąpienie z powództwem cywilnym o odszkodowanie. Sąd zażądał, pod rygorem zwrotu pozwu, przesłania danych osobowych pozwanego. Danych tych Policja nie udostępniła skarżącemu, z uwagi na to, że wnioskujący o udostępnienie nie występował w

⁷⁸ GI-DP-780/00

procesie w charakterze strony.⁸⁰ Generalny Inspektor poinformował, że organ postępowania karnego, który dysponuje informacją o osobie pozwanej, jest zobowiązany na żądanie sądu przekazać sądowi tę informację. W przedmiotowej sprawie przekazanie danych przez Policję sądowi znajduje uzasadnienie w przepisach prawa, a tym samym nie narusza ustawy o ochronie danych osobowych.

Generalny Inspektor odpowiadał również na pytanie, czy nie narusza ustawy o ochronie danych osobowych *udzielenie informacji o końcu kary skazanego*. Ubezpieczeniowy Fundusz Gwarancyjny zwrócił się do dyrektora jednego z warszawskich aresztów śledczych z prośbą o udzielenie takich informacji, powołując się na art. 90 e ust. 1, 2 i 3 ustawy z dnia 28 lipca 1990 r. o działalności ubezpieczeniowej (Dz. U. 1996 r., Nr 11, poz. 62 z późn. zm.) oraz na § 1 pkt 2 c rozporządzenia Rady Ministrów z dnia 15 kwietnia 1998 r. w sprawie organów uprawnionych i organów zobowiązanych do przeprowadzenia kontroli wykonania obowiązku zawarcia umowy ubezpieczenia oraz trybu ustalania i egzekwowania opłaty za niedopełnienie tego obowiązku (Dz. U. Nr 74, poz. 474 z późn. zm.).⁸¹ Zdaniem Generalnego Inspektora ani przepisy ustawy o działalności ubezpieczeniowej, ani przepisy powołanego rozporządzenia Rady Ministrów z dnia 15 kwietnia 1998 r. nie stanowią dostatecznej podstawy do przekazywania Ubezpieczeniowemu Funduszowi Gwarancyjnemu informacji o upływie terminu odbycia kary. Generalny Inspektor stwierdził, że wobec brzmienia art. 28 ustawy o ochronie danych osobowych, przesłanką legalności przetwarzania danych osobowych może być wyłącznie przepis prawa rangi ustawowej. Nawet zgoda osoby, której dotyczą dane nie jest wystarczającą przesłanką legalności przetwarzania danych o ukaraniu i innych wymienionych w art. 28 ust. 1 ustawy o ochronie danych osobowych.

Wśród zagadnień dotyczących udostępniania danych osobowych, często przewijała się *kwestia formy, w jakiej powinny zwracać się do Policji określone podmioty wnioskujące o udostępnienie danych osobowych*. Generalny Inspektor wskazywał, że forma w jakiej zwracają się administratorzy nie zależy od rodzaju podmiotu, który zamierza te dane uzyskać, tylko od faktu, czy pozyskane dane zostaną włączone do zbioru, czy też wykorzystane do innych celów, a ponadto, czy inne niż ustawa o ochronie danych osobowych przepisy nie regulują tego zagadnienia w odmienny sposób. Wyjaśniano w szczególności, że jeżeli firmy ubezpieczeniowe zwracające się do Policji na podstawie przepisów ustawy o działalności ubezpieczeniowej, zamierzają udostępnić dane osobowe włączyć do zbioru, nie muszą

⁷⁹ GI-DP-160/00/222

⁸⁰ GI-DP-899/00/1087

⁸¹ GI-DP-279/99/291/00

zwracać się o udostępnienie danych w trybie określonym w art. 29 ust. 3 ustawy o ochronie danych osobowych. Przepis ten znajduje bowiem zastosowanie wyłącznie wtedy, gdy dane udostępnione zostają w celu innym niż włączenie do zbioru.⁸²

Przedmiotem analizy Generalnego Inspektora Ochrony Danych Osobowych była również kwestia *dopuszczalność udostępnienia Policji kopii baz danych operatorów sieci telekomunikacyjnych* zawierających informacje o abonentach telefonicznych (imię nazwisko lub nazwa firmy, numer telefonu, adres). Komendant Główny Policji wskazał, iż udostępnienie tego rodzaju danych byłoby związane z wprowadzeniem nowoczesnych systemów wspomagania dowodzenia. System taki zapewnić ma m.in. możliwość kojarzenia danych osoby dzwoniącej z danymi zawartymi w bazie teleadresowej. Pozwoliłoby to na upewnienie się co do prawdziwości zarejestrowanych informacji przed zatwierdzeniem danego zdarzenia i podjęciem decyzji o interwencji. Policja wskazywała, że uzyskanie baz teleadresowych skróciłoby znacznie procedurę przyjmowania zgłoszenia, czas przeprowadzenia interwencji oraz uwiarygodniło zgłoszenie zdarzenia, co wobec znacznej liczby fałszywych zgłoszeń ma duże znaczenie. Dzięki dostępowi do bazy danych operatorów sieci telefonicznych powstać miałyby specjalna baza danych abonentów niepożądanych ze względu na często wywoływane przez nich złośliwe zgłoszenia.⁸³ W odpowiedzi z dnia 21 kwietnia 2000 r. skierowanej do Komendanta Głównego Policji Generalny Inspektor stwierdził, że jedyną możliwość zmiany tych procedur i stworzenia mechanizmów prawnych pozwalających Policji na uzyskanie swobodnego dostępu do baz danych operatorów sieci telekomunikacyjnych stanowi nowelizacja ustawy o Policji.⁸⁴ Należy rozróżnić dwie kategorie danych znajdujących się w bazach operatorów sieci telekomunikacyjnych. Z jednej strony są to dane dotyczące abonentów ujawnione w książce telefonicznej, zatem powszechnie dostępne. Z drugiej strony bazy te zawierają także dane dotyczące abonentów, które nie są powszechnie dostępne, jak również dane o abonentach, których numery telefonów są zastrzeżone. Nie ma żadnych przeszkód, aby Policja korzystała z danych należących do pierwszej grupy. W odniesieniu do danych należących do drugiej wymienionej kategorii Generalny Inspektor podkreślił, że ich przetwarzanie jest dopuszczalne, gdy zezwala na to przepis prawa. Z uwagi na to, że brak obecnie takiego przepisu, Policja nie może uzyskać automatycznego dostępu do całych zbiorów danych operatorów sieci. Zgodnie z obowiązującymi przepisami Policja powinna każdorazowo zwracać się do administratora

⁸² GI-DP-024/1451/00

⁸³ GI-DP-395/00

⁸⁴ GI/368/00

danych z prośbą o udostępnienie danych osobowych. Zdaniem Generalnego Inspektora uzyskanie automatycznego dostępu uniemożliwiają ponadto uregulowania prawne dotyczące kwestii technicznych. Stosownie do przepisów ustawy o ochronie danych osobowych oraz przepisów wykonawczych, każdorazowe udostępnienie danych osobowych należy odnotować. Dostęp automatyczny uniemożliwiałby spełnienie tego wymogu.

Komenda miejska policji zwróciła się do Uniwersytetu Jagiellońskiego z prośbą o comiesięczne *przesyłanie sekcji ds. nieletnich wykazów informacji o nieletnich, którzy zostali umieszczeni w Klinice Toksykologii UJ po spożyciu alkoholu oraz innych środków odurzających*.⁸⁵ Na pytanie administratora danych o zgodność z prawem takiego udostępnienia Generalny Inspektor odpowiedział, że uprawnienia Policji wiążą się jedynie z prowadzeniem konkretnego postępowania i nie stanowią podstawy do żądania udostępnienia zbioru danych osób nieletnich leczonych w Klinice Toksykologii. Zasady udostępniania informacji organom ścigania określają właściwe przepisy prawa. Żądanie przekazania danych powinno być sporządzone na piśmie, uzasadnione i zawierać odpowiednią podstawę prawną. Zasady udzielenia informacji Policji określa rozporządzenie Rady Ministrów z dnia 13 sierpnia 1996 r. w sprawie szczegółowego trybu korzystania przez policjantów z pomocy instytucji państwowych, organów administracji rządowej i samorządu terytorialnego, jednostek gospodarczych i organizacji społecznych oraz osób (Dz. U. Nr 107, poz. 501). Zgodnie z § 2 ust. 1 tego rozporządzenia policjanci w toku czynności operacyjno-rozpoznawczych, dochodzeniowo – śledczych i administracyjno - porządkowych podejmowanych w celu rozpoznawania, wykrywania przestępstw i wykroczeń, zapobiegania im oraz wykonania poleceń sądu, prokuratora, organów administracji państwowej i samorządu terytorialnego, mają m.in. prawo do żądania niezbędnej pomocy od instytucji państwowych, organów administracji rządowej i samorządu terytorialnego oraz jednostek gospodarczych prowadzących działalność w zakresie użyteczności publicznej.

Generalny Inspektor wyjaśniał również, iż nie jest właściwym organem do rozpatrywania *skarg na interwencję Policji*, o ile podczas jej dokonywania nie doszło do naruszenia zasad przetwarzania danych osobowych.⁸⁶

II. Przetwarzanie danych osobowych przez Służbę Więzienną

Do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęła skarga na niezgodne zdaniem wnoszącego przetwarzanie danych osobowych przez Zarząd Służby

⁸⁵ GI-DP-726/00/1036

Więziennej. Skarżący uważał, że *gromadzenie danych w Kartotece Skazanych i Tymczasowo Aresztowanych* narusza ustawę o ochronie danych osobowych.⁸⁷ Generalny Inspektor stwierdził, że przetwarzanie tych danych znajduje zatem podstawę prawną, o której mowa w art. 28 ust. 1 ustawy o ochronie danych osobowych. Zgodnie z art. 23 a ustawy z dnia 26 kwietnia 1996 r. o Służbie Więziennej (Dz. U. Nr 61, poz. 283 z późn. zm.), Służba Więzienna może gromadzić i wykorzystywać informacje i dane osobowe, w tym także bez zgody osób, których one dotyczą, niezbędne do realizacji zadań, o których mowa w ustawie o Służbie Więziennej.

W ocenie Generalnego Inspektora nie znajduje zastosowania przepis art. 29 ustawy o ochronie danych osobowych, gdy administrator danych, którym jest dyrektor zakładu karnego lub aresztu śledczego, udostępnia dane o aresztowanym lub osadzonym innym jednostkom organizacyjnym więziennictwa.⁸⁸

Do Biura Generalnego Inspektora Ochrony Danych Osobowych wpływały również pisma z pytaniem o zgodność z ustawą procedury związanej ze sposobem sporządzania korespondencji przez skazanych i jej odbiorem przez funkcjonariuszy Służby Więziennej.⁸⁹ Generalny Inspektor uznając, iż przedstawiona problematyka znajduje unormowanie w przepisach Kodeksu karnego wykonawczego i rozporządzeniu Ministra Sprawiedliwości w sprawie regulaminu wykonywania kary pozbawienia wolności, nie stwierdził naruszenia ustawy o ochronie danych osobowych. Nadto podkreślił, iż nie jest on uprawniony do interpretacji ustaw, w szczególności przepisów nie związanych z ochroną danych osobowych.⁹⁰

Odnosząc się do zagadnienia przetwarzania informacji o skazanym przez jednostki administracji penitencjarnej Generalny Inspektor zwrócił również uwagę na potrzebę modyfikacji art. 11 K.k.w., tj. uzupełnienie treści tego przepisu o upoważnienie do przetwarzania danych szczególnie chronionych.⁹¹

III. Przetwarzanie danych osobowych przez Wojskowe Komendy Uzupełnień

Generalny Inspektor podjął również sprawę przetwarzania danych osobowych przez Wojskowe Komendy Uzupełnień.⁹² Generalny Inspektor stwierdził, że ponieważ brak jest

⁸⁶ GI-DP-024/1442/00

⁸⁷ GI-DP-430/417/00

⁸⁸ GI-DP-295/00/777, por. także GI-DP-636/00/681

⁸⁹ GI-DP-024/1331/00

⁹⁰ Ibidem

⁹¹ Szerzej w wystąpieniu do Ministra Sprawiedliwości, sygn. GI/881/00

⁹² GI-DP-377/00/990

odpowiedniego przepisu rangi ustawowej zezwalającego na dokonywanie wpisów o stanie zdrowia w książeczce wojskowej, umieszczanie takich informacji w książeczce wojskowej narusza ustawę o ochronie danych osobowych. Zgodnie z art. 54 ustawy z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (Dz. U. 1992 r., Nr 4, poz. 16 z późn. zm.), osobom objętym ewidencją prowadzoną przez wojskowych komendantów uzupełnień wydaje się *wojskowe dokumenty osobiste* dla potrzeb powszechnego obowiązku obrony. Na podstawie art. 54 ust. 2 cytowanej ustawy, rodzaje i wzory wojskowych dokumentów osobistych, organy właściwe do ich wydawania oraz zasady dokonywania wpisów w tych dokumentach określa Minister Obrony Narodowej. Wzór książeczki wojskowej określa zarządzenie Ministra Obrony Narodowej z dnia 26 czerwca 1995 r. w sprawie książeczki wojskowej (M. P. Nr 32, poz. 374). Zgodnie z § 1 tego zarządzenia, książeczka wojskowa jest wojskowym dokumentem stwierdzającym stosunek jej posiadacza do obowiązku służby wojskowej. W myśl art. 27 ust. 1 pkt 2 ustawy o ochronie danych osobowych, przetwarzanie danych szczególnie chronionych jest dopuszczalne, jeżeli przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą i stwarza pełne gwarancje ochrony. Generalny Inspektor zwrócił się zatem do Ministra Obrony Narodowej o podjęcie działań mających na celu przywrócenie stanu zgodnego z prawem.

D. ORGANY WYMIARU SPRAWIEDLIWOŚCI

W okresie sprawozdawczym, tj. od 1 stycznia 2000 r. do 31 grudnia 2000 r. do Biura Generalnego Inspektora wpłynęło wiele skarg i zapytań prawnych dotyczących przetwarzania danych osobowych przez sądy, działających przy sądach komorników, jak również przez organy prokuratury. W myśl art. 7 ustawy z dnia 2 kwietnia 1997 r. Konstytucja Rzeczypospolitej Polskiej (Dz. U. Nr 78, poz. 483) organy władzy publicznej działają na podstawie prawa i w granicach prawa. Jak wynika z utrwalonego orzecznictwa, zasada proporcjonalności w zakresie praw człowieka i konstytucyjnych praw jednostki, o których mowa w Konstytucji, zmusza do wyrażenia poglądu, iż działanie władzy, aby uznane zostało za legalne, musi być jeszcze – dodatkowo – proporcjonalne (glosa do wyroku NSA z dnia 1 lipca 1999 r. SA/BK 208/99, OSP 2000/1/17). Przepisy prawa muszą zatem dokładnie określać zakres przedmiotowy i podmiotowy oraz zadania i tryb postępowania poszczególnych organów.

Przesłanki legalności przetwarzania danych osobowych zostały określone w ustawie o ochronie danych osobowych. Przetwarzanie danych jest dopuszczalne w sytuacjach

określonych w art. 23 ust. 1 tej ustawy, a więc m.in. wtedy, gdy zezwalają na to przepisy prawa. Działalność sądów, działających przy nich komorników sądowych oraz prokuratur uregulowana została w przepisach proceduralnych i materialnych poszczególnych dziedzin prawa, przepisach wykonawczych do tych aktów prawnych, jak również w ustawie z dnia 20 czerwca 1985 r. Prawo o ustroju sądów powszechnych (Dz. U. z 1994 r. Nr 7, poz. 25 z późn. zm.), rozporządzeniu Ministra Sprawiedliwości z dnia 17 listopada 1987 r. Regulamin wewnętrznego urzędowania sądów powszechnych (Dz. U. Nr 38, poz. 218 z późn. zm.), ustawie z dnia 20 czerwca 1985 r. o Prokuraturze (Dz. U. z 1994 r. Nr 19, poz. 70 z późn. zm.), rozporządzeniu Ministra Sprawiedliwości z dnia 11 kwietnia 1992 r. Regulamin wewnętrznego urzędowania powszechnych jednostek organizacyjnych prokuratury (Dz. U. Nr 38, poz. 163 z późn. zm.), ustawie z dnia 6 kwietnia 1990 r. o Policji (Dz. U. Nr 30, poz. 179 z późn. zm.), ustawie z dnia 29 sierpnia 1997 r. o komornikach sądowych i egzekucji (Dz. U. Nr 133, poz. 882 z późn. zm.).

Skargi związane z działalnością sądów i prokuratury w Polsce wynikały przede wszystkim z nieznanomości kompetencji przysługujących Generalnemu Inspektorowi Ochrony Danych Osobowych w ramach ustawy o ochronie danych osobowych, jak również z braku znajomości przepisów procedury cywilnej i karnej oraz wydanych na ich podstawie przepisów wykonawczych.

W 2000 r. liczba ww. skarg wzrosła do 40, przy czym zanotowano wzrost liczby skarg dotyczących działań biegłych sądowych, adwokatów, czy komorników sądowych.⁹³ Niejednokrotnie uczestnicy toczących się (lub już zakończonych) postępowań cywilnych i karnych, niezadowoleni z rozstrzygnięcia organu wymiaru sprawiedliwości, zwracali się do Generalnego Inspektora o dokonanie ponownej analizy materiału dowodowego i wydanie opinii przesądzającej spór na ich korzyść. Tym samym Generalnego Inspektora błędnie identyfikowano, jako organ instancyjny w danej sprawie. Generalny Inspektor nie będąc upoważniony z mocy przepisów prawa nie oceniał również zasadności skarg dotyczących nieprawidłowego, w przekonaniu skarżących, działania adwokatów, biegłych sądowych, czy komorników. Informując o kompetencjach Generalnego Inspektora, wskazywano jednakże przepisy prawa, wyznaczające zakres uprawnień i obowiązków przysługujących stronie (uczestnikowi postępowania) w określonych stanach faktycznych.

⁹³ Przykładowo w 1999 zarejestrowano 26 skarg [w:] Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych za okres 01.01.1999 r.-31.12.1999 r., Biuro Generalnego Inspektora Ochrony Danych Osobowych, Warszawa 2000 r.

I. Zakres i podstawy przetwarzania danych osobowych przez sądy

W 2000 r. w napływających do Biura Generalnego Inspektora Ochrony Danych Osobowych pismach najczęściej wątpliwości wywoływały *kwestie legalności i zbyt szerokiego zakresu przetwarzania przez sądy danych osobowych podmiotów uczestniczących w postępowaniu sądowym*. W ocenie Generalnego Inspektora Ochrony Danych Osobowych ustawa o ochronie danych osobowych nie upoważnia go do ingerencji w pracę niezawisłego organu oraz oceny prawidłowości rozstrzygnięcia merytorycznego i treści uzasadnienia orzeczenia sądu, o co niejednokrotnie wnioskowali skarżący w kierowanych do Biura skargach.⁹⁴ Generalny Inspektor wyjaśniał, iż w myśl art. 18 ust. 3 ustawy o ochronie danych osobowych, zasady przetwarzania danych osobowych w toku postępowania sądowego regulowane są przepisami szczegółowymi, innymi niż cytowana ustawa. Zagadnienie przetwarzania danych osobowych w toku postępowania sądowego regulują m.in. ustawa z dnia 20 czerwca 1985 r. Prawo o ustroju sądów powszechnych (Dz. U. z 1994 r., Nr 7, poz. 25 z późn. zm.) oraz ustawa z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (Dz. U. Nr 43, poz. 296 z późn. zm.), zwana dalej K.p.c. Przepisy te stanowią *lex specialis* w stosunku do przepisów ustawy o ochronie danych osobowych. Regulacja przewidziana w art. 48 prawa o ustroju sądów powszechnych wprowadziła zasadę niezawisłości sędziowskiej. Zasada ta oznacza, iż sędziowie w kwestii gromadzenia materiału dowodowego, dokonywania jego oceny, orzekania, w tym również uzasadniania decyzji podjętej w sprawie, są niezależni i podlegają tylko ustawie. Ponadto, zgodnie z art. 328 § 2 K.p.c., uzasadnienie wyroku powinno zawierać wskazanie podstawy faktycznej rozstrzygnięcia, a mianowicie: ustalenie faktów, które sąd uznał za udowodnione, dowodów, na których się oparł i przyczyn, dla których innym dowodom odmówił wiarygodności i mocy dowodowej, oraz wyjaśnienie podstawy prawnej wyroku z przytoczeniem przepisów prawa. Dlatego też sąd w trakcie toczącego się postępowania sądowego ma prawo, zgodnie z art. 232 K.p.c. dopuścić każdy dowód, który uzna za konieczny w celu wyjaśnienia wszystkich okoliczności sprawy.

Największa liczba skarg związanych z przetwarzaniem danych przez sądy dotyczyła *kwestii udostępniania danych o stronach, uczestnikach postępowań, a także o osobach nie posiadających statusu strony w procesie*. Poddawano w wątpliwość m.in. zasadność ujawniania na posiedzeniach sądu nie tylko tzw. danych zwykłych, np. imienia, nazwiska, adresu zamieszkania, wykształcenia, stanu cywilnego, ale również dowodów zawierających dane szczególnie chronione, a więc informacji odnoszących się do takich sfer życia

⁹⁴ Np. GI-DIS-430/424/00

skarżących, jak przynależność wyznaniowa, partyjna, pochodzenie rasowe, stan zdrowia, czy też życie seksualne. Zapytujący wyrażali obawy, czy ujawnienie tak szczegółowego zakresu danych jest zgodne z Konstytucją Rzeczypospolitej Polskiej, która chroni prawo każdego człowieka do prywatności. Szczególnie wiele skarg kierowano pod adresem sądów dopuszczających na rozprawie dowód z karty choroby skarżących i członków ich rodzin, dowód z badań przeprowadzanych przez poradnie psychologiczno – pedagogiczne, czy też z opinii sporządzanych przez szpitale psychiatryczne.

Generalny Inspektor nie podzielił powyższego stanowiska i uznał, iż ww. działania sądu nie stoją w sprzeczności z przepisami ustawy o ochronie danych osobowych. Ustawa o ochronie danych osobowych w art. 27 ust. 1 ustanowiła zakaz przetwarzania danych sensytywnych, tj. danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym. Jednakże w przypadku zaistnienia którejkolwiek z przesłanek określonych w ust. 2 cytowanego przepisu dopuszcza się przetwarzanie przedmiotowych danych, np. gdy przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą i stwarza pełne gwarancje ich ochrony. Generalny Inspektor poinformował, iż takie przepisy zawarte są m.in. w przepisach proceduralnych prawa karnego i prawa cywilnego.

Zagadnienie przeprowadzenia dowodów w sprawach z zakresu prawa cywilnego unormowane są m.in. w przepisach ustawy Kodeks postępowania cywilnego. Przepisy działu III powołanego Kodeksu regulują kwestie dotyczące dowodów, a więc przedmiotu i oceny tych dowodów oraz postępowania dowodowego. Przepisy dotyczące dowodów mają charakter bezwzględnie obowiązujący. Każde twierdzenie strony (powoda i pozwanego, a w postępowaniu nieprocesowym uczestnika postępowania) powinno być poparte dowodami. Zgodnie z art. 227 K.p.c. przedmiotem dowodu są fakty i sądy o faktach mające dla rozstrzygnięcia sprawy istotne znaczenie. Selekcji faktów dokonuje sąd, uwzględniając zasadę prawdy materialnej i zasadę kontrydiktoryjności. Ocena tego, który z przedstawionych dowodów jest istotny, a który nie wnosi niczego istotnego do ostatecznego rozstrzygnięcia sprawy, należy do sądu.⁹⁵

Jak wynikało z treści jednego z pism, sąd na wniosek pozwanej przekazał jej dokumentację medyczną lekarzom w celu sporządzenia przez biegłych sądowych opinii

⁹⁵ Patrz GI-DP-930/00/111

medycznej. W ocenie skarżącego osoby zobligowane przez sąd do wydania opinii nie były biegłymi sądowymi, a zatem wskazane udostępnienie nastąpiło z naruszeniem przepisów ustawy o ochronie danych osobowych. Zgodnie z art. 232 K.p.c. strony w postępowaniu cywilnym mają prawo składać wnioski dowodowe. W toku postępowania sąd ma prawo dopuścić każdy dowód przyczyniający się do wyjaśnienia sprawy; odnosi się to zarówno do dowodów zawnioskowanych na rozprawie, jak również dowodów przez stronę nie wskazanych. W wypadkach wymagających wiadomości specjalnych sąd po wysłuchaniu wniosków stron co do liczby biegłych i ich wyboru może wezwać jednego lub kilku biegłych w celu zasięgnięcia ich opinii (art. 278 § 1 K.p.c.). Tryb ustanawiania i odwoływania oraz pełnienia czynności przez biegłych sądowych określa rozporządzenie Ministra Sprawiedliwości z dnia 6 czerwca 1987 r. w sprawie biegłych sądowych i tłumaczy przysięgłych (Dz. U. Nr 18, poz. 112), które za biegłego sądowego uważa stałego biegłego w zakresie określonej gałęzi nauki, sztuki, rzemiosła lub innej umiejętności (§ 8). Istnienie kategorii „stałych” biegłych sądowych nie wyłącza możliwości, a nawet konieczności korzystania przez sądy z usług innych osób. Bieglym w konkretnej sprawie nie musi być bowiem osoba wpisana na listę biegłych sądowych. Sąd w wyroku z dnia 25 lutego 1974 r. (sygn. II KR 371/73, OSNKW 1974, Nr 6, poz. 117) wskazał, że bieglym może być także inna bezstronna osoba mająca odpowiednie (a więc porównywalne z określonymi dla biegłych sądowych) kwalifikacje. Brak jest zatem jakichkolwiek podstaw do różnego traktowania i oceny opinii, w zależności od tego, czy pochodzi ona od biegłego sądowego, czy też od biegłego powołanego w konkretnej sprawie.

Sąd, zgodnie z zasadą swobodnej oceny dowodów wyrażoną w art. 233 K.p.c., ocenia wiarygodność i moc dowodów według własnego przekonania, na podstawie wszechstronnego rozważenia materiału zebranego w trakcie toczącego się postępowania. W przekonaniu Generalnego Inspektora działania sądu, znajdując umocowanie w przepisie prawa, są tym samym zgodne z ustawą o ochronie danych osobowych. Ponadto Generalny Inspektor uznał że nie jest organem uprawnionym do przesądzania o wartości dowodu dopuszczonego przez niezawisły i niezależny sąd.⁹⁶ Odnosząc się do kwestii udostępnienia akt sprawy bieglemu, Generalny Inspektor zwrócił również uwagę na zakres takiego udostępnienia i dokonując analizy pojęcia adekwatności przetwarzania danych do realizowanego celu, o którym mowa w art. 26 ust. 1 pkt 3 ustawy, zaznaczył, iż wątpliwości budzi przekazywanie bieglemu całości akt sprawy. W związku z powyższym, w sygnalizacji

⁹⁶ Ibidem

skierowanej do Ministra Sprawiedliwości został wysunięty postulat modyfikacji przepisu art. 198 § 1 K.p.k. w taki sposób, aby upoważniał on do przekazania biegłemu akt jedynie w zakresie niezbędnym do wydania przez niego opinii.⁹⁷

Indywidualne zapytania kierowane do Generalnego Inspektora dotyczyły wyjaśnienia kwestii, czy sędzia na rozprawie cywilnej może zadawać pytania powodowi cywilnemu o przebiegu jego choroby i sposobie leczenia w obecności świadków, pozwanej oraz innych osób postronnych, w sytuacji, gdy wszystkie informacje odnoszące się do choroby skarżącego zostały wcześniej dołączone do akt sprawy.⁹⁸ Zgodnie z art. 2 ust. 1 ustawy o ochronie danych osobowych określa ona zasady postępowania przy przetwarzaniu danych osobowych oraz prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych. Zakres przedmiotowy ustawy wyznaczony treścią powyższego przepisu wskazuje, iż ustawa nie znajduje zastosowania do danych osobowych, które nie są przetwarzane w zbiorach. Zgodnie z definicją zbioru danych określoną w art. 7 pkt 1 ustawy, jest nim każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony, czy podzielony funkcjonalnie. Z powyższego wynika, iż tym co odróżnia zbiór danych od innych zestawów danych jest istnienie jednej lub kilku cech pozwalających na odnalezienie określonej informacji bez konieczności przeglądania całego zestawu lub znacznej jego części. W ocenie Generalnego Inspektora analiza przedstawionego powyżej stanu faktycznego, dokonana z uwzględnieniem przytoczonej definicji zbioru danych, prowadzi do stwierdzenia, iż w ww. przypadku nie dochodzi do przetwarzania danych osobowych w zbiorze i w związku z tym nie znajdują zastosowania uregulowania prawne ustawy o ochronie danych osobowych.⁹⁹

Podobne stanowisko Generalny Inspektor zajął w sprawie dotyczącej przyjęcia przez sąd w poczet dowodów kserokopii karty zleceń, w której znajdowała się opinia o stanie zdrowia skarżącego, a także karty zdrowia spadkodawcy, z której treścią jedna ze stron poprzez swojego pełnomocnika zapoznała wszystkich uczestników postępowania w sprawie o podział spadku.¹⁰⁰ Podkreślono przy tym, iż strony biorące udział w postępowaniu cywilnym są obowiązane z mocy prawa wskazać sądowi dowody dla stwierdzenia faktów, z których wywodzą skutki prawne (art. 232 K.p.c.). Przedłożenie sądowi przez pełnomocnika strony

⁹⁷ Szerzej w wystąpieniu Generalnego Inspektora z dnia 8 września 2000 r., sygn. GI/881/00

⁹⁸ GI-DP-977/00/1233

⁹⁹ Ibidem

¹⁰⁰ GI-DIS-223/00/943

przeciwnej, jako dowodu w postępowaniu - dokumentacji zawierającej dane osobowe skarżącego, nie narusza przepisów o ochronie danych osobowych.¹⁰¹

Podobnie jak w roku 1999, do Biura skierowano wiele zapytań w przedmiocie legalności *umieszczania przez sąd na kopertach pism wysyłanych do osób występujących w procesie, informacji o rodzaju tych pism*. W przekonaniu Generalnego Inspektora, stosowana przez organy procesowe praktyka umieszczania na kopertach, w których wysyłana jest korespondencja do stron i uczestników postępowania, informacji o rodzaju wysyłanego pisma jest praktyką nieprawidłową.¹⁰² Dotychczasowy sposób oznaczania pism nie znajduje bowiem oparcia w przepisach obowiązującego prawa, w tym w rozporządzeniu z dnia 15 grudnia 1970 r. w sprawie doręczania pism sądowych przez pocztę (Dz. U. Nr 31, poz. 226), a umieszczanie informacji o rodzaju przesyłanego pisma nie jest niezbędne do doręczenia przesyłki. Według Generalnego Inspektora umieszczenie danych o rodzaju pisma niewątpliwie narusza prywatność osoby, do której kierowana jest korespondencja, a w przypadku przesyłania pism zawierających informacje o wyniku postępowania stanowić będzie naruszenie ustawy o ochronie danych osobowych.

Mając na uwadze powyższe, Generalny Inspektor zwrócił się do Ministra Sprawiedliwości z prośbą o spowodowanie zmiany opisanej praktyki, poprzez wycofanie z użytku druku „Potwierdzenie odbioru”, który zawierał oznaczenie sprawy, wprowadzonego pismem Ministra Sprawiedliwości z dnia 21 lipca 1997 r.¹⁰³ i zastąpienie go drukiem, w treści którego nie będzie zawarta informacja o rodzaju przesyłanego pisma. Na skutek tej interwencji Ministerstwo Sprawiedliwości uznało za niedopuszczalne zamieszczenie na kopertach adresowanych do obywateli jakichkolwiek innych, poza sygnaturą akt sprawy, oznaczeń wysyłanej korespondencji i poleciło prezesom wszystkich sądów zmianę dotychczasowej praktyki oznaczania korespondencji.¹⁰⁴ Ministerstwo Sprawiedliwości poinformowało również Generalnego Inspektora, że z dniem 7 sierpnia 1999 r. wejdą w życie nowe przepisy o doręczaniu pism sądowych, tj. rozporządzenie Ministra Sprawiedliwości z dnia 17 czerwca 1999 r. w sprawie szczegółowych zasad i trybu doręczania pism sądowych w postępowaniu karnym (Dz. U. Nr 62, poz. 696) i rozporządzenie Ministra Sprawiedliwości z dnia 17 czerwca 1999 r. w sprawie szczegółowego trybu doręczania pism sądowych przez pocztę w postępowaniu cywilnym (Dz. U. Nr 62, poz. 697). Wspomniane rozporządzenia

¹⁰¹ Ibidem, podobnie patrz GI-DP-024/1217

¹⁰² GI-DP-430/1497/00

¹⁰³ Sygn. L.Dz.O.I.0133/82/96

¹⁰⁴ Sygn. O.I.0133/18/99

określają adnotacje, jakie powinny być dokonywane na kopertach i potwierdzeniach odbioru. W rozporządzeniu dotyczącym postępowania karnego, we wzorze potwierdzenia odbioru pozostała jednak rubryka „rodzaj pisma”. Wydaje się więc, że stosowanie przedmiotowych adnotacji, aczkolwiek wątpliwe w świetle zasad ochrony prywatności, nie jest sprzeczne z obowiązującym prawem.¹⁰⁵

Przedmiotem licznych zarzutów kierowanych pod adresem sądów było również *udostępnianie przez sądy danych osobowych (w tym niejednokrotnie danych szczególnie chronionych) osobom trzecim, tj. nie związanym żadnym stosunkiem procesowym z toczącym się postępowaniem*. Uznając swoje prawo do ochrony prywatności skarżący zarzucali sądom niedołożenie należytej staranności w celu ochrony interesów uczestników postępowania poprzez doręczenie kopii pism procesowych osobom trzecim, np. pełnomocnikowi strony przeciwnej.¹⁰⁶ Generalny Inspektor nie podzielił powyższego stanowiska. Ustanowiona w art. 9 K.p.c. zasada jawności wewnętrznej zakłada, że strony i uczestnicy postępowania mają prawo przeglądać akta sprawy i otrzymywać odpisy i wyciągi z tych akt. Stosownie do art. 133 § 3 k.p.c., jeżeli ustanowiono pełnomocnika procesowego lub osobę upoważnioną do odbioru pism sądowych doręczenia należy dokonać tym osobom. W związku z powyższym udostępnienie pełnomocnikowi strony pisma procesowego nie jest w rozumieniu przepisów prawa udostępnianiem pisma osobom postronnym. Z treści niektórych skarg, jakie wpłynęły do Biura Generalnego Inspektora Ochrony Danych Osobowych wynikało ponadto, iż skarżący uznając pełnomocników strony przeciwnej w procesie za osoby postronne wnosili o uznanie czynności podejmowanych przed sądem przez adwokatów za niezgodne z przepisami ustawy o ochronie danych osobowych.¹⁰⁷ W odpowiedzi na powyższe skarżących poinformowano, iż czynności podejmowane przez adwokatów regulują przepisy ustawy z dnia 26 maja 1982 r. Prawo o advokaturze (Dz. U. Nr 16, poz. 124 z późn. zm.), zwanej dalej prawem o advokaturze, a także przepisy K.p.c. Zgodnie z art. 4 ust. 1 prawa o advokaturze zawód adwokata polega na świadczeniu pomocy prawnej, a w szczególności na udzielaniu porad prawnych, sporządzaniu opinii prawnych, opracowywaniu projektów aktów prawnych oraz występowaniu przed sądami i urzędami. Dopuszczalność, zakres, sposób, czy formę reprezentacji strony przez pełnomocnika w procesie cywilnym regulują przepisy działu V Kodeksu postępowania cywilnego. Istota pełnomocnictwa procesowego polega na tym, że upoważnia ono z mocy prawa do tych wszystkich czynności procesowych, które wynikają z

¹⁰⁵ GI-DP-430/1497/00

¹⁰⁶ GI-DP-572/00/823, GI-DP-619/00/665

¹⁰⁷ GI-DP-943/00/1091

przebiegu procesu (art. 91 K.p.c.). Strona może jednak zarówno ograniczyć, jak i rozszerzyć zakres umocowania pełnomocnika na podstawie zawartej z nim umowy. Korzystając z pomocy adwokata strona, na podstawie ww. przepisów prawa może poinformować swojego pełnomocnika o wszystkich okolicznościach sprawy, mogących mieć wpływ na ostateczne jej rozstrzygnięcie przed sądem, zaś pełnomocnik, tj. występujący w sprawie adwokat, wykorzystując uzyskane informacje realizuje tym samym nadane mu ustawowo lub umownie prawo do obrony osoby reprezentowanej.¹⁰⁸

W świetle obowiązujących przepisów nie może być również uznany za osobę postronną tzw. oskarżyciel posiłkowy. Zgodnie z art. 53 K.p.k. oskarżyciel posiłkowy jest stroną i przysługują mu w związku z tym uprawnienia przewidziane dla strony w postępowaniu przed sądem. Na podstawie art. 156 § 1 K.p.k. stronom, obrońcom, pełnomocnikom i przedstawicielom ustawowym, udostępnia się akta sprawy sądowej i daje możliwość sporządzenia z nich odpisów. W ocenie Generalnego Inspektora powyższe przepisy stanowią podstawę prawną do udostępnienia oskarżycielowi posiłkowemu odpisów z dokumentów załączonych do akt sprawy.¹⁰⁹ W jednym z pism skarżąca – małżonka pozwanego w sprawie o podwyższenie obowiązku alimentacyjnego - nie występująca w sprawie w charakterze strony, zarzuciła sądowi obrazę przepisów ustawy o ochronie danych osobowych poprzez wykorzystanie w postępowaniu, toczącym się przed sądem rodzinnym i opiekuńczym, informacji o jej stanie majątkowym.¹¹⁰ W odpowiedzi na powyższe podkreślono, iż działanie sądu znajduje oparcie w przepisach prawa i jest tym samym zgodne z przesłanką określoną w art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych.

Przetwarzanie danych powinno być dokonane w oparciu o przynajmniej jedną z przesłanek wymienionych w art. 23 ust. 1 ustawy o ochronie danych osobowych. Katalog przesłanek dopuszczalności przetwarzania danych jest zamknięty, a jedną z nich jest przepis prawa. Uprawnienie do przetwarzania danych osobowych przez administratora danych nie może być domniemane, ale powinno wynikać wprost ze szczególnego przepisu prawa. Kwestie związane z orzekaniem w sprawach obowiązku alimentacyjnego regulują przepisy tytułu II działu III ustawy z dnia 25 lutego 1964 r. Kodeks rodzinny i opiekuńczy (Dz. U. Nr 9, poz. 59 z późn. zm.), zwanej dalej K.r.i o. Zakres świadczeń alimentacyjnych, zgodnie z zapisem art. 135 § 1 K.r.i o., zależy od usprawiedliwionych potrzeb uprawnionego oraz od zarobkowych i majątkowych możliwości zobowiązanego. Wydanie orzeczenia o wysokości

¹⁰⁸ Ibidem, por. GI-DIS-264/00/1238

¹⁰⁹ GI-DIS-228/00/1649, podobnie w sprawie sygn. GI-DP-613/00/580

¹¹⁰ GI-DP-430/1272/00

świadczenia alimentacyjnego wymaga m.in. uprzedniego, rzetelnego ustalenia możliwości zarobkowych oraz stosunków majątkowych osoby zobowiązanej do tego rodzaju świadczeń. Obowiązek ustalenia przedmiotowych okoliczności pośrednio wynika również z przepisu art. 233 § 1 K.p.c., zgodnie z którym sąd orzeka na podstawie wszechstronnego rozważenia zebranego materiału dowodowego.

Szczególnie duża liczba pism kierowanych do Generalnego Inspektora Ochrony Danych Osobowych w 2000 r. *dotyczyła zasadności udostępniania sądom danych osobowych przez inne organy*. Przedmiotem skarg była m.in. kwestia udostępnienia danych zgromadzonych w placówkach poradni psychologiczno – pedagogicznych. Poradnie zwracały się z pytaniem o zakres informacji udzielanych sądom na temat klientów, korzystających z ich porad, badań diagnostycznych i terapii. Wyrażano obawy, czy w sytuacji skorzystania przez sąd z dokumentacji zgromadzonej przez poradnie będą one w stanie zagwarantować dyskrecję swoim klientom.¹¹¹ Jak wynika z treści art. 23 ust. 1 pkt 2 ustawy, przetwarzanie danych jest dopuszczalne, gdy zezwalają na to przepisy prawa. Stosownie do dyspozycji zawartej w art. 248 § 1 K.p.c., każdy obowiązany jest przedstawić na zarządzenie sądu w oznaczonym terminie i miejscu dokument znajdujący się w jego posiadaniu i stanowiący dowód faktu istotnego dla rozstrzygnięcia sprawy, chyba że dokument zawiera tajemnicę państwową. Również regulacje prawne przewidziane w ustawie z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (Dz. U. z 1997 r. Nr 89, poz. 555 z późn. zm.), zwanej dalej K.p.k., przewidują, iż wszystkie instytucje państwowe, samorządowe i społeczne są obowiązane w zakresie swego działania do udzielania pomocy organom prowadzącym postępowanie karne (art. 15 § 2). W związku z powyższym należy uznać, że poradnie są zobowiązane udostępniać na żądanie sądów posiadanie dane osobowe zarówno w związku z postępowaniem karnym, jak i cywilnym.

Odnosząc się do problemu udostępnienia dokumentacji medycznej sądowi Generalny Inspektor poinformował, że stosownie do art. 6 K.p.c. akta spraw udostępniane są jedynie stronom bądź uczestnikom postępowania, natomiast zgodnie z treścią art. 156 § 1 K.p.k. akta sprawy sądowej udostępnia się jedynie stronom, obrońcom, pełnomocnikom i przedstawicielom ustawowym; w pozostałych przypadkach udostępnienie akt wymaga zgody prezesa sądu, który sprawdza zasadność wniosku o udostępnienie akt i w razie nieuzasadnionego żądania może taki wniosek odrzucić. Udostępnienie danych zawartych w aktach sprawy nie może zatem dotyczyć nieograniczonego kręgu podmiotów, albowiem

¹¹¹ GI-DP-1064/00/1571

przepisy wskazanych ustaw w znacznym stopniu krąg uprawnionych do wglądu w akta zawężają.

Do udostępnienia danych dotyczących stanu zdrowia - na żądanie sądu - zobowiązane są również takie jednostki organizacyjne, jak szpitale. Szczególnie duża liczba skarg kierowanych do Generalnego Inspektora dotyczyła bezprawnego, zdaniem skarżących, udostępniania przez szpitale i przychodnie lekarskie, dokumentacji medycznej.¹¹² Podstawą prawną upoważniającą sądy do wysuwania takich żądań jest art. 248 K.p.c.,¹¹³ natomiast podstawą prawną zobowiązującą wskazane podmioty do udostępnienia wnioskowanych danych jest art. 18 ust. 4 pkt 4 ustawy z dnia 30 sierpnia 1991 r. o zakładach opieki zdrowotnej (Dz. U. Nr 91, poz. 408 z późn. zm.), który przewiduje, iż zakład opieki zdrowotnej jest zobowiązany udostępnić dokumentację medyczną m.in. takim organom jak sądy i prokuratura, w związku z prowadzonym postępowaniem. Przepis art. 248 K.p.c. może również stanowić podstawę do wystąpienia przez sąd o udostępnienie danych znajdujących się w zasobach urzędów skarbowych.¹¹⁴ Przepis ten w szerokim zakresie reguluje obowiązek przedstawienia dokumentów i dotyczy wszelkiego ich rodzaju. Jednocześnie przewodniczący przed rozprawą może, w ramach zarządzenia mającego na celu przygotowanie rozprawy, zażądać na rozprawę od państwowej jednostki organizacyjnej (...) znajdujących się u niej dowodów, jeżeli strona sama nie może otrzymać tych dowodów (art. 208 § 1 pkt 2 K.p.c.), jak i zarządzić przedstawienie dokumentów (art. 208 § 1 pkt 5 K.p.c.), (T. Ereciński, J. Gudowski, M. Jędrzejewska, Komentarz do kodeksu postępowania cywilnego, Wydawnictwo Prawnicze, Warszawa 1997 r., s. 404 i 405). Należy przy tym zaznaczyć, że zgodnie z art. 26 ust. 1 pkt 3 ustawy, administrator danych powinien dolożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby przetwarzane dane były merytorycznie poprawne oraz adekwatne w stosunku do celów, w jakich są przetwarzane. Ze względu na istnienie wymogu adekwatności danych w stosunku do celów, w jakich są przetwarzane, możliwość żądania informacji o osobie w związku z toczącym się postępowaniem sądowym, jest ograniczona do informacji niezbędnych do wyjaśnienia sprawy. O tym jednak, które informacje należy uznać za istotne dla rozstrzygnięcia decyduje sąd.

Generalny Inspektor wielokrotnie podkreślał, że zgodnie ze swoimi kompetencjami, określonymi w art. 12 ustawy o ochronie danych osobowych, nie jest on podmiotem

¹¹² GI-DP-024/1290/1813

¹¹³ Podobnie w sprawie GI-DP-571/00/625

¹¹⁴ GI-DP-867/00/1060

upoważnionym do badania zasadności decyzji sądu. Stosownie do art. 18 ustawy, w przypadku naruszenia przepisów ustawy o ochronie danych osobowych, Generalny Inspektor może z urzędu lub na wniosek osoby zainteresowanej nakazać administratorowi danych przywrócenia stanu zgodnego z prawem. W przypadku jednak, gdy przepisy innych ustaw przewidują odrębny sposób usunięcia uchybień mogących naruszać przepisy ustawy o ochronie danych osobowych, stosuje się przepisy ustaw szczególnych (art. 18 ust. 3 ustawy). Skarżącym wyjaśniono, iż zgodnie z art. 226 K.p.c. od orzeczeń przewodniczącego wydanych w toku rozprawy strony mogą się odwołać do sądu. Ten sam organ rozpatruje odwołania na uchybienia sędziego wyznaczonego lub sądu wezwanego w zakresie zleconego im postępowania dowodowego.¹¹⁵

Pytania dotyczyły także wskazania przepisów prawa, na podstawie których sądy mogą zwracać się o udostępnienie im danych osobowych przez Zakład Ubezpieczeń Społecznych. Jak wynikało z napływających skarg, organy ZUS odmawiały udostępnienia danych dotyczących stron postępowania, powołując się na art. 29 ustawy o ochronie danych osobowych.¹¹⁶ Generalny Inspektor uznał taką argumentację za błędną, albowiem przetwarzanie danych o stanie zdrowia przez sąd dla potrzeb prowadzonego postępowania znajduje uzasadnienie w art. 27 ust. 2 pkt 2 ustawy. W myśl powołanych przepisów podstawą dopuszczalności przetwarzania przedmiotowych danych jest przepis szczególny innej ustawy zezwalający na przetwarzanie danych wrażliwych bez zgody osoby, której dane dotyczą i stwarzający pełne gwarancje ich ochrony oraz jeżeli przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem. Na podstawie art. 34 ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz. U. Nr 137, poz. 887 z późn. zm.) ZUS zapewnia rzetelność i kompletność informacji gromadzonych na kontach ubezpieczonych i na kontach płatników składek w sposób uregulowany niniejszą ustawą. Do informacji zawartych na kontach ubezpieczonych i kontach płatników składek oraz danych źródłowych będących podstawą zapisów na tych kontach stosuje się jednak przepisy ustawy o ochronie danych osobowych. Ponadto na podstawie art. 50 § 3 ustawy o systemie ubezpieczeń społecznych dane zgromadzone na koncie ubezpieczonego mogą być udostępniane sądom, prokuratorom, organom kontroli skarbowej oraz Urzędowi Nadzoru nad Funduszami Emerytalnymi, z uwzględnieniem przepisów dotyczących ochrony danych osobowych. Przywołany wyżej przepis szczególny ustawy o systemie ubezpieczeń społecznych nie tylko zezwala, ale i zobowiązuje Zakład Ubezpieczeń Społecznych do udostępnienia sądowi

¹¹⁵ GI-DP-024/1290/1813, GI-DP-65/00/111

przedmiotowych informacji. Te same zasady udostępniania danych na podstawie przepisu szczególnego obowiązują co do każdej informacji i dokumentów znajdujących się w dyspozycji ZUS-u.¹¹⁷

Indywidualne skargi dotyczyły zasadności udostępnienia sądowi danych zbieranych przez Głównego Inspektora Nadzoru Budowlanego. W ocenie jednego ze skarżących udostępnienie sądowi przez Urząd informacji zawartych w książce budowy i dotyczących wykonawców robót (przedsiębiorców), narusza przepisy ustawy o ochronie danych osobowych, zwłaszcza gdy w toczącym się postępowaniu dostęp do akt posiada firma konkurująca.¹¹⁸ W odpowiedzi na powyższe Generalny Inspektor wyjaśnił, że zgodnie z art. 6 ustawy o ochronie danych osobowych za dane osobowe uważa się każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie jej tożsamości. Definicję przedsiębiorcy określa art. 2 ust 2 ustawy z dnia 23 grudnia 1988 r. o działalności gospodarczej (Dz. U. Nr 41, poz. 324 z późn. zm.)¹¹⁹, zgodnie z którym przedsiębiorcą może być osoba fizyczna, osoba prawna, a także jednostka organizacyjna nie posiadająca osobowości prawnej, utworzona zgodnie z przepisami prawa, jeśli jej przedmiot działania obejmuje prowadzenie działalności gospodarczej. Ochroną ustawową objęte są zatem jedynie informacje dotyczące osoby fizycznej, natomiast przepisów ustawy nie stosuje się w odniesieniu do przedsiębiorców (podmiotów gospodarczych) w zakresie prowadzonej przez nich działalności gospodarczej. Oznacza to, że dane firmy, nierzadko tożsame z danymi osoby fizycznej nie podlegają ochronie przewidzianej przepisami ustaw. Ponadto skarżącego poinformowano, iż w zakresie w jakim zezwalają przepisy prawa, umożliwienie dostępu do akt nie narusza ustawy o ochronie danych osobowych.¹²⁰

W związku z przekazaniem przez Ministerstwo Sprawiedliwości sędziom i prokuratorom do wypełnienia ankiety personalnej, do Generalnego Inspektora wpłynęły pisma z pytaniem o *legalność i zakres danych osobowych ujawnianych w poszczególnych punktach ankiety bezpieczeństwa*.¹²¹ Sędziów i prokuratorów zobowiązano m.in. do ujawnienia takich danych, jak: nazwisko, ostatnie miejsce zamieszkania i pracy rodziców,

¹¹⁶ GI-DP-1056/00/1427

¹¹⁷ Ibidem

¹¹⁸ GI-DP-1107/00/1580

¹¹⁹ Obecnie zagadnienie to uregulowane jest w ustawie z dnia 17 grudnia 1999 r. Prawo działalności gospodarczej (Dz. U. Nr 101, poz. 1178 z późn. zm.) oraz w ustawie z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym (Dz. U. Nr 121, poz. 769). Zgodnie z art. 8 ust. 1 ustawy o Krajowym Rejestrze Sądowym rejestr jest jawny. Dane osób fizycznych wykonujących działalność gospodarczą zostały umieszczone, na podstawie art. 36 tej ustawy, w rejestrze przedsiębiorców.

¹²⁰ Ibidem

¹²¹ GI-DP-1190/00/1583

rodzeństwa i rodziców żony, dane o karalności sądowej lub prowadzonym postępowaniu przeciwko członkom rodziny, dane o stanie majątkowym wypełniającego ankietę i jego współmałżonka. Generalny Inspektor nie dopatrywał się w tym zakresie uchybień i poinformował, że ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95 z późn. zm.) ustanowiła obowiązek poddawania się postępowaniu sprawdzającemu przez osoby, mające uzyskać dostęp do informacji stanowiących tajemnicę państwową lub służbową, w tym wypełnienia ankiety bezpieczeństwa osobowego, stanowiącej załącznik do powołanej ustawy. W przedmiotowej ankiecie przewidziane jest również podanie danych osobowych członków rodziny oraz informacji na temat karalności i posiadanego majątku. Ustawa o ochronie informacji niejawnych stanowi zatem podstawę prawną do przetwarzania wskazywanych danych osobowych skarżących, w celu uzyskania przez daną osobę poświadczenia bezpieczeństwa. Generalny Inspektor podkreślił, iż omawiana ustawa była poddawana ocenie Trybunału Konstytucyjnego pod kątem zgodności z Konstytucją i pomimo formułowanych pod jej adresem zarzutów o taką niezgodność (zarówno przez Krajową Radę Sądownictwa, jak i Rzecznika Praw Obywatelskich) przed wydaniem przez Trybunał orzeczenia korzysta ona z domniemania zgodności z ustawą zasadniczą.¹²²

Najliczniejsza grupa zapytań i skarg, jakie wpłynęły do Biura Generalnego Inspektora Ochrony Danych Osobowych, w przedmiocie przetwarzania danych osobowych przez sądy, dotyczyła *problematyki przetwarzania danych o karalności w postępowaniu przed organami sądów*. Zgodnie z art. 28 ust. 1 ustawy o ochronie danych osobowych, przetwarzanie danych dotyczących skazań, orzeczeń o ukaraniu, mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym można prowadzić wyłącznie na podstawie ustawy. Dane dotyczące karalności zostały potraktowane przez ustawodawcę jako szczególna kategoria danych osobowych. Ich przetwarzanie jest możliwe jedynie wtedy, gdy przewidują to przepisy ustaw szczególnych. Uprawnienie to musi więc wyraźnie wynikać z przepisów prawnych o randze ustawy, odnoszących się do danego podmiotu, instytucji lub organu. W przypadku, gdy nie ma podstawy ustawowej zezwalającej na ich przetwarzanie, działanie takie należałoby uznać za niedopuszczalne. Generalny Inspektor wskazał, iż podstawą udostępnienia przez odpowiedni sąd lub organ administracji orzeczeń kończących postępowanie administracyjne lub sądowe są przepisy ustaw regulujących przebieg tych postępowań, m.in. ustawy z dnia 14 czerwca 1960 r. Kodeks

¹²² Ibidem

postępowania administracyjnego (Dz. U. z 2000 r. Nr 98, poz. 1071.), ustawy z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (Dz. U. Nr 43, poz. 296 z późn. zm.) oraz ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (Dz. U. Nr 89, poz. 555, z 1999 r. Nr 83, poz. 931).¹²³ Podstawą wydania stronie przez sąd orzeczenia o skazaniu, np. na karę grzywny jest art. 331 K.p.c., zgodnie z którym wyrok sądu cywilnego wraz z uzasadnieniem sąd doręcza tylko tej stronie, która zażądała sporządzenia uzasadnienia. W sytuacji odmowy doręczenia orzeczenia stronie przysługuje środek odwoławczy w postaci zażalenia, o którym mowa w art. 394 § 1 pkt 7 K.p.c.

W jednym z pism skarżący – powód w sprawie przed sądem cywilnym - zwrócił się do Generalnego Inspektora z zapytaniem o zasadność wykorzystania w toczącym się procesie wyroków karnych zapadłych wobec skarżącego we wcześniejszych latach.¹²⁴ W odpowiedzi na powyższe, Generalny Inspektor zwrócił uwagę na regulacje prawne dotyczące wykorzystywania dowodów w procesie cywilnym, a ponadto na orzecznictwo Sądu Najwyższego, zgodnie z którym akta innej sprawy stanowią źródło wiadomości dla innych stron i sądu: dowody przeprowadzone w innej sprawie mogą być wykorzystane jako materiał pomocniczy przy ocenie wiarygodności i mocy dowodów przeprowadzonych bezpośrednio przed sądem (OSN 1974, Nr 12, poz. 203). Generalny Inspektor podkreślił, iż w sytuacji, gdy sąd dokonuje ustaleń na podstawie zatartego skazania, postępowanie takie należy uznać za nieuprawnione. Usunięcia takiego uchybienia można dokonać jedynie w toku postępowania cywilnego, np. w postaci wniesienia apelacji od wyroku (o ile nie upłynął termin do wniesienia takiego środka zaskarżenia). W polskim systemie prawnym nie istnieje przepis, który upoważniałby jakiegokolwiek podmiot do udzielenia informacji o skazaniu, które uległo zatarciu. Instytucja zatarcia skazania została uregulowana w rozdziale XII Kodeksu karnego (art. 106 – 108). Istotą omawianej instytucji jest to, że osoba, która popełniła przestępstwo i wobec której orzeczono karę, ma prawo oczekiwać, że po upływie określonego w ustawie okresu, będzie traktowana jako osoba niekarana. Zgodnie ze stanowiskiem doktryny zatarcie skazania przywraca skazanemu status niekaranego, dlatego może on twierdzić wobec władz i urzędów, że nie był skazany (K. Buchała, A. Zoll „Komentarz do Kodeksu karnego” Zakamycze 1998 r.).

Osobna problematyka pytań dotyczyła *legalności przetwarzania danych o karalności dla celów innych niż postępowanie sądowe*. W związku z występowaniem przez zakłady pracy do sądów z pytaniem o karalność podległych pracowników, do Generalnego Inspektora

¹²³ GI-DP-869/00/1184

zwracano się wielokrotnie o wskazanie podstaw prawnych powyższego działania oraz legalności przechowywania przez zakłady pracy w ten sposób uzyskanych informacji o pracowniku.¹²⁵ Ustanowiona w art. 7 pkt. 2 ustawy o ochronie danych osobowych definicja przetwarzania danych wskazuje, iż pod pojęciem przetwarzania danych mieszczą się jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych. Zgodnie z art. 27 § 2 ustawy z dnia 20 czerwca 1985 r. Prawo o ustroju sądów powszechnych (Dz. U. z 1994 r. Nr 7, poz. 25 z późn. zm.) dane z rejestru skazanych mogą być udostępniane do celów innych niż postępowanie karne na wniosek osób, których dane te dotyczą, jak również zainteresowanych organów państwowych i samorządowych, zakładów pracy, a także jeżeli z faktem karalności danej osoby przepisy prawa lub umowy samorządowe wiążą określone skutki prawne innych podmiotów. Tryb udostępniania tych informacji i szczegółowe określenie podmiotów upoważnionych do ich otrzymywania ustala Minister Sprawiedliwości w drodze rozporządzenia. Rozporządzenie Ministrów Sprawiedliwości i Obrony Narodowej z dnia 30 sierpnia 1993 r. w sprawie rejestru osób prawomocnie skazanych, udzielania informacji z rejestru oraz trybu zbierania danych w postępowaniu karnym dotyczących tych osób (Dz. U. Nr 82, poz. 388) stanowi w § 12 ust. 2 pkt 3, że informacje z rejestru mogą być udostępnione do celów innych niż postępowanie karne na wniosek zakładów pracy, jeżeli jest to niezbędne w związku z zatrudnieniem pracowników. Z powyższego wynika zatem, że jeżeli przepisy szczególne dotyczące zatrudnienia na danym stanowisku lub w danej służbie uzależniają podjęcie pracy (służby) od stwierdzenia niekaralności kandydata, istnieje tym samym podstawa prawna do występowania przez pracodawców do sądów z zapytaniem o karalność pracownika. *A contrario* bez wykazania takiej podstawy sądy nie są upoważnione do udostępniania zakładom pracy przedmiotowych informacji. Przykładem przepisów prawnych zezwalających na przetwarzanie danych o karalności dla celów innych niż postępowanie sądowe mogą być również przepisy ustawy z dnia 10 czerwca 1994 r. o zamówieniach publicznych (Dz. U. z 1998 r. Nr 119, poz. 773 z późn. zm.), tj. art. 19 umożliwiający organom organizującym przetarg przetwarzanie danych dotyczących skazań osób ubiegających się o udzielenie zamówienia publicznego¹²⁶, czy ustawa z dnia 6 kwietnia 1990

¹²⁴ GI-DP-901/00/1112

¹²⁵ GI-DP-147/00/473

¹²⁶ Por. GI-DP-1104/00/1396

r. o Policji (Dz. U. Nr 30, poz. 179 z późn. zm.) zezwalająca w art. 25 ust. 1 na przetwarzanie danych o karalności przez organy prowadzące rekrutację kandydatów do służby.¹²⁷

Odrębna grupa spraw rozpatrywanych przez Generalnego Inspektora Ochrony Danych Osobowych dotyczyła *skarg związanych z przetwarzaniem danych o karalności przez organy penitencjarne*. Przedmiotowe skargi najczęściej kierowały osoby skazane wyrokiem sądu na karę pozbawienia wolności, jak również osoby, względem których sąd orzekł zastosowanie środka zabezpieczającego prawidłowy tok postępowania karnego. Wskazane podmioty wnioskowały o stwierdzenie naruszenia ustawy o ochronie danych osobowych przez sąd, a także przez osoby sprawujące nad nimi nadzór karny. W ocenie jednego ze skarżących przykładem powyższych naruszeń było przesłanie faksem do zakładu karnego, w którym przebywał tymczasowo aresztowany postanowienia sądu o przedłużeniu tymczasowego aresztowania.¹²⁸ Rozpatrując zasadność postawionego zarzutu Generalny Inspektor uznał, iż przesyłanie w formie faksu postanowień sądu między instytucjami uprawnionymi do przetwarzania takich danych na podstawie przepisów ustawowych nie jest sprzeczne z ustawą. Przepisami upoważniającymi do przetwarzania przedmiotowych danych przez organy powołane do wykonania kary orzeczonej przez sąd są przepisy ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (Dz. U. Nr 89, poz. 555 z późn. zm.), ustawy z dnia 6 czerwca 1997 r. Kodeks karny wykonawczy (D. U. Nr 90, poz. 557 z późn. zm.), zwanej dalej K.k.w., a także rozporządzenia Ministra Sprawiedliwości z dnia 18 sierpnia 1998 r. w sprawie zakresu informacji dotyczących osoby skazanego, przesyłanych przez sąd dyrektorowi zakładu karnego lub aresztu śledczego (Dz. U. Nr 111, poz. 702). Zgodnie z art. 11 § 1 K.k.w. sąd kierując orzeczenie do wykonania przesyła jego odpis lub wyciąg ze wzmianką o wykonalności odpowiedniemu organowi powołanemu do wykonania orzeczenia. W razie skazania tymczasowo aresztowanego lub osoby odbywającej karę pozbawienia wolności, sąd zawiadamia o tym odpowiednio dyrektora aresztu śledczego lub zakładu karnego (art. 11 § 4 K.k.w.). Osobom pozbawionym wolności (tymczasowo aresztowanym) doręcza się pismo za pośrednictwem administracji odpowiedniego zakładu (art. 134 § 2 K.p.k.). Przedstawiony przez skarżącego – oskarżonego w sprawie – stan faktyczny nie wskazywał, aby postanowienie o przedłużeniu tymczasowego aresztu było udostępnione osobom nieupoważnionym, zabrane przez osobę nieuprawnioną, uszkodzone lub zniszczone. Tym samym skarżący nie wykazał, aby sąd (będący w omawianej sprawie administratorem

¹²⁷ GI-DP-1022/00/1358

¹²⁸ GI-DP-430/1389/00

danych) nienależycie wywiązał się z obowiązku właściwego zabezpieczenia danych osobowych znajdujących się w jego posiadaniu.

Generalny Inspektor nie dopatrywał się naruszenia art. 28 ust. 1 ustawy również przy rozpatrywaniu skargi skazanego przez sąd na karę pozbawienia wolności, który wywodził, iż jego dane osobowe zostały nielegalnie wywieszone na drzwiach celi i w związku z tym z ich treścią mogły się zapoznać osoby nieuprawnione.¹²⁹ Skarżącego poinformowano, iż umieszczenie na drzwiach celi danych osobowych więźniów jest zgodne z ustalonym przez dyrekcję zakładu karnego porządkiem wewnętrznym, który jest znany każdemu z osadzonych. Podstawą prawną wydania przepisów porządkowych jest ustawa Kodeks karny wykonawczy oraz przepisy wykonawcze do tej ustawy, w tym rozporządzenie Ministra Sprawiedliwości z dnia 12 sierpnia 1998 r. w sprawie wykonywania kary pozbawienia wolności (Dz. U. Nr 111, poz. 699). Tym samym podstawą przetwarzania jest przepis prawa, co stanowi przesłankę określoną w art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych.¹³⁰

II. Przetwarzanie danych osobowych przez prokuraturę.

W roku 2000 r. do Generalnego Inspektora Ochrony Danych Osobowych wpłynęła liczna grupa pytań i skarg dotyczących przetwarzania danych osobowych przez prokuraturę. Przedmiotem zarzutów był brak podstaw i zbyt szeroki zakres danych udostępnianych dla potrzeb prowadzonego postępowania przygotowawczego przez organy prokuratury, nienależyte zabezpieczenie dokumentów zawierających dane osobowe, jak również niewłaściwa praktyka sporządzania dokumentacji przez sekretariaty prokuratur.

Przedmiotem znacznej liczby pism był *zakres danych udostępnianych organom ścigania (Policji, prokuraturze), a następnie wykorzystywanych w toczącym się dochodzeniu lub śledztwie*. Pytania dotyczyły legalności wykonania przez Policję dla potrzeb postępowania w sprawie uchylania się od obowiązku alimentacyjnego, karty daktyloskopijnej i zdjęć sygnalitycznych.¹³¹ Zgodnie z art. 6 ustawy o ochronie danych osobowych za dane osobowe uważa się każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby. Przetwarzaniem danych są natomiast jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach

¹²⁹ GI-DP-77/00/150

¹³⁰ Ibidem

¹³¹ GI-DP-100/00/652

informatycznych (art. 7 pkt 2 ustawy). Wykonanie zdjęć i pobranie linii papilarnych od danej osoby niewątpliwie pozwala na określenie jej tożsamości i jest przetwarzaniem danych osobowych w rozumieniu przepisów ustawy. Przesłanki dopuszczalności przetwarzania danych zostały określone w art. 23 ust 1 ustawy, a jedną z nich jest istnienie przepisu prawa upoważniającego administratora danych do ich przetwarzania. Zgodnie z art. 298 § 1 K.p.k. postępowanie przygotowawcze prowadzi prokurator, a w zakresie przewidzianym w ustawie – Policja. W wypadkach przewidzianych w ustawie uprawnienia Policji przysługują innym organom. W myśl art. 20 ust. 2 ustawy z dnia 6 kwietnia 1990 r. o Policji, organ ten może pobierać, gromadzić, a także wykorzystywać w celach wykrywczych i identyfikacyjnych odciski linii papilarnych, zdjęcia oraz inne dane o osobach podejrzanych o popełnienie przestępstw umyślnych, ściganych z oskarżenia publicznego, a więc także o osobach uporczywie uchylających się od obowiązku alimentacji tj. przestępstwa z art. 209 ustawy z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. Nr 88, poz. 553 z późn. zm.). Działanie organów, znajdując oparcie w przepisach prawa nie jest tym samym sprzeczne z art. 23 ust. 1 pkt 2 ustawy. Generalny Inspektor poinformował ponadto, że zgodnie z Kodeksem postępowania karnego na czynności prokuratora w czasie trwania postępowania przygotowawczego przysługuje zażalenie do prokuratora nadzrędnego, zaś w przypadku, gdy postępowanie to zakończyło się sporządzeniem aktu oskarżenia, o dopuszczalności tego typu działań decyduje sąd.

Do Generalnego Inspektora kierowano również *skargi w przedmiocie naruszenia przez organy ścigania zasad postępowania karnego, w tym skargi na beczynność organów prokuratury*. Skarżący wnosili o podjęcie działań zmierzających do uruchomienia postępowań wyjaśniających w sprawach cywilnych i karnych.¹³² Analiza treści tych pism dokonana z uwzględnieniem przepisu art. 12 ustawy o ochronie danych osobowych, określającego zakres kompetencji Generalnego Inspektora, nie pozwoliła Generalnemu Inspektorowi na dokonanie oceny wskazanych naruszeń. Zgodnie z art. 306 § 3 K.p.k., jeżeli osoba, która złożyła zawiadomienie o przestępstwie, nie zostanie w ciągu 6 tygodni powiadomiona o wszczęciu lub odmowie wszczęcia postępowania karnego, może wnieść zażalenie do prokuratora nadzrędnego albo powołanego do nadzoru nad organem, któremu złożono zawiadomienie. Wymienione organy odwoławcze są zatem jedynymi podmiotami właściwymi z mocy prawa do oceny skargi na beczynność Policji lub prokuratury.

¹³² GI-DP-430/1293/00

Szczególnie duża liczba skarg, związanych z działalnością prokuratur dotyczyła *problematyki udostępniania oskarżonym, a w postępowaniu przygotowawczym – podejrzanym, danych adresowych pokrzywdzonych i świadków czynów zabronionych, a także udostępniania danych podejrzanego podmiotom biorącym udział w postępowaniu*. Jak wynikało z wpływających pism skazani na kary pozbawienia wolności składają do prokuratury zawiadomienia o popełnienie przestępstwa przez nadzorujących ich funkcjonariuszy Służby Więziennej. Zawiadomienia powyższe okazują się niesłusznymi pomówieniami. Zgodnie jednak z wymogami Kodeksu postępowania karnego przeprowadzane jest postępowanie wyjaśniające zasadność postawionych funkcjonariuszom zarzutów i w określonym przepisami czasie (art. 305 K.p.k.) skazani otrzymują z prokuratury postanowienie o umorzeniu postępowania. Przedmiotowe postanowienie zawiera nie tylko imię i nazwisko funkcjonariusza, ale również jego adres domowy. Skazani otrzymując informację o bezzasadności skargi, są jednocześnie informowani o prywatnym adresie zamieszkania funkcjonariusza, który następnie jest wykorzystywany w celu zastraszenia rodziny osoby zatrudnionej przy prowadzeniu nadzoru w zakładach karnych.¹³³ Generalny Inspektor podzielił obawy wyrażone przez funkcjonariuszy Służby Więziennej. Prokuratura, po uzyskaniu zawiadomienia o przestępstwie jest zobowiązana do zbadania, czy wskazane fakty miały miejsce, a po przeprowadzeniu stosownych czynności wydaje postanowienie o umorzeniu postępowania przygotowawczego. Na podstawie art. 156 § 5 K.p.k. pokrzywdzonemu przysługuje prawo przeglądania akt, sporządzania odpisów i kserokopii. Uprawnienie to przewiduje także art. 306 § 1 K.p.k. Generalny Inspektor zauważył, iż w ten sposób fikcyjny pokrzywdzony posiada swobodny dostęp do protokołów przesłuchań, gdzie znajduje się także adres domowy funkcjonariusza. Dostęp do danych funkcjonariusza jest jeszcze szerszy, gdy postępowanie przygotowawcze wszczęte na skutek skargi (zawiadomienia o popełnieniu przestępstwa) skazanego wstępuje w fazę *in personam* i toczy się przeciwko konkretnie wskazanej osobie. Umorzenie postępowania na ww. etapie powoduje, iż skazanemu (fikcyjnemu pokrzywdzonemu) doręcza się postanowienie z imieniem, nazwiskiem oraz dokładnym adresem podejrzanego funkcjonariusza. Zgodnie z art. 322 K.p.k. wskazane postanowienie powinno zawierać imię i nazwisko podejrzanego, ale również w razie potrzeby inne dane o jego osobie. Przepis ten nie zobowiązuje zatem do podania informacji, o których mowa w skargach. Jednakże w praktyce organy ścigania zamieszczają w postanowieniu o umorzeniu postępowania także dokładny adres

¹³³ GI-DP-443/00/829

podejrzanego. Postępowanie takie nie wynika również z dyspozycji art. 94 K.p.k., określającego warunki formalne, jakie powinno spełniać postanowienie. Wśród danych, które ustawodawca obligatoryjnie nakazuje umieszczać w postanowieniu nie ma obowiązku umieszczania danych o adresie osoby, której postanowienie dotyczy. W związku z powyższym, Generalny Inspektor wielokrotnie sygnalizował Prokuratorowi Generalnemu potrzebę zmiany opisanej praktyki stosowanej przez prokuratorów.

Kwestia zbyt szerokiego dostępu uczestników postępowania do danych znajdujących się w aktach postępowania przygotowawczego była ponadto przedmiotem skarg osób, występujących w sprawie w charakterze świadka. Podmioty te zaniepokojone były faktem, iż podejrzany ma dostęp do ich danych osobowych w zasadzie na każdym etapie toczącego się postępowania.¹³⁴ Zgodnie z art. 184 § 1 K.p.k., jeżeli zachodzi uzasadniona obawa niebezpieczeństwa dla życia i zdrowia, wolności albo mienia w znacznych rozmiarach świadka lub osoby dla niego najbliższej, prokurator w postępowaniu przygotowawczym może wydać postanowienie o zachowaniu w tajemnicy danych osobowych świadka. W razie wydania przedmiotowego postanowienia, dane osobowe świadka pozostają wyłącznie do wiadomości prokuratora, a gdy zachodzi konieczność – również funkcjonariusza Policji prowadzącego postępowanie. Protokoły zeznań świadka wolno udostępniać wówczas oskarżonemu lub obrońcy tylko w sposób uniemożliwiający ujawnienie tożsamości świadka (art. 184 § 2 K.p.k.). Jeżeli świadek nie wystąpił z takim żądaniem, jego dane osobowe są udostępniane oskarżonemu, z mocy art. 156 § 1 K.p.k. W ocenie Generalnego Inspektora konieczna jest zmiana zapisu wyrażonego w art. 184 § 1 K.p.k. poprzez wprowadzenie takiej regulacji prawnej, która obligowałaby prokuratorów (sądy) do utajniania danych świadków w każdym przypadku. Pozostawienie danych osobowych świadków tylko do wiadomości prokuratury (sądu w procesie) w przekonaniu Generalnego Inspektora zapewniłoby skuteczniejszą niż dotychczas ochronę przed dostępem osób niepowołanych do danych osobowych świadków i stron postępowania.¹³⁵

Odnosnie *udostępniania akt sprawy karnej innym podmiotom niż strony w toku postępowania przygotowawczego* Generalny Inspektor zwrócił uwagę na art. 156 § 5 K.p.k., zgodnie z którego brzmieniem, jeżeli ustawa nie stanowi inaczej, w toku postępowania przygotowawczego stronom, obrońcom, pełnomocnikom i przedstawicielom ustawowym za zgodą prowadzącego postępowanie przygotowawcze, udostępnia się akta, umożliwia

¹³⁴ GI-DP-302/00/592, również w GI-DP-430/1413/00

¹³⁵ Problem ten wielokrotnie Generalny Inspektor Ochrony Danych Osobowych sygnalizował Ministrowi Sprawiedliwości.

sporządzanie odpisów i kserokopii oraz wydaje uwierzytelnione odpisy. Za zgodą prokuratora, akta w toku postępowania przygotowawczego mogą być w wyjątkowych wypadkach udostępnione również innym osobom.¹³⁶ Jednocześnie skarżących poinformowano, iż organem właściwym do rozpatrywania skarg na czynności prokuratora mające miejsce w toku postępowania karnego – zgodnie z przepisem § 319 rozporządzenia Ministra Sprawiedliwości z dnia 11 kwietnia 1992 r. Regulamin wewnętrznego urzędowania jednostek organizacyjnych prokuratury (Dz. U. Nr 38, poz. 163 z późn. zm.) – jest prokurator nadrzędny.

Uzasadnione wątpliwości wzbudziła również kwestia *legalności łącznego sporządzania postanowień o umorzeniu śledztwa lub dochodzenia i zarządzeń dotyczących ich wykonania, w których są wymienione dane osób nie będących stronami postępowania.*¹³⁷

Zgodnie z art. 100 § 1 K.p.k. orzeczenie lub zarządzenie wydane na rozprawie ogłasza się ustnie. Orzeczenie lub zarządzenie wydane poza rozprawą doręcza się prokuratorowi, a także stronie i osobie nie będącej stroną, którym przysługuje środek zaskarżenia, jeżeli nie brali oni udziału w posiedzeniu lub nie byli przy ogłoszeniu; w innych wypadkach o treści orzeczenia lub zarządzenia należy powiadomić strony (§ 2 cytowanego przepisu). Natomiast w myśl art. 140 K.p.k., jeżeli ustawa nie stanowi inaczej orzeczenia, zarządzenia, zawiadomienia i odpisy, które ustawa nakazuje doręczać stronom, doręcza się również obrońcom, pełnomocnikom i ustawowym przedstawicielom. Zarządzenie doręczenia nie jest zaskarżalne i w związku z tym nie podlega doręczeniu. Jak wynika z wielu pism skarżących, działanie łącznego sporządzania postanowień i zarządzeń dotyczących postanowień o umorzeniu śledztwa lub dochodzenia, a następnie rozsyłania takich danych do wszystkich wymienionych tam podmiotów jest częstą praktyką stosowaną przez prokuratorów i sekretariaty prokuratur. W ocenie Generalnego Inspektora praktyka powyższa nie może być jednak uznana za zgodną z ustawą o ochronie danych osobowych. Żaden z przepisów Kodeksu postępowania karnego nie wymaga, aby zarządzenia były umieszczone na tym samym dokumencie, co postanowienie. Żaden przepis prawa nie zobowiązuje ponadto do formułowania zarządzenia w sposób umożliwiający dostęp do danych pozostałych pokrzywdzonych. Zarządzenie takie ma charakter techniczny i nie rozstrzyga o istocie sprawy. Dodatkowe informowanie o danych adresowych uczestników postępowania wydaje się zbędne w sytuacji, gdy strona ma dostęp do akt sprawy na podstawie art. 305 § 5 K.p.k.

¹³⁶ Ibidem

Mając na uwadze powyższe, w piśmie skierowanym do Ministra Sprawiedliwości, Generalny Inspektor zasygnalizował potrzebę zmiany opisywanej praktyki.¹³⁸

Generalny Inspektor podkreślił przy tym, iż jedną z podstawowych zasad postępowania karnego jest zasada jawności, która stanowi, iż postępowanie jest m.in. jawne dla stron. Jedną ze stron postępowania przygotowawczego jest pokrzywdzony. Wielu skarżących składając zawiadomienie o popełnieniu przestępstwa uznawało, iż prokurator (ewentualnie Policja) ujawniając ich dane naruszył przepisy ustawy o ochronie danych osobowych.¹³⁹ Tymczasem składając zawiadomienie o popełnieniu przestępstwa pokrzywdzony musi się godzić z całością szczegółowych zasad postępowania, w tym z ewentualnym ujawnianiem jego adresu w aktach sprawy i pismach procesowych. Skarżących poinformowano, że w przypadku, gdy pokrzywdzony nie zgadza się z wydanym przez prokuratora postanowieniem, na podstawie art. 306 § 1 i 2 K.p.k., ma prawo do złożenia zażalenia do prokuratora nadrzędnego. W sytuacji, gdy prokurator nie przychylił się do zażalenia, kieruje je do sądu. Zgodnie z dyspozycją art. 330 § 2 K.p.k., sąd może utrzymać w mocy zaskarżone postanowienie lub uchylić je i przekazać sprawę prokuratorowi celem wyjaśnienia przedstawionych okoliczności, bądź przeprowadzenia wskazanych czynności.

W omawianym okresie sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych rozpatrywał również *skargi w przedmiocie legalności włączania na żądanie prokuratorów do prowadzonego postępowania określonych środków dowodowych, w tym dokumentów zawierających dane szczególnie chronione*.¹⁴⁰ Zapytujący wyrażali obawę, czy udostępnienie, np. dokumentacji medycznej nie pozostaje w sprzeczności z obowiązkiem zachowania tajemnicy lekarskiej. Zagadnienia związane ze wszczęciem, prowadzeniem i zakończeniem postępowania karnego zostały uregulowane w kodeksie postępowania karnego i w uchwalonych na jej podstawie przepisach wykonawczych. Zgodnie z art. 297 § 1 K.p.k. celem postępowania przygotowawczego jest m.in. wyjaśnienie okoliczności sprawy oraz zebranie i zabezpieczenie dowodów, które stosownie do przepisu art. 167 K.p.k. przeprowadza się na wniosek stron lub z urzędu. Czynności te mają prowadzić do ustalenia, czy zachodzą wystarczające podstawy do wniesienia aktu oskarżenia lub innego zakończenia postępowania. Tym samym należy stwierdzić, iż prokuratura żądając udostępnienia, np. dokumentacji medycznej – o ile była ona potrzebna do realizacji celów toczącego się

¹³⁷ GI-DP-GI-DP-880/00/1121, GI-DP-024/1259/00

¹³⁸ GI-DP-430/1413/00

¹³⁹ GI-DP-376/00/443

¹⁴⁰ GI-DP-430/1355/00, por. GI-DP-430/1258/00

postępowania – działa w oparciu o obowiązujące przepisy. Generalny Inspektor wyjaśnił ponadto, iż żądanie dostarczenia przedmiotowej dokumentacji nie pozostaje w sprzeczności z obowiązkiem zachowania tajemnicy lekarskiej, o którym mowa w ustawie z dnia 5 grudnia 1996 r. o zawodzie lekarza (Dz. U. z 1997 r. Nr 28, poz. 152 z późn. zm.). Zgodnie z art. 40 ust. 2 pkt 1 powołanego wyżej aktu prawa, lekarz ma obowiązek zachowania w tajemnicy informacji związanych z pacjentem, a uzyskanych w związku z wykonywaniem zawodu. Przepisu tego nie stosuje się, gdy tak stanowią ustawy (art. 40 ust. 2). Przepis art. 217 § 1 K.p.k. stanowi natomiast, iż rzeczy mogące stanowić dowód w sprawie należy wydać na żądanie sądu lub prokuratora. Osobę mającą rzeczy podlegające wydaniu wzywa się do wydania ich dobrowolnie, a w razie odmowy można przeprowadzić ich odebranie.

Wśród zagadnień rozpatrywanych przez Generalnego Inspektora Ochrony Danych Osobowych w 2000 r. szczególnie często pojawiała się *problematyka niewłaściwego zabezpieczenia zbiorów danych osobowych znajdujących się w zasobach prokuratur*.

Jak wynikało z doniesień prasowych dane osobowe uczestników postępowań prowadzonych przez prokuraturę były niejednokrotnie narażane na udostępnienie osobom nieupoważnionym lub na zabranie przez osobę nieuprawnioną. W związku z ujawnieniem - za pośrednictwem środków masowego przekazu – na wysypisku śmieci w Aleksandrowie Kujawskim akt sądowych, dowodów rzeczowych, wypisów aktów notarialnych, jak również wyroków z uzasadnieniami, zawierających pełne dane osobowe uczestników postępowań przed organami sprawiedliwości, Generalny Inspektor zwrócił się do Prokuratury Okręgowej we Włocławku o udzielenie informacji o przebiegu toczącego się postępowania. Jak wynikało z uzyskanych odpowiedzi prokuratura właściwa miejscowo i rzeczowo do rozpatrzenia sprawy dwukrotnie umorzyła śledztwo wobec braku ustawowych znamion czynu zabronionego. W ocenie Generalnego Inspektora umorzenie to budziło wiele wątpliwości, w związku z czym zwrócono się do Prokuratury Okręgowej o ponowne rozpatrzenie sprawy.¹⁴¹ Po rozważeniu zarzutów Generalnego Inspektora Ochrony Danych Osobowych Prokuratura Okręgowa we Włocławku uznała za słuszne podjęcie na nowo postępowania w przedmiotowej sprawie.¹⁴²

W listopadzie i grudniu 1999 r. oraz w styczniu 2000 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęła duża ilość skarg w sprawie ujawnienia na „dzikim” wysypisku śmieci w Niewolnicy Nargilewskiej k/Białegostoku materiałów ze śledztwa prowadzonego przez Prokuraturę Okręgową w Białymstoku, zawierających dane

¹⁴¹ Szerz. w piśmie do Ministra Sprawiedliwości z dnia 28 czerwca 2000 r., sygn. GI/613/00

osobowe skarżących. Generalny Inspektor zwrócił się do organów prowadzących postępowanie o ustalenie wszystkich okoliczności sprawy i osób odpowiedzialnych za właściwe zabezpieczenie materiałów kopiowanych z akt śledztwa. Prokuratura Okręgowa w Olsztynie poinformowała o umorzeniu postępowania wobec niewykrycia sprawy przestępstwa.¹⁴³ Generalny Inspektor nie podzielił powyższego stanowiska i wystąpił do Ministra Sprawiedliwości o rozważenie możliwości podjęcia na nowo przedmiotowego postępowania.¹⁴⁴ Pismem z dnia 21 lipca 2000 r. Prokurator Generalny przychylił się do wniosku Generalnego Inspektora i wydał polecenie podjęcia na nowo umorzonego postępowania przygotowawczego.¹⁴⁵

Ponadto w 2000 r. do Generalnego Inspektora - za pośrednictwem mediów – wpłynęła sprawa dotycząca przekazania do punktu skupu makulatury akt Prokuratury Rejonowej w Słupsku. Prokuratura Okręgowa w Słupsku poinformowała, iż przeznaczone na makulaturę materiały składały się głównie z akt podręcznych prokuratora w sprawach, w których wniesiono akty oskarżenia, akt postępowań, w których odmówiono ich wszczęcia, akt spraw umorzonych, a także zbiory wokand, listy obecności, pocztowe książki nadawcze i inne materiały dotyczące bezpośrednio danych osobowych stron postępowań przed organami ścigania. Na obecnym etapie postępowania ustalono, że w przedmiotowej sprawie prowadzone jest dochodzenie przez Prokuraturę Okręgową w Słupsku, które swym zakresem obejmuje oskarżenie o czyn, określony w art. 51 ust. 1 ustawy o ochronie danych osobowych.¹⁴⁶

Podobnie jak w roku 1999, w omawianym okresie sprawozdawczym zagadnieniem, które wzbudzało liczne wątpliwości była forma udostępniania danych osobowych przez inne organy na żądanie sądów i prokuratur. Urzędy Pracy, starostwa powiatowe, urzędy miejskie, a także osoby fizyczne wielokrotnie zwracały się do Generalnego Inspektora o zajęcie stanowiska w przedmiocie stosowania art. 29 ustawy o ochronie danych osobowych.¹⁴⁷

Zgodnie z art. 29 ust. 1 powołanej ustawy, w przypadku udostępnienia danych osobowych w celach innych niż włączenie do zbioru, administrator danych, o którym mowa w art. 3 ust. 1, udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa. Natomiast ust. 3 art. 29 stanowi, iż dane osobowe

¹⁴² Pismo z dnia 21 sierpnia 2000 r., sygn. PR II Dsn 238/99/Gdańsk, I Ds.16/00

¹⁴³ Pismo Prokuratury Okręgowej w Olsztynie z dnia 19 czerwca 2000 r.

¹⁴⁴ Szerzej w wystąpieniu do Ministra Sprawiedliwości z dnia 7 lipca 2000 r., sygn. GI-DIS-451/454/455/463/99, GI-DIS-38/00/1341

¹⁴⁵ Sygn. PR II Ko 1071/2000

¹⁴⁶ GI-DIS-337/00/2084

udostępnia się na pisemny, umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej. Wniosek taki powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie. Wzór takiego wniosku został określony w rozporządzeniu Ministra Sprawiedliwości i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia wzorów wniosku o udostępnienie danych osobowych, zgłoszenia zbioru do rejestracji oraz imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. Nr 80, poz. 522 z późn. zm.).

Wszystkie materiały gromadzone w formie akt, w tym akta sądowe, prokuratorskie, policyjne i inne zawierające dane osobowe, są zbiorem danych osobowych w rozumieniu art. 7 pkt 1 ustawy o ochronie danych osobowych, a organy takie, jak sądy i prokuratura występują o udostępnienie danych właśnie w celu włączenia do zbioru. Konsekwencją tego jest wyłączenie stosowania art. 29 ustawy, w wypadku udostępnienia danych w celu włączenia do tych akt.¹⁴⁸ W sytuacji, gdy art. 29 ustawy nie znajduje zastosowania, sądy i prokuratura są zobowiązane do wykazania istnienia jednej z przesłanek legalności przetwarzania danych, określonych w art. 23 i 27 ustawy o ochronie danych osobowych. Zarówno sądy, jak i prokuratura działają w ramach kompetencji przyznanych im przez prawo. Zgodnie z art. 15 § 2 K.p.k. wszystkie instytucje państwowe, samorządowe i społeczne są obowiązane w zakresie swego działania do udzielania pomocy organom prowadzącym postępowanie karne. Natomiast w myśl art. 258 ust. 1 K.p.c. każdy obowiązany jest przedstawić na zarządzenie sądu w oznaczonym terminie i miejscu dokument znajdujący się w jego posiadaniu i stanowiący dowód faktu istotnego dla rozstrzygnięcia sprawy, chyba że dokument zawiera tajemnicę państwową. Z § 58 rozporządzenia Ministra Sprawiedliwości z dnia 29 listopada 1987 r. Regulamin wewnętrznego urzędowania sądów powszechnych (Dz. U. Nr 38, poz. 218 z późn. zm.) wynika, że pisma kierowane do organów, instytucji lub osób w sprawie udzielenia informacji dotyczących stron oraz nadesłania dokumentów podpisuje przewodniczący wydziału lub sędzia.¹⁴⁹ Wskazane regulacje prawne należy uznać za podstawę merytoryczną udostępnienia przedmiotowym organom żądanych przez nie danych osobowych.¹⁵⁰

¹⁴⁷ Np. w sprawie sygn. GI-DP-422/00524, GI-DP-521/00/501, GI-DP-530/00/826, GI-DP-024/1372/00

¹⁴⁸ GI-DP-024/1459/00

¹⁴⁹ GI-DP-327/00/368

¹⁵⁰ GI-DP-024/1372/00

III. Problematyka przetwarzania danych osobowych przez komorników sądowych

Liczna grupa skarg kierowanych w 2000 r. do Generalnego Inspektora ochrony Danych Osobowych dotyczyła *zakresu i podstaw prawnych przetwarzania danych osobowych przez działających przy sądach komorników*. Szczególnie duża liczba pytań odnosiła się do zakresu informacji o uczestnikach postępowania egzekucyjnego. Zagadnieniem, które wywoływało wiele wątpliwości była kwestia legalności przetwarzania przez komorników danych osobowych właścicieli pojazdów mechanicznych oraz podstawy żądania udostępnienia takich danych przez ich administratora – starostę. W odpowiedzi na powyższe Generalny Inspektor informował, iż ustawa o ochronie danych osobowych nie zabrania przekazywania komornikom informacji dotyczących osób, przeciwko którym prowadzone jest postępowanie egzekucyjne, jeżeli dane te są niezbędne do przeprowadzenia egzekucji. Zakres uprawnień komorników określony został w ustawie Kodeks postępowania cywilnego, ustawie z dnia 29 sierpnia 1997 r. o komornikach sądowych i egzekucji (Dz. U. Nr 133, poz. 882 z późn. zm.), rozporządzeniu Ministra Sprawiedliwości z dnia 9 marca 1968 w sprawie czynności komorników (Dz. U. Nr 10, poz. 52 z późn. zm.) oraz innych przepisach szczególnych. Wskazane wyżej akty prawne zawierają przepisy zezwalające na przetwarzanie (a więc zbieranie, udostępnianie, przechowywanie) danych osobowych. Zgodnie z § 17 ww. rozporządzenia, jeżeli wierzyciel nie może uzyskać informacji niezbędnych do wszczęcia lub prowadzenia postępowania egzekucyjnego, komornik powinien postąpić zgodnie z art. 761 § 1 K.p.c. Tym samym komornicy, będący funkcjonariuszami publicznymi działającymi przy sądzie rejonowym (art. 1 ustawy o komornikach sądowych i egzekucji), posiadają podstawę prawną do przetwarzania przedmiotowych danych i żądania ich udostępnienia przez starostę.¹⁵¹ Przepis art. 761 § 1 K.p.c. pozwala organowi egzekucyjnemu zażądać od uczestników postępowania złożenia wyjaśnień oraz zasięgnąć od organów administracji publicznej, a także instytucji i osób nie uczestniczących w postępowaniu informacji niezbędnych do prowadzenia egzekucji.¹⁵² Jeżeli zatem uzyskanie przez komornika informacji o osobie, przeciwko której prowadzona jest egzekucja (np. o miejscu pracy, gdy nie przebywa w miejscu zamieszkania), jest niezbędne do przeprowadzenia egzekucji (np. do wyegzekwowania odszkodowania), to podmiot, od którego organ egzekucyjny może uzyskać

¹⁵¹ GI-DP-024/1369/00

¹⁵² GI-DP-599/00/571

niezbędne dane, powinien takie dane udostępnić.¹⁵³ Uchylenie się od spełnienia ww. żądania określa § 2 cytowanego przepisu. Tylko w sytuacji zaistnienia którejkolwiek z przesłanek wyłączających obowiązek udzielenia przedmiotowych informacji, podmiot może odmówić wskazania określonych przez komornika danych personalnych.¹⁵⁴

W jednym z pism, skarżąca – będąca poręczycielem zobowiązania zaciągniętego względem banku (wierzyciela) – zwróciła się o zbadanie zasadności ujawnienia jej danych osobowych w toczącym się postępowaniu egzekucyjnym.¹⁵⁵ Rozpatrując przedstawioną skargę Generalny Inspektor zwrócił uwagę, iż poprzez umowę poręczenia, zgodnie z art. 876 ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. Nr 16, poz. 93 z późn. zm.), zwanym dalej K.c., poręczyciel zobowiązuje się względem wierzyciela wykonać zobowiązanie na wypadek, gdyby dłużnik zobowiązania nie wykonał. W przypadku niewypłacalności dłużnika głównego zobowiązanie wobec wierzyciela przejmuje poręczyciel. Zgodnie z art. 759 § 1 K.c. czynności egzekucyjne wykonywane są przez komorników za wyjątkiem czynności zastrzeżonych dla sądów. Komornik, prowadząc zatem egzekucję przeciwko poręczycielowi, nie narusza jego praw, albowiem działa w granicach przysługujących mu ustawowo uprawnień.

Szereg uwag zamieszczanych w pismach wpływających do Generalnego Inspektora dotyczyło również *niewłaściwego, w ocenie skarżących, zabezpieczenia danych osobowych znajdujących się w posiadaniu komorników*, np. umieszczenie przez komornika pełnych informacji o uczestnikach postępowania egzekucyjnego w drzwiach mieszkania osoby, której postępowanie dotyczy.¹⁵⁶ Generalny Inspektor zauważył, iż zakres regulacji ustawy o ochronie danych osobowych podlega ograniczeniom, albowiem zgodnie z art. 18 ust. 3 ustawy, w przypadku gdy przepisy innych ustaw regulują odrębnie wykonywanie czynności, o których mowa w ust. 1 ustawy, dotyczących nakazania przez Generalnego Inspektora przywrócenia stanu zgodnego z prawem, stosuje się przepisy tych ustaw. Przykładem takich unormowań są przepisy K.p.c. regulujące m.in. zasady prowadzenia postępowania egzekucyjnego i związane z tym przetwarzanie danych przez komorników. Wszelkie zastrzeżenia uczestników postępowania egzekucyjnego powinny być zatem rozstrzygane zgodnie z przepisami kodeksu postępowania cywilnego. W myśl art. 3 ustawy o komornikach sądowych komornicy przy wykonywaniu czynności podlegają tylko ustawom i orzeczeniom

¹⁵³ Zob. artykuł „*Nie odmawiać komornikowi*” [w:] *Rzeczpospolita* z dnia 5 listopada 1999 r.

¹⁵⁴ GI-DP-024/1385/00

¹⁵⁵ GI-DP-743/00/902

¹⁵⁶ GI-DP-1047/1663

sądu. Przekroczenie uprawnień przez komornika może być przedmiotem skargi na czynność komornika kierowanej do prezesa właściwego sądu rejonowego, na podstawie art. 767 K.p.c., który w ramach sprawowanego nad komornikami nadzoru sądowego, jest uprawniony do wszczęcia postępowania dyscyplinarnego. Natomiast skargi na postępowanie komornika nie dotyczące czynności egzekucyjnych i nie objętych nadzorem prezesa sądu rejonowego, zgodnie z art. 6 ustawy o komornikach sądowych i egzekucji, rozpatrują organy samorządu komorniczego.¹⁵⁷ W związku z powyższym Generalny Inspektor nie znalazł podstaw do oceny zasadności zachowań komorników.¹⁵⁸ Ponadto zwrócono uwagę, iż w sytuacji, gdy działania komorników naruszają dobra osobiste uczestników postępowania egzekucyjnego, skarżącym przysługuje możliwość wystąpienia z roszczeniem cywilnym, o którym mowa w art. 23 i 24 K.c. do właściwego miejscowo i rzeczowo sądu powszechnego.¹⁵⁹

Indywidualne skargi dotyczyły kwestii udostępnienia przez komornika – w czasie przeprowadzanej egzekucji - informacji dotyczących dłużnika uzyskanych w toku prowadzenia innej egzekucji (np. egzekucji z rachunku bankowego).¹⁶⁰ Przepisy procedury cywilnej wskazują, że celem postępowania egzekucyjnego jest zastosowanie przez powołane do tego organy państwowe przewidzianych prawem środków przymusu w celu uzyskania na podstawie tytułu wykonawczego należnego wierzycielowi świadczenia. Na podstawie art. 889 § 1 pkt 1 K.p.c., w celu dokonania egzekucji z wierzytelności z rachunku bankowego, komornik ogólnej właściwości dłużnika przesyła do oddziału lub innej jednostki organizacyjnej banku, w którym dłużnik posiada rachunek bankowy, zawiadomienie o zajęciu wierzytelności pieniężnej dłużnika, wynikającej z posiadania rachunku bankowego, do wysokości należności będącej przedmiotem egzekucji wraz z kosztami egzekucyjnymi i wzywa bank, aby nie dokonywał wypłat z rachunku bez zgody komornika do wysokości zajętej wierzytelności, lecz przekazał bezzwłocznie zajętą kwotę na pokrycie należności albo zawiadomił komornika w terminie siedmiu dni o przeszkodzie do przekazania zajętej kwoty; zawiadomienie jest skuteczne także w wypadku niewskazania rachunku bankowego. Natomiast zgodnie z § 2 ww. przepisu równocześnie komornik przesyła wierzycielowi odpis zawiadomienia przesłanego do banku. Wobec powyższego należało uznać, iż udostępnienie komornikowi w trakcie toczącego się postępowania egzekucyjnego informacji o innych z

¹⁵⁷ Zob. GI-DIS-430/439/00

¹⁵⁸ GI-DP-230/00/259, podobnie w sprawach sygn. GI-DP-980/00/1409, GI-DP-1205/00/1616

¹⁵⁹ GI-DP-420/00/1040

¹⁶⁰ GI-DIS-209/00/917

toczących się wobec tego samego podmiotu postępowań egzekucyjnych znajdując oparcie w przepisach prawa nie narusza tym samym ustawy o ochronie danych osobowych.¹⁶¹

W związku z faktem, iż unormowany tryb uzyskiwania przez organ egzekucyjny wyjaśnień i informacji niezbędnych do wszczęcia i prowadzenia egzekucji nie reguluje wprost formy ich udostępniania, do Generalnego Inspektora napłynęło wiele pytań dotyczących sposobu występowania komorników o udostępnienie przez inne organy żądanych przez nich danych osobowych.¹⁶² Zgodnie z treścią art. 29 dane osobowe udostępnia się osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów ustawy. Innym osobom i podmiotom można udostępnić dane osobowe, jeżeli w sposób wiarygodny uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą. Prowadzenie zbiorów przez komorników dokonuje się w oparciu o przepisy Kodeksu postępowania cywilnego, ustawy o komornikach sądowych i egzekucji oraz rozporządzenia Ministra Sprawiedliwości w sprawie czynności komorników, a zatem w ocenie Generalnego Inspektora nie będzie miał zastosowania przepis art. 29 ustawy, albowiem jego treść odnosi się wyłącznie do danych udostępnianych w celach innych niż włączenie do zbioru. W tej sytuacji komornicy nie są zobowiązani występować o udostępnienie im określonych danych na wniosku, którego wzór określił Minister Spraw Wewnętrznych i Administracji w rozporządzeniu w sprawie określenia wzorów wniosku o udostępnienie danych osobowych, zgłoszenia zbioru danych do rejestracji oraz imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych.¹⁶³

Obok zagadnień związanych z przetwarzaniem danych przez sądy, prokuraturę oraz komorników sądowych, w roku 2000 do Generalnego Inspektora kierowano również uwagi dotyczące *skargi i zapytania dotyczące bezprawnego w ocenie skarżących przetwarzania danych osobowych zawartych w akcie notarialnym*. W jednym z pism skarżąca poinformowała, iż jej dane oraz dane zmarłego współmałżonka zostały bezprawnie umieszczone w akcie notarialnym, sporządzonym przy zakupie mieszkania w 1996 r.¹⁶⁴ Wnosząc skargę poinformowano, iż ustawa o ochronie danych osobowych weszła w życie w dniu 30 kwietnia 1998 r. (z wyjątkiem artykułów: 8-11, 13, 45, 55-59), a zatem przepisy w niej zawarte nie mają zastosowania do sytuacji mających miejsce przed tą datą. Przetwarzanie

¹⁶¹ Ibidem

¹⁶² GI-DP-105/00/503

¹⁶³ GI-DP-327/00/368

¹⁶⁴ GI-DIS-98/00/506

danych osobowych, które odbywało się przed datą 30 kwietnia 1998 r., nie podlega więc przepisom ww. ustawy. Jednocześnie Generalny Inspektor zwrócił uwagę, iż ustawa o ochronie danych osobowych odnosi się wyłącznie do osób żyjących, a zatem legalność przetwarzania danych osób zmarłych nie może być oceniana z punktu widzenia omawianej ustawy. Ponadto skarżących informowano, iż kwestia ustalenia istnienia lub nieistnienia stosunku prawnego wynikającego z aktu notarialnego nie należy do kompetencji Generalnego Inspektora, ale może być ewentualnie podniesiona w drodze powództwa cywilnego przed sądem powszechnym.¹⁶⁵

E. PRZETWARZANIE DANYCH OSOBOWYCH W ZAKRESIE OCHRONY ZDROWIA

Spośród licznej grupy skarg i pytań, jakie wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w okresie od 1 stycznia 2000 r. do 31 grudnia 2000 r., jednym z najbardziej spornych zagadnień była kwestia przetwarzania danych osobowych dotyczących stanu zdrowia. Ustawa o ochronie danych osobowych włączyła dane o stanie zdrowia do kategorii tzw. danych wrażliwych i ustanowiła zakaz ich przetwarzania. W tej samej kategorii danych, na podstawie art. 27 ustawy, zostały umieszczone dane o kodzie genetycznym, nałogach, życiu seksualnym, a także dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową.

Zakaz przetwarzania danych wrażliwych stanowi jeden z przejawów konstytucyjnej zasady ochrony prywatności. Ustawa o ochronie danych osobowych przewiduje jednak pewne odstępstwa od powyższego zakazu. Na podstawie art. 27 ust. 2 ustawy przetwarzanie danych o stanie zdrowia jest dopuszczalne, gdy:

- 1) osoba, której dane dotyczą, wyrazi zgodę na piśmie, chyba że chodzi o usunięcie jej danych,
- 2) przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą i stwarza pełne gwarancje ich ochrony,
- 3) przetwarzanie takich danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby, gdy osoba, której dane dotyczą nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora,

¹⁶⁵ Ibidem

- 4) jest to niezbędne do wykonania statutowych zadań kościołów i innych związków wyznaniowych, stowarzyszeń, fundacji lub innych niezarobkowych organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, pod warunkiem, że przetwarzanie danych dotyczy wyłącznie członków tych organizacji lub instytucji albo osób utrzymujących z nimi stałe kontakty w związku z ich działalnością i zapewnione są pełne gwarancje ochrony przetwarzania danych,
- 5) przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem,
- 6) przetwarzanie jest niezbędne do wykonywania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie,
- 7) przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych,
- 8) przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą.

I. Przetwarzanie danych osobowych przez Kasy Chorych.

Pomimo dwuletniego okresu, jaki upłynął od rozpoczęcia reformy służby zdrowia, nie ustały wątpliwości dotyczące przetwarzania danych osobowych przez organy służby zdrowia (26 skarg). Podobnie jak w 1999 r., w omawianym okresie sprawozdawczym największa liczba pytań kierowanych do Generalnego Inspektora Ochrony Danych Osobowych dotyczyła spraw związanych z funkcjonowaniem Kas Chorych. Obawy budził przede wszystkim *zakres danych przekazywanych między poszczególnymi Kasami, jak również zakres informacji udostępnianych Kasom przez poszczególnych świadczeniodawców.*

Generalny Inspektor poinformował, iż zakres danych, do przetwarzania których uprawnione są Kasy Chorych, określony został w przepisach ustawy z dnia 6 lutego 1997 r. o powszechnym ubezpieczeniu zdrowotnym (Dz. U. Nr 28, poz. 153 z późn. zm.). Zgodnie z art. 141 a ust. 2 cytowanej ustawy, dla realizacji zadań wymienionych w ust. 1 tego przepisu, Kasy Chorych mają prawo przetwarzania następujących danych osobowych:

- 1) imię i nazwisko,
- 2) PESEL,
- 3) data urodzenia,
- 4) płeć,

- 5) stopień pokrewieństwa z opłacającym składkę,
- 6) adres zamieszkania,
- 7) stopień niepełnosprawności, jeżeli dziecko ukończyło 26 lat,
- 8) udzielone ubezpieczonemu świadczenia zdrowotne, których charakterystyka zawiera m.in.
 - 9) rodzaj udzielonego świadczenia,
 - 10) świadczeniodawcę wykonującego usługę,
 - 11) świadczeniodawcę zlecającego usługę,
 - 12) rozpoznanie według międzynarodowej klasyfikacji chorób, urazów i zatruc związane z wykonywaną usługą.

Na podstawie wyżej wymienionej ustawy zostało wydane rozporządzenie Ministra Zdrowia i Opieki Społecznej z dnia 15 stycznia 1999 r. w sprawie ustalenia niezbędnych danych gromadzonych przez świadczeniodawców oraz w systemach informatycznych Kas Chorych, a także zakresu i procedury wymiany danych pomiędzy Kasami Chorych oraz Kasami Chorych a świadczeniodawcami, Urzędem Nadzoru Ubezpieczeń Zdrowotnych i Krajowym Związkiem Kas Chorych (Dz. U. Nr 7, poz. 66 z późn. zm.), zwane dalej rozporządzeniem. Przepisy rozporządzenia szczegółowo określają, jakie dane gromadzą w systemach informatycznych świadczeniodawcy oraz Kasy Chorych, wskazują zakres danych przekazywanych przez świadczeniodawców Kasom Chorych, a ponadto, jakie dane przekazują Kasy Chorych między sobą oraz do Krajowego Związku Kas Chorych i Urzędu Nadzoru Ubezpieczeń Zdrowotnych. Przekazywanie danych przez świadczeniodawców Kasom Chorych zostało uregulowane szczegółowo w § 3 i 4 cytowanego rozporządzenia. W myśl § 3 ust. 2 świadczeniodawcy usług medycznych są zobowiązani do przekazywania Kasom Chorych, z którymi mają zawarte umowy, na ich wniosek, następujące dane dotyczące świadczeń wykonanych na rzecz ubezpieczonych w nich osób:

- 1) mer ewidencyjny PESEL pacjenta, jeżeli został nadany,
- 2) numer karty ubezpieczenia,
- 3) numer służący do potwierdzenia wykonania świadczenia, uzyskany z karty ubezpieczenia – w przypadku, gdy karta jest stosowana do potwierdzenia świadczeń,
- 4) kod rodzaju świadczenia,
- 5) kod rozpoznania medycznego związanego z udzielonym świadczeniem według międzynarodowej klasyfikacji chorób, urazów i zatruc,
- 6) opłata wniesiona przez pacjenta,
- 7) dopłata ze strony Kasy Chorych,

- 8) numer REGON świadczeniodawcy wykonującego,
- 9) typ komórki organizacyjnej świadczeniodawcy, w której wykonano świadczenie,
- 10) data początku wykonania świadczenia,
- 11) data wykonania (końca wykonywania) świadczenia,
- 12) numer REGON świadczeniodawcy zlecającego,
- 13) typ komórki organizacyjnej świadczeniodawcy zlecającego,
- 14) numer prawa wykonywania zawodu lekarza zlecającego,
- 15) data zlecenia.

Kasy Chorych mają zatem prawo uzyskiwać dane osobowe od świadczeniodawców w zakresie uregulowanym przepisami powyższego rozporządzenia.¹⁶⁶ Nie istnieje natomiast podstawa prawna do przekazywania Kasie Chorych jakichkolwiek danych dotyczących osób ubezpieczonych, jeżeli pomiędzy Kasą Chorych a świadczeniodawcą nie została zawarta umowa o udzielanie świadczeń zdrowotnych.¹⁶⁷

Zgodnie z § 4 ww. rozporządzenia świadczeniodawcy są zobowiązani przekazywać regionalnej Kasie Chorych, na obszarze której prowadzą działalność, wymienione wyżej dane oraz symbol Kasy Chorych, w której ubezpieczony jest pacjent, dotyczące świadczeń wykonywanych na rzecz ubezpieczonych w Kasach Chorych, z którymi nie mają zawartej umowy.

Ponieważ zakres danych określonych w rozporządzeniu nie pokrywa się z zakresem danych określonych w przepisach o randze ustawy, zarówno podmioty upoważnione do przekazywania określonych danych, jak i podmioty występujące o ich udostępnienie występowały do Generalnego Inspektora o ich interpretację w świetle ustawy o ochronie danych osobowych. Znaczna część pytań kierowanych do Biura wynikała z nieznamomości ustawy o powszechnym ubezpieczeniu zdrowotnym i przepisów wykonawczych wydanych na podstawie tej ustawy.¹⁶⁸ Kasy Chorych mogą przekazywać dane osobowe wyłącznie podmiotom określonym w przepisach ww. rozporządzenia lub takim, które spełniają inną przesłankę legalności przetwarzania danych. Brak jest uzasadnienia dla udostępniania przez Kasy Chorych informacji innego rodzaju, niż te, których zakres przedmiotowy wyznaczony został obowiązującymi przepisami prawa.¹⁶⁹ W świetle powyższego podzielono obawy skarżących odnoszące się do zbyt szerokiego zakresu wglądu Kas w dokumentację szpitalną i

¹⁶⁶ GI-DP-172/00/270, GI-DP-024/1269/00

¹⁶⁷ GI-DP-1096/00/1745

¹⁶⁸ Np. GI-DP-52/00/115

¹⁶⁹ Patrz GI-DP-1097/00/1886

ambulatoryjną (np. sprawdzanie historii chorób, zleceń lekarskich, kart informacyjnych wydawanych pacjentowi, zawierających rozpoznanie oraz przebieg choroby i leczenia).¹⁷⁰

Wątpliwości wzbudzało również *przekazywanie między Kasami Chorych danych o pacjencie* (np. zawierających między innymi numer ewidencyjny PESEL, datę zapisu i nazwę jednostki POZ/LR, w której ubezpieczony złożył deklarację wyboru lekarza).¹⁷¹ Stosownie do art. 141a ust. 2 pkt 2 ustawy z dnia 6 lutego 1997 r. o powszechnym ubezpieczeniu zdrowotnym (Dz. U. Nr 28, poz. 153 z późn. zm.), dla realizacji zadań, o których mowa w ust. 1 tego przepisu, Kasy Chorych są uprawnione do przetwarzania numeru PESEL. Pytających poinformowano również, że stosownie do rozporządzenia, Kasy Chorych przekazują między sobą dane dotyczące świadczeń wykonanych na rzecz ubezpieczonych w innych Kasach Chorych, otrzymane od świadczeniodawców, a gromadzone na podstawie § 4 cytowanego rozporządzenia. Ponadto, Kasy mogą przekazywać dane o świadczeniodawcach, określone w § 2 pkt 1 rozporządzenia. Przekazywanie pomiędzy Kasami danych wykraczających poza wyżej opisane szczegółowe regulacje jest nadmierne i na gruncie przepisów prawa nieuprawnione.¹⁷² Generalny Inspektor podkreślił ponadto, iż zakres danych, jakie mają być przekazywane świadczeniodawcom, określony w rozporządzeniu, jako katalog zamknięty, nie może być zmieniony w drodze umowy.¹⁷³ Ewentualna zmiana zakresu przekazywanych danych może się odbyć jedynie na drodze zmiany odpowiednich przepisów.¹⁷⁴

W napływających do Biura pismach wielokrotnie zwracano się do Generalnego Inspektora o wyrażenie opinii w przedmiocie *zakresu żądania we wzajemnych rozliczeniach pomiędzy Kasami informacji o pacjentach* zawierających, np.: numer legitymacji szkolnej, bądź studenckiej, książeczki inwalidy wojskowego lub wojennego, czy też numeru świadczenia emerytalno – rentowego z ZUS i KRUS.¹⁷⁵ Informacje, jakie mogą być przekazywane między Kasami Chorych w celu wzajemnych rozliczeń, zostały wskazane w § 5 rozporządzenia Ministra Zdrowia i Opieki Społecznej w sprawie ustalenia zakresu niezbędnych danych gromadzonych przez świadczeniodawców oraz w systemach informatycznych Kas Chorych, a także zakresu i procedury wymiany danych pomiędzy Kasami Chorych a świadczeniodawcami, Urzędem Nadzoru Ubezpieczeń Zdrowotnych i

¹⁷⁰ GI-DP-249/00/278

¹⁷¹ GI-DP-485/00/496

¹⁷² Ibidem

¹⁷³ GI-DP-281/00/430

¹⁷⁴ GI-DP-214/00/211

¹⁷⁵ GI-DP-214/00/211

Krajowym Związkiem Kas Chorych. Analiza tego przepisu wskazuje, iż nie zezwala on na przekazywanie w zastępstwie numeru karty ubezpieczenia innych danych, niż dane określone w § 3. Nie istnieją bowiem podstawy prawne do zwiększania zakresu udostępnienia przez świadczeniodawców danych, ponad te, które wynikają z cytowanego rozporządzenia. Przepis § 5 rozporządzenia nie przewiduje ponadto możliwości wzajemnego udostępniania przez Kasy Chorych całych posiadanych przez nie zbiorów danych.¹⁷⁶

Ważnym problemem poruszonym przez świadczeniodawców była *kwestia dopuszczalności kserowania przez Kasy Chorych dokumentacji medycznej w związku z kontrolą świadczenia usług medycznych oraz ocena zakresu takiej kontroli*.¹⁷⁷ Generalny Inspektor poinformował, iż uprawnienia kontrolne nadała Kasom Chorych ustawa o powszechnym ubezpieczeniu zdrowotnym. Kasa Chorych przeprowadza lub zleca kontrolę bieżącej realizacji umowy o udzielenie świadczeń, a w szczególności kontrolę sposobu korzystania ze świadczeń przez ubezpieczonych, dostępności i jakości świadczeń oraz zasad organizacji ich udzielania (art. 61 ust. 1 pkt 1). Na podstawie art. 61 ust. 3 ww. ustawy podmiot kontrolowany zobowiązany jest do przedłożenia niezbędnych dokumentów, udzielania informacji i pomocy podczas kontroli. Zgodnie ze wskazanymi przepisami kontrola obejmuje dokumentację medyczną i jakość udzielonych świadczeń. Nie pozostaje zatem w sprzeczności z przepisami udostępnienie dokumentacji medycznej i innych dokumentów związanych z kontrolą jakości usług.¹⁷⁸ Kontroli mogą dokonywać wyłącznie upoważnieni przez Kasę Chorych lekarze, pielęgniarki, położne oraz przedstawiciele innych zawodów medycznych, o ile zakres kontroli ich dotyczy. Zakres danych przekazywanych przez świadczeniodawców – podmiot kontrolowany - organom kontroli nie może być szerszy, niż wskazany w § 3 i 4 wyżej cytowanego rozporządzenia. Podkreślono także, iż określenie w art. 141 a ustawy o powszechnym ubezpieczeniu zdrowotnym zakresu danych, do przetwarzania których upoważnione są Kasy Chorych, nie powinno być traktowane jako upoważnienie do kserowania dokumentacji medycznej.

Szczególnie wiele pytań kierowały do GIODO Okręgowe Izby Aptekarskie w związku z *wykonywaniem przez Kasy Chorych czynności kontrolnych w aptekach*.¹⁷⁹ Generalny Inspektor poinformował, iż podstawą prawną przeprowadzenia przez Kasy Chorych kontroli w aptekach jest przepis art. 61 ustawy o powszechnym ubezpieczeniu

¹⁷⁶ GI-DP-723/00/1049

¹⁷⁷ Patrz GI-DP-118/00/634, GI-DP-143/00/240, GI-DP-680/00/741

¹⁷⁸ GI-DP-249/00/278

¹⁷⁹ GI-DP-459/00635, GI-DP-334/00, GI-DP-024/1410/00

zdrowotnym. Dodatkowo, na podstawie przepisu art. 141b pkt 1 ww. ustawy, apteki są zobowiązane do udostępniania na żądanie Kas Chorych do wglądu recepty i przekazywać niezbędne dane rozliczeniowe, których rodzaj określi minister właściwy do spraw zdrowia w porozumieniu z Naczelną Radą Aptekarską. Wskazane regulacje prawne nie nadają osobom kontrolującym w imieniu Kas Chorych prawa do kserowania recept, natomiast wyraźnie uprawniamy Kasy jedynie do wglądu do nich. Wyprowadzenie z przywołanych przepisów uprawnienia do kserowania recept byłoby, w ocenie Generalnego Inspektora, zbyt szeroką interpretacją uprawnień Kas Chorych. Odrębnym zagadnieniem związanym z przetwarzaniem przez Kasy danych osobowych w trakcie przeprowadzanej przez nie kontroli w aptekach była kwestia *zakresu udostępniania danych zawartych w receptach lekarskich*.¹⁸⁰ Zgodnie z § 1 rozporządzenia Ministra Zdrowia i Opieki Społecznej z dnia 30 grudnia 1998 r. w sprawie recept lekarskich (Dz. U. Nr 164, poz. 1195 z późn. zm.) recepty wystawiane przez lekarzy powinny zawierać m.in. następujące dane: imię, nazwisko, wiek i adres osoby, dla której została wystawiona recepta, ilość leku, jego nazwę, sposób dawkowania, datę wystawienia recepty, podpis lekarza wystawiającego receptę oraz odcisk jego pieczęci, zawierającej imię, nazwisko, posiadaną specjalność, a także zaświadczenie o prawie wykonywania zawodu wyrażone symbolem lub kodem paskowym.¹⁸¹ W przypadku recepty wystawionej przez lekarza psychiatrę, lekarza zatrudnionego w poradni zdrowia psychicznego lub zatrudnionego w publicznym zakładzie opieki zdrowotnej dla osób pozbawionych wolności, pieczęć lekarza wystawiającego receptę może nie zawierać adresu i numeru telefonu. Ponadto apteki przekazują Kasom Chorych zestawienia zbiorcze recept; wzór takiego zestawienia określa rozporządzenie Ministra Zdrowia i Opieki społecznej z dnia 27 listopada 1998 r. w sprawie zbiorczego zestawienia recept podlegających refundacji przez Kasy Chorych (Dz. U. Nr 148, poz. 979 z późn. zm.). Na podstawie powyższych przepisów Kasy Chorych są uprawnione zarówno do przetwarzania danych osobowych zawartych na receptach, jak i do żądania udokumentowania wykonania świadczeń medycznych, przy czym żądania te nie mogą wykraczać poza upoważnienie w nich zawarte. Żaden przepis prawa nie upoważnia aptek do zbierania danych takich jak, np. numery PESEL i udostępniania ich Kasom Chorych, a zatem Kasy Chorych nie mogą żądać od aptek danych, do przetwarzania których apteki nie są uprawnione.

Warunkiem udostępnienia innych danych, niż znajdujące się na receptach, jest uzgodnienie przez Radę Krajowego Związku Kas Chorych (obecnie Minister Zdrowia) z

¹⁸⁰ GI-DP-686/00/1610, GI-DP-665/00/745

Naczelną Radą Aptekarską ich rodzaju. Na podstawie delegacji zawartej w art. 141b ustawy o powszechnym ubezpieczeniu zdrowotnym, kompetencje do określenia zakresu przekazywanych danych (w granicach określonych w art. 141a ustawy o powszechnym ubezpieczeniu zdrowotnym), przysługują tym właśnie podmiotom. Generalny Inspektor zauważył, iż z brzmienia art. 141b nie wynika, aby ustawodawca chciał pozostawić Kasom Chorych wyłączną kompetencję do określenia danych, które mają im być przekazywane. W sytuacji, gdy porozumienie, o którym mowa w art. 141b nie istnieje, należy uznać że apteki nie są uprawnione do udostępniania Kasom Chorych danych osobowych innych, niż znajdujące się na receptach.¹⁸² Wielokrotnie pytający zwracali się do Generalnego Inspektora o zbadanie zgodności cytowanego wyżej rozporządzenia Ministra Zdrowia i Opieki Społecznej w sprawie recept lekarskich z ustawą o ochronie danych osobowych. W odpowiedzi na powyższe, Generalny Inspektor informował, iż nie jest organem właściwym do oceny zgodności przepisów innych ustaw z ustawą o ochronie danych osobowych i kompetentnym do występowania z wnioskiem do Trybunału Konstytucyjnego.¹⁸³

W omawianym okresie sprawozdawczym stwierdzono, iż Kasy Chorych, wymuszają na placówkach medycznych i lekarzach ujawnianie danych o stanie zdrowia ubezpieczonych. Od udostępnienia tych informacji uzależniano nieraz zawarcie umowy, a w późniejszym czasie – zapłatę należności za udzielone świadczenie i rozliczenie finansowe kontraktu. Praktyka ta została przez Generalnego Inspektora uznana za naruszającą ustawowe uprawnienia Kas Chorych i prawa ubezpieczonych.¹⁸⁴ Jak wynikało z treści wielu napływających pism, *Kasy Chorych żądały od oferentów (świadczeniodawców), przy składaniu ofert na zawieranie umów o udzielanie świadczeń zdrowotnych, list osób, które złożyły deklarację o korzystaniu z usług danej placówki podstawowej opieki zdrowotnej, zawierających dane osobowe pacjentów w postaci imienia, nazwiska, numeru PESEL, daty urodzenia, płci oraz adresu.* Generalny Inspektor po przeprowadzeniu czynności wyjaśniających uznał powyższe żądanie za niezgodne z przepisami ustawy o ochronie danych osobowych.¹⁸⁵ Zgodnie z art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych przetwarzanie danych jest dopuszczalne wtedy, gdy zezwalają na to przepisy prawa. Sposób i zakres przetwarzanych danych osób ubezpieczonych przez Kasy Chorych został określony w

¹⁸¹ Zob. GI-DP-661/00/883

¹⁸² GI-DP-686/00/1610

¹⁸³ Np. GI-DP-1112/00/1735. Na marginesie należy zauważyć, że obecnie trwają prace nad nowelizacją cytowanego rozporządzenia, której celem jest ograniczenie zakresu przedmiotowego informacji znajdujących się na receptach.

¹⁸⁴ Por. artykuł „Ochrona danych osobowych w kasach chorych” [w:] *Gazeta Prawna* z dnia 4 sierpnia 2000 r.

rozdziale 7a ustawy o powszechnym ubezpieczeniu zdrowotnym oraz w wydany na jej podstawie rozporządzeniu wykonawczym.

Obowiązek przeprowadzenia konkursu ofert na zawieranie przez Kasy Chorych umów o udzielanie świadczeń zdrowotnych został wprowadzony przepisem art. 54 ust. 1 ustawy o powszechnym ubezpieczeniu zdrowotnym. Natomiast tryb składania ofert oraz sposób przeprowadzenia konkursu reguluje rozporządzenie Ministra Zdrowia i Opieki Społecznej z dnia 27 listopada 1998 r. w sprawie konkursu ofert na zawieranie przez Kasy Chorych umów o udzielanie świadczeń zdrowotnych (Dz. U. Nr 148, poz. 978 z późn. zm.), wydane na podstawie art. 54 ust. 2 wskazanej ustawy. Przepisy powyższego rozporządzenia nie nakładają jednak na oferentów obowiązku dołączenia do oferty listy osób (wraz z dotyczącymi ich danymi osobowymi), które zadeklarowały chęć korzystania z usług danej placówki. W ocenie Generalnego Inspektora przedmiotowego obowiązku nie można wyprowadzić z brzmienia § 6 pkt 3 wskazanego rozporządzenia, zgodnie z którym zamawiający w ogłoszeniu o konkursie ofert jest zobligowany określić warunki, jakie powinna spełniać oferta. Obowiązek taki, aby nie pozostawał w sprzeczności z przepisem art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych, powinien wynikać wprost z przepisów prawa. Nie może on zostać narzucony przez Kasy Chorych. Podstawy prawnej do żądania przez Kasy Chorych przedmiotowej listy nie stanowi również art. 141a ust. 1 ustawy o powszechnym ubezpieczeniu zdrowotnym. Wskazany przepis wylicza enumeratywnie cele, dla realizacji których Kasa Chorych może pozyskiwać i przetwarzać dane osób ubezpieczonych. Żaden z nich nie uprawnia Kasy Chorych do żądania danych tych osób, które złożyły deklarację o korzystaniu z usług danego ośrodka.¹⁸⁶ Według Generalnego Inspektora wymóg dołączania do oferty przedmiotowej listy nie znajduje także uzasadnienia w przepisach rozporządzenia. Regulują one bowiem przekazywanie Kasom Chorych przez świadczeniodawców, z którymi Kasy Chorych mają zawarte umowy, danych dotyczących świadczeń wykonanych na rzecz osób ubezpieczonych w zakresie określonym w § 3 powyższego rozporządzenia.

W tej sytuacji żądanie od oferentów przez Kasy Chorych, przy składaniu ofert na zawieranie umów o udzielenie świadczeń zdrowotnych, list osób, które złożyły deklarację o korzystaniu z usług danej placówki podstawowej opieki zdrowotnej, zawierających dane osobowe pacjentów, jako nie znajdujące uzasadnienia we wskazanych wyżej przepisach, pozostaje w sprzeczności z art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych. W

¹⁸⁵ GI-DIS-32/00/1343

związku z powyższym, zarówno w wystąpieniu do Ministra Zdrowia i Opieki Społecznej, jak również w sygnalizacji wystosowanej do Urzędu Nadzoru Ubezpieczeń Zdrowotnych, Generalny Inspektor postulował podjęcie działań mających na celu wyeliminowanie niezgodnych z przepisami ustawy o ochronie danych osobowych praktyk stosowanych przez Kasy Chorych, wskazując przy tym, iż wystarczające do przeprowadzenia konkursu ofert jest informowanie Kasy Chorych wyłącznie o liczbie pacjentów, którzy będą korzystać z usług danego ośrodka, bez przekazywania Kasie dotyczących ich danych osobowych.¹⁸⁷

Podobne stanowisko Generalny Inspektor zajął w sprawie skarg dotyczących *przekazywania danych osobowych pacjentów, którzy zrezygnowali z usług danej Kasy Chorych*.¹⁸⁸ Skoro osoby, których dane dotyczą, nie wyraziły na to zgody, a przepisy prawa nie przewidują obowiązku przekazywania takich danych, żądanie Kas w tym przedmiocie uznano za bezprawne.

Niektóre Kasy Chorych - przed zawarciem umowy o finansowanie usług - żądały od świadczeniodawców list zatrudnionego u nich personelu medycznego (w tym imiennych list lekarzy).¹⁸⁹ Generalny Inspektor wielokrotnie podkreślał, iż żaden z przepisów rozporządzenia nie upoważnia świadczeniodawcy do przekazywania jakichkolwiek danych osobowych Kasie Chorych, w fazie przed zawarciem umowy o finansowanie usług. Dotyczy to również danych osób zatrudnionych u świadczeniodawcy. Skoro więc osoby, których dane dotyczą, nie wyraziły zgody na ich przetwarzanie, zaś przepis prawa nie przewiduje obowiązku przekazywania takich danych, nie jest prawnie dopuszczalne przekazywanie Kasie Chorych danych lekarzy i innych pracowników świadczeniodawcy usług medycznych.¹⁹⁰ W odpowiedzi na kierowane przez Generalnego Inspektora do Ministra Zdrowia sugestie, do Biura wpłynęły dwa projekty rozporządzeń wykonawczych do ustawy ubezpieczeniowej, rozszerzających wyliczony w tej ustawie katalog danych, które Kasom wolno zbierać.¹⁹¹ Projekty dopuszczają przetwarzanie takich danych jak, np.: NIP, numer karty ubezpieczeniowej, numer identyfikacyjny pacjenta, rodzaj i numer dowodu tożsamości (gdy nie nadano PESEL), datę wykonania usługi medycznej.

W omawianym okresie sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych zajął się również *oceną zakresu danych osobowych zawartych w "skierowaniu do*

¹⁸⁶ Ibidem

¹⁸⁷ Por. wypowiedź Generalnego Inspektora Ochrony Danych Osobowych w artykule „*Kasy Chorych chcą wiedzieć za dużo*” [w:] *Rzeczpospolita* z dnia 28 czerwca 2000 r.; zob. GI-DP-188/00/1331

¹⁸⁸ GI-DP-188/00/1331

¹⁸⁹ GI-DP-024/1281/00, GI-DP-024/1326/00

¹⁹⁰ GI-DP-361/00/914

szpitala psychiatrycznego”.¹⁹² Jak wynikało z uzyskanych informacji Kasy Chorych podczas udzielania tzw. “promes”, tj. zgody na leczenie pacjenta poza obszarem Kasy, żądały one, jako załącznika do wniosku, kserokopii przedmiotowego skierowania. W ocenie Generalnego Inspektora przetwarzanie przez Kasę Chorych danych osobowych znajdujących się w ww. skierowaniu nie posiada podstawy prawnej z uwagi na fakt, iż informacje zawarte w skierowaniu wykraczają poza zakres ustanowiony w rozporządzeniu Ministra Zdrowia i Opieki Społecznej w sprawie ustalenia zakresu niezbędnych danych gromadzonych przez świadczeniodawców (...).¹⁹³ Ponieważ ww. rozporządzenie nie zobowiązuje świadczeniodawców do udostępnienia Kasom Chorych imienia, nazwiska, daty urodzenia oraz adresu zamieszkania świadczeniobiorcy, Kasy Chorych nie są uprawnione do otrzymywania tych kategorii danych.

Przedmiotem analizy Generalnego Inspektora były ponadto zapytania w przedmiocie zasadności przekazania Kasom Chorych przez Wojewódzkie Centra Analiz i Nadzoru w Ochronie Zdrowia danych zawartych w rejestrze usług medycznych.¹⁹⁴ Wojewódzki rejestr usług medycznych był prowadzony przez wojewodów na podstawie art. 32 ustawy z dnia 30 sierpnia 1991 r. o zakładach opieki zdrowotnej (Dz. U. Nr 91, poz. 408 z późn. zm.) oraz na podstawie rozporządzenia Ministra Zdrowia i Opieki Społecznej z dnia 27 czerwca 1996 r. w sprawie książeczek usług medycznych (Dz. U. Nr 92, poz. 420). Przepisy powyższe zostały uchylone ustawą z dnia 20 czerwca 1997 r. o zmianie ustawy o zakładach opieki zdrowotnej oraz o zmianie niektórych innych ustaw (Dz. U. Nr 104, poz. 661 z późn. zm.). Zgodnie z art. 16 ust. 2 tej ustawy, z dniem 1 stycznia 1999 r. zadania związane z prowadzeniem rejestrów usług medycznych stają się zadaniami kas powszechnego ubezpieczenia zdrowotnego. W tej sytuacji zbiory wojewódzkiego rejestru usług medycznych powinny być przekazane przez dotychczasowych administratorów właściwej terytorialnie Kasie Chorych.

Innym problemem, który pojawiał się w treści napływających pism, była zasadność odmowy przekazania Kasom Chorych danych znajdujących się w zasobach ZUS. Na zgłaszane przez Kasy żądanie przekazania danych, oddziały ZUS udzielały odpowiedzi odmownej, argumentując swoje stanowisko treścią art. 34 ust. 3 ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz. U. Nr 137, poz. 887 z późn. zm.) w związku z art. 29 ust. 3 ustawy o ochronie danych osobowych.¹⁹⁵

¹⁹¹ Por. artykuł „Resort zdrowia sankcjonuje bezprawne praktyk” [w:] *Rzeczpospolita* z dnia 27 lipca 2000 r.

¹⁹² GI-DP-878/00/1329

¹⁹³ Ibidem

¹⁹⁴ GI-DP-106/00/378

¹⁹⁵ GI-DP-024/1215/00

Ustawa o powszechnym ubezpieczeniu zdrowotnym w art. 51 ust. 3 stanowi, iż w razie nieodprowadzania składki za ubezpieczonego przez zobowiązanego płatnika, przez okres dłuższy niż 30 dni, Kasa Chorych obciąża tego płatnika kosztami świadczenia udzielonego ubezpieczonemu. Do opłacenia składek na ubezpieczenie zdrowotne za każdy miesiąc kalendarzowy w trybie, na zasadach oraz w terminie przewidzianym dla składek na ubezpieczenie społeczne, zobowiązane są bez uprzedniego wezwania osoby i jednostki, o których mowa w art. 23 –25 ustawy, a jeżeli do tych osób i jednostek nie stosuje się przepisów o ubezpieczeniu społecznym – w terminie do 15 dnia następnego miesiąca (art. 26 ust. 1). Na podstawie art. 26 ust. 5 ww. ustawy, Kasa Chorych jest uprawniona do nieodpłatnego dostępu do informacji o ubezpieczonym i opłacanej przez niego składce, w zakresie niezbędnym do realizacji ubezpieczenia zdrowotnego, znajdującej się w Zakładzie Ubezpieczeń Społecznych oraz w Kasie Rolniczego Ubezpieczenia Społecznego. Tym samym przetwarzanie przedmiotowych danych następuje na podstawie przesłanki określonej w art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych.¹⁹⁶

Generalny Inspektor nie podzielił natomiast stanowiska Kas Chorych w przedmiocie zasadności udostępniania im przez oddziały ZUS informacji o ubezpieczonych korzystających z bezpłatnych recept.¹⁹⁷ Wprawdzie art. 141a ust. 2 ustawy o powszechnym ubezpieczeniu zdrowotnym przyznaje Kasie uprawnienie do przetwarzania danych osobowych ubezpieczonych dla realizacji zadań określonych w art. 141a ust. 1 tej ustawy, jednak ani powołana ustawa, ani rozporządzenie nie zalicza Zakładu Ubezpieczeń Społecznych do podmiotów zobowiązanych do przekazywania Kasie Chorych informacji. Odmienna sytuacja ma miejsce w przypadku udostępniania Kasie informacji do kontroli wykonywania obowiązków w zakresie ubezpieczenia zdrowotnego. Na podstawie art. 142 ust. 3 ustawy o powszechnym ubezpieczeniu zdrowotnym Kasa Chorych jest bowiem upoważniona do przetwarzania przedmiotowych danych otrzymanych od Zakładu Ubezpieczeń Społecznych, w związku z czym zarówno ZUS, jak i KRUS obowiązane są do udostępnienia informacji określonych w powołanym przepisie.¹⁹⁸

W omawianym okresie sprawozdawczym Kasy Chorych często zwracały się o wyjaśnienia związane z prawidłowym wykonaniem obowiązku informacyjnego¹⁹⁹. Obowiązek informacyjny jest jednym z podstawowych obowiązków administratora danych

¹⁹⁶ Tak w piśmie Generalnego Inspektora Ochrony Danych Osobowych do Urzędu Nadzoru Ubezpieczeń Zdrowotnych z dnia 30 września 2000 r., sygn. GI-DP-024/1215/00/1692

¹⁹⁷ GI-DP-982/00/1480

¹⁹⁸ Ibidem.

¹⁹⁹ GI-DP-1207/00/1627

względem. Precyzyjne wypełnienie tego obowiązku gwarantuje, że osoba, której dane dotyczą, uzyska wyczerpującą informację odnośnie przetwarzania jej danych osobowych, co w konsekwencji umożliwi jej ewentualne skorzystanie z uprawnień wynikających z przepisu art. 32 ust. 1 ustawy o ochronie danych osobowych. Kasy informowano o treści art. 24 ustawy, regulującego zakres obowiązku informacyjnego, w przypadku zbierania danych od osoby, której one dotyczą. Trudności interpretacyjne wywoływała treść art. 25 ustawy. Generalny Inspektor podkreślał, iż w przypadku zbierania danych nie od osoby, której one dotyczą, wykonanie obowiązku informacyjnego ma niezwykle istotne znaczenie. Każdej bowiem osobie przysługuje prawo kontroli przetwarzania danych, które jej dotyczą, w tym m.in. do uzyskania informacji o źródle, z którego pochodzą oraz o celu i zakresie zbierania danych. Niektórzy administratorzy danych twierdzili, że obowiązek informacyjny, o którym mowa w art. 25 ust. 1 ustawy, wykonują za pośrednictwem mediów. W ocenie Generalnego Inspektora zamieszczenie ogłoszeń w mediach nie gwarantuje, iż wszystkie osoby, uprawnione z mocy art. 25 ustawy faktycznie przedmiotowe informacje otrzymały. Odnośnie tych administratorów danych, którzy pozyskali dane od innych podmiotów i nie dopełnili obowiązku informacyjnego bezpośrednio po utrwaleniu danych, wydawano decyzje administracyjne nakazujące przywrócenie stanu zgodnego z prawem.²⁰⁰

II. Udostępnianie danych medycznych przez podmioty opieki zdrowotnej

Znaczna liczba skarg i pytań kierowanych do Biura Generalnego Inspektora Ochrony Danych Osobowych w 2000 r. dotyczyła *legalności udostępnienia dokumentacji medycznej przez jednostki służby zdrowia takim podmiotom, jak zakłady ubezpieczeń w celu likwidacji szkody, czy wypłaty odszkodowania*.²⁰¹

W myśl ogólnych zasad dotyczących umowy ubezpieczenia zawartych w przepisach ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. Nr 16, poz. 93 z późn. zm.) zakład ubezpieczeń zobowiązuje się przez umowę ubezpieczenia do spełnienia określonego świadczenia, w razie zajścia przewidzianego w umowie wypadku (art. 805 K.c.). W celu ustalenia wysokości świadczenia, zakład ubezpieczeń wyjaśnia okoliczności konieczne do ustalenia odpowiedzialności zakładu. Stosownie do art. 6 ustawy z dnia 28 lipca 1990 r. o działalności ubezpieczeniowej (Dz. U. z 1996 r. Nr 11, poz. 408 z późn. zm.) sposób prowadzenia postępowania polegającego na ustaleniu wysokości szkody oraz wypłaty odszkodowań lub świadczeń ustala zakład ubezpieczeń w ogólnych warunkach ubezpieczeń.

²⁰⁰ Np. GI-DEC-DP-27/00

Zgodnie z art. 18 ust. 3 pkt 6 ustawy z dnia 30 sierpnia 1991 r. o zakładach opieki zdrowotnej (Dz. U. Nr 91, poz. 62 z późn. zm.), zakład opieki zdrowotnej udostępnia zakładowi ubezpieczeniowemu, w związku z prowadzonym przez niego postępowaniem, dokumentację medyczną osób korzystających ze świadczeń zdrowotnych zakładu. Ustawową podstawą przetwarzania danych jest zatem z art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych, który dopuszcza przetwarzanie danych sensytywnych, jeżeli przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą i stwarza pełne gwarancje ich ochrony. Udostępnianie dokumentacji medycznej organom rentowym, zakładom ubezpieczeniowym oraz zespołom do spraw orzekania o stopniu niepełnosprawności, w związku z prowadzonym przez nie postępowaniem, przez zakłady opieki zdrowotnej (m.in. szpitale, sanatoria, przychodnie, ośrodki zdrowia, poradnie, pogotowia ratunkowe, itp.), nie może być zatem, wbrew twierdzeniom skarżących, uznane za nielegalne. Dokumentacja ta (zgodnie z brzmieniem art. 18 ust. 3 pkt 6 ustawy o zakładach opieki zdrowotnej), może zostać udostępniona wyłącznie w związku z prowadzonym postępowaniem. Oznacza to, że nie jest dopuszczalne jej udostępnienie do celów, np. oceny ryzyka ubezpieczeniowego. Udostępnienie w tym celu może nastąpić wyłącznie za zgodą pacjenta (tj. na podstawie art. 18 ust. 3 pkt 1 ww. ustawy).²⁰²

Kolejnym zagadnieniem rozpatrywanym w roku 2000 była *kwestia zasadności żądania przez świadczeniodawców usług medycznych innych dokumentów weryfikujących ubezpieczenie zdrowotne, niż dokumenty określone w przepisach*. Zgodnie z art. 51 ust. 1 ustawy o powszechnym ubezpieczeniu zdrowotnym ubezpieczony ubiegający się o świadczenie z ubezpieczenia zdrowotnego jest obowiązany przedstawić kartę ubezpieczenia. Intencją tego przepisu jest weryfikacja uprawnienia ubezpieczonego do świadczenia. Rozporządzenie Rady Ministrów z dnia 18 marca 1999 r. w sprawie karty ubezpieczenia zdrowotnego, trybu jej wydawania i unieważniania (Dz. U. Nr 30, poz. 289) przewiduje w § 1 następujące formy karty ubezpieczenia:

- 1) kartę ubezpieczenia z układem elektronicznym,
- 2) kartę ubezpieczenia bez układu elektronicznego,
- 3) książeczkę usług medycznych.

Ustawa o powszechnym ubezpieczeniu zdrowotnym stanowi w art. 169f, że do dnia wydania ubezpieczonemu karty ubezpieczenia, dowodem ubezpieczenia jest każdy dokument, który do dnia 31 grudnia 1998 r. potwierdzał uprawnienia do świadczeń oraz książeczka

²⁰¹ Np. GI-DIS-58/00/268, GI-DIS-179/00/961, GI-DP-789/00/927

rejestr usług medycznych. Jak wielokrotnie sygnalizowano Generalnemu Inspektorowi, świadczeniodawcy (często na żądanie Kas Chorych) wymagają takiego dokumentu ubezpieczenia, który jednoznacznie wykaże, że karta ubezpieczenia (książeczka usług medycznych) jest aktualna. Swoje żądania świadczeniobiorcy argumentują faktem, iż książeczka usług medycznych nie jest dostatecznym dowodem ubezpieczenia, ponieważ jest wydawana bezterminowo i w sytuacji, gdy ubezpieczony przestał płacić składki, nie ma obowiązku jej zwrotu. W szczególności zakłady świadczące usługi medyczne żądały legitymacji ubezpieczeniowej wraz z ostatnim dowodem wpłat na ubezpieczenie lub z ostatnim odcinkiem renty lub emerytury. Dokumenty te informują o dochodach świadczeniobiorcy, a jeśli pacjent prowadzi działalność gospodarczą, informują także o jego pracownikach. Informacje takie, w ocenie Generalnego Inspektora, wkraczają w sferę prywatności świadczeniobiorcy, zaś ich żądanie utrudnia dostęp do świadczeń medycznych, szczególnie w sytuacji, gdy pacjent odmawia ich podania. Zgodnie z art. 23 ustawy o ochronie danych osobowych przetwarzanie danych jest dopuszczalne wyłącznie po spełnieniu jednej z przesłanek enumeratywnie wymienionych w tym przepisie. Przetwarzanie danych jest legalne m.in. wówczas, gdy zezwala na to przepis prawa (art. 23 ust. 1 ustawy o ochronie danych osobowych). Z brzmienia tego przepisu wynika, iż wymaganie innych dokumentów niż wskazane w art. 169f ustawy o ubezpieczeniu zdrowotnym, jest niezgodne z prawem. W związku z powyższym przedmiotowe żądania świadczeniodawców należy traktować jako bezpodstawne. Jednocześnie, jak zauważył Generalny Inspektor, jest uzasadnione, aby świadczeniodawcy mogli zweryfikować uprawnienie świadczeniobiorców do bezpłatnych świadczeń.²⁰³

Mając na uwadze powyższe, Generalny Inspektor Ochrony Danych Osobowych zwrócił się do Ministra Zdrowia o rozważenie możliwości przygotowania projektu nowelizacji przepisów w taki sposób, aby karta ubezpieczenia jednoznacznie wykazywała fakt posiadania uprawnień do świadczeń zdrowotnych.²⁰⁴

Na tle napływających do Biura skarg i pytań Generalny Inspektor Ochrony Danych Osobowych zauważył ponadto, iż z jednej strony art. 141a ustawy o powszechnym ubezpieczeniu zdrowotnym zawiera wyczerpujący katalog danych, których przetwarzanie jest dopuszczalne bez zgody osoby, której dane dotyczą, a równocześnie art. 16 tej ustawy w punkcie 11 precyzuje dane, które powinno zawierać zgłoszenie. Są to: “wskazanie Kasy

²⁰² GI-DP-265/00/350, GI-DP-306/00/317, GI-DP-324/00/477, GI-DP-897/001413

²⁰³ Por. GI-DP-024/1312/00

²⁰⁴ Szerzej w piśmie z dnia 29 sierpnia 2000 r., sygn. GI-DP-606/00/1318

Chorych, nazwisko, pierwsze i drugie imię, nazwisko rodowe, płeć, adres zamieszkania, numer PESEL, data urodzenia oraz numer NIP w przypadku osób, którym nadano ten numer. Gdy osoba zgłaszana do ubezpieczenia zdrowotnego nie ma nadanego numeru PESEL i numeru NIP, zgłoszenie powinno zawierać rodzaj i numer dowodu tożsamości. Zgłoszenie powinno zawierać również następujące dane dotyczące członków rodziny objętej ubezpieczeniem: nazwisko, pierwsze i drugie imię, nazwisko rodowe, płeć, stopień pokrewieństwa, datę urodzenia, adres zamieszkania, stopień niepełnosprawności, numer PESEL oraz numer NIP w przypadku osób, którym nadano ten numer.” Analiza powołanych przepisów prowadzi do stwierdzenia, że zgłaszający jest obowiązany dostarczyć Kasie Chorych drugie imię, nazwisko rodowe oraz - w pewnych sytuacjach - numer NIP lub rodzaj i numer dowodu tożsamości, zaś Kasa Chorych nie ma prawa tych danych przyjąć i przetwarzać.²⁰⁵

W ocenie Generalnego Inspektora ustawodawca nie przewidział również sytuacji, gdy osoba zgłaszana do ubezpieczenia nie podaje w całości danych osobowych i w interesie tej osoby ZUS i KRUS powinny zweryfikować lub uzupełnić posiadane dane z danymi zawartymi w ewidencji ludności (dotyczy to, np. podania prawidłowego numeru PESEL, drugiego imienia czy nazwiska rodowego osoby ubezpieczonej). W świetle powyższego byłoby zatem celowe (w ewentualnej nowelizacji dotychczasowej ustawy) uwzględnienie prawa tychże podmiotów do uzyskiwania stosownych informacji z rejestrów publicznych, albowiem w chwili obecnej zarówno organy rządowe, jak i samorządowe kategorycznie odmawiają pomocy w weryfikacji danych osób ubezpieczonych.²⁰⁶

Uwzględniając szczególny charakter danych osobowych dotyczących stanu zdrowia, niezależnie od faktu, czy dane dotyczą pacjentów ubezpieczonych czy nieubezpieczonych, w przekonaniu Generalnego Inspektora celowym byłoby również uregulowanie kwestii zakresu danych przekazywanych w zestawieniach dotyczących finansowania świadczeń zdrowotnych z budżetu państwa na mocy rozporządzenia z dnia 27 października 1999 r. w sprawie zasad i trybu finansowania z budżetu państwa świadczeń zdrowotnych udzielanych bezpłatnie przez publiczne zakłady opieki zdrowotnej (Dz. U. Nr 91, poz. 1040) analogicznie do zakresu danych przewidzianego w rozporządzeniu z dnia 15 stycznia 1999 r. w sprawie ustalenia zakresu niezbędnych danych gromadzonych przez świadczeniobiorców (...).²⁰⁷ Jak wynikało z napływających do Biura pism, publiczne zakłady opieki zdrowotnej udzielające na podstawie

²⁰⁵ Szerzej w wystąpieniu Generalnego Inspektora z dnia 26 stycznia 2000 r., sygn. GI/100/2000

²⁰⁶ Ibidem

²⁰⁷ Patrz wystąpienie Generalnego Inspektora do Ministra Zdrowia z dnia 26 maja 2000 r., sygn. GI/486/00

art. 165 ust. 1 i 2 ustawy o powszechnym ubezpieczeniu zdrowotnym, bezpłatnych świadczeń zdrowotnych na rzecz osób nieubezpieczonych, zostały zobowiązane przez Ministerstwo Zdrowia (na mocy pisma kierowanego przez Podsekretarza Stanu w Ministerstwie Zdrowia do wszystkich wojewodów) do przedstawienia Departamentowi Budżetu i Finansów Ministerstwa oraz Pełnomocnikowi Wojewody ds. Zdrowia zestawień, które mają zawierać m.in. dane pacjentów oraz tytuł uprawnienia do bezpłatnych świadczeń. W załączonym do powyższego pisma formularzu *zestawienia świadczeń zdrowotnych udzielanych na rzecz osób nie posiadających uprawnień z tytułu ubezpieczenia zdrowotnego udzielonych w 1999 r.* wymagane jest podanie imienia i nazwiska osoby, której udzielono świadczenia. Generalny Inspektor zauważył, iż ustawodawca nie określił wzoru formularza zestawienia w postaci załącznika do ww. rozporządzenia, ani też wzór taki nie stanowi integralnej części rozporządzenia. Nie istnieje zatem podstawa prawna dla podania w zestawieniu imienia i nazwiska osoby, której udzielono świadczenia. Ponieważ w § 5 rozporządzenia ustawodawca posłużył się sformułowaniem “dane osobowe umożliwiające identyfikację”, zbędne i nadmierne wydaje się ujawnienie imienia i nazwiska w przedmiotowym zestawieniu, jedynie w celu dokonania rozliczeń finansowych, skoro świadczeniodawcy są z mocy prawa upoważnieni do przetwarzania numeru PESEL.

W związku z powyższym, w sygnalizacji skierowanej do Ministra Zdrowia Generalny Inspektor podkreślił, iż ujawnienie imienia i nazwiska pacjenta dla ww. celów stoi w sprzeczności z przepisami ustawy o ochronie danych osobowych, która do przetwarzania danych szczególnie chronionych wymaga umocowania ustawowego dla zagwarantowania odpowiedniego poziomu zabezpieczenia informacji o osobie. Dla celów identyfikacji wystarczające jest podanie numeru PESEL, bez konieczności podawania imienia i nazwiska, co uniemożliwi osobom trzecim zapoznanie się z tożsamością osoby ubezpieczeniowej. Żądanie podania imienia i nazwiska jest nieadekwatne i nie znajduje podstaw w przepisach prawa. W tej sytuacji konieczne jest określenie przez ustawodawcę wzoru formularza zestawienia świadczeń zdrowotnych, o którym mowa w art. 165 ust. 1 i 2 ustawy o powszechnym ubezpieczeniu zdrowotnym, udzielanych bezpłatnie przez publiczne zakłady opieki zdrowotnej.²⁰⁸

Samodzielne Zakłady Opieki Zdrowotnej, aby móc przetwarzać dane osobowe, powinny legitymować się przepisem prawa, który im na to zezwala. Tymczasem, jak wynikało z sygnałów docierających do Generalnego Inspektora Ochrony Danych Osobowych

²⁰⁸ Ibidem

w roku 2000, szereg ZOZ-ów zwracało się do organów samorządu terytorialnego o sporządzenie wykazu osób zamieszkałych w danym rejonie, zawierającego imiona, nazwiska, adresy zameldowania na pobyt stały i czasowy oraz numery PESEL, z powoływaniem się na bliżej nieokreślone zarządzenie Prezesa Urzędu Nadzoru Ubezpieczeń Zdrowotnych. Podkreślano przy tym, iż dane te są niezbędne do sporządzania statystyk dla Kas Chorych. W ocenie Generalnego Inspektora, niejednokrotnie przedstawianej na łamach mediów, przedmiotowe żądania są niezgodne z przepisami ustawy o ochronie danych, szczególnie z art. 23 ust. 1 pkt 2.²⁰⁹ Podkreślano przy tym, iż obowiązujące rozporządzenie dotyczy wyłącznie przetwarzania danych przez podmioty określone w tytule tego aktu prawnego. Nie ma w nim żadnego przepisu umożliwiającego udostępnianie danych świadczeniodawcom przez organy samorządowe. Dopóki zatem żądający nie wykaże odpowiedniej przesłanki uprawniającej go do przetwarzania wnioskowanych danych, nie istnieją podstawy do ich przekazania przez gminy.

Szereg pytań dotyczyło *legalności prowadzenia i archiwizowania dokumentacji medycznej przez zakłady opieki zdrowotnej*.²¹⁰ Zgodnie z art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych przetwarzanie danych o stanie zdrowia jest możliwe pod warunkiem, że przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą i stwarza pełne gwarancje ich ochrony. Dla zakładów opieki zdrowotnej podstawą do przetwarzania danych związanych z każdym udzielanym świadczeniem jest § 1 rozporządzenia Ministra Zdrowia i Opieki Społecznej z dnia 15 stycznia 1999 r. W myśl art. 18 ust. 1 ustawy z dnia 30 sierpnia 1991 r. o zakładach opieki zdrowotnej (Dz. U. Nr 91, poz. 408 z późn. zm.), zakład opieki zdrowotnej jest obowiązany prowadzić dokumentację medyczną osób korzystających ze świadczeń zakładu. Do dnia 6 czerwca 1998 r. obowiązywało, wydane na podstawie powołanej ustawy, rozporządzenie Ministra Zdrowia i Opieki Społecznej z dnia 17 grudnia 1992 r. w sprawie dokumentacji medycznej, sposobu jej prowadzenia oraz szczegółowych warunków jej udostępniania (Dz. U. z 1993 r. Nr 3, poz. 13). Zgodnie z § 47 i § 50 powyższego rozporządzenia, zakończona dokumentacja zbiorcza przechowywana była w archiwum zakładu przez okres 10 lat. W nowym brzmieniu art. 18 ust. 6 ustawy o zakładach opieki zdrowotnej ustawodawca deleguje Ministra Zdrowia i Opieki Społecznej do wydania, po zasięgnięciu opinii Naczelnej Rady Lekarskiej, rozporządzenia, w którym określi rodzaje dokumentacji, sposób jej prowadzenia i

²⁰⁹ Szerzej w artykule „Jakie dane ZOZ może uzyskać od gminy” [w:] *Gazeta Samorządu i Administracji*, Nr 14/15 z dnia 3 lipca 2000 r.

²¹⁰ GI-DP-024/1410/00

szczegółowe warunki jej udostępnienia. Do chwili obecnej Minister Zdrowia i Opieki Społecznej nie wydał jednak przedmiotowego rozporządzenia. W obecnym stanie prawnym nie istnieje zatem akt prawny, który w sposób generalny określałby warunki prowadzenia i archiwizowania dokumentacji medycznej. W poszczególnych aktach prawnych istnieją natomiast przepisy, które odnoszą się do powyższego zagadnienia. Dla przykładu – zgodnie z § 11 rozporządzenia Ministra Zdrowia i Opieki Społecznej z dnia 15 września 1997 r. w sprawie rodzajów dokumentacji medycznej służby medycyny pracy oraz sposobu jej prowadzenia i przechowywania (Dz. U. Nr 120, poz. 768), okres przechowywania indywidualnej dokumentacji medycznej służby medycyny pracy wynosi 20 lat. Taki sam okres przechowywania dokumentacji medycznej indywidualnej wewnętrznej służby medycyny pracy PKP, wskazany został w § 17 rozporządzenia Ministra Transportu i Gospodarki Morskiej z dnia 20 sierpnia 1999 r. w sprawie rodzajów dokumentacji medycznej oraz sposobu jej prowadzenia i udostępniania przez zakłady opieki zdrowotnej utworzone przez przedsiębiorstwo państwowe „Polskie Koleje Państwowe” (Dz. U. Nr 75, poz. 851). Analiza powołanych przepisów wskazuje na niezbędność archiwizacji dokumentacji medycznej. Jednocześnie zgodnie z art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych, administrator danych jest obowiązany przechowywać dane w postaci umożliwiającej identyfikację osób, których one dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania. Tym samym zakład opieki zdrowotnej, występując w roli administratora danych, osiąga cel przetwarzania po upływie okresu archiwizacji dokumentacji medycznej.²¹¹ W związku z powyższym, Generalny Inspektor Ochrony Danych Osobowych dwukrotnie wskazywał Ministrowi Zdrowia na konieczność wydania aktu prawnego, który regulowałby przedstawione zagadnienia.

Do Generalnego Inspektora Ochrony Danych Osobowych wpływały ponadto liczne zapytania od ośrodków i towarzystw zajmujących się rehabilitacją osób po zawale serca, w przedmiocie uzyskiwania informacji o tych osobach z ewidencji szpitalnej, poradni medycznej i innych podmiotów wskazanych w ustawie, jako zakład opieki zdrowotnej. Pytający podkreślali, iż prowadzona przez nie działalność nie ma charakteru działalności gospodarczej, a materiały uzyskiwane z jej przebiegu nie mają charakteru komercyjnego.²¹² Generalny Inspektor informował, iż dotarcie do ww. informacji jest tylko wówczas dozwolone, gdy znajduje to uzasadnienie w przepisie szczególnym innej ustawy, niż ustawa o ochronie danych osobowych, przy jednoczesnym stworzeniu pełnej gwarancji ochrony danych

²¹¹ Ibidem

osobowych. Przepisami takimi są przykładowo: przepisy ustawy z dnia 5 grudnia 1996 r. o zawodzie lekarza (Dz. U. z 1997 r. Nr 28, poz. 152 z późn. zm.) oraz ustawa o zakładach opieki zdrowotnej. Zgodnie z pierwszą z przywołanych ustaw, lekarz ma obowiązek zachowania w tajemnicy informacji związanych z pacjentem, uzyskanych w związku z wykonywaniem zawodu (art. 40). Przepis ten nie znajduje zastosowania m.in. w sytuacji, gdy pacjent lub jego przedstawiciel ustawowy wyraża zgodę na ujawnienie tajemnicy po uprzednim poinformowaniu o niekorzystnych dla pacjenta skutkach tego ujawnienia, bądź gdy tak stanowią odrębne przepisy. Informacja, że dana osoba została poddana leczeniu jest również rodzajem informacji o stanie zdrowia i w związku z tym objęta została tajemnicą lekarską.

Zgodnie z art. 18 ust. 3 ustawy o zakładach opieki zdrowotnej, zakład udostępnia dokumentację medyczną wyłącznie: pacjentowi lub jego przedstawicielowi ustawowemu bądź osobie upoważnionej przez pacjenta, zakładom opieki zdrowotnej, jednostkom organizacyjnym tych zakładów i osobom wykonującym zawód medyczny poza zakładami opieki zdrowotnej, jeżeli dokumentacja ta jest niezbędna do zapewnienia ciągłości świadczeń zdrowotnych, właściwym do spraw zdrowia organom państwowym oraz organom samorządu lekarskiego w zakresie niezbędnym do wykonywania kontroli i nadzoru, Ministrowi Zdrowia i Opieki Społecznej, sądom, prokuratorom oraz sądom i rzecznikom odpowiedzialności zawodowej, w związku z prowadzonym postępowaniem, uprawnionym na mocy odrębnych ustaw organom i instytucjom, jeżeli badanie zostało przeprowadzone na ich wniosek, organom rentowym, zakładom ubezpieczeniowym oraz zespołom do spraw orzekania o stopniu niepełnosprawności, w związku z prowadzonym przez nie postępowaniem, rejestrom usług medycznych, w zakresie niezbędnym do prowadzenia rejestrów.

Ponieważ żaden z wymienionych przepisów nie daje podstawy do udostępnienia przez zakłady opieki zdrowotnej przedmiotowych danych ośrodkom rehabilitacji, ich przekazywanie będzie naruszeniem ustawy o ochronie danych osobowych. W takiej sytuacji, w ocenie Generalnego Inspektora Ochrony Danych Osobowych, jedyną drogą dotarcia do osób potrzebujących jest prowadzenie kampanii informacyjnej w środkach masowego przekazu, czy też poprzez ulotki oraz informacje przekazywane przez lekarzy i placówki udzielające pomocy medycznej. Działania takie nie będą naruszeniem tajemnicy lekarskiej, a jednocześnie umożliwią wypełnienie celów ośrodka.²¹³ Z kolei nie stanowi naruszenia ustawy o ochronie danych osobowych, w świetle zacytowanych wyżej przepisów, *udostępnienie*

²¹² GI-DP-213/00/271

*przez ZOZ-y historii choroby pacjenta lekarzowi rodzinnemu, jako podmiotowi wymienionemu w art. 18 ust. 3 ustawy o zakładach opieki zdrowotnej, jeżeli dokumentacja ta jest niezbędna do zapewnienia ciągłości świadczeń zdrowotnych, czy też takiemu organowi, jak sąd, jeżeli przetwarzanie danych jest niezbędne do dochodzenia praw przed sądem (w myśl art. 27 ust. 2 pkt 5 ustawy o ochronie danych osobowych).*²¹⁴

Pytania kierowane do Generalnego Inspektora dotyczyły również *legalności i zakresu udostępniania danych o pacjentach organowi założycielskiemu ZOZ-u.*²¹⁵ Zakres danych, jakie mogą być przetwarzane przez organ nadzoru wynika m.in. z ustawy o zakładach opieki zdrowotnej oraz rozporządzenia Ministra Zdrowia z dnia 18 listopada 1999 r. w sprawie szczegółowych zasad sprawowania nadzoru nad samodzielnymi publicznymi zakładami opieki zdrowotnej i nad jednostkami transportu sanitarnego (Dz. U. Nr 94, poz. 1097 z późn. zm.). W świetle art. 67 powyższej ustawy, nadzór nad zakładami opieki zdrowotnej sprawuje podmiot, który utworzył zakład. Podmiot ten dokonuje kontroli i oceny działalności zakładu opieki zdrowotnej, która obejmuje w szczególności realizację zadań statutowych, dostępność i poziom udzielanych świadczeń, prawidłowość gospodarowania mieniem, gospodarkę finansową. Zbieranie informacji w związku z realizacją powyższych zadań i w zakresie niezbędnym do ich prawidłowego wykonania nie jest zatem sprzeczne z przepisami ustawy o ochronie danych osobowych. Generalny Inspektor podkreślił przy tym, iż żądanie udostępnienia danych o stanie zdrowia pacjenta, powinno znajdować podstawę w przepisach rangi ustawowej. Takiego upoważnienia dla organu założycielskiego nie zawiera ustawa o zakładach opieki zdrowotnej, natomiast przepisy powołanego wyżej rozporządzenia nie mogą stanowić podstawy do przetwarzania danych „wrażliwych”.²¹⁶

Liczne wątpliwości ZOZ-ów wzbudzała *kwestia udostępniania osobom trzecim informacji telefonicznych o samym fakcie pobytu pacjenta w szpitalu.*²¹⁷ Generalny Inspektor uznał, iż sama informacja o fakcie leczenia w szpitalu lub innym ośrodku zdrowia z podaniem rodzaju placówki, w jakiej przebywa pacjent, czy oddziału, na którym jest leczony przekazana innej osobie, stanowić będzie przetwarzanie danych o stanie zdrowia, tym samym dane takie będą podlegać szczególnej ochronie przewidzianej w art. 27 ust. 2 ustawy o ochronie danych osobowych. W świetle art. 32 ust. 1 ustawy o zawodzie lekarza, lekarz ma obowiązek udzielać pacjentowi lub jego ustawowemu przedstawicielowi przystępnej informacji o jego

²¹³ Zob. GI-DP-213/00/271

²¹⁴ GI-DIS-309/00/2001, GI-DP-808/00/969

²¹⁵ GI-DP-225/00/836

²¹⁶ Ibidem

²¹⁷ GI-DP-225/00/836, GI-DP-814/00/1139

stanie zdrowia, rozpoznaniu, proponowanych oraz możliwych metodach diagnostycznych, leczniczych, dających się przewidzieć następstwach ich zastosowania albo zaniechania, wynikach leczenia oraz rokowaniu. Zarówno ustawa o zawodzie lekarza, jak i ustawa o ochronie danych osobowych nie określają, w jaki sposób dane mogą być udostępniane, w szczególności, czy informacje o pobycie pacjenta w szpitalu mogą być udzielone innym osobom telefonicznie. Ocena możliwości udostępnienia danych uwarunkowana jest okolicznościami konkretnego przypadku. Jeżeli pacjent wyraża zgodę na udzielenie przedmiotowych informacji ściśle określonym osobom, ich przekazanie powinno opierać się na przekonaniu, iż osoba telefonująca jest uprawniona do ich pozyskania. Ustawa o ochronie danych nakłada na administratora danych, jakim w omawianym przypadku jest szpital, określone obowiązki, które w przypadku udostępniania danych sensytywnych stanowić będą istotne ograniczenia w przekazywaniu ich przez telefon. Szpital jest więc zobowiązany, na podstawie art. 36 ustawy o ochronie danych osobowych, do właściwego zabezpieczenia danych znajdujących się w jego zasobach, tzn. do zastosowania takich środków technicznych i organizacyjnych, które zabezpieczą dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem. Generalny Inspektor zauważył, iż udzielenie informacji telefonicznie nie daje pewności, że w ich posiadanie nie wejdzie osoba nieuprawniona, co w przypadku danych wrażliwych jest szczególnie istotne. W sytuacji, gdy osoba przebywająca w szpitalu nie jest zdolna do wyrażenia zgody na udostępnienie jej danych, np. jest nieprzytomna, zastosowanie znajdzie art. 31 ust. 6 ustawy o zawodzie lekarza, zgodnie z którym, jeżeli pacjent nie ukończył 16 lat lub jest nieprzytomny, bądź niezdolny do zrozumienia znaczenia informacji, lekarz udziela informacji przedstawicielowi ustawowemu, a w razie jego braku lub gdy porozumienie z nim jest niemożliwe – opiekunowi faktycznemu pacjenta. W sytuacji, gdy pacjent nie życzy sobie, aby dane o fakcie jego pobytu w szpitalu były udostępniane nawet najbliższym członkom rodziny, szpital nie ma prawa takich danych udostępniać.²¹⁸ Osoba, której dane dotyczące stanu zdrowia i sposobu leczenia zostały ujawnione, na podstawie art. 150 ustawy o powszechnym ubezpieczeniu zdrowotnym jest uprawniona do żądania od podmiotu odpowiedzialnego za dokonanie naruszeń odpowiedniej sumy pieniężnej - tytułem zadośćuczynienia za doznaną krzywdę.

²¹⁸ W opinii Generalnego Inspektora odmowa udzielenia informacji najbliższej rodzinie o fakcie pobytu jej członka w szpitalu w pewnych sytuacjach może budzić wątpliwości, jako nieracjonalna i nieuzasadniona. Z drugiej jednak strony niezwykle istotne jest zapewnienie osobie leczonej prywatności, co znajduje odzwierciedlenie zarówno w regulacjach ustawy o zawodzie lekarza, jak i ustawy o ochronie danych osobowych (...) zob. GI-DP-814/00/1139

Pośród pytań kierowanych przez zakłady opieki zdrowotnej do Generalnego Inspektora znalazły się również pytania dotyczące zasad przetwarzania danych osobowych pacjentów, którzy nie ukończyli 18-ego roku życia.²¹⁹ Szpitale dziecięce zwracały się o udzielenie odpowiedzi, czy przy gromadzeniu przedmiotowych danych powstaje po stronie administratora danych obowiązek uzyskiwania pisemnej zgody rodziców lub innych opiekunów prawnych dzieci. Odnosząc się do powyższego zagadnienia Generalny Inspektor poinformował, iż podstawą przetwarzania ww. danych jest art. 27 ust. 2 pkt 7 ustawy o ochronie danych osobowych, zgodnie z którym dopuszcza się przetwarzanie danych o stanie zdrowia, jeżeli jest ono dokonywane w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych. W tej sytuacji nie jest konieczne wyrażenie zgody przedstawicieli prawnych pacjentów na przetwarzanie danych ich podopiecznych.²²⁰ Jednakże w sytuacjach, gdy dane osobowe pacjentów mają być wykorzystywane w innych celach, np. reklamowania placówki medycznej, promowania usług danego lekarza, wyrażenie pisemnej zgody przez osobę, której dane dotyczą, jest warunkiem koniecznym dla takiego przetwarzania danych.

W omawianym okresie sprawozdawczym przedmiotem analizy Generalnego Inspektora była kwestia *powiadamiania przez szpitale o fakcie hospitalizacji pracowników ich zakładów pracy*. Samodzielne publiczne zakłady opieki zdrowotnej jako podstawę wskazanych działań podawały § 11 ust. 2 rozporządzenia Ministra Zdrowia i Opieki Społecznej z dnia 17 maja 1996 r. w sprawie orzekania o czasowej niezdolności do pracy (Dz. U. Nr 63, poz. 302 z późn. zm.). Generalny Inspektor zauważył, iż powołane rozporządzenie zostało wydane na podstawie art. 50 ust. 2 ustawy z dnia 17 grudnia 1974 r. o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa (Dz. U. z 1983 r., Nr 30, poz. 143 z późn. zm.), która straciła moc obowiązującą. Na podstawie art. 59 ust. 14 aktualnie obowiązującej ustawy z dnia 25 czerwca 1999 r. o świadczeniach pieniężnych z tytułu ubezpieczenia społecznego w razie choroby i macierzyństwa (Dz. U. Nr 60, poz. 636 z późn. zm.) zostało wydane rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 27 lipca 1999 r. w sprawie szczegółowych zasad i trybu wystawiania zaświadczeń lekarskich, wzoru zaświadczenia lekarskiego i zaświadczenia lekarskiego wydanego w wyniku kontroli lekarza orzecznika Zakładu Ubezpieczeń Społecznych (Dz. U. Nr 65, poz. 741). W zakresie

²¹⁹ GI-DP-024/1366/00

dotyczącym zasad i trybu wystawiania zaświadczeń lekarskich, zgodnie z § 8 powyższego rozporządzenia, straciło moc rozporządzenie Ministra Zdrowia i Opieki Społecznej z dnia 17 maja 1996 r. w sprawie orzekania o czasowej niezdolności do pracy. W ocenie Generalnego Inspektora skutkiem takiego sposobu uchylenia przepisów rozporządzenia w sprawie orzekania o czasowej niezdolności do pracy jest błędna praktyka szpitali, polegająca na wysyłaniu zawiadomienia o hospitalizacji pracownika do zakładu pracy, w którym jest zatrudniony.²²¹ Trudności interpretacyjne pogłębia fakt, że jeżeli § 11 rozporządzenia w sprawie orzekania o czasowej niezdolności do pracy, w części dotyczącej powiadamiania zakładu pracy o pobycie w szpitalu jego pracownika, nie został uchylony, pozostałby w sprzeczności z art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych, bowiem do przetwarzania danych dotyczących stanu zdrowia niezbędne jest umocowanie ustawowe. W związku z powyższym zwrócono się do Ministra Zdrowia o zajęcie stanowiska w przedmiotowej kwestii.²²² Do chwili obecnej takie stanowisko nie zostało jednak przedstawione.

Przedmiotem licznych pytań kierowanych do Generalnego Inspektora Ochrony Danych Osobowych w roku 2000 była ponadto *kwestia dopuszczalności wpisywania przez lekarzy kodów usług i kodów MKCH (Międzynarodowej Klasyfikacji Chorób) do książeczek usług medycznych*.²²³ Zagadnienie to uregulowane zostało w załączniku nr 3 do rozporządzenia Rady Ministrów z dnia 18 marca 1999 r. w sprawie karty ubezpieczenia zdrowotnego, trybu jej wydawania i unieważniania (Dz. U. Nr 30, poz. 289), który zawiera wzór kuponu części wymiennej książeczki usług medycznych. W przedmiotowym wzorze umieszczona została rubryka na umieszczenie kodu usługi i kodu MKCH. W związku z powyższym, wpisywanie przez lekarzy do książeczek usług medycznych takich danych, jak kod rodzaju świadczenia, oraz kod rozpoznania medycznego znajduje umocowanie w przepisie prawa, wyczerpując tym samym dyspozycję art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych.

Z napływających w 2000 r. do Generalnego Inspektora sygnałów wynikało, iż funkcjonujące w Polsce *Regionalne Rejestry Nowotworów* zawierają informacje o zachorowaniach na nowotwory złośliwe. Pytania dotyczyły podstawy prawnej funkcjonowania takich jednostek, zakresu przetwarzania przez nich danych osób chorujących

²²⁰ Ibidem

²²¹ Pismo do Ministra Sprawiedliwości z dnia 8 maja 2000 r., sygn. GI/407/00

²²² Ibidem

²²³ GI-DP-76/00/136

na raka, jak również legalności działań profilaktycznych wobec członków rodzin tych osób.²²⁴ Regionalne Rejestry Nowotworów wskazywały, iż podstawa prawna ich funkcjonowania została określona w przepisach Instrukcji Ministrów Zdrowia i Opieki Społecznej, Obrony Narodowej, Spraw Wewnętrznych, Komunikacji oraz Sprawiedliwości z dnia 28 marca 1962 r. w sprawie zgłaszania przypadków nowotworów złośliwych i podejrzanych jako złośliwe (Monitor Polski Nr 30, poz. 141). Z ustaleń poczynionych przez Generalnego Inspektora wynikało, iż instrukcja powyższa nie obowiązuje, nie został także uchwalony żaden inny akt regulujący kwestie przetwarzania danych o osobach chorych na nowotwory złośliwe. Z chwilą wejścia w życie ustawy o ochronie danych osobowych, tj. z dniem 30 kwietnia 1998 r. przetwarzanie danych o stanie zdrowia powinno odbywać się tylko na podstawie aktu prawnego o randze ustawy. Niedopuszczalne w takiej sytuacji jest istnienie luki prawnej dotyczącej przetwarzania danych osób dotkniętych chorobą nowotworową. W związku z powyższym postulowano do Ministra Zdrowia o wprowadzenie normy prawnej o randze ustawy, stanowiącej podstawę gromadzenia i wykorzystywania powyższych danych, a także tworzącej gwarancję ochrony osób dotkniętych chorobą.²²⁵ Wystąpienie w jednej rodzinie kombinacji nowotworów stwarza wysokie prawdopodobieństwo ich genetycznego pochodzenia oraz stwarza konieczność objęcia badaniem i poddania obserwacji członków takiej rodziny. Społecznie uzasadnione jest więc objęcie zapisem ustawowym kwestii przetwarzania przedmiotowych danych dla celów profilaktyki i stworzenie regulacji prawnej umożliwiającej poradnikom profilaktycznym dostęp do takich danych w celu wczesnego wykrycia choroby i podjęcia jej leczenia.²²⁶

Odrębna grupa zagadnień, rozpatrywanych przez Generalnego Inspektora w omawianym okresie sprawozdawczym dotyczyła *zakresu informacji o pacjentach, jakie zobowiązane były udzielać poradnie psychologiczno – pedagogiczne na żądanie innych organów, np. sądów.*²²⁷ W ocenie Generalnego Inspektora podstawą prawną wysuwanych przez sądy żądań są przepisy procedury karnej i cywilnej. W myśl art. 248 § 1 Kodeksu postępowania cywilnego, każdy zobowiązany jest przedstawić na zarządzenie sądu w oznaczonym terminie i miejscu dokument znajdujący się w jego posiadaniu i stanowiący dowód faktu istotnego dla rozstrzygnięcia sprawy, chyba że dokument zawiera tajemnicę państwową. Natomiast zgodnie z art. 15 § 2 Kodeksu postępowania karnego, wszystkie

²²⁴ GI-DP-53/00/955, GI-DP-462/00/955

²²⁵ Por. GI/609/00

²²⁶ Ibidem

²²⁷ GI-DP-1064/00/1571, por. GI-DP-377/00/990

instytucje państwowe i społeczne w zakresie swego działania są zobowiązane do udzielania pomocy organom prowadzącym postępowanie karne. Dokumenty, które sądy w ten sposób uzyskują, podlegają ochronie na zasadach określonych w przepisach K.p.c. i K.p.k.²²⁸ Informacja o stanie zdrowia oskarżonego, w szczególności o stanie zdrowia psychicznego, jest niezbędna dla ustalenia jego odpowiedzialności karnej, jak również może mieć wpływ na wymiar kary. W wyroku z dnia 5 marca 1998 r. (sygn. Akt II KKN 325/96) Sąd Najwyższy orzekł, iż jakkolwiek wiadomości o stanie zdrowia oskarżonego nie należą do danych charakteryzujących osobowość sprawcy, zbieranych stosownie do art. 213 § 1 K.p.k., tak ich uzyskanie ma istotne znaczenie w tych, określonych wyraźnie w przepisach ustaw karnych, przypadkach, w których orzeczenia sądu – podejmowane na podstawie i w trybie tych przepisów – wiedzę tę muszą uwzględnić. Dla przykładu należy wskazać przepisy art. 74 § 2 pkt 2 w związku z art. 202 K.p.k., stanowiące o przeprowadzeniu dowodu z biegłych w celu ustalenia poczytalności oskarżonego, jeżeli okoliczności ujawnione w toku postępowania wskazują i uzasadniają taką konieczność oraz obowiązku oskarżonego poddania się badaniom psychologicznym i psychiatrycznym, oraz art. 79 § 1 pkt 3 K.p.k. stanowiący o konieczności wyznaczenia obrońcy, gdy zachodzi uzasadniona wątpliwość co do poczytalności oskarżonego. Skoro zatem zbieranie w postępowaniu karnym informacji o stanie zdrowia oskarżonego znajduje uzasadnienie w przepisach prawa, to tym samym zgodne jest z przepisem art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych.²²⁹

Uznając potrzebę szczególnej ochrony danych wrażliwych, a zwłaszcza danych o stanie zdrowia psychicznego, Generalny Inspektor ze szczególną starannością analizował pisma dotyczące przetwarzania tej kategorii danych przez podmioty wskazane w treści skarg i w uzasadnionych stanem faktycznym przypadkach przeprowadzał postępowania wyjaśniające. Jak wykazało jedno z postępowań, wraz z likwidacją poradni psychiatrycznej, w której praktykantom – studentom psychologii - zakładano karty “Historii choroby psychiatrycznej”, wszystkie informacje dotyczące praktykantów zostały przekazane szpitalowi psychiatrycznemu, który następnie dokonywał ich przetwarzania, tj. przechowywał jako kartoteki byłych pacjentów. Generalny Inspektor nie znalazł podstaw do przechowywania przedmiotowych danych w zbiorach pacjentów, w sytuacji, gdy dane zebrano w związku z odbywaniem przez studentów praktyk zawodowych. Oprócz naruszenia

²²⁸ Szerzej w części I pkt D sprawozdania dotyczącym przetwarzania danych osobowych przez organy wymiaru sprawiedliwości.

²²⁹ GI-DP-1144/00/1559, szerzej o tematyce przetwarzania danych o stanie zdrowia w postępowaniu karnym i cywilnym w części I pkt D „Sprawozdania ...”, dotyczącej przetwarzania danych osobowych przez sądy, prokuraturę i komorników sądowych.

przepisu art. 26 ust. 1 pkt 2 ustawy o ochronie danych, szpital nie wykazał żadnej z przesłanek legalności przetwarzania danych wrażliwych, o których mowa w art. 27 ustawy. W związku z powyższym Generalny Inspektor w wydanej decyzji administracyjnej nakazał szpitalowi zaprzestanie sporządzania historii chorób stażystom i usunięcie takich danych ze zbioru danych studentów odbywających studenckie praktyki zawodowe.²³⁰

Przedmiotem skarg była ponadto zasadność udostępnienia przez poradnie opinii dotyczących stanu zdrowia uczniów pobierających naukę w danej placówce takim podmiotom, jak szkoły.²³¹ Dyrektorzy szkół wyjaśniali, iż zarządzane przez nich placówki, w celu uzyskania diagnozy oraz określenia odpowiednich form kształcenia i opieki nad uczniem, niejednokrotnie są zobowiązane do uzyskania opinii psychologiczno – pedagogicznej. Zgodnie z § 5 rozporządzenia Ministra Edukacji Narodowej z dnia 11 czerwca 1993 r. w sprawie organizacji i zasad działania publicznych poradni psychologiczno – pedagogicznych oraz innych publicznych poradni specjalistycznych (Dz. U. Nr 67, poz. 322) dzieci z odchyleniami i zaburzeniami rozwojowymi oraz dzieci z zaburzeniami zachowania, wobec których stosowane przez nauczyciela różne formy opieki i pomocy nie przynoszą pożądanych wyników, powinny zostać przez przedszkole, szkołę lub placówkę skierowane do poradni psychologiczno – pedagogicznej celem uzyskania diagnozy oraz określenia odpowiednich form terapii, kształcenia i opieki. Ponadto zgodnie z § 3 ust. 1 zarządzenia nr 15 Ministra Edukacji Narodowej z dnia 25 maja 1993 r. (Dz. U. MEN 93.6.19) w sprawie zasad udzielania uczniom pomocy psychologicznej i pedagogicznej, pomoc psychologiczna i pedagogiczna jest udzielana na wniosek ucznia, nauczyciela, pedagoga, psychologa, rodziców (opiekunów prawnych) lub innych osób. Powyższa pomoc może być organizowana w szkole w formie zajęć dydaktyczno – wyrównawczych, zajęć specjalistycznych, klas wyrównawczych, terapeutycznych i świetlic terapeutycznych. Jednocześnie § 11 ww. zarządzenia określa zasady udzielania m.in. przez pedagoga lub psychologa szkolnego, pomocy swoim uczniom, we współpracy z poradniami psychologiczno – pedagogicznymi i innymi poradniami specjalistycznymi w zakresie metod i form pomocy udzielanej uczniom oraz w zakresie specjalistycznej diagnozy w indywidualnych przypadkach jak również we współpracy z nauczycielami, rodzicami, pielęgniarką, organami szkoły i instytucjami pozaszkolnymi. Generalny Inspektor informował administratorów danych zawartych w opiniach wydawanych przez poradnie psychologiczne o konieczności zabezpieczenia takiej

²³⁰ GI-DEC-DP-92/00

²³¹ GI-DIS-184/00/1081

dokumentacji oraz o możliwości jej udostępnienia jedynie podmiotom do tego uprawnionym na podstawie przepisów prawa.²³²

Nie narusza ustawy o ochronie danych osobowych udostępnienie dokumentacji medycznej przez inspektora sanitarnego podmiotom, o których mowa w art. 18 ust. 3 ustawy o zakładach opieki zdrowotnej.²³³ Zgodnie z art. 15 ustawy z dnia 14 marca 1985 r. o Inspekcji Sanitarnej (Dz. U. z 1998 r. Nr 90, poz. 575 z późn. zm.) inspektor sanitarny wykonuje zadania przy pomocy podległej mu stacji sanitarno – epidemiologicznej będącej zakładem opieki zdrowotnej. Dokumentacja medyczna może być przez inspektora sanitarnego udostępniona także szkole wyższej lub jednostce badawczo- rozwojowej do wykorzystania dla celów naukowych, bez ujawniania nazwiska i innych danych umożliwiających identyfikację osoby, której dokumentacja dotyczy. Zgodnie z art. 40 ust. 2 pkt 7 ustawy o zawodzie lekarza, z obowiązku zachowania tajemnicy lekarz jest zwolniony, jeżeli jest to niezbędne dla celów naukowych. Generalny Inspektor podkreślał przy tym, iż ujawnienie tajemnicy lekarskiej może nastąpić tylko w ściśle określonym zakresie.²³⁴

Do Biura Generalnego Inspektora wpływały ponadto pytania fundacji, odnoszące się do *legalności udostępniania danych o stanie zdrowia dla celów naukowych, na wniosek różnych placówek badawczych*.²³⁵ Jak wynika z treści art. 26 ust. 1 pkt 2 ustawy o ochronie danych osobowych administrator danych jest zobowiązany zapewnić, aby dane były przetwarzane zgodnie z celami, dla których zostały zebrane. Odstępstwo od powyższej zasady możliwe jest w sytuacji określonej w art. 26 ust. 2 pkt 1 i 2 ww. ustawy, tj. jeżeli nie naruszy to praw i wolności osoby, której dane dotyczą oraz następuje w celach badań naukowych, dydaktycznych, historycznych lub statystycznych oraz z zachowaniem przepisów art. 23 i art. 25 (z możliwością odstąpienia od obowiązku informacyjnego w przypadkach określonych w art. 25 ust. 2 ustawy). W związku z powyższym, a także mając na uwadze przepisy ustawy o zakładach opieki zdrowotnej i zawodzie lekarza, Generalny Inspektor stanął na stanowisku, iż przetwarzanie danych o stanie zdrowia i ich udostępnianie, np. uczelniom medycznym,²³⁶ będzie zgodne z ustawą o ochronie danych osobowych, jeżeli dane te zbierane są bezpośrednio od osób zgłaszających się do fundacji, osoby te wyrażą zgodę na przetwarzanie ich danych przez fundację, a wskazane dane będą przekazywane akademii medycznej wyłącznie dla celów badań naukowych. Jak wywodziły niektóre fundacje, od udostępnienia

²³² GI-DIS-184/00/1082

²³³ GI-DP-340/00/369

²³⁴ Ibidem

²³⁵ GI-DP-09/00/663, GI-DP-435/00/816

²³⁶ Ibidem

danych (np. o stopniu niepełnosprawności dzieci biorących udział w programie wymiany polsko – ukraińskiej w 1999 i 2000 r.) niejednokrotnie uzależniona była kwestia przekazania fundacji środków finansowych od określonych organów rządowych.²³⁷ W myśl art. 71 ustawy z dnia 26 listopada 1998 r. o finansach publicznych (Dz. U. Nr 155, poz. 1014 z późn. zm.) jednostki nie zaliczone do sektora finansów publicznych, w tym fundacje i stowarzyszenia mogą otrzymywać dotacje celowe na realizację zadań zleconych, na podstawie umów zawartych z dysponentem części budżetowej. Umowa taka powinna określać m.in. tryb kontroli wykonywania zadania oraz sposób rozliczenia udzielonej dotacji celowej i zasady zwrotu niewykorzystanej części dotacji. Z przepisu tego nie wynika jednak uprawnienie do przetwarzania danych o stanie zdrowia bez zgody osoby, której dane dotyczą. Pisemna zgoda osoby, której dane dotyczą (lub jej przedstawiciela ustawowego) jest w tej sytuacji jedyną przesłanką uzasadniającą przetwarzanie danych o stopniu niepełnosprawności.²³⁸ Zgoda osób, których dane dotyczą powinna być wyraźna, a w szczególności nie może być domniemana z oświadczenia woli innej treści.²³⁹ Jednocześnie Generalny Inspektor zauważył, iż w przypadku zbierania danych o osobach niepełnosprawnych, które mają dotyczyć wyłącznie ilości, wieku i płci tych osób, rodzaju i stopnia ich niepełnosprawności oraz posiadania lub braku pracy, dane te nie pozwalają na określenie tożsamości konkretnej osoby albowiem charakteryzują jedynie grupę osób traktowanych jako całość. Bez dodania imion i nazwisk, adresów lub innych danych identyfikujących poszczególne osoby, informacje te nie mogą być uznane za dane osobowe w rozumieniu ustawy o ochronie danych osobowych. W związku z powyższym zbieranie przez określony podmiot danych o osobach niepełnosprawnych, wyłącznie w celach statystycznych, we wskazanym zakresie nie podlega rygorom ustawy o ochronie danych osobowych.²⁴⁰

Odrębna kategoria spraw, które wpływały do Biura Generalnego Inspektora związana była z udostępnianiem danych osobowych pacjentów na żądanie pracodawców. W związku z faktem, iż zakłady pracy zwróciły się do zakładów opieki zdrowotnej o udostępnienie informacji związanych z przebiegiem leczenia ich pracowników oraz rodzajem przeprowadzonych badań, zakłady opieki zdrowotnej wielokrotnie zwracały się do Generalnego Inspektora o zajęcie stanowiska w kwestii legalności i ewentualnego zakresu udostępnienia przedmiotowych danych.²⁴¹

²³⁷ GI-DP-737/00/1044

²³⁸ Por. 843/00/1133 lub GI-DP-99/00/154.

²³⁹ Stosownie do definicji zgody, o której mowa w art. 7 pkt 5 ustawy o ochronie danych osobowych

²⁴⁰ Zob. GI-DP-625/00/830

²⁴¹ GI-DP-912/00/1348

Generalny Inspektor poinformował, iż podstawą do zlecenia ZOZ-om przez zakłady pracy przeprowadzania wstępnych i okresowych badań lekarskich są przepisy Kodeksu pracy. Na ich podstawie pracodawca nie może dopuścić pracownika do pracy bez aktualnego orzeczenia lekarskiego stwierdzającego brak przeciwwskazań do pracy na określonym stanowisku. Natomiast w myśl art. 229 Kodeksu pracy, pracodawca zobowiązany jest przechowywać orzeczenia wydane na podstawie badań lekarskich. Zgodnie z rozporządzeniem Ministra Zdrowia i Opieki Społecznej z dnia 30 maja 1996 r. w sprawie przeprowadzenia badań lekarskich pracowników, zakresu profilaktycznej opieki zdrowotnej nad pracownikami oraz orzeczeń lekarskich wydawanych do celów przewidzianych w Kodeksie pracy (Dz. U. Nr 69, poz. 332 z późn. zm.), badanie profilaktyczne kończy się orzeczeniem lekarskim stwierdzającym brak przeciwwskazań do pracy na określonym stanowisku. Stosownie do § 3 ust. 4 rozporządzenia, orzeczenia lekarskie są wydawane w formie zaświadczeń, których wzory, w zależności od rozpoznania, określają załączniki 1 i 2 do powyższego aktu prawnego. Zaświadczenie takie powinno zawierać: pieczęć zakładu opieki zdrowotnej, dane pracownika w postaci imienia, nazwiska, daty urodzenia, zakład i stanowisko pracy, informację o braku przeciwwskazań do pracy na danym stanowisku lub ich wskazanie, a także datę następnego badania. W ocenie Generalnego Inspektora nie istnieje podstawa prawna do ujawniania zakładowi pracy zestawień nazwisk z rodzajem przeprowadzonych badań profilaktycznych. Dysponując cennikiem i określeniem rodzaju badania, jakie powinno być przeprowadzone u danego pracownika, zakłady pracy są w stanie określić wysokość przewidywanych z tego tytułu kosztów. Zaświadczenie przedstawiane zakładom pracy, w opinii Generalnego Inspektora, mogłoby zawierać informacje o ilości danego rodzaju badań przeprowadzonych u określonej liczby osób oraz o kosztach jednostkowego badania. Odnośnie informacji związanych ze stanem zdrowia pracownika, nie zebranych w związku z badaniami profilaktycznymi bądź okresowymi, Generalny Inspektor zauważył, iż jedyną przesłanką uprawniającą pracodawcę do przetwarzania takich danych jest zgoda osób, których dane dotyczą.²⁴²

W jednym z pism, pracodawca – ZOZ – zwrócił się do Generalnego Inspektora Ochrony Danych Osobowych o udzielenie informacji odnośnie legalności udostępnienia danych dotyczących pracowników zatrudnionych w ZOZ-ie firmie zajmującej się dystrybucją informacji medycznych.²⁴³ Generalny Inspektor stwierdził, iż dane osobowe lekarzy pracujących w ZOZ-ie zostały zebrane wyłącznie dla celów związanych z wykonywaniem

²⁴² Szerzej zob. GI-DP-912/001348

umowy o pracę i w związku z tym przekazanie innemu podmiotowi danych osobowych dla celów innych niż ten, dla którego zostały zebrane, jest dopuszczalne jedynie po uzyskaniu zgody osób, których dane dotyczą. Nie wymaga natomiast zgody pracownika udostępnianie jego danych pracowników przez pracodawcę podmiotowi, z którym zakład pracy związany jest umową o świadczenie usług medycznych.²⁴⁴

Generalnemu Inspektorowi Ochrony Danych Osobowych wielokrotnie również sygnalizowano niewłaściwe zabezpieczenie zbiorów zawierających dane o stanie zdrowia. Uznając potrzebę należytego zabezpieczenia wszystkich kategorii danych osobowych, a szczególnie danych o stanie zdrowia, należących do kategorii szczególnie chronionych, Generalny Inspektor wnikliwie rozpatrywał każdą skargę, zwracał się do organów ścigania o przekazanie wszelkich informacji mogących mieć wpływ na ocenę zasadności skargi, jak również o poinformowanie o sposobie zakończenia prowadzonego przez te organy postępowania.²⁴⁵

Zgodnie z art. 52 ustawy o ochronie danych osobowych, kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku. Jak wynikało z doniesień mediów, jedna z firm medyczno - farmaceutycznych umieściła na pobliskim wysypisku śmieci karty szczepień swoich pacjentów zawierające m.in. imię, nazwisko, adres zamieszkania, podpis oraz informacje dotyczące stanu zdrowia pacjenta. Przeprowadzona w siedzibie firmy kontrola potwierdziła powyższe informacje, w związku z czym, po przeprowadzeniu postępowania administracyjnego, Generalny Inspektor Ochrony Danych Osobowych wydał decyzję administracyjną nakazującą usunięcie uchybień w procesie przetwarzania danych.²⁴⁶ Ponadto, kierując się dyspozycją art. 19 ustawy o ochronie danych osobowych, Generalny Inspektor skierował do prokuratury zawiadomienie o popełnieniu przestępstwa.²⁴⁷

Administrator danych o stanie zdrowia powinien dołożyć szczególnej staranności, aby dane znajdujące się w jego posiadaniu były należycie chronione. Wprawdzie ustawa nie określiła rodzaju środków technicznych i organizacyjnych, które administrator winien zastosować w celu należytego wywiązania się z obowiązku, o którym mowa w art. 36 ustawy,

²⁴³ GI-DP-1158/001588

²⁴⁴ GI-DP-759/00/916

²⁴⁵ GI-DIS-138/00/739, GI-DIS-18/00/300

²⁴⁶ Decyzja z dnia 2 czerwca 2000 r. (sygn. GI-DEC-DP-32/00). Po wniesieniu odwołania przez stronę, Generalny Inspektor Ochrony Danych Osobowych utrzymał decyzję w mocy (GI-DEC-DP-51/00).

²⁴⁷ Pismo z dnia 13 stycznia 2000 r. (GI-DIS-K-1/00, zawiadomienie 3/2000)

pozostawiając tę kwestię do uznania administratorowi danych, nie mniej jednak z treści przepisów ustawy wynika, że dane powinny być chronione rzetelnie i skutecznie, tzn. w sposób zapobiegający nie tylko samemu udostępnieniu ich osobie nieupoważnionej, ale i możliwości powstania takiej sytuacji, której skutkiem będzie przedmiotowe udostępnienie. Z treści wielu pism, które wpłynęły do Biura Generalnego Inspektora w 2000 roku wynika, że przyczyną niewłaściwego zabezpieczenia danych o stanie zdrowia była lekkomyślność i niedbalstwo administratorów danych (najczęściej lekarzy prowadzących prywatną praktykę), polegające, np. na udostępnieniu danych osobom, które nie wykazały podstaw prawnych do przetwarzania danych.²⁴⁸ W takich sytuacjach Generalny Inspektor niezwłocznie zawiadamiano prokuraturę o naruszeniu ustawy o ochronie danych osobowych.²⁴⁹ Należy zauważyć, iż reakcją prokuratury na ww. zawiadomienia, podobnie jak w większości postępowań wszczętych na wniosek Generalnego Inspektora, było umorzenie postępowania bądź ze względu na znikomy stopień społecznej szkodliwości czynu, bądź na brak znamion czynu zabronionego. W związku z powyższym GODO zwracał się o podjęcie postępowań bezpośrednio do Prokuratora Generalnego RP, który najczęściej przychylił się do argumentacji Generalnego Inspektora i zobowiązywał właściwe organy do ponownego rozpatrzenia sprawy.

Analiza pytań i skarg, jakie wpłynęły do Generalnego Inspektora w omawianym okresie sprawozdawczym pozwoliła na stwierdzenie, iż przepisy dotyczące ochrony danych osobowych w służbie zdrowia nie są spójne. Niektóre uregulowania dają szeroki dostęp do informacji o pacjencie, a inne nadmiernie go zawężają. Przykładem może być ustawa o powszechnym ubezpieczeniu zdrowotnym, która nakazuje przekazywać znacznie więcej danych do ubezpieczenia, niż zezwala gromadzić Kasom Chorych. Brakuje ponadto aktów wykonawczych do tej ustawy, m.in. rozporządzenia dotyczącego wykazu dokumentacji medycznej. Przeprowadzane przez Generalnego Inspektora kontrole w kilku Regionalnych Kasach Chorych ujawniły, iż zakres danych wymaganych od świadczeniodawców wykracza poza zakres określony przepisami prawa, a informacje o pacjentach zawarte w zbiorach Kas nie są należycie zabezpieczone. Wiele z kontrolowanych publicznych i niepublicznych zakładów opieki zdrowotnej nie dopełniło spoczywającego na nich, z mocy art. 24 i 25 ustawy o ochronie danych osobowych, obowiązku informacyjnego.²⁵⁰ W związku z powyższym Generalny Inspektor zwracał się do jednostek kontrolowanych o złożenie

²⁴⁸ Np. GI-DP-164/00/2220, GI-DIS-452/853/00

²⁴⁹ Ibidem, zaw. 36/00, zaw. 19/00

²⁵⁰ Np. DIS-K-28/00, DIS-K-29/00,

wyjaśnień w zakresie stwierdzonych uchybień i przesłanie materiałów potwierdzających ich usunięcie. Sprawy są w toku.²⁵¹

III. Inne sprawy

W omawianym okresie sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych badał ponadto zasadność *żądania przez okręgową radę adwokacką dokumentacji lekarskiej byłego aplikanta adwokackiego*.²⁵² Analiza art. 4 c ust. 2 ustawy z dnia 26 maja 1982 r. Prawo o adwokaturze (Dz. U. Nr 16, poz. 124 z późn. zm.) prowadzi do stwierdzenia, iż okręgowa rada adwokacka jest uprawniona jedynie do zaznajomienia się z opiniami lub orzeczeniami lekarskimi. Z uwagi na to, że dokumentacja medyczna zawiera dane wykraczające poza ten zakres (np. historia choroby), żądanie okręgowej rady adwokackiej nie znajduje uzasadnienia w przepisach prawa.

F. PRZETWARZANIE DANYCH OSOBOWYCH PRZEZ SPÓŁDZIELNIE I WSPÓLNOTY MIESZKANIOWE

W roku 2000 zanotowano wzrost skarg dotyczących przetwarzania danych osobowych przez spółdzielnie oraz wspólnoty mieszkaniowe (90 skarg i pytań prawnych). Podobnie jak w latach ubiegłych, w omawianym okresie sprawozdawczym najczęściej wątpliwości wywoływał zakres przetwarzania danych członków spółdzielni i udostępnienie danych osobom nieupoważnionym. Obawy skarżących budziło również niewłaściwe zabezpieczenie danych znajdujących się w zasobach spółdzielni i wspólnot mieszkaniowych.

Największa grupa skarg dotyczyła kwestii zasadności umieszczania na klatkach schodowych, spisach lokatorów i domofonach danych osobowych członków spółdzielni zawierających m.in. imię, nazwisko i numer mieszkania.²⁵³ Skarżących informowano, iż zamieszczanie przedmiotowych danych we wskazanych miejscach jest przetwarzaniem danych, stosownie do definicji przetwarzania danych o której mowa w art. 7 pkt 2 ustawy o ochronie danych osobowych. Dopuszczalność przetwarzania uwarunkowana jest spełnieniem jednej z przesłanek określonych w art. 23 ust. 1 ustawy. Przesłanką taką może być szczególnie przepis prawa zezwalający na przetwarzanie danych (art. 23 ust. 1 pkt 2) albo

²⁵¹ Np. DIS-K-60/00, DIS-K-64/00, DIS-K-68/00, DIS-K-69/00

²⁵² GI-DP-598/00/602

²⁵³ GI-DP-28/00/70, GI-DP-663/00/704, GI-DP-906/00/1212

zgoda osoby, której dane dotyczą (art. 23 ust. 1 pkt 1). Ponieważ żaden z przepisów ustawy z dnia 16 września 1982 r. Prawo spółdzielcze (Dz. U. z 1995 r., Nr 54, poz. 288 z późn. zm.), jak również ustawy z dnia 15 grudnia 2000 r. o spółdzielniach mieszkaniowych (Dz. U. z 2001 r. Nr 4, poz. 27 z późn. zm.) nie reguluje kwestii upubliczniania list lokatorów, Generalny Inspektor wskazywał, iż działanie spółdzielni powinno opierać się o przesłankę wyrażoną w art. 23 ust. 1 pkt 1 ustawy, tj. zgodę osoby, której dane dotyczą, chyba że chodzi o usunięcie dotyczących ją danych. Definicję zgody zawiera przepis art. 7 pkt 5 ustawy, określając ją jako oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie, nie może być ona jednak domniemana ani dorozumiana. Oznacza to, że istnienia zgody nie można wywnioskować z innych faktów niż wyraźne, niewątpliwe w swojej treści, oświadczenie woli osoby, której dane osobowe mają być przetwarzane. Oznacza to również, iż zgody nie można domniemywać z milczenia osoby zainteresowanej lub braku pisemnego zastrzeżenia dotyczącego przetwarzania jej danych. Przepis art. 23 wymaga, aby zgoda była wyraźna, nie wymaga natomiast formy pisemnej. Wymóg formy pisemnej wyrażenia zgody określony jest przy przetwarzaniu szczególnej kategorii danych, tj. danych wrażliwych, do których nie zaliczają się takie dane jak imię, nazwisko i adres zamieszkania lokatorów.²⁵⁴ Zgodnie z powyższym, jeżeli lokatorzy nie wyrazili rzeczowej zgody, brak podstaw ku temu, aby wymienione dane figurowały na tablicy ogłoszeń i administrator danych powinien je niezwłocznie usunąć. Informowano ponadto, iż ustawa o ochronie danych osobowych nie reguluje ani problematyki ponoszenia kosztów umieszczania lub usunięcia danych z tablic ogłoszeniowych i z uwagi na fakt, że obowiązki wynikające z ustawy spoczywają na administratorze danych uznać należy, że w tym zakresie przedmiotowe działania obciążają spółdzielnie.²⁵⁵

Podobne stanowisko Generalny Inspektor zajął w sprawie legalności ujawniania przez spółdzielnie list spółdzielców zadłużonych.²⁵⁶ Żaden z przepisów prawa spółdzielczego nie zezwala na ujawnianie list osób zadłużonych w spółdzielni na klatkach schodowych, w wydawanych biuletynach,²⁵⁷ czy na zgromadzeniu walnym członków spółdzielni.²⁵⁸ Również w tym przypadku wobec braku stosownych regulacji w prawie spółdzielczym, zastosowanie znajduje przesłanka wskazana w art. 23 ust. 1 pkt 1 ustawy o ochronie danych osobowych, tj.

²⁵⁴ GI-DP-663/00/704

²⁵⁵ GI-DP-28/00/70

²⁵⁶ GI-DP-38/00/166, GI-DP-169/00/257

²⁵⁷ GI-DP-1049/00/1586

²⁵⁸ GI-DP-900/00/1273, GI-DP-892/00/2377

zgoda osoby, której dane dotyczą. Jak wynika z utrwalonego orzecznictwa, informacja o zadłużeniu z tytułu zalegania z płatnością czynszu należy do sfery prywatności i podlega ochronie na podstawie przepisów o ochronie dóbr osobistych. Zagadnienia tego dotyczy wyrok Sądu Apelacyjnego w Białymstoku z dnia 14 czerwca 1995 r. (I ACr 143/95), jak również wyrok Sądu Apelacyjnego w Krakowie z dnia 17 listopada 1995 r. (I ACr 559/95), które w swoich sentencjach uznały, iż opublikowanie przez spółdzielnię mieszkaniową informacji o stanie zadłużenia jej członków jest działaniem bezprawnym, naruszającym ich dobro osobiste w postaci prawa do prywatności (art. 23 K.c.). Wobec braku zgody na ujawnienie stanu zadłużenia osobom trzecim administracja budynków mieszkalnych powinna niezwłocznie usunąć jej dane z listy lokatorów zadłużonych. Zapytujących ponadto informowano o możliwości dochodzenia ewentualnych roszczeń na drodze cywilnego postępowania sądowego.²⁵⁹

Odnosząc się do kwestii upublicznienia samego adresu zamieszkania i wysokości zaległości czynszowej (lub innej sytuacji prawnej) określonego dłużnika Generalny Inspektor zauważył, iż w świetle art. 6 ustawy o ochronie danych osobowych, za dane osobowe uważa się każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby. Wskazane zaś wyżej informacje nie pozwalają na ustalenie, kto jest lokatorem w danym mieszkaniu, ani kto faktycznie w lokalu zamieszkuje, a zatem nie stanowią w rozumieniu ustawy danych osobowych.²⁶⁰ Nie narusza ustawy, z tych samych względów prawnych, publikowanie przez spółdzielnię zbiorczych danych statystycznych o zadłużeniu bloku.²⁶¹

Rozpatrując zagadnienie ujawniania list dłużników Generalny Inspektor zwrócił uwagę, iż wobec braku podstawy prawnej upoważniającej spółdzielnię do upowszechniania danych jej dłużników dochodzi do kolizji interesu dłużnika, który nie partycypuje w kosztach utrzymania spółdzielni i który nie wyraża zgody na ujawnienie swoich danych osobowych, z interesem pozostałych członków spółdzielni, którzy ponoszą koszty za nie płacących. Interesy obu stron powinny być wyważone, dlatego też sygnalizowano właściwym organom potrzebę nowelizacji dotychczas obowiązującego prawa spółdzielczego, poprzez umieszczenie stosownego zapisu regulującego kwestię upubliczniania informacji o zadłużeniu, jeśli podawanie takich informacji jest niezbędne dla zabezpieczenia interesów spółdzielni.²⁶²

²⁵⁹ GI-DP-424/00/460, GI-DP-634/00/962, GI-DP-1038/00/1270

²⁶⁰ GI-DP-320/00/616, GI-DP-024/1636/00, GI-DP-024/1827/00

²⁶¹ GI-DP-024/1523/00

²⁶² GI-DP-892/00/2377, GI-DP-900/00

Wątpliwości wzbudzała również praktyka spółdzielni polegająca na wywieszaniu odpisów uchwał podjętych przez organy spółdzielni w budynku biura spółdzielni i innych budynkach mieszkalnych dotyczących, np. informacji o wykluczeniu danego członka spółdzielni.²⁶³ Przy rozpatrywaniu przedmiotowego zagadnienia zauważono, iż w sytuacji, gdy uchwały organów spółdzielni nie będą zawierać danych osobowych, będą obojętne z punktu widzenia ustawy o ochronie danych osobowych, która nie chroni informacji nie spełniających wymogów definicji danych osobowych z art. 6 ustawy. Zgodnie z przepisami prawa spółdzielczego uchwały są jawne dla członków spółdzielni. Jeżeli członek spółdzielni zostanie wykluczony uchwałą walnego zgromadzenia, to również ta uchwała i protokół z obrad danego organu są jawne. W świetle regulacji art. 30 Prawa spółdzielczego, członkowie spółdzielni mają prawo mieć dostęp do informacji o tym, kto jest członkiem spółdzielni, a kto został z niej wykluczony. Z treści przepisów prawa spółdzielczego nie wynika jednak, że przedmiotowe informacje mogą być udostępniane publicznie, np. poprzez wywieszenie w miejscach publicznie dostępnych. Działanie takie należałoby uznać za sprzeczne z ustawą o ochronie danych, tym bardziej, że poprzez wskazane działanie spółdzielnia nie tylko narusza przepisy ustawy o dopuszczalności przetwarzania danych, ale stwarza również możliwość zapoznania się z danymi swoich członków także innym osobom nie będącym spółdzielcami (art. 36 ustawy).²⁶⁴ Generalny Inspektor nie rozpatrywał przy tym legalności podejmowanych przez organy spółdzielni uchwał, statutów i regulaminów wewnętrznych, odsyłając w tym zakresie do organów właściwych do ich rozpatrzenia.²⁶⁵

Zupełnie odmiennie kształtuje się sytuacja dotycząca zasadności i zakresu udostępnienia danych o właścicielach lokali, stanie ich zadłużenia i udziałach w tzw. wspólnocie mieszkaniowej pozostałym członkom tej wspólnoty.²⁶⁶ Do wspólnot mieszkaniowych tworzonych na podstawie ustawy z dnia 24 czerwca 1994 r. o własności lokali (Dz. U. Nr 85, poz. 388 z późn. zm.) stosuje się, w zakresie nieuregulowanym w tej ustawie, przepisy ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. Nr 16, poz. 93 z późn. zm.), zwanego dalej K.c. Z przepisów Księgi Drugiej Tytułu I Działu IV Kodeksu cywilnego wynika, iż współwłaściciele dla prawidłowego zarządzania współwłasnością, muszą znać dane osobowe pozostałych współwłaścicieli. W związku z tym, nie wydaje się, aby udostępnienie danych członków wspólnoty pozostałym jej członkom było

²⁶³ GI-DP-730/00/1137

²⁶⁴ GI-DP-730/00/1137

²⁶⁵ Ibidem, GI-DP-644/00/797

²⁶⁶ GI-DP-830/00/1176, GI-DP-1150/00/1395

niedopuszczalne, tym bardziej, iż jest ono racjonalnie uzasadnione koniecznością zarządzania wspólną nieruchomością i prawem do kontroli nad zarządcą nieruchomości wspólnej, wynikającego w tym wypadku także z art. 29 ust. 3 ustawy o własności lokali. Ponadto z art. 16 ust. 1 tej ustawy wynika, że jeżeli właściciel lokalu zalega długotrwale z zapłatą należnych od niego opłat lub wykracza w sposób rażący lub uporczywy przeciwko obowiązującemu porządkowi domowemu albo przez swoje niewłaściwe zachowanie czyni korzystanie z innych lokali lub nieruchomości wspólnej uciążliwym, wspólnota mieszkaniowa może w trybie procesu żądać sprzedaży lokalu w drodze licytacji na podstawie przepisów kodeksu postępowania cywilnego o egzekucji z nieruchomości. Skorzystanie z tego uprawnienia przez wspólnotę wymaga znajomości danych osobowych współwłaściciela, która może być niezbędna do ustalenia, np. większości udziałów we współwłasności, odwołania zarządcy i innych wynikających z przepisów czynności wymagających współpracy współwłaścicieli. Generalny Inspektor podkreślał, iż zakres danych udostępnianych współwłaścicielom powinien być adekwatny do ich potrzeb związanych z przewidzianym przez przepisy celem udostępnienia. Nie jest więc dopuszczalne udostępnienie danych, których przetwarzanie nie jest niezbędne do realizacji kontroli nad administratorem budynku lub realizacji uprawnienia, o którym mowa w art. 16 ustawy o własności lokali.²⁶⁷ W udzielanych odpowiedziach prawnych zaznaczano, iż unormowania wynikające z ustawy o własności lokali oraz ustawy Kodeks cywilny, stanowią wyjątek od obowiązującej reguły zakazu udostępniania danych osobowych o członkach danej wspólnoty. Powyższe akty prawne przewidują zarówno prawo innych podmiotów do przetwarzania przedmiotowych danych, jak i prawo poszczególnych członków wspólnoty do pozyskania danych innych członków znajdujących się w tym samym zbiorze danych osobowych.²⁶⁸ W związku z tym udostępnienie informacji o zaległościach w opłatach ponoszonych przez mieszkańców, związanych z kosztami utrzymania nieruchomości wspólnej, zalegających z opłatami uznawano za znajdujące oparcie w przesłance określonej w art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych. W świetle przywołanych przepisów, w sytuacji, gdy współwłaścicielem (członkiem wspólnoty) jest gmina, nie zaś osoby, które wynajmują lokale od gminy, właściciele zrzeszeni we wspólnocie mogą uzyskać jedynie informację ogólną o fakcie zajmowania określonych lokali przez lokatorów gminnych. Obowiązku udzielania przedmiotowej informacji wspólnocie nie mają także prywatni właściciele lokali, którzy swoje mieszkania odnajmują na wolnym rynku.²⁶⁹ Za

²⁶⁷ GI-DP-146/00/310

²⁶⁸ GI-DP-1034/00/1307, GI-DP-024-1252/00

²⁶⁹ GI-DP-1057/00/1357

obojętne z punktu widzenia ustawy o ochronie danych osobowych uznawano natomiast udostępnianie rozliczenia kosztów utrzymania nieruchomości wspólnej bez odniesienia do danych osobowych poszczególnych współwłaścicieli (wobec braku spełnienia wymogów określonych w art. 6 ustawy).²⁷⁰

Indywidualne pytania odnosiły się do oceny w świetle ustawy o ochronie danych osobowych legalności działań zarządu wspólnoty mieszkaniowej, np. przekazywania danych o członkach wspólnoty w ramach realizacji umowy zawartej przez zarząd z firmą zajmującą się ochroną mienia, w sytuacji, gdy część członków wspólnoty nie wyraziła zgody na przetwarzanie ich danych.²⁷¹ Dokonując analizy prawnej przedstawionej sytuacji Generalny Inspektor nie dopatrywał się naruszenia przepisów ustawy o ochronie danych osobowych. Wspólnota mieszkaniowa może nabywać prawa i zaciągać zobowiązania, pozywać i być pozywana. Tworzy ją ogół właścicieli, których lokale wchodzą w skład określonej nieruchomości (art. 6 ustawy o własności lokali). W sytuacji, gdy zarząd wspólnoty zawarł umowę, dotyczy ona wszystkich członków wspólnoty, którzy są stronami tej umowy. W związku z tym, druga strona umowy uprawniona jest do przetwarzania danych swoich kontrahentów w ramach realizacji stosunku umownego, spełniając tym samym przesłankę określoną w art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych.

Z kwestią udostępniania danych o właścicielach wspólnoty związane było również pytanie, czy pisemne ponaglenia do właścicieli zadłużonych we wspólnocie mogą być dostarczane, np. przez członka zarządu wspólnoty.²⁷² Generalny Inspektor stanął na stanowisku, iż członek zarządu działając w imieniu wspólnoty mieszkaniowej jest osobą uprawnioną do przetwarzania danych. Przy doręczaniu upomnień osobom nie wywiązującym się z obowiązku uiszczania opłat administrator danych powinien jednak zadbać o to, aby upomnienia te nie zostały udostępnione osobom nieupoważnionym.²⁷³

Odrębna grupa zagadnień rozpatrywanych w omawianym okresie sprawozdawczym związana była z badaniem zasadności odmawiania spółdzielcom prawa wglądu do rejestru członków spółdzielni z powoływaniem się przez zarządy spółdzielni mieszkaniowych na ustawę o ochronie danych osobowych. Stanowiska powyższego nie podzielono, albowiem pozostawało ono w sprzeczności z obowiązującymi przepisami prawa spółdzielczego. Zgodnie z art. 30 ustawy Prawo spółdzielcze, zarząd spółdzielni prowadzi rejestr członków

²⁷⁰ GI-DP-1162/00/1734

²⁷¹ GI-DP-877/00/1085

²⁷² GI-DP-674/00/1328

²⁷³ Ibidem

zawierający ich imiona i nazwiska oraz miejsce zamieszkania (w odniesieniu do członków będących osobami prawnymi – ich nazwę i siedzibę), wysokość zadeklarowanych i wniesionych udziałów, wysokość wniesionych wkładów, ich rodzaj, jeżeli są to wkłady niepieniężne, zmiany tych danych, datę przyjęcia w poczet członków, datę wypowiedzenia członkostwa i jego ustania, a także inne dane przewidziane w statucie. Członek spółdzielni, jego małżonek i wierzyciel członka lub spółdzielni, ma prawo przeglądać rejestr. Z przepisu art. 30 Prawa spółdzielczego wynika zatem, iż dane zawarte w rejestrze członków spółdzielni są jawne dla spółdzielców i zarząd nie może odmówić ich udostępnienia z powoływaniem się na ustawę o ochronie danych osobowych. W świetle przywołanego przepisu spółdzielnia nie może również odmówić udostępnienia danych osobowych członka spółdzielni jego wierzycielom, jako podmiotom upoważnionym do wglądu w rejestr członków spółdzielni.²⁷⁴ Generalny Inspektor wielokrotnie przy tym podkreślał, iż ustawa o ochronie danych osobowych nie może służyć jako usprawiedliwienie nie wypełnienia obowiązków nałożonych przez inne przepisy prawne.²⁷⁵ Postanowienia ustawy o ochronie danych nie uzasadniają odmowy udostępnienia danych z rejestru. Przepisy prawa spółdzielczego są w tym zakresie *lex specialis* wobec ustawy o ochronie danych osobowych. Niemniej jednak członkowie spółdzielni nie mogą poznać nazwisk osób podnajmujących mieszkania, czy też mieszkających w nich, a nie będących członkami spółdzielni lub ich małżonkami. Jeśli nawet spółdzielnia takie dane posiada, można je udostępnić tylko podmiotom upoważnionym na mocy przepisów prawa.²⁷⁶

Indywidualne pytania dotyczyły legalności udostępniania przez spółdzielnie danych osobowych jej członków takim podmiotom, jak urzędy skarbowe, w związku z toczącym się postępowaniem wyjaśniającym (np. dane o właścicielu określonej nieruchomości, wysokości opłacanego czynszu).²⁷⁷ Odmowa udostępnienia przedmiotowych informacji wynikała najczęściej z nieznamości zarówno przepisów ustawy o ochronie danych osobowych, jak i przepisów innych ustaw. Generalny Inspektor informował wówczas, że Urząd Skarbowy, jako organ podatkowy, działa w oparciu o przepisy ustawy z dnia 29 sierpnia 1997 r. Ordynacja podatkowa (Dz. U. Nr 137, poz. 926 z późn. zm.) oraz wydanych na jej podstawie przepisów wykonawczych. Zgodnie z art. 122 ww. ustawy, w toku postępowania organy podatkowe mają ustawowy obowiązek podejmować wszelkie niezbędne działania w celu

²⁷⁴ GI-DP-788/00/1542/00, GI-DP-024/1382/00

²⁷⁵ GI-DP-810/00/968, GI-DP-1319/00/1754

²⁷⁶ GI-DP-58/00/109

²⁷⁷ GI-DP-024/1453/00

dokładnego wyjaśnienia stanu faktycznego oraz załatwienia sprawy.²⁷⁸ Natomiast w myśl art. 82 § 1 Ordynacji podatkowej, osoby prawne, jednostki organizacyjne nie mające osobowości prawnej oraz osoby fizyczne prowadzące działalność gospodarczą lub wykonujące wolny zawód są obowiązane do sporządzania i przekazywania informacji na pisemne żądanie organu podatkowego – o zdarzeniach wynikających ze stosunków cywilnoprawnych albo z prawa pracy, mogących mieć wpływ na powstanie obowiązku podatkowego lub wysokość zobowiązania podatkowego osób lub jednostek. Żądania organu podatkowego znajdując zatem podstawę w przepisach prawa wyczerpują tym samym przesłankę określoną w art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych. Generalny Inspektor informował ponadto, iż dane, którymi dysponuje spółdzielnia, nie mogą być udostępniane, wbrew twierdzeniom wielu skarżących, w oparciu o przepisy art. 29 ustawy o ochronie danych osobowych.²⁷⁹ Zasady wynikające z art. 29 ustawy znajdują zastosowanie jedynie wobec podmiotów wymienionych w art. 3 ust. 1 ustawy, tj. administratorów będących organami państwowymi, organami samorządu terytorialnego, lub innymi państwowymi i komunalnymi jednostkami organizacyjnymi bądź też podmiotami niepaństwowymi realizującymi zadania publiczne. Natomiast zgodnie z art. 1 § 1 prawa spółdzielczego spółdzielnia jest dobrowolnym zrzeszeniem nieograniczonej liczby osób, o zmiennym składzie osobowym i zmiennym funduszu udziałowym, które w interesie swoich członków prowadzi wspólną działalność gospodarczą, nie jest więc podmiotem określonym w art. 3 ust. 1 ustawy o ochronie danych osobowych.²⁸⁰

Analiza skarg, które napłynęły do Biura GODO w roku 2000 wykazała, iż szczególnie często zarzucano spółdzielniom niewykonanie obowiązku informacyjnego i niewłaściwe zabezpieczenie danych osobowych ich członków. W celu ustalenia okoliczności spraw, a zwłaszcza stwierdzenia, czy naruszenie ustawy rzeczywiście miało miejsce, Generalny Inspektor przeprowadzał postępowania wyjaśniające i w sytuacji potwierdzenia stawianych zarzutów wydawał decyzje administracyjne nakazujące spółdzielniom usunięcie uchybień w procesie przetwarzania danych.

²⁷⁸ Także w wyroku NSA w Warszawie z dnia 10 marca 2000 r., sygn. III SA 474/99

²⁷⁹ Zgodnie z art. 29 ust. 1 ustawy o ochronie danych osobowych, w przypadku udostępniania danych osobowych w celach innych niż włączenie do zbioru, administrator danych, o którym mowa w art. 3 ust. 1, udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

²⁸⁰ GI-DP-1002/00/1249

Obawy budzi wciąż niska świadomość spółdzielni co do konieczności realizacji spoczywającego na nich, jako administratorze danych obowiązku informacyjnego (art. 24 ustawy o ochronie danych). Przykładem naruszenia wskazanego obowiązku było postępowanie jednej z największych warszawskich spółdzielni, która odmówiła niektórym swoim członkom prawa wglądu do ich akt członkowskich, jak również nie udzieliła wyczerpujących informacji o sposobie i zakresie przetwarzania danych zawartych w tym zbiorze, argumentując takie postępowanie prawomocnym wykluczeniem tych osób z grona członków spółdzielni. Jak wykazało postępowanie wyjaśniające, w aktach członkowskich skarżących figurowały uchwały wykluczające ich z pocztu członków spółdzielni, podjęte przez grupę nie będącą organem spółdzielni i nie posiadającą umocowania prawnego do podejmowania jakichkolwiek decyzji w imieniu spółdzielni. Wobec powyższego uznano, iż wszelkie decyzje podjęte w imieniu i na rzecz spółdzielni przez rzeczoną grupę osób nie wywarły skutków prawnych. Również Sąd Apelacyjny w Warszawie w wyroku z dnia 30 stycznia 1997 r. (sygn. akt I ACr 933/96) wskazał, iż uchwały tej grupy z punktu widzenia prawa są tzw. uchwałami nieistniejącymi. Ponieważ spółdzielnia pomimo wielokrotnych próśb skarżących nie usunęła uchybień w procesie przetwarzania ich danych, Generalny Inspektor w decyzji administracyjnej nakazał spółdzielni udzielenie skarżącym informacji o sposobie i zakresie przetwarzania dotyczących ich danych, jak również, z mocy art. 32 ust. 1 pkt 6 ustawy o ochronie danych osobowych, zażądał dokonania sprostowania przedmiotowych danych poprzez usunięcie z akt członkowskich nie mających mocy prawnej uchwał o wykluczeniu ze spółdzielni.²⁸¹ Rozstrzygnięcie Generalnego Inspektora Ochrony Danych Osobowych poparł w całości Naczelny Sąd Administracyjny, który w wyroku z dnia 25 września 2000 r. (sygn. II SA 640/00) oddalił skargę spółdzielni, zarzucającej m.in. Generalnemu Inspektorowi „(...) ingerencje w stosunki cywilnoprawne łączące spółdzielnię z jej członkami”.²⁸²

Przedmiotem analizy - pod kątem należytego wykonania obowiązku informacyjnego - była również treść ankiety rozsyłanej przez jedną z rad osiedlowych okolicznym mieszkańcom.²⁸³ Ankieta zawierała m.in. oświadczenie o zgodzie na przetwarzanie danych oraz informację o dobrowolności jej wypełniania, jak również o celu przeprowadzenia, tj. poprawy bezpieczeństwa mieszkańców osiedla. Uznając, iż podstawą przetwarzania danych będzie zgoda osób, których dane dotyczą i z uwagi na wyczerpujący zakres informacji o

²⁸¹ GI-DP-DEC-6/00, GI-DP-DEC-73/00, GI-DEC-DP-91/00

²⁸² Por. artykuł „Uchwały, których nie było” [w:] Rzeczpospolita z dnia 26 września 2000 r.

²⁸³ GI-DP-430/1874/00

przetwarzaniu danych spółdzielców, Generalny Inspektor nie stwierdził naruszenia przepisów ustawy o ochronie danych osobowych.

W wielu przysyłanych do Generalnego Inspektora pismach członkowie spółdzielni skarżyli się na niewłaściwe wykonywanie przez spółdzielnie obowiązku zabezpieczenia danych ich dotyczących.²⁸⁴ Przykładem uchybienia obowiązkowi zabezpieczenia danych spółdzielców było umieszczanie wydruków o sytuacji prawnej członka spółdzielni, w tym informacji o zaległościach czynszowych, w niezaklejonych kopertach lub bez kopert, umieszczenie takich pism w drzwiach mieszkania określonego lokatora lub wywieszenie w gablocie na klatce schodowej, doręczenia niezabezpieczonych pism poprzez dozorcę lub innego pracownika spółdzielni.²⁸⁵ Nadane spółdzielniom, na podstawie ustawy Prawo spółdzielcze i zawartych umów, prawo przetwarzania danych osobowych ich członków nie oznacza, iż dane te mogą być przetwarzane w sposób niekontrolowany. Przetwarzanie powinno się odbywać w taki sposób, aby danym zapewnić bezpieczeństwo przynajmniej w stopniu wymaganym przez przepisy o ochronie danych osobowych. Spółdzielnia (tj. administrator danych) przekazując dane jest zobowiązana, w myśl art. 36 ustawy, do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanym danym, a w szczególności powinna zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem. W sytuacji, gdy dane osobowe w imieniu pracodawcy przetwarza osoba zatrudniona przy ich przetwarzaniu lub podmiot, któremu powierzono przetwarzanie danych (np. dozorca budynku), nie można mówić o przetwarzaniu przez osoby nieupoważnione. Osoby takie, zgodnie z art. 39 ust. 2 ustawy, zobowiązane są do zachowania danych w tajemnicy, również po ustaniu zatrudnienia. Powinny zostać również zaznajomione z przepisami dotyczącymi ochrony danych osobowych, zgodnie z rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 80, poz. 521).²⁸⁶ W przypadku ujawnienia informacji osobom nieupoważnionym, osoby takie mogą być pociągnięte do odpowiedzialności karnej.²⁸⁷ W ocenie Generalnego Inspektora

²⁸⁴ GI-DP-430/1710/00

²⁸⁵ GI-DP-430/1710/00

²⁸⁶ GI-DP-39/00/762

²⁸⁷ Na mocy art. 266 § 1 kodeksu karnego, kto wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu, ujawnia lub wykorzystuje informację z którą zapoznał się w związku z pełnioną funkcją, wykonywaną

pozostawienie informacji o sytuacji prawnej członków spółdzielni (np. wezwanie do zapłaty zaległego czynszu) w drzwiach mieszkań, w niezabezpieczonej formie (bez kopert), umożliwia osobom nieupoważnionym zapoznanie się z ich treścią.²⁸⁸ Działanie takie narusza ponadto konstytucyjne zasady tajemnicy korespondencji i prawnej ochrony życia prywatnego. Stanowisko Generalnego Inspektora potwierdza również przyjęta linia orzecznictwa sądów, zgodnie z którą przesłanie dłużnikowi przez wierzyciela upomnienia do zapłaty zaległej należności w sposób umożliwiający zapoznanie się z treścią upomnienia przez inne niż adresat osoby, stanowi naruszenie dobra osobistego, jakim jest tajemnica korespondencji, podlegająca ochronie na podstawie art. 23 K.c. (wyrok Sądu Apelacyjnego w Łodzi z dnia 11 lipca 1995 r., sygn. I ACr 529/95).²⁸⁹ Generalny Inspektor nie oceniał stopnia naruszenia dóbr osobistych, odsyłając skarżących do organów właściwych do ich rozpoznania.²⁹⁰ Natomiast w sytuacji naruszenia przepisów o zabezpieczeniu danych osobowych (art. 36-39 ustawy o ochronie danych osobowych) wydawano decyzje nakazujące przywrócenie stanu zgodnego z prawem. Zwracano się ponadto do spółdzielni o wyciągnięcie konsekwencji służbowych wobec pracowników odpowiedzialnych za dokonanie naruszeń.²⁹¹

Podobnie jak w latach ubiegłych, w omawianym okresie sprawozdawczym spółdzielnie wielokrotnie zwracały się o wyjaśnienia związane z realizacją *obowiązku rejestracyjnego*.²⁹² W udzielanych odpowiedziach Generalny Inspektor zwracał uwagę na treść art. 43 ust. 1 pkt 4 ustawy o ochronie danych osobowych, na podstawie którego z obowiązku rejestracji zbioru danych zwolnieni są administratorzy danych dotyczących osób u nich zatrudnionych, zrzeszonych lub uczących się. Wyjaśniano, iż dyspozycja powyższego przepisu odnosi się do zbioru zawierającego wyłącznie dane członków spółdzielni. Jeżeli jednak zbiór zawiera dane najemców, którzy nie są członkami spółdzielni, spółdzielnia jest zobowiązana do zarejestrowania takiego zbioru.²⁹³

pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

²⁸⁸ GI-DP-1206/00/1574

²⁸⁹ Zob. GI-DP-1066/00/1289

²⁹⁰ Np. GI-DP-024/1470/00

²⁹¹ GI-DP-21/00/DIS-432/99

²⁹² GI-DP-373/00/483

²⁹³ Ibidem

G. STOSUNKI PRACY

W związku ze stosowaniem ustawy o ochronie danych osobowych Generalny Inspektor zajmował się blisko 200 sprawami związanymi z przetwarzaniem danych w ramach stosunków pracy.

Nadal najliczniejsze sprawy z tej dziedziny dotyczyły ujawnienia określonych informacji z akt osobowych pracowników, kompetencji poszczególnych podmiotów do przeprowadzania kontroli, wykorzystywania określonych informacji do prywatnych celów. Wiele spraw dotyczyło także zbyt szerokiego zakresu danych, np. gromadzenia w sposób niezgodny z prawem oświadczeń majątkowych. Zaniepokojenie Generalnego Inspektora budziły też przypadki przetwarzania przez pracodawców informacji o karalności pracowników,²⁹⁴ uzyskiwanych z Centralnego Rejestru Skazanych, co - o ile brak jest wyraźnego upoważnienia ustawowego - stanowi przestępstwo określone w art. 49 ust. 1 ustawy o ochronie danych osobowych.

Generalny Inspektor powołany został do kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych. W zakresie jego kompetencji mieści się zatem nie tylko sama ochrona danych osobowych, ale także podnoszenie świadomości prawnej obywateli. Wielokrotnie do Generalnego Inspektora Ochrony Danych Osobowych docierały sygnały o przypadkach nadinterpretacji ustawy o ochronie danych osobowych, czy wykorzystywania jej jako pretekstu mającego na celu nieudostępnienie danych osobowych.

Generalny Inspektor nadal otrzymywał pytania, czy pracownicy powinni wyrażać *pisemną zgodę na przetwarzanie ich danych osobowych*, związanych ze stosunkiem pracy oraz na *prowadzenie dokumentacji kadrowej*.²⁹⁵ Pytano także, jak należy postępować w przypadku nie wyrażenia zgody przez pracowników. Generalny Inspektor wyjaśniał, że wystarczające jest spełnienie którejkolwiek przesłanki przetwarzania danych określonej w ustawie o ochronie danych osobowych. W takich przypadkach przetwarzanie danych odbywa się na podstawie przesłanki określonej w art. 23 ust. 1 pkt 2, tj. na podstawie przepisów prawa.

Wątpliwości pojawiały się także w kwestii *wypełniania ankiet i oświadczeń majątkowych*. Pytano na przykład, na jakiej podstawie zobowiązanym do złożenia

²⁹⁴ Obecnie zagadnienie to reguluje ustawa z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz. U. Nr 50, poz. 580 z późn. zm.)

²⁹⁵ GI-DP-150/00/165

oświadczenia majątkowego jest pracownik Kasy Rolniczego Ubezpieczenia Społecznego.²⁹⁶ W odpowiedzi stwierdzono, że stosownie do art. 17 ust. 4 ustawy z dnia 16 września 1982 r. o pracownikach urzędów państwowych (Dz. U. Nr 31, poz. 214 z późn. zm.), urzędnik państwowy jest obowiązany złożyć oświadczenie o swoim stanie majątkowym przy nawiązaniu stosunku pracy oraz na żądanie kierownika urzędu, wobec czego przetwarzanie tego rodzaju danych osobowych pozostaje w zgodzie z przepisami ustawy o ochronie danych osobowych.

W myśl art. 8 ust. 1 ustawy z dnia 4 marca 1994 o zakładowym funduszu świadczeń socjalnych (Dz. U. z 1996 r. Nr 70 poz. 335 z późn. zm.) wysokość dopłat z Funduszu zależy od sytuacji życiowej, rodzinnej i materialnej osoby uprawnionej. Zatem wymaganie przez pracodawcę od pracownika określonych *danych dotyczących sytuacji życiowej, rodzinnej i majątkowej* jest zgodne z przepisami prawa.²⁹⁷ Regulamin wewnętrzny zakładu powinien określać zasady przyznawania środków funduszu na poszczególne cele i rodzaje działalności socjalnej oraz zasady i warunki korzystania z usług i świadczeń finansowych z funduszu (art. 8 ust. 2 ustawy o zakładowym funduszu świadczeń socjalnych), w tym tryb udostępniania informacji i przyznawania świadczeń socjalnych, oraz zasady podawania do wiadomości pracowników listy osób, które korzystają ze świadczeń z funduszu socjalnego. O ile oświadczenia o stanie majątkowym są odpowiednio zabezpieczone, mają do nich dostęp wyłącznie osoby uprawnione, nie można mówić o naruszeniu ustawy o ochronie danych osobowych.

Do GIODO zwrócił się pismem z dnia 8 marca 2000 r. Rzecznik Praw Obywatelskich z prośbą o zbadanie zgodności z prawem zarządzenia Nr 100 Zarządu PKP z dnia 17 września 1999 r. w sprawie składania *oświadczeń o stanie majątkowym przez osoby zajmujące stanowiska kierownicze* w przedsiębiorstwie państwowym PKP oraz o podjęcie, w ramach posiadanych kompetencji, stosownych działań.²⁹⁸ W powyższym piśmie RPO zwrócił uwagę, że kwestionowane zarządzenie wydane zostało na podstawie art. 36 ustawy z dnia 6 lipca 1995 r. o przedsiębiorstwie państwowym Polskie Koleje Państwowe (Dz. U. Nr 95, poz. 474 z późn. zm.). Przepisu tego nie można jednak interpretować, jako upoważniającego Zarząd PKP do wydawania zarządzeń sprzecznych z powszechnie obowiązującym prawem. W ocenie Rzecznika Praw Obywatelskich zarządzenie to naruszało art. 298¹ ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 1998 r. Nr 21, poz. 94 z późn. zm.), zwanej dalej

²⁹⁶ GI-DP-116/00

²⁹⁷ GI-DP-648/00

²⁹⁸ GI-DP-687/00

K.p., oraz przepisy rozporządzenia Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika (Dz. U. Nr 62, poz. 286). Jak zaznaczył RPO przepisy tego rozporządzenia nie przewidują możliwości zbierania i przechowywania przez pracodawcę oświadczeń pracowników o ich stanie majątkowym. Podstawę taką mogłyby stanowić jedynie przepisy szczególne rangi ustawowej. W tej sprawie zajął stanowisko Minister Transportu i Gospodarki Morskiej. W piśmie z dnia 16 lutego 2000 r. skierowanym do Rzecznika Praw Obywatelskich stwierdził on, że zarządzenie to ma na celu uniknięcie nadużyć ze strony osób zajmujących kierownicze stanowiska w przedsiębiorstwie. Jednocześnie, zdaniem Ministra Transportu i Gospodarki Morskiej, fakt, że oświadczenia te są składane dobrowolnie i nie obwarowane żadnymi sankcjami, przemawia za tym, że nie zostały naruszone przepisy Konstytucji, a w szczególności art. 51. Ponadto, jak stwierdzono w tym piśmie, treść ww. zarządzenia nie narusza art. 298¹ K.p. oraz wydanego na jego podstawie rozporządzenia ministerialnego, ponieważ pracownik jest uprawniony do składania pracodawcy dokumentów o posiadanych kwalifikacjach. RPO zwrócił jednak uwagę, że informacje o stanie majątkowym nie mogą w żadnym razie stanowić świadectwa posiadania przez pracownika jakichkolwiek kwalifikacji zawodowych. Generalny Inspektor również uznał to zarządzenie za niezgodne z prawem, wskazując w szczególności, że art. 36 ustawy o przedsiębiorstwie państwowym PKP przewiduje jedynie możliwość wydawania przez Zarząd PKP zarządzeń wewnętrznych, instrukcji służbowych i regulaminów normujących organizację i działalność PKP. Z delegacji tej nie wynika jednak możliwość nałożenia na członków kierownictwa PKP obowiązku składania oświadczeń majątkowych.²⁹⁹

W odniesieniu do oświadczeń majątkowych składanych przez pracowników pojawiały się także wątpliwości, czy dane w nich zgromadzone podlegają ochronie przewidzianej w ustawie o ochronie danych osobowych, oraz czy zbiory takie podlegają rejestracji zgodnie z art. 40 tej ustawy.³⁰⁰ W odpowiedzi Generalny Inspektor stwierdził, że dane zbierane na formularzu, którego wzór określony został w rozporządzeniu Prezydenta RP z dnia 31 grudnia 1997 r. w sprawie ustalenia wzorów formularzy oświadczeń o prowadzeniu działalności gospodarczej i o stanie majątkowym (Dz. U. Nr 162, poz. 1106) są danymi osobowymi i podlegają ochronie przewidzianej dla tych danych. Formularze te opatrzone są klauzulą „poufne” i w tym zakresie znajduje zastosowanie ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11 poz. 95 z późn. zm.). Ponadto formularze takie

²⁹⁹ pismo z dnia 5 czerwca 2000 r. znak: GI/533/00

włączane są do akt osobowych poszczególnych pracowników i w związku z tym nie tworzą osobnego zbioru. Tym samym nie wymagają zgłoszenia do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.

Nie należy wyłącznie do sfery *prywatności informacja o dodatkowym zatrudnieniu pracowników Straży Miejskiej*.³⁰¹ Ujawnienie informacji o dodatkowym zatrudnieniu określonej liczby osób oraz wskazanie stanowisk kierowniczych, na których zatrudnione osoby prowadzą dodatkową działalność zarobkową nie stanowi naruszenia ustawy o ochronie danych osobowych. Nie można mówić o danych osobowych w odniesieniu do informacji wskazujących wyłącznie na liczbę osób podejmujących dodatkową działalność zarobkową, ze względu na to, że dane takie nie umożliwiają zidentyfikowania określonej osoby.

Przepisy prawa nie zawierają wyraźnego uregulowania, które zezwalałoby pracodawcy na *przetwarzanie danych o przynależności związkowej pracowników*.³⁰² Generalny Inspektor wskazywał, że do przetwarzania tego rodzaju informacji niezbędne jest wyrażenie przez pracowników zgody na piśmie. Zgodnie z art. 30 ust. 2¹ zd. 1 ustawy z dnia 23 maja 1991 r. o związkach zawodowych (Dz. U. Nr 55, poz. 234 z późn. zm.), w indywidualnych sprawach ze stosunku pracy, w których przepisy prawa pracy zobowiązują pracodawcę do współdziałania z zakładową organizacją związkową, pracodawca jest obowiązany zwrócić się do tej organizacji o informację o pracownikach korzystających z jej obrony, zgodnie z przepisami ust. 1 i 2. Nieudzielenie tej informacji w ciągu 5 dni zwalnia pracodawcę od obowiązku współdziałania z zakładową organizacją związkową w sprawach dotyczących pracowników. Podstawę do przetwarzania danych o przynależności związkowej mogą stanowić przepisy ustawy Kodeks pracy. Zgodnie z art. 52 § 3 tej ustawy, pracodawca podejmuje decyzję w sprawie rozwiązania umowy o pracę po zasięgnięciu opinii reprezentującej pracownika zakładowej organizacji związkowej, którą zawiadamia o przyczynie uzasadniającej rozwiązanie umowy. Przepisy te nie nakładają jednak bezpośrednio na pracodawcę generalnego obowiązku przetwarzania danych o przynależności związkowej pracowników.

W omawianym okresie sprawozdawczym zmniejszyła się liczba pytań dotyczących *dopuszczalności występowania pracodawców o udzielenie informacji z Centralnego Rejestru Skazanych* na temat karalności kandydata do pracy lub pracownika.³⁰³

³⁰⁰ GI-DP-445/00

³⁰¹ GI-DP-472/00

³⁰² GI-DP-363/00/372

³⁰³ GI-DP-421/00/476 – (obecnie kwestia ta uregulowana jest w ustawie z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym – Dz. U. Nr 50, poz. 580 z późn. zm.)

Generalny Inspektor wskazywał, że jest to dopuszczalne w przypadku, gdy przepis ustawy w sposób wyraźny zezwala na takie przetwarzanie danych. Zgodnie z art. 27 § 2 ustawy z dnia 20 czerwca 1985 r. Prawo o ustroju sądów powszechnych (Dz. U. 1994 r., Nr 7 poz. 25 z późn. zm.), dane z rejestru skazanych mogą być udostępniane do celów innych niż postępowanie karne, na wniosek osób, których dane te dotyczą, jak również zainteresowanych organów państwowych i samorządowych, zakładów pracy, a także jeżeli z faktem karalności danej osoby przepisy prawa lub umowy międzynarodowe wiążą określone skutki prawne. Ponadto § 12 ust. 2 pkt 3 rozporządzenia Ministrów Sprawiedliwości i Obrony Narodowej z dnia 30 sierpnia 1993 r. w sprawie prowadzenia rejestru osób prawomocnie skazanych, udzielania informacji z rejestru oraz trybu zbierania danych w postępowaniu karnym dotyczących tych osób (Dz. U. Nr 82, poz. 388) określa, że informacje z rejestru mogą być udostępnione do celów innych niż postępowanie karne na wniosek zakładów pracy, jeżeli jest to niezbędne w związku z zatrudnieniem pracowników. Z uwagi jednak na treść art. 28 ustawy o ochronie danych osobowych, zgodnie z którym przetwarzanie danych dotyczących skazań może odbywać się wyłącznie na podstawie odpowiedniego przepisu rangi ustawy, Generalny Inspektor stanął na stanowisku, że przetwarzanie tego rodzaju danych jest dopuszczalne, gdy przepisy ustawy w sposób wyraźny przewidują możliwość uzyskania tej informacji lub uzależniają objęcie danego stanowiska, czy funkcji, od wcześniejszej niekaralności kandydata do pracy.

Ustawa o ochronie danych osobowych nie nakłada na pracodawcę przetwarzającego dane osobowe kandydatów do pracy *obowiązku zwrotu złożonych dokumentów*.³⁰⁴ Zgodnie z art. 36 ustawy o ochronie danych osobowych administrator danych jest zobowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną. Jeżeli określone dane nie są już niezbędne dla realizacji celu, dla którego zostały zgromadzone, celowe jest ich usunięcie lub takie przekształcenie, które uniemożliwi zidentyfikowanie osoby, której dotyczą.

Pytania dotyczyły również zasadności wymagania od pracodawców prowadzących zakłady pracy chronionej *kserokopii umów o pracę z personelem medycznym* zatrudnionym w tychże zakładach.³⁰⁵ Generalny Inspektor odpowiadał, że wojewoda może

³⁰⁴ GI-DP-910/00/1618

³⁰⁵ GI-DP-932/00/1636

żądać udostępnienia informacji w zakresie niezbędnym do stwierdzenia przesłanek, od których zaistnienia prawo uzależnia przyznanie statusu zakładu pracy chronionej.

Zgodnie z art. 28 ust. 1 ustawy z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych (Dz. U. Nr 123, poz. 776 z późn. zm.) pracodawca prowadzący działalność gospodarczą przez okres co najmniej 12 miesięcy, zatrudniający nie mniej niż 20 pracowników w przeliczeniu na pełny wymiar czasu pracy i osiągający wskaźniki zatrudnienia osób niepełnosprawnych, o których mowa w pkt 1 przez okres co najmniej 6 miesięcy, uzyskuje status pracodawcy prowadzącego zakład pracy chronionej, jeżeli m.in. jest zapewniona doraźna i specjalistyczna opieka lekarska, poradnictwo i usługi rehabilitacyjne. Przepis ten określa zatem warunki, jakie pracodawca musi spełnić, aby uzyskać status zakładu pracy chronionej, nadawany przez wojewodę. Organ decydujący w sprawie przyznania statusu zakładu pracy chronionej powinien niewątpliwie dysponować dokumentami i danymi potwierdzającymi fakty wymagane przez przepisy powyższej ustawy dla podjęcia decyzji w sprawie. Z postanowień zawartych w art. 28 ust. 1 pkt 3 tej ustawy, a także w art. 30 ust. 4 wynika, że istnieje podstawa do przetwarzania informacji o zatrudnieniu personelu medycznego przez wojewodę. Ponadto należy zwrócić uwagę na przepis art. 75 § ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2000 r. Nr 98, poz. 1071), z którego wynika, że jako dowód należy dopuścić wszystko, co może przyczynić się do wyjaśnienia sprawy, a nie jest sprzeczne z prawem. W szczególności dowodem mogą być dokumenty, zeznania świadków, opinie biegłych oraz oględziny. Ustawa o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych nie przesądza, jakie informacje są wystarczające dla potwierdzenia wymogów określonych przez cytowane przepisy. Przy ich stosowaniu należy jednak pamiętać o regulacji zawartej w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych, zgodnie z którą dane osobowe winny być adekwatne w stosunku do celów, w jakich są przetwarzane.

Generalny Inspektor Ochrony Danych Osobowych został poinformowany, iż kandydaci na funkcjonariuszy Inspekcji Celnej są poddawani *badaniom poligraficznym* w celu ustalenia ich przydatności do pracy. Przeprowadzone postępowanie administracyjne wykazało, iż kandydaci na funkcjonariuszy Inspekcji Celnej byli poddawani badaniom poligraficznym, w czasie których zadawano pytania odnoszące się do prywatnej sfery ich życia. Zdaniem Dyrektora Biura Organizacji i Kontroli Generalnego Inspektoratu Celnego stosowanie tego rodzaju badań wynikało ze specyfiki ustawowych zadań nałożonych na

Inspekcję Celną oraz wymogu, aby pracownicy Inspekcji mieli nienaganną opinię.³⁰⁶ W wyniku przeprowadzonego postępowania Generalny Inspektor nakazał usunięcie danych zebranych w sposób niezgodny z prawem. Nie negując prawa Generalnego Inspektora Celnego do dokonywania swobodnej selekcji spośród kandydatów na funkcjonariuszy, Generalny Inspektor Ochrony Danych Osobowych zauważył, że selekcja ta musi być zgodna z przepisami prawa, w tym także z przepisami o ochronie danych osobowych. Cel przetwarzania danych – wybór najlepszych kandydatów na funkcjonariuszy - może zostać osiągnięty jedynie w sposób zgodny z prawem. Zakres informacji wymaganych przy badaniu poligraficznym zdecydowanie wykraczał poza adekwatny zakres, a więc nie był konieczny do prawidłowej oceny kandydata na funkcjonariusza. Ocena przydatności kandydata może być oparta o przesłanki dozwolone przepisami prawa i jednocześnie w pełni zapewniać realizację zadań nałożonych na administratora, z uwzględnieniem ich specyfiki. Generalny Inspektor Celny, jako pracodawca, ma wystarczającą różnorodność środków umożliwiających dokonanie kompleksowej oceny kandydata i jego przydatności do pracy (np. rozmowa kwalifikacyjna prowadzona przez specjalistę z zakresu rekrutacji pracowników, listy polecające, itp. stanowią wystarczającą podstawę do weryfikacji, czy kandydat ma nienaganną opinię). Zadawanie pytań wkraczających w prywatną sferę życia kandydatów na funkcjonariuszy jest zbędne do dokonania oceny ich przydatności do służby, a więc jest nieadekwatne w stosunku do celu, jakiemu ma służyć. Generalny Inspektor stwierdził także, że zgoda osoby, której dane dotyczą, nie w każdym przypadku jest przesłanką upoważniającą administratora do przetwarzania danych. Na mocy art. 28 ust. 1 ustawy, przetwarzanie danych dotyczących skazań, orzeczeń o ukaraniu, mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym można prowadzić wyłącznie na podstawie ustawy. Stosownie do art. 31 ust. 1 pkt 2 ustawy z dnia 6 czerwca 1997 r. o Inspekcji Celnej (Dz. U. Nr 71, poz. 449 z późn. zm.), funkcjonariuszem Inspekcji Celnej może być osoba, która ma nienaganną opinię i nie była karana za przestępstwo popełnione z winy umyślnej. Przepis ten upoważnia Generalnego Inspektora Celnego do zasięgania informacji o karalności kandydatów na funkcjonariuszy wyłącznie w zakresie wskazanym w tej ustawie. Generalny Inspektor stwierdził także, iż wyniki badania poligraficznego ze względu na ustawowe wykluczenie tego badania z kategorii środków dowodowych (art. 171 § 4 Kodeksu postępowania karnego), nie mogą wpływać na ocenę przydatności kandydatów do pracy, w tym kandydatów na funkcjonariuszy Inspekcji Celnej. Pracodawca ponosi przy

³⁰⁶ GI-DEC-DP-33/00/524

zatrudnianiu pracowników ryzyko osobowe, którego nie może ograniczać przy użyciu środków niezgodnych z przepisami prawa, w tym z przepisami o ochronie danych osobowych. W wydanej decyzji Generalny Inspektor nakazał usunięcie zebranych poprzez badania poligraficzne danych oraz zaprzestanie zbierania danych przy użyciu badań poligraficznych, jako nieadekwatnych w stosunku do celu ich przetwarzania.³⁰⁷

Przetwarzanie danych osobowych pracowników bez ich zgody odbywa się jedynie w zakresie i trybie określonym przepisami prawa. Ustawa Kodeks pracy w art. 94 pkt 9 a nakłada na pracodawcę obowiązek prowadzenia dokumentacji związanej z zatrudnieniem i akt osobowych pracowników. Sposób przetwarzania danych precyzuje rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika (Dz. U. Nr 62, poz. 286).

Nie narusza przepisów o ochronie danych osobowych *przekazywanie danych o pracownikach pomiędzy poszczególnymi komórkami zakładu pracodawcy*, jako działanie dokonywane przez tego samego administratora danych.³⁰⁸ Nie stanowi to w szczególności udostępniania danych innemu podmiotowi.

Do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęła skarga dotycząca ujawnienia informacji o przebiegu zatrudnienia, uzyskanym wykształceniu oraz informacji o zwolnieniach lekarskich, terminach leczenia i placówkach, w których się ono odbywało, jednemu z pracowników administratora danych.³⁰⁹ Generalny Inspektor zwracał jednak uwagę, że wygłaszanie opinii kwestionujących kwalifikacje zawodowe pracownika, mających zdyskredytować go w oczach innych pracowników, stanowi nie tyle naruszenie przepisów o ochronie danych osobowych, lecz przepisów o ochronie dóbr osobistych. W związku z tym istnieje możliwość dochodzenia praw na drodze postępowania cywilnego przed sądem powszechnym, na zasadach ogólnych wynikających z art. 23 i 24 Kodeksu cywilnego.

Jak wynikało z treści jednego pisma przejęcie przez spółkę innego podmiotu było uzależnione od tego, czy pracownicy spółki przejmowanej zgodzą się podjąć pracę na warunkach zaproponowanych przez przejmującego. W związku z tym spółka przejmująca złożyła *oferty pracy wszystkim pracownikom podmiotu przejmowanego, kierując je na ich*

³⁰⁷ Ibidem

³⁰⁸ GI-DP-513/00/507

³⁰⁹ GI-DIS-430/393/00

adres prywatny uzyskany z akt osobowych od podmiotu, który miałby zostać przejęty.³¹⁰ Generalny Inspektor nie dopatrył się w tej sprawie naruszenia ustawy o ochronie danych osobowych, ponieważ przetwarzanie danych przez podmiot zamierzający dokonać przejęcia, opiera się na przesłance określonej w art. 23 ust. 1 pkt 5. Ponadto przekazanie danych osobowych pracowników nie wiąże się ze zmianą celu ich przetwarzania, a działania pracodawcy zostały podjęte w interesie pracowników. Generalny Inspektor, stosownie do przepisów ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. 1998 r., Nr 21, poz. 94 z późn. zm.), wskazał ponadto, iż w sytuacji przejęcia zakładu przez innego pracodawcę, nowy pracodawca wstępuje w prawa i obowiązki dotychczasowego.

Do Generalnego Inspektora zwrócił się z prośbą o zajęcie stanowiska w sprawie zgodności z ustawą o ochronie danych osobowych działający na terenie jednego z przedsiębiorstw zakładowy ośrodek badania opinii pracowniczych, zajmujący się głównie *badaniem nastrojów załogi*. Sondaże przeprowadzane były na grupie reprezentatywnej wybranej z całej populacji zatrudnionych w zakładzie. Do przeprowadzania tego rodzaju badań socjologicznych niezbędne było uzyskanie wglądu w dane demograficzne charakteryzujące załogę, gdyż bez ich znajomości nie można było określić liczebności i składu uczestników przygotowywanego sondażu.³¹¹ W odpowiedzi Generalny inspektor stwierdził, że aby uzyskać dane osobowe umożliwiające prowadzenie badań nastrojów załogi, ośrodek musi uzyskać uprzednio zgodę osób, których dane dotyczą. Obowiązkiem administratora danych jest dołożenie szczególnej staranności w celu ochrony interesów osób, których dane dotyczą i zapewnienie, aby dane tych osób zbierane były dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami. Możliwe jest jednak, w myśl art. 26 ust. 2 ustawy o ochronie danych osobowych, przetwarzanie danych w celu innym niż ten, dla którego zostały zebrane (w omawianym przypadku dla celów zatrudnienia), jeżeli nie narusza to praw i wolności osoby, której dane dotyczą oraz następuje w celach badań naukowych, dydaktycznych, historycznych lub statystycznych z zachowaniem art. 23 i 25 ustawy. Generalny Inspektor wyraził pogląd, że podmiotem, który byłby uprawniony do zmiany celu przetwarzania danych w oparciu o art. 26 ust. 2 ustawy jest, np. jednostka badawczo-rozwojowa, który wykorzystuje dane w celach badań naukowych, dydaktycznych, historycznych lub statystycznych. W myśl art. 1 ustawy z dnia 26 lipca 1985 r. o jednostkach badawczo-rozwojowych (Dz. U. 1991 r., Nr 44, poz. 194 z późn. zm.) jednostkami badawczo-rozwojowymi są państwowe jednostki organizacyjne

³¹⁰ GI-DP-157/00

wyodrębnione pod względem prawnym, organizacyjnym i ekonomiczno-finansowym, tworzone w celu prowadzenia badań naukowych i prac rozwojowych, których wyniki powinny znaleźć zastosowanie w określonych dziedzinach gospodarki narodowej i życia społecznego, a ponadto posiadają osobowość prawną. Ośrodek badania opinii pracowniczych, nie odpowiadając wymogom tej definicji, nie spełnia podstawowego kryterium podmiotowego określonego w ustawie, które upoważniałoby do zmiany celu przetwarzania danych pracowników.

Do Generalnego Inspektora Ochrony Danych Osobowych zwróciło się starostwo powiatowe z pytaniem, czy dopuszczalne jest udostępnienie dziennikarzowi informacji o tym, czy jeden z pracowników w określonych dniach przebywał na urlopie wypoczynkowym, w pracy lub na delegacji służbowej. Informacje te dziennikarz zamierzał opublikować.³¹² Generalny Inspektor zwrócił uwagę, że wykorzystanie czasu pracy przez pracownika wykonującego w ramach stosunku pracy zadania władzy publicznej, nie należy do sfery jego prywatności. Z przepisu art. 61 ustawy zasadniczej wynika, że obywatel ma prawo do uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne, a tym samym do uzyskiwania informacji w zakresie, w jakim wykonują one zadania władzy publicznej i gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa. Zasada jawności życia publicznego wynika też z art. 11 ustawy z dnia 26 listopada 1998 r. o finansach publicznych (Dz. U. Nr 155, poz. 1014 z późn. zm.), który stanowi, że procesy związane z gromadzeniem i rozdysponowywaniem środków publicznych (w tym wydatki budżetu samorządu terytorialnego) są jawne. Zasady udzielania prasie informacji o działalności organów administracji państwowej określa m.in. art. 4 ustawy z dnia 26 stycznia 1984 r. Prawo prasowe (Dz. U. Nr 5, poz. 24 z późn. zm.), który przewiduje, że organy państwowe, przedsiębiorstwa państwowe i inne państwowe jednostki organizacyjne, a w zakresie działalności społeczno-gospodarczej również organizacje spółdzielcze i osoby prowadzące działalność gospodarczą na własny rachunek, są obowiązane do udzielania prasie informacji o swojej działalności. Odmowa udzielenia tej informacji może nastąpić jedynie ze względu na ochronę tajemnicy państwowej i służbowej oraz innej tajemnicy chronionej ustawą. Jednocześnie, zgodnie z art. 14 ust. 6 tej ustawy, nie wolno bez zgody osoby zainteresowanej publikować informacji oraz danych dotyczących prywatnej sfery życia, chyba że wiąże się to bezpośrednio z działalnością publiczną danej osoby. W świetle przywołanych przepisów, pojęciem prywatności ustawodawca nie obejmuje sfery działalności

³¹¹ GI-DP-317/00

publicznej człowieka, a także tej sfery działań czy zachowań, które ogólnie są pojmowane jako osobiste lub prywatne, a wiążą się ściśle z podejmowaną przez niego działalnością publiczną. Przepisy te, zdaniem Generalnego Inspektora wskazują, że wszelkie działania, czy to organów władzy publicznej, czy też poszczególnych osób pełniących funkcje publiczne, w zakresie w jakim wykonują one zadania publiczne lub gospodarują mieniem komunalnym albo majątkiem Skarbu Państwa, poddane zostały kontroli społecznej. Z tak pojętej zasady jawności życia publicznego wynika obowiązek, nałożony na instytucje i osoby pełniące funkcje publiczne, rzetelnego informowania społeczeństwa o swojej działalności. Podejmowanie działań w ramach wykonywania obowiązków wynikających ze stosunku pracy przez osoby zatrudnione w jednostkach samorządu terytorialnego nie należy więc do prywatnej sfery życia tych osób. Pracownicy nie występują tu w swoim własnym imieniu, a w imieniu organu powołanego do wypełniania zadań publicznych. Jako pracownicy samorządowi są funkcjonariuszami publicznymi w zakresie wykonywania nałożonych przez pracodawcę obowiązków służbowych.

Na pytanie o dopuszczalność udostępnienia danych o stanowisku pracy, czasie pracy, wysokości wynagrodzenia miesięcznego, premii i innych przychodów, do wglądu związkom zawodowym, odpowiadano, że ustawa o ochronie danych osobowych nie dotyczy takich informacji, ponieważ nie stanowią one danych osobowych w rozumieniu art. 6. Z tego samego powodu można również podać do publicznej wiadomości informacje o wynagrodzeniu osób pełniących stanowiska funkcyjne w okręgowej radzie lekarskiej.³¹³

Stanowi naruszenie ustawy o ochronie danych osobowych *udostępnienie prywatnego numeru telefonu oraz adresu zamieszkania pracownikom firmy* polegające na wprowadzeniu tych informacji do książki adresowej programu poczty elektronicznej na komputerze każdego użytkownika.³¹⁴ Generalny Inspektor uznał, że działanie takie stanowi zmianę celu przetwarzania danych osobowych gromadzonych na podstawie kodeksu pracy i przepisów wykonawczych i brak jest podstaw do udostępniania prywatnych danych pracowników innym pracownikom.

Przekazanie dokumentów dotyczących pracownika innej osobie zatrudnionej u administratora danych może stanowić naruszenie przewidzianego w art. 36 obowiązku zabezpieczenia danych, niezależnie od tego, że może naruszać przepisy o ochronie dóbr

³¹² GI-DP-873/00/1101, GI-DP-512/00, GI-DP-314/00

³¹³ GI-DP-133/00, GI-DP-548/00

³¹⁴ GI-DP-311/00/445

osobistych pracownika.³¹⁵ W odpowiedzi na jedno z pytań Generalny Inspektor stwierdził, że ustawa o ochronie danych osobowych nie różnicuje obowiązków administratorów wobec zbiorów danych osobowych w oparciu o kryterium obowiązku rejestracji zbioru.³¹⁶ W związku z powyższym, wobec zbiorów danych osobowych nie podlegających rejestracji należy zachować takie same zasady bezpieczeństwa, takie same procedury, jak wobec zbiorów podlegających temu obowiązkowi. Niezbędne jest zatem prowadzenie *ewidencji osób zatrudnionych przy przetwarzaniu danych* również w odniesieniu do osób pracujących przy przetwarzaniu danych w zbiorach nie podlegających rejestracji. Ustawa o ochronie danych osobowych nie określa formy, w jakiej powinno nastąpić to upoważnienie pracownika do przetwarzania danych osobowych.³¹⁷ Wskazywano, że dopuszczalne jest umieszczenie takiego upoważnienia w zakresie obowiązków pracownika. Konieczne jest jednak zamieszczenie odrębnej klauzuli o upoważnieniu pracownika do przetwarzania danych osobowych. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 80, poz. 521) stanowi w § 4, że indywidualny zakres czynności osoby zatrudnionej przy przetwarzaniu danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę tych danych przed niepożądanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem – w stopniu odpowiednim do zadań tej osoby przy przetwarzaniu danych osobowych. Upoważnienia tego nie można domniemywać z samego faktu zatrudnienia.

Nadal często pojawiają się wątpliwości dotyczące *udostępniania dokumentacji pracowniczej innym, upoważnionym do uzyskania wglądu na mocy przepisów prawa, podmiotom*. Wgląd do dokumentacji pracowniczej powinien mieć wyłącznie pracodawca. Udostępnienie tej dokumentacji innemu podmiotowi może odbywać się na podstawie wyższego, szczególnego przepisu prawa.

Zgodnie z art. 5 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. 1995 r., Nr 13, poz. 59 z późn. zm.), kontrola działalności samorządu terytorialnego prowadzona jest pod względem legalności, gospodarności i rzetelności. Jednocześnie na podstawie art. 29 ustawy o Najwyższej Izbie Kontroli upoważnieni przedstawiciele Najwyższej Izby Kontroli mają prawo wglądu do wszelkich dokumentów związanych z

³¹⁵ GI-DP-660/00

³¹⁶ GI-DP-792/00/938

³¹⁷ GI-DP-486/00515

działalnością jednostek kontrolowanych. Generalny Inspektor stwierdził zatem, że kontrolerzy NIK mają wgląd w dokumentację zawierającą dane osobowe, o ile informacje w tej dokumentacji zawarte wiążą się z problematyką kontroli, tj. są niezbędne do dokonania właściwej oceny działalności jednostki kontrolowanej z punktu widzenia kryterium legalności, gospodarności i rzetelności. Dotyczy to zarówno danych „zwykłych”, jak i „wrażliwych”, których przetwarzanie jest dopuszczalne na zasadach określonych w art. 27 ustawy o ochronie danych osobowych.³¹⁸

Do Generalnego Inspektora zwrócono się ze skargą dotyczącą *ujawnienia przez NIK wysokości wynagrodzenia otrzymywanego przez prezesa zarządu oraz dyrektora jednej ze spółek, kontrolowanej w zakresie wykorzystania pomocy państwa oraz realizacji zobowiązań finansowych na rzecz państwa*.³¹⁹ Generalny Inspektor stwierdził, że za dane osobowe ustawa rozumie każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie jej tożsamości (art. 6 ustawy). Zgodnie z tą definicją, za daną osobową może być uznana tylko taka informacja, która w sposób bezbłędny umożliwi identyfikację osoby. Może to być, np. imię, nazwisko, niepowtarzalny numer PESEL, NIP, niepowtarzalny kod genetyczny. Informacja dotycząca wysokości wynagrodzenia uzyskiwanego przez określoną osobę należy raczej do sfery dóbr osobistych, chronionych przepisami kodeksu cywilnego, nie zaś do sfery danych osobowych. Wysokość wynagrodzenia nie jest informacją bezpośrednio wskazującą na tożsamość określonej osoby. Nie identyfikuje ona wprost tej osoby i w związku z tym nie może być uznana za daną osobową zgodnie z polską definicją danych osobowych.

Zgodnie z art. 61 ust. 1 Konstytucji RP obywatel ma prawo m.in. do uzyskania informacji o działalności jednostek organizacyjnych w zakresie, w jakim gospodarują one majątkiem Skarbu Państwa. Wydatkowanie środków na wynagrodzenie osób pełniących funkcje kierownicze w spółkach, które otrzymały dotacje państwowe jest formą gospodarowania majątkiem Skarbu Państwa. Ocena działalności kontroli przeprowadzonej przez inspektorów NIK nie leży w sferze uprawnień Generalnego Inspektora Ochrony Danych Osobowych, których zakres wyznacza treść art. 12 ustawy o ochronie danych osobowych. NIK działa w oparciu o przepisy Konstytucji Rzeczypospolitej oraz ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 1995 r. Nr 13, poz. 59 z późn. zm.). Jest to naczelny organ kontroli państwowej, który podlega wyłącznie Sejmowi.

Generalny Inspektor uznał również, że nie jest organem właściwym do oceny legalności przedstawienia prasie przez NIK do publikacji przedmiotowych informacji. Prasa,

³¹⁸ GI-DP-328/00

zgodnie z Konstytucją Rzeczypospolitej Polskiej, korzysta z wolności wypowiedzi i urzeczywistnia prawo obywateli do ich rzetelnego informowania, jawności życia publicznego oraz kontroli i krytyki społecznej (art. 1 ustawy z dnia 26 stycznia 1984 r. Prawo prasowe (Dz. U. Nr 5, poz. 24 z późn. zm.). W myśl art. 4 ust. 1 cytowanej ustawy, organy państwowe (a takim organem jest niewątpliwie NIK), przedsiębiorstwa państwowe i inne państwowe jednostki organizacyjne, a w zakresie działalności społeczno-gospodarczej również organizacje spółdzielcze i osoby prowadzące działalność są obowiązane do udzielania prasie informacji o swojej działalności. Generalny Inspektor wskazał, że przepisy tej samej ustawy chronią prawo do prywatności i zgodnie z art. 14 ust. 6 nie wolno bez zgody osoby zainteresowanej publikować informacji oraz danych dotyczących prywatnej sfery życia, chyba że wiąże się to bezpośrednio z działalnością publiczną danej osoby. W konkluzji stwierdzono, że w omawianej sprawie znaleźć mogą ewentualnie zastosowanie przepisy prawa prasowego oraz instrumenty prawne przewidziane w przypadku naruszeń dóbr osobistych (art. 23 i art. 24 K.c.).

Odpowiadając na pytanie, czy *pracodawca ma prawo potrącać z wynagrodzenia członków związku składkę członkowską*, Generalny Inspektor stwierdzał, że dane o przynależności związkowej, jako dane wrażliwe zostały – co do zasady – objęte przez ustawodawcę zakazem przetwarzania. Ich gromadzenie i wykorzystanie jest dopuszczalne m.in. po uzyskaniu pisemnej zgody osoby, której dane dotyczą. Dane o pracownikach, niezbędne pracodawcy do pobierania składek członkowskich na rzecz związku zawodowego, są w istocie danymi o przynależności związkowej i ich przetwarzanie jest dopuszczalne po uzyskaniu pisemnej zgody pracownika.

Brak jest natomiast podstaw do *udostępniania organizacji związkowej akt osobowych pracownika i innej dokumentacji*, bez zgody tego pracownika, w przypadku realizacji przez związek zawodowy uprawnień określonych w art. 38 i 112 Kodeksu pracy.

W jednej ze spraw podkreślano, że pracodawcy odmawiają *udostępnienia list płac* motywując ten fakt obowiązaniem ustawy o ochronie danych osobowych. Uniemożliwia to kontrolę wykonania przez pracodawcę porozumienia, w wyniku którego przyznane zostały podwyżki.³²⁰ Generalny Inspektor wskazywał, że zgodnie z art. 6 ustawy o ochronie danych osobowych za dane osobowe uważa się każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby. W sytuacji, gdy tożsamość danej osoby jest znana, ujawnienie danych o wysokości wynagrodzeniu może stanowić ewentualnie

³¹⁹ GI-DP-793/00/1789, GI-DP-794/00, GI-DP-795/00

naruszenie dóbr osobistych pracownika.³²¹ Jak stwierdził Generalny Inspektor w piśmie do Prezesa Zakładu Ubezpieczeń Społecznych z dnia 4 lipca 2000 r., konstytucyjne prawo do informacji oraz ograniczony zakres prywatności osób sprawujących funkcje publiczne dają możliwość udzielenia informacji na temat wysokości rocznych nagród wypłaconych dyrektorom Zakładu Ubezpieczeń Społecznych.³²² Ustawa o ochronie danych osobowych nie daje podstawy prawnej do odmowy udzielania informacji o wysokości wynagrodzenia osoby publicznej, bowiem wynagrodzenie takiej osoby należy do sfery dóbr osobistych, nie zaś do sfery ochrony danych osobowych.

Podobnie Generalny Inspektor uznał, że *ujawnienie danych o wykształceniu i przygotowaniu zawodowym* danej osoby należy do problematyki ochrony dóbr osobistych, a nie danych osobowych.³²³ W odniesieniu do posła lub senatora, przepisem, który stanowi przesłankę legalności przetwarzania danych osobowych jest art. 19 ustawy z dnia 9 maja 1996 r. o wykonywaniu mandatu posła i senatora (Dz. U. Nr 73, poz. 350 z późn. zm.), na mocy którego poseł lub senator w wykonywaniu mandatu ma prawo, jeśli nie narusza dóbr osobistych innych osób, do uzyskania informacji i materiałów oraz wgląd w działalność organów administracji rządowej i samorządu terytorialnego, a także spółek Skarbu Państwa oraz zakładów i przedsiębiorstw państwowych i samorządowych z zachowaniem przepisów o tajemnicy ustawowo chronionej.

Kompetencje regionalnych izb obrachunkowych oraz inspektorów dokonujących kontroli gospodarki finansowej jednostek samorządu terytorialnego określa ustawa z dnia 7 października 1992 r. o regionalnych izbach obrachunkowych (Dz. U. Nr 85, poz. 428 z późn. zm.). Art. 8 ust. 1 pkt 8 tej ustawy stanowi, że inspektorzy do spraw kontroli gospodarki finansowej, w związku z wykonywaną kontrolą, mają *prawo dostępu do danych osobowych dotyczących kwalifikacji i uposażenia* pracowników samorządowych. W tym zakresie można więc udostępnić dotyczące pracownika dane osobowe. Należy podkreślić, iż ww. ustawa jest jedyną, która w tak wyraźny sposób podkreśla prawo do żądania przedmiotowych informacji. Z tego powodu nie ma na jej gruncie sporów kompetencyjnych, jakie występują, np. na gruncie ustawy samorządowej.

Do Generalnego Inspektora Ochrony Danych Osobowych zwrócono się z pytaniem o *dopuszczalność udostępniania inspektorom Państwowej Inspekcji Pracy dokumentacji*

³²⁰ GI-DP-454/00/447

³²¹ GI-DP-440/00

³²² GI-DP-804/00

³²³ GI-DP-633/00

*pracowniczej oraz kserowania tej dokumentacji.*³²⁴ Generalny Inspektor stwierdził, że z przepisów ustawy z dnia 6 marca 1981 r. o Państwowej Inspekcji Pracy (Dz. U. z 1985 r. Nr 54 poz. 276 z późn. zm.) nie wynika uprawnienie do przetwarzania danych zawartych w dokumentacji pracownika kontrolowanego zakładu pracy w zakresie szerszym, niż jest to konieczne do realizacji zadań PIP wynikających z art. 8 tej ustawy. Zgodnie z treścią wskazanego przepisu do zadań PIP należy nadzór i kontrola przestrzegania przez zakłady pracy prawa pracy, w szczególności przepisów i zasad bezpieczeństwa i higieny pracy, przepisów dotyczących stosunku pracy, wynagrodzenia za pracę i innych świadczeń wynikających ze stosunku pracy, czasu pracy, urlopów, ochrony pracy kobiet, zatrudniania młodocianych i osób niepełnosprawnych, oraz inicjowanie przedsięwzięć w sprawach ochrony pracy w rolnictwie indywidualnym. Natomiast zgodnie z art. 20 ust. 4 ww. ustawy, inspektor pracy ma prawo żądania okazania dokumentów dotyczących budowy i przebudowy oraz uruchomienia zakładu, planów i rysunków technicznych, dokumentacji technicznej i technologicznej, wyników ekspertyz, badań i pomiarów dotyczących produkcji bądź innej działalności zakładu, jak również dostarczania mu próbek surowców i materiałów używanych, wytwarzanych lub powstających w toku produkcji bądź innej działalności zakładu, gdy mają one związek z przeprowadzaną kontrolą. Z przepisów tych nie wynika prawo wglądu w całość akt osobowych pracowników. Podkreślono także, że stwierdzenie, czy akta personalne są prowadzone, nie musi się wiązać z wglądem w ich pełną treść.

Podobnie ustawa z dnia 14 marca 1985 r. o Inspekcji Sanitarnej (Dz. U. Nr 90, poz. 575 z późn. zm.), która określa zakres działania inspekcji sanitarnej, nie przewiduje wglądu w całość akt osobowych pracowników zatrudnionych u danego pracodawcy.³²⁵

Skoro jednym z zadań inspektora pracy jest kontrola wykonywania postanowień § 1 rozporządzenia Ministra Pracy i Polityki Społecznej z dnia 28 maja 1996 roku w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika (Dz. U. Nr 62, poz. 286), nic nie stoi na przeszkodzie sprawdzeniu zakresu skompletowanej dokumentacji pracowniczej, sposobu jej prowadzenia i przechowywania itd., bez zaznajamiania się z treścią przedmiotowej dokumentacji. Stąd, np. wydanie kserokopii całości dokumentacji inspektorowi PIP jest niedopuszczalne, podczas gdy należy umożliwić mu sprawdzenie, czy wymagane przez rozporządzenie dokumenty istnieją.

³²⁴ GI-DP-446/00

³²⁵ GI-DP-477/00

Zgodnie z § 37 ust. 1 rozporządzenia Rady Ministrów z dnia 28 września 1993 r. w sprawie obrony cywilnej (Dz. U. Nr 93, poz. 429), działalność planistyczną i prace organizacyjne w zakresie obrony cywilnej wykonują wszystkie organy, jednostki organizacyjne, instytucje i podmioty gospodarcze, na których ciąży obowiązek przygotowania i realizacji zadań obrony cywilnej. Prace organizacyjne obejmują w szczególności tworzenie formacji obrony cywilnej oraz prowadzenie ewidencji osób przeznaczonych do pełnienia służby w obronie cywilnej. Dopuszczalne jest zatem *gromadzenie przez starostwo informacji o osobach zatrudnionych w danej jednostce w celu opracowania ewidencji służącej zobrazowaniu struktury zatrudnienia w Obronie Cywilnej, zorganizowaniu szkolenia kadr itp.*³²⁶ Nie jest natomiast dopuszczalne *udostępnienie członkowi powiatowej rady zatrudnienia imiennego wykazu pracowników zatrudnionych w powiatowym urzędzie pracy w ramach robót publicznych.*³²⁷ Kompetencje powiatowych rad zatrudnienia określone zostały w ustawie z dnia 14 grudnia 1994 r. o zatrudnieniu i przeciwdziałaniu bezrobociu (Dz. U. 1997 r., Nr 25, poz. 128 z późn. zm.) oraz w rozporządzeniu Ministra Pracy i Polityki Socjalnej z dnia 21 marca 1995 r. w sprawie organizacji i trybu działania rad zatrudnienia oraz zasad uczestnictwa w posiedzeniach rad zatrudnienia innych organów oraz przedstawicieli nauki, organizacji i instytucji nie reprezentowanych w radach zatrudnienia (Dz. U. Nr 1995 r., Nr 38, poz. 188 z późn. zm.). W myśl art. 6a pkt 6 ustawy o zatrudnieniu i przeciwdziałaniu bezrobociu, powiatowe urzędy pracy obowiązane są współdziałać z powiatowymi radami zatrudnienia w zakresie ograniczania bezrobocia i jego negatywnych skutków, a w szczególności rozdziału i wykorzystania środków Funduszu Pracy oraz Państwowego Funduszu Rehabilitacji Osób Niepełnosprawnych. Powiatowe rady zatrudnienia są organami opiniodawczo-doradczymi starostów, a do zakresu ich działania należy m.in. inspirowanie przedsięwzięć zmierzających do pełnego i racjonalnego zatrudnienia, ocena racjonalności gospodarki środkami Funduszu Pracy oraz inne określone w przepisach ustawy o zatrudnieniu i przeciwdziałaniu bezrobociu zadania. Przepisy te nie formułują jednak uprawnień poszczególnych członków powiatowej rady zatrudnienia do żądania udostępnienia imiennego wykazu pracowników zatrudnionych w ramach robót publicznych. W przedstawionej sytuacji Generalny Inspektor uznał, że dopuszczalne byłoby udostępnienie takiego wykazu powiatowej radzie zatrudnienia (a nie konkretnemu jej członkowi działającemu we własnym imieniu) wówczas, gdy wykaz byłby niezbędny do oceny racjonalności gospodarki środkami Funduszu Pracy.

³²⁶ GI-DP-266/00

W ocenie Generalnego Inspektora zgodne z ustawą o ochronie danych osobowych jest *żądanie okazania list pracowników zatrudnionych przez podmiot*, który ma wykonać określone zlecenie w trybie ustawy z dnia 10 czerwca 1994 r. o zamówieniach publicznych (Dz. U. z 1998 r., Nr 119, poz. 773 z późn. zm.).³²⁸ W myśl art. 22 tej ustawy, zamawiający może, a w niektórych przypadkach jest zobowiązany zażądać od dostawców lub wykonawców potwierdzenia m.in. tego, że zatrudnia pracowników zdolnych do wykonania zamówienia.

Wątpliwości budziła także *dopuszczalność udostępnienia firmie prowadzącej audyt umów o pracę oraz imiennych list płac pracowników spółki*.³²⁹ Generalny Inspektor przywołał przepisy ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. Nr 121, poz. 591 z późn. zm.), w szczególności art. 65 ust. 1, zgodnie z którym celem firmy badającej sprawozdanie finansowe jest sprawdzenie, czy jest ono prawidłowe i czy rzetelnie i jasno przedstawia sytuację majątkową i finansową, wynik finansowy oraz rentowność badanej jednostki. Jednocześnie, w myśl art. 67 ust. 1 tej ustawy, kierownik badanej jednostki udostępnia biegłemu rewidentowi, przeprowadzającemu badanie sprawozdania finansowego, księgi rachunkowe oraz dokumenty stanowiące podstawę dokonanych w nich zapisów oraz wszelkie dokumenty mogące mieć wpływ na sformułowanie oceny biegłego rewidenta o sytuacji majątkowej i finansowej badanej jednostki, jak również udziela wyczerpujących informacji, wyjaśnień i oświadczeń, niezbędnych do sporządzenia raportu i wyrażenia opinii. Generalny Inspektor uznał jednak, że nie jest uprawniony do wydawania opinii dotyczących innych ustaw, w szczególności nie jest uprawniony do przesądzania, które dokumenty mogą być udostępniane, a które nie.

Zasady i interpretacje prezentowane w odpowiedziach na pytania nie dotyczą udostępniania danych osobowych zmarłych pracowników. Z uwagi na to, iż ustawa o ochronie danych osobowych wyraźnie stanowi w art. 2, iż „Ustawa określa zasady postępowania przy przetwarzaniu danych osobowych oraz prawa osób fizycznych (...)”, zasady określone w ustawie dotyczą wyłącznie osób fizycznych.³³⁰

Generalny Inspektor stwierdził również, że nie narusza ustawy o ochronie danych osobowych *udzielenie członkom wspólnoty mieszkaniowej informacji o wysokości wynagrodzenia dozorca posesji*.³³¹ Podstawę prawną stanowi w takim przypadku przepis art.

³²⁷ GI-DP-429/00

³²⁸ GI-DP-809/00/1134

³²⁹ GI-DP-36/00

³³⁰ GI-DP-579/00/639

³³¹ GI-DP-219/00

29 ust. 3 ustawy z dnia 24 czerwca 1994 r. o własności lokali (Dz. U. Nr 85, poz. 388 z późn. zm.). Stanowi on, że każdy właściciel lokalu ma prawo kontroli działalności zarządu. Każdy z członków ma zatem prawo do oceny prawidłowości prowadzonej przez zarząd wspólnoty mieszkaniowej gospodarki finansowej.

Nie stanowi przesłanki legalności *udostępniania danych osobowych pracowników spółdzielni jej członkom* art. 3 ustawy z dnia 16 września 1982 r. Prawo spółdzielcze (Dz. U. 1995 r., Nr 54, poz. 288 z późn. zm.).³³² Stanowi on, że majątek spółdzielni jest prywatną własnością jej członków. W literaturze przedmiotu wskazuje się jednak, że znaczenie tego przepisu sprowadza się jedynie do podkreślenia, że majątek spółdzielni w sensie ekonomicznym stanowi prywatną, a nie uspołecznioną formę własności. W myśl art. 46 ustawy prawo spółdzielcze, nadzór i kontrolę nad działalnością spółdzielni sprawuje rada wybierana przez walne zgromadzenie, zebranie przedstawicieli lub zebranie grup członkowskich. Do zakresu działania tej rady należy badanie sprawozdań finansowych oraz inne przewidziane w ustawie lub statucie spółdzielni zadania. W celu realizowania swoich zadań rada może żądać od zarządu, członków i pracowników spółdzielni wszelkich sprawozdań i wyjaśnień, przeglądać księgi i dokumenty oraz sprawdzać bezpośrednio stan majątku spółdzielni. Generalny Inspektor stwierdził, że w tego rodzaju sprawach członkowie spółdzielni są żywotnie zainteresowani sprawowaniem efektywnej kontroli nad sposobem wydatkowania pieniędzy stanowiących majątek spółdzielni. Z uwagi na to, Generalny Inspektor Ochrony Danych Osobowych zwrócił się do Rzecznika Praw Obywatelskich z prośbą o podjęcie odpowiednich działań w tej kwestii. Zagadnienie to powinno jednak być przedmiotem rozstrzygnięcia Sądu.

Szczególne trudności pojawiły się wobec konieczności odpowiedzi na pytanie, czy *uczelnia wyższa ma prawo opublikowania składu osobowego uczelni*, w którym zamieszczone byłyby takie informacje jak: stopień naukowy, imię i nazwisko pracownika, nazwa wydziału, na którym dana osoba pracuje, telefon służbowy i adres e-mail pracownika.³³³ Stwierdzono, że skład pracowników uczelni, zawierający tego rodzaju informacje, nie stanowi informacji o charakterze prywatnym, wobec czego nie jest konieczne uzyskiwanie zgody pracownika na przetwarzanie tych informacji, a pracownik nie może żądać zaprzestania przetwarzania danych ściśle związanych z działalnością pracodawcy.

W działalności Generalnego Inspektora bardzo często pojawiały się pytania dotyczące zgodności z prawem nałożenia na pracowników *obowiązku noszenia*

³³² GI-DP-637/00/1484

identyfikatorów zawierających imiona i nazwiska pracowników.³³⁴ Obowiązek noszenia takich identyfikatorów może wynikać z wewnętrznych uregulowań wydanych przez pracodawcę, np. z regulaminu pracy wydanego na podstawie art. 104 § 1 Kodeksu pracy, który ustala organizację i porządek pracy, jak również związane z tym prawa i obowiązki pracowników. Granice swobody podmiotu ustalającego regulamin pracy w wyborze problemów, które mogą być przedmiotem jego postanowień, określa art. 104¹ § 1 K.p. Pracownicy w związku z zatrudnieniem muszą podporządkować się przepisom wewnętrznym obowiązującym u danego pracodawcy. Określone informacje o nich muszą być udostępniane, np. w celu prawidłowego funkcjonowania zakładu i realizowania przez niego swych zadań. Wskazywano ponadto, że dane te korzystają z ochrony w ograniczonym stopniu z uwagi na to, że są one danymi pracownika, np. urzędu, a nie pochodzą ze sfery życia prywatnego. W odniesieniu do funkcjonariuszy Służby Więziennej podstawę noszenia identyfikatorów stanowi § 31 rozporządzenia Ministra Sprawiedliwości z dnia 12 czerwca 1997 r. w sprawie określenia wzorów umundurowania, oznak służby, dystynkcji, znaków identyfikacyjnych i wyposażenia specjalnego funkcjonariuszy Służby Więziennej oraz zasad i sposobów noszenia umundurowania i orderów, odznaczeń, medali, odznak oraz znaków identyfikacyjnych (Dz. U. Nr 84, poz. 537).³³⁵ Zgodnie z tym przepisem, znakami identyfikacyjnymi są identyfikator foliowany ze zdjęciem, identyfikator numeryczny, identyfikator funkcyjny. Identyfikator foliowany prócz zdjęcia zawiera także nazwę jednostki organizacyjnej Służby Więziennej, numer identyfikatora, datę i podpis wystawcy, nazwisko i imię, stopień służbowy i stanowisko funkcjonariusza.

Niedopuszczalne jest wykorzystywanie danych osobowych przetwarzanych w związku z zatrudnieniem do innych celów. W szczególności wysyłanie przez zarząd spółki akcyjnej materiałów reklamowych od akcjonariuszy do zatrudnionych przez spółkę akwizytorów, stanowi niewątpliwie naruszenie art. 26 ust. 2 ustawy o ochronie danych osobowych. Działanie takie wyczerpuje znamiona czynu zabronionego określonego w art. 49 ust. 1 tej ustawy.³³⁶

Nadal częste były pytania dotyczące wypełnienia przez administratorów danych obowiązku informacyjnego.³³⁷ Pytano w szczególności, czy obowiązek informacyjny, o którym mowa w art. 24 ustawy o ochronie danych osobowych należy spełnić w stosunku do

³³³ GI-DP-221/00, GI-DP-223/00, GI-DP-596/00/737

³³⁴ GI-DP-330/00/394, GI-DP-507/00/529, GI-DP-528/00, GI-DP- 534/00/820, GI-DP-577/00/723

³³⁵ GI-DP-564/00/769

³³⁶ GI-DP-438/00/478

³³⁷ GI-DP-387/00

wszystkich osób, zarówno zatrudnionych aktualnie, jak i byłych pracowników, emerytów i rencistów. Odpowiadano, że administrator danych ma obowiązek poinformowania wyłącznie tych osób, których dane zostały zebrane po wejściu ustawy w życie. Administrator danych (pracodawca), który uzyskuje określone dane od pracownika (kandydata do pracy), w momencie uzyskiwania danych zobowiązany jest do poinformowania w szczególności o celu zbierania danych, o prawie wglądu w dane oraz o obowiązku podania danych (i o podstawie prawnej tego obowiązku), jeżeli dane uzyskiwane są wyłącznie w zakresie wymaganym przez przepisy prawa pracy.³³⁸ Jeśli jednak administrator danych zamierza gromadzić dane w szerszym zakresie (np. na podstawie zgody pracownika) musi także poinformować pracownika o dobrowolności udzielenia informacji.

Pytano również, czy administrator, który na podstawie innych przepisów prawnych jest obowiązany do *archiwizowania danych osobowych byłych pracowników*, powinien dokonać zgłoszenia takiego zbioru danych.³³⁹ W odpowiedzi stwierdzano, że art. 43 ust. 1 pkt 4 zwalnia administratora danych osób zatrudnionych u niego od obowiązku zgłoszenia zbioru do rejestracji. Z uwagi na to, że ustawodawca nie wskazał, że zwolnieniu od rejestracji podlegają wyłącznie zbiory danych osób zatrudnionych obecnie u danego pracodawcy, należy przyjąć, że nie podlegają rejestracji również zbiory zawierające dane o byłych pracownikach danego administratora.

H. PRZETWARZANIE DANYCH OSOBOWYCH W SEKTORZE TELEKOMUNIKACJI

W 2000 r. do Biura Generalnego Inspektora wpłynęło ok. 90 skarg i pytań prawnych dotyczących działalności podmiotów działających w sektorze telekomunikacyjnym. Przedmiotem ich były przede wszystkim zagadnienia dotyczące odmowy udostępnienia danych abonenta, udostępnienia danych osobom nieupoważnionym, zasadności sporządzania kserokopii dokumentów tożsamości przez operatorów sieci telefonii komórkowej i stacjonarnej przy zawieraniu umów o świadczenie usług telekomunikacyjnych oraz zakresu danych wymaganych przy zawieraniu takich umów. Wiele wątpliwości zostało rozstrzygniętych wraz z wejściem w życie ustawy z dnia 21 lipca 2000 r. Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852), obowiązującej od 1 stycznia 2001 r. Do 31 grudnia 2000 r. aktem prawnym, na podstawie którego rozpatrywano zasadność zarzutów

³³⁸ GI-DP-247/00/345

³³⁹ GI-DP-268/00/250

stawianych podmiotom świadczącym usługi telekomunikacyjne była ustawa z dnia 23 listopada 1990 r. o łączności (Dz. U. z 1995 r. Nr 117, poz. 564 z późn. zm.) oraz wydane na jej podstawie przepisy wykonawcze.

Podstawy prawne i zakres przetwarzania danych osobowych przez operatorów sieci telekomunikacyjnej użytku publicznego.

Podobnie jak w 1999 r., w omawianym okresie sprawozdawczym liczne pytania dotyczyły *zakresu informacji udostępnianych abonentowi*. Szczególnie wiele wątpliwości wzbudzała *odmowa udostępniania informacji o numerach telefonów przez pracowników Telekomunikacji Polskiej S.A. z powoływaniem się na przepisy ustawy o ochronie danych osobowych, w sytuacji, gdy pytający nie znał kompletnych danych abonenta*.³⁴⁰ Skarżących informowano, że ustawa o ochronie danych nie uniemożliwia udostępnienia danych osobowych w sytuacjach, gdy zezwalają na to przepisy prawa. Podmioty świadczące usługi telekomunikacyjne działają w oparciu o przepisy ustawy z dnia 23 listopada 1990 r. o łączności (Dz. U. z 1995 r. Nr 117, poz. 564) oraz przepisów wykonawczych. Obowiązki operatora sieci telekomunikacyjnej użytku publicznego zostały określone w rozporządzeniu Ministra Łączności z dnia 8 lutego 1996 r. w sprawie ogólnych warunków świadczenia usług telekomunikacyjnych w sieci telekomunikacyjnej użytku publicznego (Dz. U. Nr 20, poz. 93 z późn. zm.). Przepisy § 4 ust. 1 pkt 5 i 6 cytowanego rozporządzenia przewidują obowiązek operatora sieci zapewnienia publicznego dostępu do spisu własnych abonentów, jeśli abonent nie zastrzeże poufności tej informacji, a także obowiązek zapewnienia własnym abonentom informacji o numerach stacji abonenckich osiągniętych z ich stacji abonenckiej.³⁴¹ Skarżących informowano, iż zakres udzielanych informacji powinien ograniczać się do numeru telefonu, imienia, nazwiska oraz ewentualnie nazwy ulicy (w sytuacji powtarzalności imienia i nazwiska wskazanego abonenta). Odmowę udostępniania danych we wskazanym zakresie, np. przez pracowników biur numerów, uznawano za nieuzasadnioną.³⁴² Natomiast za wykraczające poza przedmiotowy zakres uznawano podanie pełnych danych adresowych o abonencie.³⁴³

³⁴⁰ GI-DIS-84/00

³⁴¹ GI-DP-430/1758/00

³⁴² GI-DP-286/00/228, GI-DP-359/00/707

³⁴³ GI-DIS-215/00

W celu uniknięcia dalszych trudności interpretacyjnych w wielu pismach kierowanych w roku 1999 i 2000 do Ministra Łączności, Generalny Inspektor sygnalizował potrzebę doprecyzowania zakresu danych zawartych w spisie abonentów, która jednocześnie umożliwiałaby abonentowi złożenie zastrzeżenia dotyczącego zawężenia lub rozszerzenia zakresu danych umieszczanych w spisie.³⁴⁴ Skutkiem powyższych działań było umieszczenie w nowym prawie telekomunikacyjnym przepisu art. 70 dokładnie określającego jakie dane abonenta mogą być umieszczone w publicznie dostępnym spisie.³⁴⁵

Przedmiotem wielu skarg i zapytań prawnych była ponadto zasadność odmowy udzielenia informacji o rozmowach telefonicznych przychodzących na numer stacji abonenckiej skarżących. Generalny Inspektor wielokrotnie podkreślał, iż *rozporządzenie w sprawie ogólnych warunków świadczenia usług telekomunikacyjnych w sieci użytku publicznego nie uprawnia operatora sieci do ujawniania własnym abonentom informacji o numerach z cudzych stacji abonenckich*. Jak wynikało z licznych skarg abonenci niepokojeni tzw. głuchymi telefonami nie mają możliwości uzyskania wykazu (bilingu) numerów przychodzących na numer ich stacji abonenckiej.³⁴⁶ W tej sytuacji abonenci zwracają się do prokuratury o podjęcie stosownych działań, ale i tutaj spotykają się z odmową wszczęcia postępowania karnego, czyn ten nie stanowi bowiem przestępstwa, a jedynie wykroczenie. Prokuratury informowały Generalnego Inspektora, iż pokrzywdzony, który sam nie jest w stanie uzyskać informacji o numerach urządzeń abonenckich inicjujących połączenie telekomunikacyjne, nie ma możliwości obrony swoich praw; nie może bowiem złożyć wniosku o ukaranie za powyższe wykroczenie, skoro nie jest mu znana osoba sprawcy, zaś operatorzy telefonii odmawiają udostępnienia informacji mogących doprowadzić do jej ustalenia. W odpowiedzi na powyższe Generalny Inspektor wyjaśniał, iż działanie operatorów sieci telekomunikacyjnej znajdując oparcie w przepisach prawa nie może być uznane za niezgodne z ustawą o ochronie danych osobowych (art. 23 ust. 1 pkt 2 ustawy). Pokrzywdzonym abonentom zwracano jednak uwagę, iż nie są oni pozbawieni możliwości dochodzenia swych praw. W przypadku złośliwego niepokojenia abonenta tzw. głuchymi telefonami, postępowanie takie stanowi wykroczenie opisane w art. 107 ustawy z dnia 20

³⁴⁴ Np. GI/317/99, GI/513/99, GI/343/99

³⁴⁵ Zgodnie z art. 70 ust. 1 ustawy z dnia 21 lipca 2000 r. Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852) dane osobowe zawarte w publicznie dostępnym spisie abonentów, a także udostępniane za pomocą służb informacyjnych operatora powinny być ograniczone do numeru abonenta lub znaku identyfikującego abonenta (pkt 1), nazwiska i imion abonenta (pkt 2), nazwy miejscowości, w której znajduje się zakończenie sieci udostępnione abonentowi (pkt 3), nazwę ulicy, przy której znajduje się zakończenie sieci udostępnione abonentowi (pkt 4).

³⁴⁶ Np. GI-DP-384/00/574, GI-DP-406/00/466, GI-DP-024/1854/00

maja 1971 r. Kodeks wykroczeń (Dz. U. Nr 12, poz. 114 z późn. zm.), w myśl którego, kto w celu dokuczenia innej osobie złośliwie wprowadza ją w błąd lub w inny sposób złośliwie niepokoi, podlega karze ograniczenia wolności, grzywny do 1500 złotych albo karze nagany. Zgodnie z zasadą legalizmu, organy ścigania są zobowiązane ścigać sprawców przestępstw i wykroczeń w przypadku zaistnienia podejrzenia ich popełnienia. W sytuacji podejrzenia popełnienia wykroczenia z art. 107 Kodeksu wykroczeń pokrzywdzony może się zwrócić do Policji o podjęcie środków niezbędnych do ustalenia sprawcy(ów) opisanego czynu. Natomiast policja zgodnie z art. 19 ustawy z dnia 20 maja 1971 r. Kodeks postępowania w sprawach o wykroczenia (Dz. U. Nr 12, poz. 116 z późn. zm.), w celu ustalenia, czy istnieją podstawy do wystąpienia z wnioskiem o ukaranie i zebrania danych niezbędnych do sporządzenia takiego wniosku, w miarę potrzeby i w granicach swojej właściwości, może wystąpić z żądaniem złożenia wyjaśnień i opinii oraz wydania albo okazania dokumentu mającego stanowić niezbędny dowód w sprawie. Na podstawie art. 15 ust. 1 pkt 6 i 7 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2000 r. Nr 101, poz. 1092 z późn. zm.) oraz zgodnie z § 2 rozporządzenia Rady Ministrów z dnia 13 sierpnia 1996 r. w sprawie szczegółowego trybu korzystania przez policjantów z pomocy instytucji państwowych, organów administracji rządowej i samorządu terytorialnego, jednostek gospodarczych i organizacji społecznych oraz osób (Dz. U. Nr 107, poz. 501), Policja może się zwrócić w toku czynności służbowych podejmowanych w celu rozpoznania i wykrywania przestępstw i wykroczeń, z żądaniem niezbędnej pomocy od instytucji państwowych, organów administracji rządowej i samorządu terytorialnego, jednostek gospodarczych prowadzących działalność w zakresie użyteczności publicznej oraz innych jednostek gospodarczych, organizacji społecznych oraz osób. Policja może się zwracać do operatorów sieci również na podstawie art. 20c ustawy o Policji, zgodnie z którym dane identyfikujące abonenta sieci telekomunikacyjnej lub zakończenia sieci, między którymi wykonano połączenie, oraz dane dotyczące uzyskania lub próby uzyskania połączenia między określonymi zakończeniami sieci, a także okoliczności i rodzaj wykonywanego połączenia, mogą być ujawnione Policji oraz przetwarzane przez Policję – wyłącznie w celu zapobiegania lub wykrywania przestępstw.

Policja zatem, w ramach przysługujących jej ustawowo uprawnień, może się zwrócić do operatora sieci o udostępnienie informacji o numerach połączeń telefonicznych

przychodzących na numer osoby pokrzywdzonej, zaś operator sieci na mocy obowiązujących przepisów prawa jest zobowiązany udostępnić przedmiotowe dane.

Niezależnie od powyższego, Generalny Inspektor zauważył, iż konstrukcja przepisu § 4 ust. 1 pkt 6 rozporządzenia Ministra Łączności w sprawie ogólnych warunków świadczenia usług w sieci telekomunikacyjnej użytku publicznego, utrudnia działanie pokrzywdzonych i organów ścigania podejmowanych w celu wykrycia potencjalnych sprawców wykroczeń, dlatego też zwrócił się do Przewodniczącego Sejmowej Komisji Transportu i Łączności o uwzględnienie możliwości wprowadzenia stosownych zapisów ustawowych w pracach nad nowym prawem telekomunikacyjnym. Podniósł przy tym uwagę, iż Dyrektywa 97/66/EC Parlamentu i Rady Unii Europejskiej z dnia 15 grudnia 1998 r. w sprawie przetwarzania danych osobowych i ochrony danych w sektorze telekomunikacyjnym, w art. 8 dopuściła możliwość udzielenia abonentowi informacji o numerach telefonów przychodzących na jego stację abonencką.³⁴⁷ Jednakże analiza przepisów obowiązującej od 1 stycznia 2001 r. ustawy z dnia 21 lipca 2000 r. Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852) wskazuje, iż problem ten nie został rozstrzygnięty.

Generalny Inspektor nie znalazł również podstaw dla *udostępnienia przez Telekomunikację Polską S.A. danych abonentów, o które wnioskowały Urzędy Skarbowe*, powołujące przy tym przepisy postępowania egzekucyjnego w administracji.³⁴⁸ Zgodnie z art. 36 § 1 ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 1991 r. Nr 36, poz. 161 z późn. zm.), organ egzekucyjny może żądać od uczestników postępowania złożenia wyjaśnień oraz zasięgnąć od organów administracji państwowej i instytucji informacji niezbędnych do prowadzenia egzekucji. Telekomunikacja Polska S.A nie jest organem państwowym (instytucją) i nie uczestniczy w postępowaniu podatkowym na prawach strony, a tym samym nie może znaleźć w stosunku do niej zastosowanie dyspozycja ww. przepisu.

Liczna grupa spraw, które napływały do Generalnego Inspektora dotyczyła legalności *umieszczania w książce telefonicznej danych osobowych bez zgody osoby, której dane dotyczą*. Problem ten szeroko wyjaśniany w 1999 r. wzbudzał również liczne wątpliwości w omawianym roku 2000. Skargi powyższe uznawano za bezzasadne z uwagi na fakt, iż operator sieci telekomunikacyjnej użytku publicznego jest prawnie zobowiązany do zapewnienia publicznego dostępu do spisu własnych abonentów, którzy nie zastrzegli poufności takich informacji, np. w momencie zawierania umowy o świadczenie usług

³⁴⁷ GI/412/00, GI-DP-384/00/574

telekomunikacyjnych.³⁴⁹ Zasadna natomiast okazała się skarga dotycząca opublikowania w książce telefonicznej zastrzeżonego numeru telefonu, pomimo zawartej w umowie klauzuli o zastrzeżeniu numeru telefonu i nie wyrażeniu zgody na publikowanie, bądź podawanie tych danych przez służby informacyjne Telekomunikacji.³⁵⁰ Jak ustalono, przedmiotowa publikacja nastąpiła wskutek zaniedbania pracownika Spółki i w związku z tym administrator danych podjął działania zmierzające do przywrócenia stanu zgodnego z prawem. Analiza innej skargi doprowadziła do ustalenia, iż pomimo złożenia przez abonenta zastrzeżenia numeru telefonu, udostępniono osobom nieupoważnionym jego pełne dane adresowe.³⁵¹ Generalny Inspektor nie skorzystał z przysługujących mu uprawnień, określonych w art. 19 ustawy (uprawnienie do kierowania do organu powołanego do ścigania przestępstw zawiadomienia o popełnieniu przestępstwa), gdyż postępowanie karne już zostało wszczęte z zawiadomienia skarżącego.

Wraz z rozwojem nowoczesnych środków masowego przekazu pojawił się nowy problem dotyczący legalności *publikacji książek telefonicznych w internecie*.³⁵² Polska Izba Informatyki i Telekomunikacji wyrażała obawy, czy publikacja takiej bazy danych na stronach internetowych nie wywoła negatywnych skutków dla ich administratorów. Mając na uwadze fakt, iż operator sieci telekomunikacyjnej jest zobowiązany do zapewnienia publicznego dostępu do spisu własnych abonentów, jeżeli abonent nie zastrzeże poufności tej informacji, to tym samym, jeśli cel przetwarzania pozostaje taki sam, w ocenie Generalnego Inspektora nic nie stoi na przeszkodzie, aby operator sieci udostępnił spis swoich abonentów również w formie elektronicznej, w tym np. w internecie. W wielu pismach skarżący podnosili problem danych nieprawdziwych (nieaktualnych), umieszczanych w publicznie dostępnych spisach abonentów, wprowadzających w błąd potencjalnych klientów firm. W takich sytuacjach Generalny Inspektor badał, czy nie została naruszona zasada adekwatności przetwarzania danych określona w art. 26 ustawy o ochronie danych, a w razie stwierdzenia jej naruszenia wzywał administratorów danych do przywrócenia stanu zgodnego z prawem.³⁵³

Odrębna grupa spraw rozpatrywanych przez Generalnego Inspektora dotyczyła praktyki operatorów sieci telekomunikacyjnych polegającej na *kopiowaniu dokumentów*

³⁴⁸ GI-DP-024/1573/00

³⁴⁹ GI-DIS-369/00, GI-DP-573/00/567

³⁵⁰ GI-DIS-253/00

³⁵¹ GI-DIS-227/00

³⁵² GI-DP-74/00/109

³⁵³ GI-DP-430/1758/00

*tożsamości i zbyt szerokiego zakresu danych osobowych wymaganych od klienta przy zawieraniu umowy o świadczenie usług telekomunikacyjnych.*³⁵⁴ Niektórzy z operatorów twierdzili, że kopiowanie wybranych stron dokumentów stanowi niezbędny warunek zawarcia umowy i odbywa się za wyraźną zgodą klienta. Przeprowadzone postępowania wyjaśniające nie potwierdziły powyższych twierdzeń. W ocenie Generalnego Inspektora praktyka sporządzania kserokopii dokumentów prowadzi do gromadzenia danych osobowych zbędnych przy zawieraniu umowy o wykonanie usługi, a zawierających dane ze sfery prywatnej klienta, m.in. imiona rodziców, datę i miejsce urodzenia, stan cywilny, adnotacje o zatrudnieniu. Tym samym dochodzi do naruszenia przepisu art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych, zgodnie z którym administrator danych powinien dołożyć należytej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności obowiązek zapewnienia, aby dane przetwarzane były zgodnie z prawem, zbierane dla oznaczonych, zgodnych z prawem celów, merytorycznie poprawne i adekwatne do celów, w jakich są przetwarzane. Sporządzanie kserokopii dokumentów prowadzi również do udostępnienia danych osób trzecich, zbędnych do zawarcia umowy, a jednak włączanych do zbioru danych firmy w wyniku sporządzania przedmiotowych kopii.³⁵⁵ Za szczególnie naganną, niezgodną z ustawą o ochronie danych, uznano praktykę uzależniania zawarcia umowy od zgody na kserowanie dokumentów. Jak wykazała jedna z inspekcji operator nie respektował własnego wewnętrznego regulaminu świadczenia usług telekomunikacyjnych, zgodnie z którym w razie wątpliwości co do autentyczności dokumentów wymagane było jedynie okazanie dokumentów dodatkowych, a nie obowiązek sporządzania ich kserokopii. Szczególna ochrona abonenta powinna wynikać z faktu, iż umowa do której on przystępuje jest rodzajem umowy adhezyjnej, gdzie klient nie może negocjować jej warunków, a jedynie je przyjąć, bądź zrezygnować z usług operatora. Powoduje to, że obowiązki nakładane na klienta powinny być precyzyjnie określone i zgodne z przepisami prawa. Umowa powinna być ukształtowana w sposób umożliwiający jej wykonanie; powinna zawierać oznaczenie strony w zakresie niezbędnym do jej identyfikacji. Wobec operatorów dokonujących ww. naruszeń wydawano decyzje nakazujące ograniczenie przetwarzania danych do minimum niezbędnego do zawarcia umowy o świadczenie usług telekomunikacyjnych, tj. imienia, nazwiska, adresu zamieszkania, numeru PESEL lub daty urodzenia, numeru identyfikacji

³⁵⁴ GI-DP-337/00/926, GI-DP-385/00/1065

³⁵⁵ Na marginesie należy zauważyć, iż na podstawie art. 18 ustawy z dnia 20 sierpnia 1997 r. (Dz. U. Nr 113, poz. 733) zmieniającej ustawę z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych (Dz. U. z 1984 r. Nr 32, poz. 174 z późn. zm.) z dniem 1 stycznia 2001 r. został znacznie ograniczony zakres informacji zawartych w dowodzie osobistym (art. 37 ustawy o ewidencji ludności i dowodach osobistych).

podatkowej oraz aktualnego miejsca pracy abonenta. Nakazywano ponadto zaprzestania kopiowania dokumentów klientów.³⁵⁶ Stanowisko Generalnego Inspektora zostało podzielone również przez Rzecznika Praw Obywatelskich, który przystąpił do prowadzonego przed NSA postępowania administracyjnego.³⁵⁷ W przekonaniu Rzecznika Praw Obywatelskich dla zabezpieczenia interesów operatora sieci wystarczą dane wskazane przez GODO, zaś gromadzenie przez operatora sieci telekomunikacyjnej kserokopii oryginalnych dokumentów identyfikacyjnych budzi obawy ich wykorzystania do celów sprzecznych z prawem przez osoby niepowołane.³⁵⁸ Ostateczne rozstrzygnięcie przedmiotowej kwestii dokonane zostanie przez Naczelny Sąd Administracyjny.

Do Generalnego Inspektora wpływały również pytania związane z legalnością działań operatorów telefonii komórkowej, polegającej na sprzedaży przysługujących im wierzytelności wraz z danymi osobowymi dłużników - abonentów innym podmiotom.³⁵⁹ Zgodnie z postanowieniami przepisu art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych przetwarzanie danych jest dopuszczalne wtedy, gdy zezwalają na to przepisy prawa. W przypadku przelewu wierzytelności przepisem regulującym zakres uprawnień wierzyciela jest art. 509 § 1 ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. Nr 16, poz. 93 z późn. zm.), zgodnie z którym wierzyciel może bez zgody dłużnika przenieść wierzytelność na osobę trzecią (przelew), chyba że sprzeciwiałoby się to ustawie, zastrzeżeniu umownemu albo właściwości zobowiązania. Generalny Inspektor uznał, iż ww. zagadnienie powinno być rozpatrywane w świetle art. 3851 i nast. Kodeksu cywilnego, jak również ustawy z dnia 2 marca 2000 r. o ochronie praw konsumentów oraz o odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny (Dz. U. Nr 22, poz. 271). Z istoty umowy przelewu wynika, że zgoda dłużnika na jej zawarcie jest wymagana tylko wtedy, gdy w umowie łączącej wierzyciela z dłużnikiem wyłączono możliwość przeniesienia wierzytelności na osobę trzecią. Zgodnie z art. 510 § 1 Kodeksu cywilnego przelew wierzytelności może nastąpić w drodze umowy sprzedaży, zamiany darowizny lub innej umowy zobowiązującej do przeniesienia wierzytelności. Wobec powyższego, udostępnienie danych osobowych dłużnika nabywcy wierzytelności nie stanowi naruszenia przepisów ustawy o ochronie danych osobowych.

³⁵⁶ Np. GI-DP-DEC-35/00

³⁵⁷ Ibidem, GI-DP-41/00/1345

³⁵⁸ Szerz. w „Zbędne informacje w posiadaniu firmy”, Prawo co Dnia z 23-24 września 2000 r.

³⁵⁹ Np. GI-DP-024/1444/00, GI-DP-024/1477/00

Odmienne natomiast przedstawia się stan prawny w odniesieniu do umów zawieranych z udziałem konsumentów, tj. z osobami, które zawierają umowę z przedsiębiorcą w celu bezpośrednio nie związanym ze swoją działalnością gospodarczą (art. 384 § 3 Kodeksu cywilnego i § 3 pkt 2 rozporządzenia Rady Ministrów z dnia 30 maja 1995 r. w sprawie szczegółowych warunków zawierania i wykonywania umów sprzedaży rzeczy ruchomych z udziałem konsumentów – Dz. U. Nr 64, poz. 328 z późn. zm.). Zgodnie bowiem z nowym brzmieniem - zmiana dokonana na skutek wejścia w życie przepisów ustawy z dnia 2 marca 2000 r. o ochronie niektórych praw konsumentów oraz o odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny (Dz. U. Nr 22, poz. 271) - obowiązującego do dnia 1 lipca 2000 r. przepisu art. 385 § 1 Kodeksu cywilnego, postanowienia umowy zawieranej z konsumentem nie uzgodnione indywidualnie nie wiążą go, jeżeli kształtują jego prawa i obowiązki w sposób sprzeczny z dobrymi obyczajami, rażąco naruszając jego interesy (niedozwolone postanowienia umowne). Nie dotyczy to postanowień określających główne świadczenia stron, w tym cenę lub wynagrodzenie, jeżeli zostały sformułowane w sposób jednoznaczny. Zgodnie z art. 385 § 3 pkt 5 Kodeksu cywilnego w razie wątpliwości uważa się, że niedozwolonymi postanowieniami umownymi są te, które w szczególności zezwalają kontrahentowi konsumenta na przeniesienie praw i przekazanie obowiązków wynikających z umowy bez zgody konsumenta. Tym samym postanowienia umowy zawieranej z konsumentem dopuszczające przeniesienie wierzytelności na osobę trzecią bez zgody konsumenta, stosownie do art. 385 § 1 w związku z art. 385 § 3 pkt 5 Kodeksu cywilnego, są bezskuteczne z mocy prawa.

Jednocześnie Generalny Inspektor Ochrony Danych Osobowych informował, iż stosownie do przyznanych mu ustawowo kompetencji, nie posiada umocowania do dokonywania oceny prawidłowości zawierania klauzul umownych na podstawie przepisów prawa cywilnego, a w szczególności oceny (należytego lub nienależytego) wykonania zawieranych umów cywilno-prawnych. Organami upoważnionymi do ww. działań mogą być, np. sąd powszechny i Urząd Ochrony Konkurencji i Konsumentów.

Niekiedy udostępnianie danych osobowych abonentów dłużników dokonywane było na podstawie umowy powierzenia łączącej operatora sieci – administratora danych - z innym podmiotem, zawartej w celu windykacji zaległych należności. Generalny Inspektor informował wówczas o treści art. 31 ustawy o ochronie danych osobowych, podkreślając

równocześnie, iż podmiot, któremu dane powierzono uprawniony jest do ich przetwarzania wyłącznie w zakresie i w celu w umowie tej przewidzianym.³⁶⁰

W jednym z pism pytający podważał zasadność *odmowy przez Telekomunikację Polską S.A. danych abonentów nieznanych osobie reklamującej rachunek telefoniczny*.³⁶¹ Zgodnie z obowiązującym w 2000 roku stanem prawnym ogólne warunki i szczegółowy tryb postępowania reklamacyjnego określone zostały w wydanym na podstawie art. 71 ust. 5 ustawy o łączności rozporządzeniu Ministra Łączności z dnia 28 maja 1996 r. w sprawie reklamacji usług telekomunikacyjnych o charakterze powszechnym (Dz. U. Nr 64, poz. 309). Ponieważ przepisy powyższego rozporządzenia nie przewidują szczególnych zasad przetwarzania danych osobowych abonentów, dlatego też w zakresie przetwarzania danych dla potrzeb postępowania reklamacyjnego zastosowanie znajdują przepisy ustawy o ochronie danych osobowych. Administrator danych nie może zatem udostępnić danych abonentów nieznanych osobie reklamującej rachunek telefoniczny, jeżeli nie posiada ku temu odpowiedniej podstawy prawnej.³⁶² Obawy budziła również kwestia *zakresu danych osobowych wymaganych od abonentów przez pracowników biur obsługi klienta w trakcie odwoławczego postępowania reklamacyjnego*.³⁶³ Zgodnie z § 6 ust. 1 ww. rozporządzenia w wypadku negatywnego załatwienia reklamacji odwołanie wnosi się do organu odwoławczego, o którym mowa w § 5 ust. 2 pkt 4 rozporządzenia, w terminie 14 dni od daty doręczenia pisma, za pośrednictwem jednostki organizacyjnej załatwiającej reklamację w I instancji. Podmiot rozpatrujący odwołanie jest zobowiązany zidentyfikować osobę, która je składa, aby upewnić się, czy złożenie pisma następuje przez osobę uprawnioną. Działanie takie, w ocenie Generalnego Inspektora, jest częścią umowy wiążącej abonenta z firmą telekomunikacyjną i znajduje umocowanie w art. 23 ust. 1 pkt 3 ustawy o ochronie danych osobowych. Nie oznacza to jednak, że administrator danych może w ten sposób pozyskane dane przetwarzać w sposób dowolny; z mocy art. 26 ust. 1 pkt 2 ustawy jest zobowiązany zapewnić, aby były one zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, z zastrzeżeniem ust. 2. Ponadto na administratorze danych spoczywa obowiązek właściwego ich zabezpieczenia, wynikający z art. 36 ustawy.

Przepisy ustawy o ochronie danych osobowych, a w szczególności art. 12 tej ustawy, nie uprawniają Generalnego Inspektora do prowadzenia spraw w zakresie

³⁶⁰ GI-DP-909/00/1210

³⁶¹ GI-DP-024/1751/00

³⁶² Ibidem

³⁶³ GI-DP-1118/00/1573

wykrywania i ścigania przestępstw oraz podważania postanowień organów powołanych do ich ścigania, a należących do ich właściwości.³⁶⁴ Mając na uwadze powyższe, Generalny Inspektor nie oceniał zasadności skarg dotyczących faktu zaistnienia (lub nieistnienia) zaległości w opłatach za korzystanie z sieci telekomunikacyjnej,³⁶⁵ ani nie udzielał informacji dotyczących danych określonych abonentów, o co niejednokrotnie wnioskowali klienci sieci telefonii komórkowych i stacjonarnej, którym odmówiono udostępnienia danych.³⁶⁶ Generalny Inspektor nie badał ponadto prawidłowości treści umów cywilnoprawnych.³⁶⁷ W przypadku sporów między stronami umowy, co do zgodności z prawem trybu renegocjacji zawartej umowy cywilnoprawnej odsyłano do sądu powszechnego, jako organu właściwego do rozstrzygnięcia sprawy.³⁶⁸

Jak wynika z treści art. 39 ustawy o łączności opłaty za usługi telekomunikacyjne ustala operator sieci telekomunikacyjnej. Przed zawarciem umowy każdy klient jest zobowiązany do zapoznania się z regulaminem wewnętrznym operatora sieci. W regulaminie tym określony jest zakres, sposób oraz zasady świadczenia usług. Regulamin taki stanowić może, iż opłaty w zakresie usług podstawowych i dodatkowych (np. zastrzeżenie danych) zawarte są w cenniku określającym wysokość opłat. Jednocześnie klient podpisując umowę o świadczenie usług telekomunikacyjnych składa oświadczenie, że otrzymał, zapoznał się i akceptuje warunki umowy, regulamin świadczenia usług telekomunikacyjnych oraz cennik świadczenia usług. Umowa ma charakter dobrowolny, a zatem poprzez zawarcie umowy z operatorem sieci abonent wyraża równocześnie zgodę na proponowane przez niego warunki i zobowiązuje się do ich przestrzegania.³⁶⁹

W omawianym okresie sprawozdawczym Generalny Inspektor wielokrotnie stykał się z sygnałami dotyczącymi *przetwarzania danych abonentów w celach marketingowych bez zgody osoby, której dane dotyczą*.³⁷⁰ Operatorzy telefonii komórkowej, których działalności dotyczyła większa część przedmiotowych skarg, uzasadniali takie działania faktem zawarcia umowy z abonentem. Ponadto zdarzały się przypadki warunkowania zawarcia umowy o świadczenie usług telekomunikacyjnych od wyrażenia jego zgody na przetwarzanie danych w celach marketingowych. Generalny Inspektor podkreślał, iż postanowienia umowy abonenckiej nie mogą być tak skonstruowane, aby zawarcie umowy uzależnione było od

³⁶⁴ GI-DP-1213/00/1860, GI-DP-430/1335/00

³⁶⁵ GI-DP-1213/00/1860, GI-671/00

³⁶⁶ GI-DP-946/00/1161

³⁶⁷ GI-DP-590/00/1005

³⁶⁸ GI-DP-1011/00/1377

³⁶⁹ GI-DP-480/00/991, GI-671/00

wyrażenia zgody na przetwarzanie danych w celach marketingowych.³⁷¹ U podłoża takiego stanowiska stoi przepis art. 7 pkt 5 ustawy o ochronie danych osobowych, zgodnie z którym zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. Abonent zawierając umowę wyraża bowiem zgodę na przetwarzanie danych w granicach określonych stosunkiem umownym i nie wykraczających poza ten stosunek. O ile zatem operator ma zamiar przysyłać swojemu klientowi materiały marketingowe, to konieczne jest zawarcie odrębnego oświadczenia woli, z którego jednoznacznie będzie wynikać zgoda osoby, której dane dotyczą na przetwarzanie jej danych w celach wykraczających poza treść umowy, tj. w celach marketingowych, reklamowych, informacyjnych.³⁷² W wyniku interwencji GODO operatorzy podjęli działania zmierzające do dostosowania zasad obowiązujących przy zawieraniu umów o świadczenie usług telekomunikacyjnych do przepisów o ochronie danych osobowych.

Odnosnie skarg związanych z *udostępnieniem przez operatorów sieci telekomunikacyjnej danych abonentów – podmiotów gospodarczych* informowano, iż ustawa o ochronie danych osobowych nie znajduje zastosowania do informacji o przedsiębiorcach.³⁷³ Stanowisko powyższe uzasadnione jest treścią art. 2 ust. 1 ustawy, zgodnie z którym ustawa o ochronie danych osobowych określa zasady postępowania przy przetwarzaniu danych osobowych oraz prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych. Natomiast dane przedsiębiorcy, jako podmiotu występującego w obrocie gospodarczym nie podlegają ochronie w myśl przepisów ustawy, ponieważ nie są danymi osoby fizycznej. Wiele skarg dotyczyło *udostępniania danych klientów osobom niepowołanym, na skutek wadliwego działania urządzeń telekomunikacyjnych*.³⁷⁴ Po interwencji GODO stwierdzono, że opracowana została procedura przysyłania danych osobowych z wykorzystaniem urządzeń telekomunikacyjnych, która reguluje m.in. kwestie odpowiedzialności za przesłane dane osobowe oraz postępowanie w sytuacji nieprawidłowości w transmisji.

Analiza wielu skarg, które wpłynęły do Biura w roku 2000 potwierdziła, iż operatorzy świadczący usługi telekomunikacyjne naruszają ustawę o ochronie danych osobowych poprzez niedopełnienie lub tylko częściowe dopełnienie obowiązku

³⁷⁰ Szerzej w decyzji Generalnego Inspektora z dnia 25 września 2000 r. (GI-DEC-DP-72/00)

³⁷¹ GI-DIS-99/00

³⁷² GI-DIS-61/00, GI-DP-024/54/01

³⁷³ GI-DP-1011/00/1377, GI-DP-430/1886/00

³⁷⁴ GI-DIS-4/00

informacyjnego, o którym mowa w art. 24 ustawy.³⁷⁵ W celu zbadania zgodności przetwarzania danych osobowych z obowiązującymi przepisami ustawy o ochronie danych Generalny Inspektor poprzez swoich inspektorów przeprowadzał liczne kontrole w siedzibach firm telekomunikacyjnych.³⁷⁶ Zebrany materiał pozwolił na ustalenie faktu, iż operatorzy sieci telefonii komórkowej nie wywiązywali się z nałożonego na nich przez ustawę obowiązku informacyjnego.³⁷⁷ W niektórych umowach o świadczenie usług telekomunikacyjnych nie informowano abonentów o ich prawach wynikających z art. 24 ustawy o ochronie danych osobowych. Skargi dotyczyły również niewykonania obowiązku z art. 36 ustawy, tj. niewłaściwego zabezpieczenia danych poprzez udostępnienie osobie nieuprawnionej wykazu rozmów telefonicznych. Zaobserwowano ponadto nieprawidłowości w funkcjonowaniu systemów informatycznych, służących do przetwarzania danych, brak stosownych instrukcji określających sposób zarządzania systemem przetwarzania, niewłaściwe zabezpieczenie pomieszczeń, w których odbywa się proces przetwarzania danych, brak określenia zakresu odpowiedzialności osób zatrudnionych przy przetwarzaniu za ochronę przetwarzania danych, czy stosowanie aplikacji informatycznych nie dających możliwości udostępnienia na piśmie informacji wymaganych przez rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 80, poz. 521). Administratorzy danych w większości przypadków, po przedstawieniu im wniosków pokontrolnych, usuwali stwierdzone w trakcie kontroli uchybienia i dostarczali dokumenty potwierdzające ich usunięcie. W stosunku do pozostałych podmiotów w celu przywrócenia stanu zgodnego z prawem wydawano decyzje administracyjne nakazujące operatorom sieci telefonii usunięcie uchybień w procesie przetwarzania danych ich klientów.³⁷⁸ Generalny Inspektor zwracał się ponadto o pociągnięcie do odpowiedzialności dyscyplinarnej osoby winne naruszeń.³⁷⁹

³⁷⁵ GI-DP-885/00/1320, GI-DP-1113/00/1672, GI-DP-024/1859/00

³⁷⁶ DIS-K-15/00

³⁷⁷ DIS-K-91/00

³⁷⁸ Np. GI-DEC-28/00

³⁷⁹ GI-DIS-227/00

I. PRZETWARZANIE DANYCH OSOBOWYCH PRZEZ BANKI, ZWIĄZEK BANKÓW POLSKICH I INSTYTUCJE WSPÓŁPRACUJĄCE Z BANKAMI

Zasady prowadzenia działalności bankowej określa ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. Nr 140, poz. 939 z późn. zm.). Na podstawie ustawy banki mogą dokonywać czynności bankowych wymienionych w art. 5 tej ustawy, oraz podejmować inne działania, o których stanowi art. 6 ustawy Prawo bankowe. Z problematyką ochrony danych osobowych wiąże się przede wszystkim kwestia przepływu informacji w związku z prowadzeniem działalności bankowej. Do tego zagadnienia odnoszą się przepisy art. 104, 105 i 106 ustawy Prawo bankowe. W art. 104 zdefiniowane zostało pojęcie tajemnicy bankowej, która obejmuje wszystkie wiadomości, dotyczące czynności bankowych i osób będących stroną umowy, uzyskane w czasie negocjacji oraz związane z zawarciem umowy z bankiem i jej realizacją, z wyjątkiem wiadomości, bez których ujawnienia nie jest możliwe należyte wykonanie zawartej przez bank umowy. Tajemnica bankowa obejmuje także wszelkie informacje dotyczące osób, które nie będąc stroną umowy dokonały czynności pozostających w związku z zawarciem takiej umowy. Wyjątki mogą zostać określone w ustawie. Regulacja ustawy z 29 sierpnia 1997 r. Prawo bankowe znacznie rozszerzyła zakres tajemnicy bankowej w stosunku do ustawy z 31 stycznia 1989 r. Prawo bankowe (Dz. U. 1992 r., Nr 72, poz. 359 z późn. zm.), wprowadziła także w art. 104, 105 i 106 szereg wyjątków od obowiązku zachowania tajemnicy bankowej. Nie są to wszakże jedyne przepisy dopuszczające możliwość uchylecia tajemnicy bankowej. Do najważniejszych regulacji prawnych dotyczących tej kwestii zaliczyć należy także ordynację podatkową z dnia 29 sierpnia 1997 r. (Dz. U. Nr 137, poz. 926 z późn. zm.), ustawę z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. Nr 100, poz. 442 z późn. zm.) i ustawę z dnia 29 września 1994 r. o rachunkowości (Dz. U. 121, poz. 591 z późn. zm.).

W omawianym okresie sprawozdawczym Generalny Inspektor rozpatrywał 95 spraw związanych z działalnością banków i innych instytucji finansowych. Największe zaniepokojenie budziła liczba spraw, w których podnoszono brak odpowiednich zabezpieczeń zbiorów danych oraz udostępnianie danych osobom nieuprawnionym. Powyższe skargi stanowiły nie tylko naruszenie ustawy o ochronie danych osobowych, lecz również przepisów Prawa bankowego. Ponadto często sygnalizowano przypadki niewywiązywania się banków z obowiązku informowania nałożonego na nie przepisami ustawy o ochronie danych osobowych. Jednocześnie w przypadku wszczęcia postępowania przez Generalnego

Inspektora zdarzały się sytuacje, gdy odmawiano mu określonych informacji powołując się właśnie na przepisy o tajemnicy bankowej. Przypadki naruszeń sygnalizowane były Komisji Nadzoru Bankowego i Związkowi Banków Polskich.

Zgodnie z art. 105 ust. 1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. Nr 140, poz. 939 z późn. zm.), bank ma obowiązek udzielać informacji stanowiących tajemnicę bankową innym bankom o wierzytelnościach oraz o obrotach i stanach rachunków bankowych, w zakresie w jakim informacje te są niezbędne w związku z udzielaniem kredytów, pożyczek pieniężnych, gwarancji bankowych i poręczeń oraz czynnościami obrotu dewizowego, a także w związku z konsolidacją sprawozdań finansowych - bankom należącym do bankowej grupy kapitałowej. Wykorzystanie powyższych informacji powinno nastąpić wyłącznie w granicach przedmiotowego upoważnienia (art. 105 ust. 3 ustawy Prawo bankowe). Generalny Inspektor uznał zatem, że *przekazywanie informacji o wierzytelnościach pomiędzy bankami należącymi do bankowej grupy kapitałowej (ale tylko w związku z konsolidacją ww. sprawozdań)*, a tym bardziej pomiędzy oddziałami tego samego banku, nie narusza przepisów o ochronie danych osobowych.³⁸⁰

Podobnie jak w 1999 r, również w omawianym okresie sprawozdawczym wiele skarg dotyczyło *przekazywania informacji o wierzytelnościach Związkowi Banków Polskich*.³⁸¹ Generalny Inspektor wydawał decyzje odmawiające nakazania usunięcia danych osobowych oraz wskazywał, że przetwarzanie danych w ramach Systemu Międzybankowej Informacji Gospodarczej - "Bankowy Rejestr" nie narusza ustawy o ochronie danych osobowych.

Administrator danych osobowych jest upoważniony do przetwarzania danych tylko w przypadku zaistnienia przynajmniej jednej z przesłanek określonych w art. 23 ust. 1 ustawy o ochronie danych osobowych. Wykazanie którejkolwiek z przesłanek wymienionych w powyższym przepisie jest warunkiem koniecznym dla stwierdzenia legalności procesu przetwarzania danych osobowych w zbiorze. Jedną z przesłanek dopuszczalności przetwarzania danych jest zgoda osoby, której dane dotyczą. Wyrażenie zgody jest jednak zbędne w sytuacji, gdy podstawą legitymującą administratora danych do ich przetwarzania jest przepis prawa lub inna z przesłanek z art. 23 ust. 1 pkt 3 – 5 ustawy.

³⁸⁰ GI-DIS-269/2000

³⁸¹ GI-DEC-DP-80/00, GI-DP-802/00, GI-DP-024/1639/00

Banki mogą poza tym, na podstawie art. 105 ust 4 cytowanej ustawy, utworzyć instytucję do zbierania i udostępniania bankom informacji o wierzytelnościach oraz o obrotach i stanach rachunków bankowych w zakresie, w jakim informacje te są potrzebne w związku z udzielaniem kredytów, pożyczek pieniężnych, gwarancji bankowych i poręczeń.

Na mocy Regulaminu Wymiany Informacji w Systemie Międzybankowej Informacji Gospodarczej – „Bankowy Rejestr”, system ten polega na przyjmowaniu i gromadzeniu przez Związek Banków Polskich informacji o klientach banków, a następnie kontaktowaniu się banków zainteresowanych takimi informacjami. W załączniku nr 1 do regulaminu zostały określone kryteria klasyfikowania klientów do systemu z uwzględnieniem postanowień Uchwały Nr 13/98 Komisji Nadzoru Bankowego z dnia 22 grudnia 1998 r. w sprawie zasad tworzenia rezerw na ryzyko związane z działalnością banków (Dz. Urz. NBP Nr 29, poz. 65). Do systemu kwalifikuje się osoby fizyczne nie będące przedsiębiorcami gdy:

- nie zostały spłacone trzy kolejne raty kredytu,
- nie zostały uregulowane trzy kolejne płatności z tytułu należnych bankowi odsetek,
- nie zostały uregulowane zobowiązania wobec banku z tytułu gwarancji bankowej,
- poręczyciel, który uchyla się od regulowania zobowiązań osoby fizycznej wobec banku.

Usunięcie informacji o kliencie z systemu następuje w szczególności:

- w razie śmierci osoby fizycznej,
- po zakończeniu upadłości lub likwidacji przedsiębiorcy,
- po umorzeniu postępowania egzekucyjnego,
- po dwóch latach od uregulowania zobowiązań lub ustaniu przyczyny zgłoszenia do rejestru.

Procedura wymiany informacji o klientach polega na tym, że bank interesujący się konkretnym klientem (bank pytający) zwraca się z pytaniem do Związku Banków Polskich, a Związek w zakresie posiadanych w systemie informacji udziela odpowiedzi na temat klienta. Jeżeli bank pytający chce uzyskać bardziej wyczerpujące informacje, kontaktuje się z bankiem, który zgłosił klienta do systemu (informacje o banku zgłaszającym przekazuje bankowi pytającemu Związek Banków Polskich). Wymiana informacji ma być dokonywana w sposób zapewniający zachowanie tajemnicy bankowej. Podstawą przetwarzania danych osobowych w „Bankowym Rejestrze” są przepisy prawa bankowego, które zezwalają bankom

na utworzenie wspólnie z bankowymi izbami gospodarczymi, instytucji do zbierania i udostępniania bankom informacji o wierzytelnościach oraz o obrotach i stanach rachunków bankowych w zakresie, w jakim informacje te są potrzebne w związku z udzielaniem kredytów, pożyczek pieniężnych, gwarancji bankowych i poręczeń. Nie ulega wątpliwości, iż dla realizacji powyższego celu niezbędne jest przetwarzanie danych osobowych. Dane klientów, wraz z informacjami o wierzytelnościach (byłych i obecnych) są przetwarzane w „Bankowym Rejestrze” w związku z tym, że informacje te są potrzebne w celu udzielenia kredytów, pożyczek pieniężnych, gwarancji bankowych i poręczeń. Generalny Inspektor uznał, iż spełniona została przesłanka przetwarzania danych określona w art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych.

Opierając się na przepisie art. 32 ust. 2 ustawy o ochronie danych osobowych Związek Banków Polskich niejednokrotnie przekazywał Generalnemu Inspektorowi pisma klientów banków z żądaniem zaprzestania przetwarzania ich danych osobowych. Związek Banków Polskich podkreślał również, że żądania te nie odpowiadają treści przepisu art. 32 ust. 1 pkt 7 ustawy o ochronie danych osobowych, ponieważ brak w nich odpowiedniego uzasadnienia wskazującego na sytuację, dla której Związek Banków Polskich powinien zaprzestać przetwarzania tych danych osobowych.³⁸² Generalny Inspektor zwrócił się z pismem do Dyrektora Generalnego Związku Banków Polskich przekazując swoją opinię w tej sprawie oraz sygnalizując konieczność wyjaśnienia tej kwestii. Opinia ta powtórzona została w publikacji prasowej Generalnego Inspektora zamieszczonej w dzienniku „Rzeczpospolita” z dnia 12 czerwca 2000 r. Generalny Inspektor wyjaśnił, że stosownie do art. 32 ust. 1 pkt. 7 ustawy o ochronie danych osobowych, każdej osobie której dane są przetwarzane, przysługuje prawo wniesienia, w przypadkach wymienionych w art. 23 ust. 1 pkt. 4 i 5, pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację. Powołany przepis wyraźnie ogranicza prawo żądania zaprzestania przetwarzania danych jedynie do sytuacji, gdy przetwarzanie danych osobowych jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego lub, gdy jest ono niezbędne do wypełniania usprawiedliwionych celów administratora danych, o których mowa w art. 3 ust. 2 ustawy, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą. Generalny Inspektor podkreślał, że Związek Banków Polskich przetwarzając dane osobowe w Systemie Międzybankowej Informacji Gospodarczej czyni to na podstawie przesłanki wynikającej z art. 23 ust. 1 pkt 2 ustawy. Na przetwarzanie danych zezwala

³⁸² GI-DP-568/00, GI-DP-569/00, GI-DP-609/00, GI-DP-682/00, GI-DP-714/00, GI-DP-715/00, GI-DP-716/00

bowiem przepis art. 105 ust. 4 Prawa bankowego. W związku z powyższym, jeżeli osoby, których dane są przetwarzane w Systemie Międzybankowej Informacji Gospodarczej, spełniają kryteria wynikające z załącznika nr 1 do Regulaminu Wymiany Informacji w Systemie Międzybankowej Informacji Gospodarczej, to osobom tym nie przysługuje uprawnienie złożenia żądania zaprzestania przetwarzania ich danych osobowych. W konsekwencji, składanie w powyższych okolicznościach żądania zaprzestania przetwarzania danych osobowych, należy uznać za bezskuteczne. Wobec powyższego, Generalny Inspektor prosił o poinformowanie osób zgłaszających żądania, o których mowa w art. 32 ust. 1 pkt 7 ustawy, iż te żądania nie mogą być uwzględnione ze względu na brak uprawnienia do ich składania. Niedopuszczalne, zdaniem Generalnego Inspektora, jest informowanie klientów banku, iż przysługuje im uprawnienie do złożenia żądania zaprzestania przetwarzania ich danych osobowych w Systemie Międzybankowej Informacji Gospodarczej, a przesyłanie do Generalnego Inspektora tego rodzaju pism wynika z błędnej interpretacji art. 32 ust. 1 pkt. 7 ustawy.

Innym, nie mniej istotnym problemem, było nagminne niewypełnianie obowiązku informacyjnego w stosunku do klientów, których dane osobowe były przekazywane do "Bankowego Rejestru".³⁸³ Zgodnie z art. 24 ust. 1 ustawy o ochronie danych osobowych, w przypadku zbierania danych osobowych od osoby, której dane dotyczą, administrator danych jest zobowiązany poinformować tę osobę o uprawnieniach w zakresie określonym w pkt 1-4 tego przepisu. Banki nie informowały swoich klientów o przysługujących im prawach, albo też wykonywały obowiązek informacyjny częściowo. Generalny Inspektor uznając, że nie zachodzą żadne przesłanki zwalniające od tego obowiązku, zwrócił się do Prezesa Związku Banków Polskich o podjęcie stosownych działań pod kątem zgodności z ustawą o ochronie danych osobowych w celu usunięcia nieprawidłowości w funkcjonowaniu Systemu oraz instytucji bankowych.

W związku ze skargami dotyczącymi przetwarzania danych osobowych przez banki w związku z procedurą udzielania kredytu, w sytuacji, gdy umowa kredytu nie została zawarta Generalny Inspektor informował, że zgodnie z art. 70 ust. 1 Prawa bankowego, bank uzależnia przyznanie kredytu od zdolności kredytowej kredytobiorcy.³⁸⁴ Kredytobiorca jest obowiązany przedłożyć na żądanie banku dokumenty i informacje niezbędne do dokonania oceny tej zdolności. Przywołany przepis stanowi podstawę prawną do przetwarzania przez

³⁸³ GI-DP-024/1282/00

³⁸⁴ GI-DP-430/1351/00

bank danych osobowych niezbędnych do oceny zdolności kredytowej osoby ubiegającej się o przyznanie kredytu, w związku z koniecznością oceny zdolności kredytowej tej osoby.

Zgodnie z art. 131 Prawa bankowego, działalność banków oraz oddziałów i przedstawicielstw banków zagranicznych podlega nadzorowi sprawowanemu przez Komisję Nadzoru Bankowego w zakresie i na zasadach określonych w tej ustawie i w ustawie z dnia 29 sierpnia 1997 r. o Narodowym Banku Polskim (Dz. U. Nr 140, poz. 938). Zgodnie z art. 133 ust. 2 pkt 2 Prawa bankowego, czynności podejmowane w ramach nadzoru bankowego polegają w szczególności na badaniu zgodności udzielanych kredytów (...) z obowiązującymi w tym zakresie przepisami prawa. Zgodnie z art. 9 tej ustawy w bankach działa kontrola wewnętrzna, która sprawdza legalność i prawidłowość działalności prowadzonej przez bank oraz prawidłowość i rzetelność składanych sprawozdań i informacji.

Zachowanie w programie komputerowym informacji dotyczących potencjalnego kredytobiorcy potwierdza fakt, iż badanie zdolności kredytowej klienta zostało przeprowadzone, natomiast zachowanie dokumentów przedłożonych bankowi jest dowodem na to, iż dane, na podstawie których oceniano zdolność kredytową polegają na prawdzie i pochodzą od kredytobiorcy. W świetle przywołanych przepisów obligujących bank do wewnętrznej kontroli legalności i prawidłowości prowadzonej działalności oraz prawidłowości i rzetelności składanych sprawozdań i informacji oraz koniecznością wykazania się przed organem sprawującym nadzór legalnością wykonywanych czynności, w związku z procedurą udzielania kredytów, konieczne jest, aby bank posiadał dokumenty niezbędne do dowodzenia zasadności podjętych przez siebie decyzji. Bank przechowuje więc w swoich zbiorach dokumenty i informacje będące podstawą stwierdzenia legalności podjętych przez siebie działań. Dlatego też w zbiorach tej instytucji znajdują się zarówno informacje dotyczące potencjalnych kredytobiorców jak i dokumenty dostarczone przez te osoby w związku z procedurą udzielania kredytów. Należy więc stwierdzić, iż przechowywanie danych w zbiorach banku jest niezbędne do prawidłowego wypełniania obowiązków tego podmiotu określonych w przepisach prawa. Z powyższego wynika, iż przechowywanie danych osobowych oraz dokumentów zgromadzonych w związku z wnioskiem o udzielenie kredytu, pomimo odstąpienia przez klienta od dalszych starań o jego uzyskanie, jest działaniem legalnym, zgodnym z przepisami ustawy o ochronie danych osobowych.

Jednocześnie Generalny Inspektor wskazywał, że wprowadzie art. 12 ustawy o ochronie danych osobowych upoważnia go do kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych, jednak uprawnienie to nie obejmuje kontroli

prawidłowości wykonywania przez określone instytucje obowiązków wynikających z przepisów odrębnych. W tym przypadku na podstawie § 41 oraz § 42 ust. 2 pkt 2 lit. g uchwały Komisji Nadzoru Bankowego Nr 1/98 z dnia 3 czerwca 1998 r. w sprawie szczegółowych zasad rachunkowości banków i sporządzania informacji dodatkowej (Dz. Urz. NBP, Nr 14, poz. 27) bank ma obowiązek archiwizacji dokumentów przez okres 5 lat. Generalny Inspektor uznał, że przetwarzanie danych byłych klientów polegające na ich przechowywaniu, odbywa się zgodnie z przesłanką określoną w art. 23 ust. 1 pkt 2 ustawy, tj. zgodnie z uchwałą wydaną na mocy upoważnienia wyrażonego w art. 81 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. Nr 121, poz. 591 z późn. zm.) przez co nie narusza ustawy o ochronie danych osobowych.³⁸⁵

Generalny Inspektor wyjaśniał także, że zgoda osoby, której dotyczą dane osobowe, nie jest jedyną przesłanką legalności przetwarzania danych.³⁸⁶ Przetwarzanie jest także dopuszczalne, gdy jest niezbędne osobie, której dane dotyczą w celu wywiązania się z umowy, której jest stroną. Na mocy art. 23 ust. 1 pkt 3 ustawy o ochronie danych osobowych *bank może przetwarzać dane w celu wykonania postanowień zawartej umowy kredytu* (art. 23 ust. 1 pkt 3 ustawy o ochronie danych osobowych).

Natomiast podstawę *przetwarzania danych osobowych w celu marketingowym własnych produktów banku* stanowi art. 23 ust. 1 pkt 5 ustawy, zgodnie z którym przetwarzanie danych jest dopuszczalne także wówczas, gdy jest niezbędne do wypełnienia usprawiedliwionych celów administratorów danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą. W takim jednak przypadku osobie, której dotyczą dane, przysługuje prawo do wniesienia sprzeciwu wobec przetwarzania danych w celu marketingowym lub przekazywania danych innemu administratorowi danych, jeżeli przy zawieraniu umowy kredytu nie wyraziła zgody na przetwarzanie danych osobowych w celu promowania produktów banku (art. 32 ust. 1 pkt 8 ustawy). Ponadto wskazano, że wykorzystanie danych osobowych dla potrzeb marketingowych podmiotów finansowych innych niż bank, może się odbywać wyłącznie na podstawie odrębnej zgody osoby, której dane dotyczą.³⁸⁷

Generalny Inspektor otrzymał pismo, z którego wynikało, że jeden z banków przy *wpłatach na rachunki bankowe* wymagał od klientów zgody na przetwarzanie danych osobowych. Jednakże ze złożonych przez przedstawicieli banku wyjaśnień wynikało, że bank

³⁸⁵ GI-DIS-91/00

³⁸⁶ GI-DIS-206/00, GI-DP-453/00

³⁸⁷ GI-DP-448/00

uzyskuje zgodę wyłącznie od klientów, którzy zawarli umowę przed wejściem ustawy o ochronie danych osobowych w życie.³⁸⁸ Generalny Inspektor wyjaśnił, że bank jest uprawniony do przetwarzania określonej kategorii danych, ponieważ działanie takie znajduje podstawę w odpowiednich przepisach Prawa bankowego. Przetwarzanie danych jest niezbędne do realizowania czynności bankowych będących przedmiotem jego działalności, wymaganie zgody jest zatem zbędne.

Generalny Inspektor wyjaśniał także wątpliwości, czy bank podejmując *czynności zmierzające do wyegzekwowania swoich należności wynikających z zawartych umów rachunku bankowego, umów kredytowych*, a także innych umów objętych zakresem czynności bankowych, w szczególności zlecając wykonanie tych czynności firmie windykacyjnej, nie narusza ustawy o ochronie danych osobowych.³⁸⁹ W odpowiedzi zwrócono uwagę, że w tego rodzaju sprawach administratorem danych nadal pozostaje bank. Jeżeli zatem bank zleci przetwarzanie danych innemu podmiotowi, zgodnie z dyspozycją art. 31 ustawy, spełniając przy tym wynikające z tego przepisu obowiązki, nie narusza tym samym ustawy o ochronie danych osobowych. Jednocześnie zaznaczono, że zawarcie umowy powierzenia z firmą windykacyjną nie zwalnia banku z odpowiedzialności za przestrzeganie przepisów ustawy.

Na pytanie, *czy banki są uprawnione do żądania od swoich klientów zaświadczeń o niekaralności*, Generalny Inspektor odpowiadał, że działanie takie nie jest dopuszczalne. Wszędzie bowiem tam, gdzie przepisy ustaw szczególnych nie tworzą podstaw prawnych do przetwarzania danych o karalności określonej osoby, przetwarzanie takich informacji jest zabronione. Odbieranie oświadczeń o tym, że osoby nie były karane, oraz że nie toczy się przeciwko nim postępowanie karne, czy karno-skarbowe, jest gromadzeniem danych o karalności tych osób.³⁹⁰ Zgodnie z art. 28 ust. 1 ustawy o ochronie danych osobowych przetwarzanie danych dotyczących skazań można prowadzić wyłącznie na podstawie ustawy. Jeśli więc ustawa wprost nie upoważnia banku do gromadzenia tego typu informacji o pracownikach i klientach tej instytucji, bank nie może przetwarzać ich bez względu na to, czy odbywałoby się to za zgodą, czy bez zgody osoby, której dane dotyczą.³⁹¹

Jeden z banków zwrócił się do Generalnego Inspektora ze skargą na odmowę *udostępnienia przez spółdzielnię danych osobowych dłużników banku*.³⁹² W myśl art. 96

³⁸⁸ GI-DIS-218/00

³⁸⁹ GI-DP-024/1317/00

³⁹⁰ GI-DP-024/1390/00

³⁹¹ GI-DP-147/00

³⁹² GI-DP-308/00

Prawa bankowego banki, na podstawie ksiąg banków lub innych dokumentów związanych z dokonywaniem czynności bankowych mogą wystawiać bankowe tytuły egzekucyjne. Bankowy tytuł egzekucyjny może być podstawą egzekucji prowadzonej według przepisów Kodeksu postępowania cywilnego po nadaniu przez sąd klauzuli wykonalności. Na podstawie art. 61 ustawy z dnia 6 lipca 1982 r. o księgach wieczystych i hipotece (Dz. U. Nr 12, poz. 147 z późn. zm.), księgę wieczystą dla nieruchomości nie stanowiącej własności państwowej zakłada się na wniosek właściciela nieruchomości lub osoby, której przysługuje ograniczone prawo rzeczowe, albo na wniosek wierzyciela, jeżeli przysługuje mu prawo, które może być wpisane w księdze wieczystej. Wierzyciel może być zatem wnioskodawcą w postępowaniu o założenie księgi wieczystej wszczętym w związku z koniecznością dokonania w księdze wieczystej wpisu wniosku o egzekucję z tej nieruchomości (por. uchwała SN z 24 września 1986 r., sygn. U III CZP 63/86 OSNC 1987/10/151).

Zgodnie z § 49 rozporządzenia Ministra Sprawiedliwości z dnia 18 marca 1992 r. w sprawie wykonania przepisów o księgach wieczystych i hipotece (Dz. U. Nr 29 poz. 128 z późn. zm.) wniosek o założenie księgi wieczystej dla własnościowego spółdzielczego prawa do lokalu powinien zawierać w szczególności określenie miejsca położenia i powierzchni lokalu, wymienienie osoby, której przysługuje własnościowe spółdzielcze prawo do lokalu, powołanie tytułu nabycia własnościowego spółdzielczego prawa do lokalu oraz oświadczenie zarządu spółdzielni o przyjęciu w poczet członków spółdzielni, wyszczególnienie obciążających własnościowe prawo do lokalu ograniczonych praw rzeczowych lub ograniczeń w rozporządzaniu lub oświadczenie wnioskodawcy, że nie wie o istnieniu takich praw lub ograniczeń. Z przepisów tych wynika niewątpliwie kompetencja do przetwarzania danych osobowych dłużników przez bank oraz zakres zbieranych danych. Przepisy art. 61 ustawy o hipotece, oraz § 49 cytowanego wyżej rozporządzenia stanowią przesłankę legalności przetwarzania danych, o której mowa w art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych (przepis prawa).

Zasady udostępniania danych osobowych członków przez spółdzielnię określają ponadto przepisy ustawy dnia 16 września 1982 r. Prawo spółdzielcze (Dz. U. 1995 r. Nr 54, poz. 288 z późn. zm.). Na podstawie art. 30 Prawa spółdzielczego zarząd spółdzielni prowadzi rejestr członków zawierający ich imiona i nazwiska oraz miejsce zamieszkania, wysokość zadeklarowanych i wniesionych udziałów, wysokość wniesionych wkładów, ich rodzaj, jeżeli są to wkłady niepieniężne, zmiany tych danych, datę przyjęcia w poczet członków, datę wypowiedzenia członkostwa i jego ustania, a także inne dane przewidziane w

statucie. Generalny Inspektor stwierdził brak podstaw prawnych do udostępniania bankom informacji w zakresie szerszym niż wynikający z dyspozycji art. 30 Prawa spółdzielczego.

Do Generalnego Inspektora Ochrony Danych Osobowych zwracano się także z prośbą o zajęcie stanowiska w kwestii *dopuszczalności udostępnienia przez spółdzielnię mieszkaniową dokumentów niezbędnych do kontroli prawidłowości spłaty kredytu mieszkaniowego udzielonego przez bank na sfinansowanie kosztów realizacji spółdzielczego budownictwa mieszkaniowego*.³⁹³ W odpowiedzi Generalny Inspektor stwierdził, że art. 6 pkt 1 ustawy z dnia 30 listopada 1995 r. o pomocy państwa w spłacie niektórych kredytów mieszkaniowych, refundacji bankom wypłaconych premii gwarancyjnych oraz zmianie niektórych ustaw (Dz. U. Nr 5, poz. 32 z późn. zm.) przewiduje, iż w celu pomocy państwa w spłacie kredytów mieszkaniowych, z budżetu państwa przekazywane są bankom środki w wysokości oprocentowania obliczanego według stopy procentowej ustalonej przez Radę Ministrów, pod warunkiem dokonywania przez kredytobiorcę spłat w wysokości wynikającej z przepisów tej ustawy. Na podstawie art. 6 pkt 2 wskazanej ustawy, z tytułu przejściowego wykupienia odsetek od kredytów mieszkaniowych przez Skarb Państwa, bank, który udzielił kredytu, zobowiązany jest wobec Skarbu Państwa do administrowania i egzekwowania zadłużenia kredytobiorców. Kredytobiorcą, na podstawie art. 2 pkt 4 ww. ustawy jest również członek spółdzielni mieszkaniowej zajmujący lokal obciążony kredytem zaciągnięty przez spółdzielnię. W związku z tym, Skarb Państwa, przeznaczając pewne środki z budżetu państwa na pomoc w spłacie określonych ustawą kredytów mieszkaniowych warunkuje otrzymanie tej pomocy od dokonywania przez kredytobiorcę spłat w wysokości wynikającej z przepisów ustawy. Jako egzekutora tych należności ustawa wyznacza bank, który udzielił kredytu. Tym samym bank kredytujący budownictwo mieszkaniowe jest upoważniony do kontroli dokumentacji dotyczącej zadłużenia poszczególnych członków spółdzielni z tytułu kredytu mieszkaniowego, będących w świetle przepisów ustawy kredytobiorcami. Jest to, zdaniem Generalnego Inspektora, dostateczna podstawa prawna powodująca, że spełniona zostaje przesłanka przetwarzania danych określona w art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych. Udostępnienie zatem bankowi informacji dotyczących stanu zadłużenia z tytułu kredytu w poszczególnych lokalach przez zarząd spółdzielni mieszkaniowej nie jest naruszeniem przepisów ustawy o ochronie danych osobowych.

Generalny Inspektor odpowiadał na pytania dotyczące dopuszczalności *udzielania przez banki informacji w trybie określonym w art. 29 ustawy o ochronie danych osobowych*.

³⁹³ GI-DP-925/00

Wątpliwości banków dotyczyły w szczególności wzajemnej relacji przepisów o tajemnicy bankowej do przepisów ustawy o ochronie danych osobowych.³⁹⁴ Generalny Inspektor wskazywał, że zgodnie z art. 5 ustawy o ochronie danych osobowych, jej przepisów nie stosuje się, jeżeli przepisy innych ustaw przewidują dalej idącą ochronę. Tak właśnie jest w przypadku wzajemnego stosunku przepisów ustawy prawo bankowe i przepisów ustawy o ochronie danych osobowych, a udostępnienie danych objętych tajemnicą bankową powinno następować na podstawie art. 105 ustawy Prawo bankowe. Jednocześnie Generalny Inspektor podkreślił, że banki nie należą do podmiotów wymienionych w art. 3 ust. 1 ustawy o ochronie danych osobowych, wobec czego do udostępniania przez nie danych nie stosuje się przepisu art. 29 tej ustawy.

Zgodnie z art. 104 ust. 1 ustawy Prawo bankowe, banki i osoby w nich zatrudnione oraz osoby, za których pośrednictwem bank wykonuje czynności bankowe, są obowiązane zachować tajemnicę bankową, która obejmuje wszystkie wiadomości:

1) dotyczące czynności bankowych i osób będących stroną umowy, uzyskane w czasie negocjacji oraz związane z zawarciem umowy z bankiem i jej realizacją, z wyjątkiem wiadomości, bez których ujawnienia nie jest możliwe należyte wykonanie zawartej przez bank umowy,

2) dotyczące osób, które nie będąc stroną umowy, o której mowa w pkt 1 dokonały czynności pozostających w związku z zawarciem takiej umowy, z wyjątkiem przypadków, gdy ustawa przewiduje ujawnienie takich czynności.

Z przepisu ust. 2 wskazanego wyżej art. 104 ustawy Prawo bankowe wynika, że banku nie obowiązuje zachowanie tajemnicy wobec strony umowy. Natomiast wiadomości te nie mogą być ujawnione osobom trzecim, poza szczególnymi przypadkami, określonymi w ustawie. Z uwagi na powyższe nie jest również dopuszczalne *ujawnienie danej osobie informacji o numerze konta jej małżonka*.³⁹⁵

Pytano również, czy jest dopuszczalne umieszczenie danych poręczycieli w rejestrze niesolidnych dłużników, bez uprzedniego postawienia całej należności w natychmiastowy stan płatności.³⁹⁶ W odpowiedzi Generalny Inspektor stwierdził, że umieszczenie na liście osoby, która nie jest obowiązana do spłaty należności może naruszać przepisy ustawy o ochronie danych osobowych. Zgodnie z art. 876 § 1 ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. Nr 16, poz. 93 z późn. zm.), przez umowę poręczenia poręczyciel

³⁹⁴ GI-DP-464/00

³⁹⁵ GI-DP-1179/00

³⁹⁶ GI-DP-024/1650/00

zobowiązuje się względem wierzyciela wykonać zobowiązanie na wypadek, gdyby dłużnik zobowiązania nie wykonał. Jednocześnie art. 880 K.c. stanowi, że jeżeli dłużnik opóźnia się ze spełnieniem świadczenia, wierzyciel powinien zawiadomić o tym niezwłocznie poręczyciela. W myśl art. 881 K.c. w braku odmiennego zastrzeżenia poręczyciel jest odpowiedzialny jak współdłużnik solidarny. Poręczyciel, mimo że odpowiada za cudzy dług, to jednak wykonuje własne zobowiązanie względem wierzyciela. Może on zatem być uznany za niesolidnego dłużnika tylko wówczas, gdy nie wywiązuje się lub niewłaściwie wywiązuje się z zaciągniętego przez siebie zobowiązania (poręczenia). Sam fakt, że osoba, której dług został poręczony, nie wypełnia swojego zobowiązania nie oznacza, że niesolidnym dłużnikiem jest także poręczyciel. Poręczyciel odpowiada za dług dopiero wówczas, gdy dłużnik nie wykonuje swojego zobowiązania. Dług ten musi być oczywiście wymagalny, choć niekoniecznie w całości. O zakresie odpowiedzialności poręczyciela przesądza treść umowy poręczenia lub, w jej braku, przepisy prawa oraz zakres zobowiązania dłużnika.

Zgodnie z art. 75 Prawa bankowego, w razie stwierdzenia przez bank kredytujący, że warunki udzielenia kredytu nie zostały dotrzymane, lub w razie zagrożenia terminowej spłaty kredytu z powodu złego stanu majątkowego kredytobiorcy, bank może m.in. wypowiedzieć umowę kredytu w całości lub w części.

Odpowiedzialność poręczyciela nie jest zatem uzależniona od zażądania przez bank spłaty całej należności kredytowej. Zgodnie z art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych, administrator danych jest obowiązany do zapewnienia, aby dane przez niego gromadzone były merytorycznie poprawne. Jeżeli osoba niesłusznie figuruje w zbiorze danych, jako niesolidny dłużnik, stanowi to naruszenie ustawy o ochronie danych osobowych.

Generalny Inspektor zajmował się sprawą udostępniania danych osobowych klientów banków osobom niepowołanym, poprzez *niewłaściwie ustawione monitory* na stanowisku obsługi klienta. Wielokrotne skargi klientów kierowane bezpośrednio do banku pozostawały bez odpowiedzi. Dopiero podjęcie tej sprawy przez Generalnego Inspektora, umożliwiło wyeliminowanie tego rodzaju zjawisk. Nieprawidłowości polegały na tym, że w chwili otwierania nowego konta, na monitorze umieszczonym w taki sposób, by klient mógł kontrolować poprawność danych zbieranych przez bank, pojawiały się dane osobowe wszystkich pozostałych klientów tego banku noszących to samo nazwisko. W złożonych Generalnemu Inspektorowi wyjaśnieniach stwierdzono, że funkcja przeglądania danych osobowych klientów o tym samym nazwisku uruchomiona została przez bank na skutek

zastosowania przez pracownika nieprawidłowej procedury.³⁹⁷ W celu wyeliminowania takich przypadków procedura została zmodyfikowana w taki sposób, aby pracownik nie miał możliwości uruchomienia funkcji sprawdzania na stanowisku obsługi klienta zlokalizowanym na sali operacyjnej. Jednocześnie, na skutek interwencji Generalnego Inspektora, wprowadzono dodatkowy element ochrony fizycznej monitorów przed wglądem do nich osobom nieuprawnionym (poprzez powleczenie ich specjalną folią uniemożliwiającą odczytanie informacji osobie patrzącej na monitor pod kątem ostrym). Jednocześnie poinformowano, że pracownicy winni uchybień zostali ukarani dyscyplinarnie.

Szczególnie niepokojące były sygnały, z których wynikało, że banki nie dopełniają podstawowego obowiązku spoczywającego na nich, jako na administratorze danych, mianowicie *obowiązku aktualizacji danych, tj. zapewnienia, aby gromadzone przez banki informacje odpowiadały rzeczywistemu stanowi rzeczy*. Do Generalnego Inspektora kierowano pisma, z których wynikało, że banki wysyłają określone informacje, takie jak wyciągi z rachunków bankowych, zestawienia, a nawet karty kredytowe na *nieaktualne adresy klientów*, pomimo że zgłaszali oni zmianę miejsca zamieszkania. Nagminnie, o czym świadczy także liczba telefonów, było *ignorowanie dyspozycji klientów dotyczących adresu, pod którym chcieliby oni otrzymywać korespondencję z banku*.³⁹⁸ Generalny Inspektor odpowiadał, że obowiązki spoczywające z mocy ustawy o ochronie danych osobowych na administratorach danych dotyczą w szczególności banków. Są one obowiązane zatem do odpowiedniego zabezpieczenia danych oraz do zapewnienia, by były one merytorycznie poprawne. W żadnym wypadku nie usprawiedliwia uchybień w tym zakresie rozbudowana struktura organizacyjna, ani wadliwie działający system informatyczny.³⁹⁹ Generalny Inspektor pouczał także, o przysługującym osobom korzystającym z usług banków, prawie do kontroli przetwarzania danych, które ich dotyczą.⁴⁰⁰

W związku ze znaczną liczbą tego rodzaju spraw, oraz z uwagi na dotkliwość skutków ewentualnych naruszeń, Generalny Inspektor zwrócił uwagę Prezesa Związku Banków Polskich na fakt, że spowodowane brakiem aktualizacji danych przypadki ujawnienia tajemnicy bankowej, stanowią nie tylko istotną uciążliwość dla klientów banku oraz osłabiają zaufanie klientów do tychże instytucji, ale również naruszają przepisy ustawy o ochronie danych osobowych.⁴⁰¹

³⁹⁷ GI-DIS-430/386/00

³⁹⁸ GI-DP-024/1929/00

³⁹⁹ GI-DP-841/00

⁴⁰⁰ GI-DP-024/1747/00

⁴⁰¹ GI/194/00

Niektóre przypadki naruszenia przepisów, zarówno ustawy Prawo bankowe, jak i przepisów ustawy o ochronie danych osobowych, wynikały z *niedoskonałości systemu PESEL*, przy czym na skutek interwencji Generalnego Inspektora podjęto czynności mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.⁴⁰²

Niezwykle istotną gwarancją przewidzianą w przepisach ustawy o ochronie danych osobowych dla osób, których dane są przetwarzane jest formułowana w art. 26 ust. 1 ustawy o ochronie danych osobowych zasada adekwatności.⁴⁰³

Poważne zaniepokojenie Generalnego Inspektora wzbudziły sygnały o *wykonywaniu przez banki kserokopii dowodów osobistych lub paszportów*. Generalny Inspektor wskazywał, że tego rodzaju praktyki naruszają przepisy o ochronie danych osobowych. Na bankach spoczywa obowiązek dołożenia należytej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności obowiązek zapewnienia, aby dane te przetwarzane były zgodnie z prawem, zbierane dla oznaczonych, zgodnych z prawem celów, merytorycznie poprawne i adekwatne do celów, w jakich są przetwarzane. Z przepisów Prawa bankowego wynika, że świadczenie przez banki usług bankowych na rzecz ich klientów następuje na mocy zawartej między nimi pisemnej umowy. Dla oznaczenia stron tej umowy niezbędne jest dysponowanie przez banki informacjami o imieniu i nazwisku klienta, dacie jego urodzenia, numerze PESEL, adresie oraz aktualnym miejscu pracy. Przetwarzanie jakichkolwiek innych danych osobowych klientów banków, zdaniem Generalnego Inspektora, uznać należy za naruszające zasadę adekwatności. Generalny Inspektor zauważył, że żaden z przepisów Prawa bankowego nie wskazuje ani w formie obligatoryjnej, ani fakultatywnej na konieczność kopiowania dokumentacji celem identyfikacji jej właściciela, a zatem żaden z tych przepisów nie uprawnia banku, jako administratora danych do sporządzania kserokopii dokumentów osób, których dane dotyczą. Istota zarzutu Generalnego Inspektora Ochrony Danych Osobowych odnosiła się do praktyki gromadzenia zbyt szerokiego zakresu danych klientów, niezależnie od tego, czy uzyskanie danych następuje na skutek okazania (i przepisania), czy kopiowania dokumentu klienta. Wskazane sposoby pozyskiwania danych prowadzą bowiem, w ocenie Generalnego Inspektora, do tego samego skutku – pozyskania zakresu danych nieadekwatnego do celu ich przetwarzania. Jest to praktyka nie znajdująca uzasadnienia w obowiązujących przepisach.

Generalny Inspektor podkreślił, że dowód osobisty, oprócz danych niezbędnych do potwierdzenia tożsamości i aktualnego miejsca zamieszkania klienta banku zawiera także

⁴⁰² GI-DIS-107/00

dane z jego sfery prywatnej, które są zbędne dla realizacji umowy kredytowej, a które są jednak włączane do zbioru danych banku w wyniku sporządzania kopii dokumentu. Są to informacje odnoszące się do osób trzecich, tj. imiona rodziców, nazwisko panięńskie matki, informacje o dzieciach lub innych osobach pozostających pod opieką klienta banku. O ile podstawą do przetwarzania danych klienta jest konieczność wywiązania się z umowy lub zgoda podmiotu danych, o której mowa w art. 23 ust. 1 pkt 1 ustawy, to taka podstawa nie istnieje w odniesieniu do danych o osobach trzecich (rodziców i dzieci klienta). Zgodnie bowiem z definicją zgody osoby, której dane dotyczą, zawartą w art. 7 pkt 5 ustawy, jest to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiała z oświadczenia woli o innej treści. Przedmiotowe działanie prowadzi do pozyskania danych całkowicie zbędnych dla realizacji umowy kredytu zawieranej z bankiem, a więc przetwarzania danych nieadekwatnych do osiągnięcia celu przetwarzania.

Generalny Inspektor zauważył, iż legalność przetwarzania danych osobowych nie może być uzależniona od subiektywnej oceny administratora danych. Przetwarzając dane osobowe klientów bank ingeruje w ich dobro prawne, jakim jest zagwarantowane konstytucyjnie prawo do prywatności i wyłącznego dysponowania swoimi danymi (art. 47 Konstytucji). W sytuacji zawierania umowy prawo to musi być z oczywistych względów ograniczone, gdyż strony stosunków cywilnoprawnych powinny być oznaczone. Zgodnie jednak z art. 26 ust. 1 pkt 3 ustawy administrator danych przetwarzający dane powinien dołożyć należytej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane. W związku z powyższym, przetwarzanie danych osobowych, a przez to naruszanie wyłącznego prawa podmiotu do dysponowania nimi, powinno być ograniczone do minimum koniecznego dla realizacji umowy.

Przeprowadzane w bankach inspekcje wykazywały niejednokrotnie *naruszenie podstawowych obowiązków określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych* (Dz. U. Nr 80, poz. 521). W wydawanych decyzjach Generalny Inspektor nakazywał, m.in. zamieszczanie w

⁴⁰³ GI-DP-933/00

indywidualnym zakresie czynności każdej osoby zatrudnionej przy przetwarzaniu danych osobowych zakresu odpowiedzialności tej osoby za ochronę danych przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem - w stopniu odpowiednim do zadań tej osoby przy przetwarzaniu danych, zgodnie z § 4 cytowanego wyżej rozporządzenia. Nakazywano również, wprowadzenie takich zmian, by system informatyczny, w którym przetwarzane są dane osobowe umożliwiał udostępnienie na piśmie, w powszechnie zrozumiałej formie, treści danych osobowych o każdej osobie, której dane są przetwarzane, wraz z informacjami o żądaniu, o którym mowa w art. 32 ust. 1 pkt 7 ustawy o ochronie danych osobowych, po jego uwzględnieniu, oraz sprzecznie określonym w art. 32 ust. 1 pkt 8 ustawy.⁴⁰⁴

J. DZIAŁALNOŚĆ MARKETINGOWA

Na gruncie ustawy o ochronie danych osobowych największe kontrowersje budzą działania firm marketingowych. W powszechnej świadomości to przede wszystkim działalność tych podmiotów kojarzy się z naruszaniem przepisów o ochronie danych osobowych. Pod pojęciem przetwarzania danych w celu marketingowym nie można jednak rozumieć wyłącznie działalności firm wyspecjalizowanych w analizie rynku, które zajmują się profesjonalnie handlem bazami danych, udostępniającymi wyniki swoich badań innym podmiotom gospodarczym, czy wykorzystujących zebrane przez siebie dane osobowe do przeprowadzenia odpowiednich kampanii reklamowych. Skargi, z którymi zetknął się Generalny Inspektor Ochrony Danych Osobowych dotyczyły również marketingu własnych produktów takich podmiotów, jak: banki, zakłady ubezpieczeniowe i fundusze emerytalne, zakłady energetyczne, czy telefonie komórkowe, a także promowania przez ww. administratorów danych produktów i usług oferowanych przez inne podmioty.⁴⁰⁵ Analiza materiału zebranego w roku 2000 pozwoliła na ustalenie, iż w porównaniu do roku 1999 (200 skarg), w omawianym okresie sprawozdawczym utrzymała się wysoka liczba skarg związanych z działalnością marketingową firm – zarejestrowano ok. 190 skarg. Wielość oraz różnorodność skarg i pytań prawnych, a także wyniki przeprowadzonych kontroli i postępowań administracyjnych wykazały, iż przetwarzanie danych w ramach obrotu marketingowego dokonywane było najczęściej niezgodnie z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.). Przy

⁴⁰⁴ GI-DP-DEC/3/00

⁴⁰⁵ Powyższa problematyka została poruszona w pozostałych działach części I Sprawozdania.

czym należy zauważyć, iż wielokrotnie skargi te dotyczyły działalności tych samych, co w latach 1998 -1999 firm marketingowych.⁴⁰⁶

W omawianym okresie sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych ponownie stanął przed problemem rozstrzygnięcia zakresu pojęcia marketingu wewnętrznego i zewnętrznego, jak również zakresu praw i obowiązków podmiotów uczestniczących w reklamie i promocji produktów i usług. Ponieważ polska ustawa o ochronie danych nie sprecyzowała pojęcia marketingu, posiłkowano się często definicją zawartą w art. 1 Rekomendacji R(85)20 Komitetu Ministrów Rady Europy, zgodnie z którym przez „marketing bezpośredni” należy rozumieć ogół działań, jak również wszelkich dotyczących go usług pomocniczych umożliwiających oferowanie produktów i usług, bądź przekazywanie oświadczeń kierowanych do ludności – za pośrednictwem kurierów, telefonów lub innych bezpośrednich środków – w celach informacyjnych bądź w celu wywołania reakcji ze strony osoby zainteresowanej.

Należy podkreślić, że choć w zakresie cytowanej definicji mieści się wysyłanie przez różne podmioty przesyłek bezadresowych, w stosunku do takiej działalności przepisy ustawy nie znajdują zastosowania, gdyż w niniejszej sytuacji nie dochodzi do przetwarzania danych osobowych.

Uwzględniając charakter działalności marketingowej należy wskazać, iż administratorzy danych przetwarzający dane w tym celu przede wszystkim są obowiązani legitymować się przesłanką przetwarzania, o której mowa w art. 23 ust. 1 pkt 1, tj. gdy osoba, której dane dotyczą wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych. Oprócz zgody osoby, której dane dotyczą, przesłanką zezwalającą, w pewnych okolicznościach, na przetwarzanie danych osobowych jest art. 23 ust.1 pkt 5 ustawy, tj. przetwarzanie danych jest dopuszczalne wtedy, gdy jest niezbędne do wypełnienia usprawiedliwionych celów administratora danych, o którym mowa w art. 3 ust. 2, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą.

Wielu administratorów danych nie ma świadomości, iż naruszają oni ustawę o ochronie danych osobowych. Podmioty te wychodząc z założenia, że raz zebrane dane stają się ich własnością, zmieniają cel przetwarzania danych, np. *dane zebrane w celu zawarcia lub wywiązania się z umowy są wykorzystywane w innym niż pierwotnie celu*. Zgodnie z art. 26 ust. 1 pkt 2 ustawy o ochronie danych osobowych administrator przetwarzający dane powinien dołożyć należytej staranności w celu ochrony osób, których dane dotyczą,

⁴⁰⁶ Przykładem mogą być takie firmy, jak: Przegląd Reader's Digest Sp. z o. o., IMP Sp. z o. o., ZXY Sp. z o. o.,

a w szczególności jest obowiązany zapewnić, aby dane te były zbierane dla oznaczonych zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami. Ukształtowana w przytoczonym przepisie jedna z fundamentalnych zasad ochrony danych osobowych, tj. zasada niezmienności celu przetwarzania danych wskazuje, że administrator danych może wykorzystywać informacje znajdujące się w prowadzonych przez niego zbiorach jedynie w ściśle określonym celu, dla realizacji którego zostały zgromadzone. Zmiana celu przetwarzania może nastąpić jedynie po spełnieniu jednej z przesłanek dopuszczalności przetwarzania, określonych w art. 23 ust. 1 ustawy. Osoba, której dane dotyczą powinna być dokładnie, wyczerpująco i w sposób dla niej zrozumiały poinformowana o celach przetwarzania danych. Tylko pod tym warunkiem udzielona zgoda jest prawnie skuteczna.⁴⁰⁷

W sytuacji, gdy prowadzona akcja marketingowa nie mieściła się w zakresie określonym celami działania, w wydawanych decyzjach administracyjnych Generalny Inspektor nakazywał przywrócenie stanu zgodnego z prawem poprzez wykorzystanie posiadanych w zbiorze danych tylko w celu, dla którego zostały zebrane.⁴⁰⁸ Nakazywano, np. modyfikację formuły zgody, która spowoduje jej udzielenie w sposób niezależny od przetwarzania danych dla celów realizacji umowy. W ocenie Generalnego Inspektora powinna to być odrębna i wyraźna zgoda osoby, której dane dotyczą, gdyż przez zgodę, w myśl art. 7 pkt 5 ustawy, rozumie się oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie. Zatem zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.⁴⁰⁹

Źródłem innych uchybień było przekonanie, iż raz udzielona zgoda na przetwarzanie danych określonej osoby wyrażona w stosunku do jednego podmiotu może być przedmiotem sukcesji prawnej, dlatego też przenoszono zgodę na inne podmioty, udostępniając (zbywając) równocześnie zbiory danych firmom, które wykorzystywały je przy organizacji akcji promocyjnych.⁴¹⁰ W takich przypadkach zwracano uwagę na regulacje prawne ustawy o ochronie danych, w których przedmiotowe działania są dopuszczalne jedynie w razie wyraźnego zastrzeżenia i uzyskania nowej wyraźnej zgody, której nie można

MedAdress Polonia Sp. z o. o.

⁴⁰⁷ GI-DP-868/00/1119

⁴⁰⁸ GI-DP-DEC-44/00/680

⁴⁰⁹ GI-DEC-DP-8/00

⁴¹⁰ GI-DIS-2/00, GI-DIS-20/00, GI-DIS-62/00, GI-DIS-73/00

domniemywać.⁴¹¹ Poza nielicznymi wyjątkami ustawa o ochronie danych osobowych nie przewiduje obowiązku wyrażenia zgody w określonej formie. Oświadczenie to może zatem zostać złożone w formie pisemnej, ustnej lub jakiejkolwiek innej (np. przez naciśnięcie ikony w programie komputerowym, w formie telefonicznej lub za pomocą innych urządzeń teletransmisji danych) pod warunkiem, że w sposób dostateczny i wyraźny ujawnia wolę osoby składającej to oświadczenie.⁴¹² Podkreślano przy tym, iż w razie ewentualnego sporu ciężar dowodu spoczywa na administratorze danych.⁴¹³

W omawianym okresie sprawozdawczym zaobserwowano również wzrost liczby skarg dotyczących *przekazywania danych osobowych w celach marketingowych za granicę, bez wiedzy lub wyraźnej zgody osób, których dane dotyczą*.⁴¹⁴ Przeprowadzone wskutek jednej ze skarg postępowanie wyjaśniające ujawniło, że dealerzy znanej firmy samochodowej przekazują informacje o klientach do centrali przedsiębiorstwa, znajdującej się poza granicami Polski. Wprawdzie firma zwróciła się o wyrażenie zgody na przetwarzanie danych określonego klienta i poinformowała o przekazywaniu danych jego dotyczących innym spółkom z nią współpracującym i dealerom firmy, jednakże nie poinformowano komu konkretnie dane zostały przekazane. Nie uwzględniono również faktu, iż zgody wymaga nie tylko samo przetwarzanie danych, ale i zmiana celu, dla którego dane te zostały zebrane.⁴¹⁵ Jeżeli przekazywanie danych pomiędzy podmiotami następuje w oparciu o zawartą między nimi umowę, to wobec braku zgody skarżącego na wykorzystywanie jego danych w celach marketingowych nie może być uznane za dopuszczalne wykorzystanie ich w tym celu.⁴¹⁶ W związku z powyższym, Generalny Inspektor nakazywał niewykorzystywanie danych osobowych klientów w celach marketingowych w sytuacji, gdy administratorzy ci przetwarzają dane w powyższy sposób na innej podstawie, niż zgoda osoby, której dane dotyczą.⁴¹⁷

Zgoda osoby uprawnionej ma wprawdzie charakter priorytetowy, lecz nie jest jedyną przesłanką, na podstawie której można przetwarzać dane osobowe. W wielu z kierowanych do Biura pism podnoszono fakt naruszenia ustawy o ochronie danych osobowych poprzez przesyłanie niezamówionych zestawów publikacji, stanowiących część serii wydawniczej. W wyniku przeprowadzonych czynności wyjaśniających w jednej ze spraw Generalny

⁴¹¹ GI-DP-DEC-44/00

⁴¹² GI-DP- 1117/00/1619, GI-DP-024/1260/00

⁴¹³ GI-DP-495/00/731

⁴¹⁴ GI-DP-1732/00, GI-DIS-136/99/54/00

⁴¹⁵ Por. artykuł „Bez wiedzy i zgody klienta” [w:] Prawo i Gospodarka z dnia 22 grudnia 2000 r.

⁴¹⁶ GI-DEC-DP-7/00

inspektor ustalił, że spółka przetwarzała dane skarżącej na podstawie art. 23 ust. 1 pkt 3 ustawy (umowa prenumeraty), w oparciu o złożone zamówienie tzw. „zestawu inauguracyjnego”. Wraz ze zwrotem paczki inauguracyjnej spółka zaprzestała świadczenia usługi na rzecz skarżącej.⁴¹⁸ Wyjaśnił ponadto, iż w sytuacji gdy dane są przetwarzane w oparciu o zawartą z klientem umowę nie jest konieczne uzyskiwanie zgody osoby, której dane dotyczą. W tego rodzaju sytuacjach nie przysługuje również sprzeciw, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.⁴¹⁹

Jak Generalny Inspektor zauważył, w roku 2000 administratorzy danych (zwłaszcza sektor prywatny) - częściej niż w roku 1999 – przetwarzając dane w zbiorze, legitymowali się przesłanką dopuszczalności przetwarzania danych z art. 23 ust. 1 pkt 5 ustawy o ochronie danych osobowych (gdy jest to niezbędne do wypełnienia usprawiedliwionych celów administratora danych, o których mowa w art. 3 ust. 2 ustawy).⁴²⁰ W takich sytuacjach Generalny Inspektor informował skarżących o prawie do kontroli przetwarzania danych, prawie wniesienia pisemnego umotywowanego żądania zaprzestania przetwarzania danych ze względu na szczególną sytuację, a także o prawie wniesienia sprzeciwu wobec przetwarzania danych osoby, gdy administrator zamierza je przetwarzać w celach marketingowych lub wobec przekazania danych osobowych innemu administratorowi.⁴²¹ W przypadku wniesienia sprzeciwu dalsze przetwarzanie danych, np. poprzez przysyłanie kolejnych ankiet, ulotek itp. materiałów promocyjnych, jest niedopuszczalne, bowiem zgodnie z art. 32 ust. 3, w razie wniesienia sprzeciwu wobec przetwarzania danych osobowych w celach marketingowych, dalsze przetwarzanie kwestionowanych danych jest niedopuszczalne.⁴²² Wiele tego rodzaju informacji udzielono również osobom telefonującym do Biura Generalnego Inspektora Ochrony Danych Osobowych, które prosiły o spowodowanie, aby administratorzy ich danych przestali przetwarzać te dane w celu marketingowym.

Analiza liczby skarg, jakie napłynęły do Generalnego Inspektora w omawianym okresie sprawozdawczym wykazała, iż najliczniejsza ich grupa dotyczyła nieuwzględnienia przez firmy marketingowe sprzeciwu osób, których dane są wykorzystywane w celach marketingowych.⁴²³ Niektóre z firm postępowanie takie argumentowały nieprawidłową w ich ocenie, ustną formą wniesionego sprzeciwu, inne firmy żądanie zaprzestania przetwarzania

⁴¹⁷ GI-DEC-DP-7/00, GI-DEC-DP-17/00

⁴¹⁸ GI-DIS-128/00, GI-DIS-226/00, GI-DIS-430/447/00

⁴¹⁹ GI-DP-1079/00/1544

⁴²⁰ GI-DP-024/1435/00

⁴²¹ GI-DIS-156, 157/00, GI-DIS-172,173/00

⁴²² GI-DP-430/1356/00

danych nie traktowały jako tożsamego z instytucją sprzeciwu.⁴²⁴ Zgodnie z art. 32 ust. 1 pkt 8 ustawy, każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do wniesienia sprzeciwu wobec przetwarzania tych danych, w przypadku, gdy nie wyraziła wcześniej na to zgody. Sprzeciw można złożyć wobec przetwarzania danych dla celów marketingowych, niezależnie od tego, czy administrator danych to firma marketingowa czy podmiot, którego podstawowym przedmiotem działalności nie jest działalność marketingowa, jak też wobec przekazywania innemu administratorowi niezależnie od tego, w jakim celu dane zostały zebrane i w jakim są udostępnione.⁴²⁵ Ustawa nie określa formy przedmiotowego sprzeciwu, tak więc każdą czynność podmiotu danych, z której wynika jego żądanie zaprzestania wykorzystania kwestionowanych danych w celach marketingowych, uznać należy za sprzeciw w rozumieniu przepisu art. 32 ust. 1 pkt 8 ustawy. Sprzeciw taki w ocenie Generalnego Inspektora nie może być też dorozumiany z oświadczenia woli o innej treści lub z innej czynności prawnej lub faktycznej, o ile wynika z niej wyraźnie żądanie zaprzestania przetwarzania danych. Z chwilą wniesienia sprzeciwu dalsze przetwarzanie danych osobowych jest niedopuszczalne. Interwencje Generalnego Inspektora, a niejednokrotnie sam fakt jego powiadomienia przez osoby pokrzywdzone, przyczyniły się w większości przypadków do uznania sprzeciwu przez firmy marketingowe.⁴²⁶ Wobec winnych naruszeń (nie dostosowania działalności do wymogów ustawy) prowadzono postępowania administracyjne zakończone wydaniem decyzji nakazującej usunięcie danych. Niezależnie od powyższego Generalny Inspektor powiadamiał organy ścigania o fakcie popełnienia przestępstwa określonego w art. 49 ustawy.⁴²⁷

W 2000 r. Generalny Inspektor Ochrony Danych Osobowych otrzymał również wiele sygnałów dotyczących niedopełnienia przez administratora danych obowiązku informacyjnego, określonego w art. 24 i 25 ustawy o ochronie danych osobowych. Zastrzeżenia budził brak informacji o dobrowolności bądź obowiązku podania danych, a także nieprecyzyjne określenie celów marketingowych, które często formułowano, jako cele własne podmiotów wysyłających ankiety, ulotki informacyjne czy kwestionariusze.⁴²⁸

⁴²³ GI-DIS-62/00, GI-DIS-73/00

⁴²⁴ GI-DIS-2/00, GI-DIS-20/00

⁴²⁵ GI-DP-430/1225/00

⁴²⁶ Np. w sprawach GI-DIS-81/00, GI-DIS-117/00, GI-DIS-121/00, GI-DIS-327/00, GI-DP-122/00/256

⁴²⁷ Zgodnie z art. 49 ust. 1 ustawy o ochronie danych osobowych, kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne, albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Np. w sprawach GI-DIS-2/00, GI-DIS-438/99/4/00, GI-DIS-20/00, GI-DIS-136/99/54/00, GI-DIS- 56/00, GI-DIS-62/00, GI-DIS-73/00, GI-DIS-82/00

⁴²⁸ GI-DIS-97/00, GI-DIS-56/00, GI-DIS-204/00

Generalny Inspektor wielokrotnie informował, że oprócz obowiązku wykazania przesłanki legalności przetwarzania danych z art. 23 ust. 1 ustawy, spoczywają na nim i inne obowiązki określone w jej przepisach. Jednym z tych obowiązków jest obowiązek informacyjny. Ustawa o ochronie danych osobowych porządkując przepływ informacji i nakładając szereg ograniczeń ustanowiła tym samym konieczną równowagę pomiędzy interesem zarówno osoby przetwarzającej dane osobowe jak i tej, której dane są przetwarzane. Należy podkreślić, że przedmiotowy obowiązek jest instrumentem pozwalającym osobom uprawnionym na rzeczywiste sprawowanie kontroli przetwarzania ich danych osobowych. Obowiązek informowania osób o przetwarzaniu ich danych osobowych znajduje swoją podstawę prawną w przepisach art. 24 i 25 ustawy o ochronie danych osobowych. W przypadku zbierania danych od osoby, której dane dotyczą administrator danych jest zobowiązany poinformować tę osobę o:

- 1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku,
- 2) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
- 3) prawie wglądu do swoich danych oraz ich poprawiania,
- 4) dobrowolności albo obowiązku podania danych, a jeśli taki obowiązek istnieje, o jego podstawie prawnej.

W ocenie Generalnego Inspektora poinformowanie osoby powinno nastąpić w chwili zbierania danych, a precyzując termin – przed przystąpieniem do gromadzenia informacji. Z powyższego obowiązku zostali zwolnieni wyłącznie administratorzy, którym ustawa zezwala na przetwarzanie danych bez ujawnienia faktycznego celu ich zbierania (np. Policja), jak również gdy tak stanowią przepisy szczególne (np. ustawa o ochronie informacji niejawnych).

W przypadku zbierania danych osobowych nie od osoby, której dane dotyczą, administrator jest zobowiązany, zgodnie z art. 25 ustawy, poinformować tę osobę, bezpośrednio po utwaleniu zebranych danych, a więc po zapisaniu danych w sposób umożliwiający ich dalsze przetwarzanie o:

- 1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku,
- 2) celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych,

- 3) źródle danych,
- 4) prawie wglądu do swoich danych oraz ich poprawiania,
- 5) uprawnieniach wynikających z art. 32 ust. 1 pkt. 7 i 8, tj. prawie wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację oraz wniesienia sprzeciwu wobec przetwarzania jej danych, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazania jej danych osobowych innemu administratorowi; uprawnienia te przysługują wyłącznie w sytuacji, gdy administrator przetwarza dane na podstawie art. 23 ust. 1 pkt. 4 i 5 ustawy, a więc, gdy przetwarzanie jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego oraz, gdy jest niezbędne do wypełnienia usprawiedliwionych celów administratorów danych, o których mowa w art. 3 ust. 2 ustawy, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą.

Przedmiotowy obowiązek powinien być dopełniony przed wysłaniem oferty promocyjnej. W związku z powyższym, dopełnienie obowiązku informacyjnego wraz z równoczesnym wysłaniem oferty promocyjnej, wbrew twierdzeniom niektórych firm, nie może być uznane za działanie prawidłowe. W decyzjach administracyjnych Generalny Inspektor podkreślał, iż osoba, której dane zostały zebrane nie od osoby, której bezpośrednio dotyczą, ma prawo być poinformowana o każdej dotyczącej jej zmianie z art. 25 ust. 1 ustawy informacji, np. zmianie adresu siedziby administratora danych, czy jego nazwy.⁴²⁹ Liczna grupa skarżących utraciła kontrolę nad obiegiem swoich danych osobowych poprzez niedopełnienie względem nich obowiązku informacyjnego w zakresie źródła pozyskania danych. W takich sytuacjach interweniował Generalny Inspektor wydając, np. decyzję nakazującą poinformowanie o pełnym adresie siedziby administratora danych.⁴³⁰

Generalny Inspektor wyjaśnił ponadto, iż obowiązek informacyjny, o którym mowa w art. 24 i 25 ustawy, spoczywa na administratorze danych zebranych od dnia wejścia w życie ustawy, tj. od dnia 30 kwietnia 1998 r. *A contrario* obowiązek ten nie obciąża administratorów danych zebranych przed wejściem w życie przedmiotowej ustawy.⁴³¹

W ramach realizacji obowiązku informacyjnego mieści się również realizacja uprawnień osoby, której dane dotyczą wynikających z art. 32 i 33 ustawy o ochronie danych osobowych. Z mocy ww. przepisów administrator danych jest zobligowany do udostępnienia

⁴²⁹ GI-DEC-DP-21/00, GI-DP-DEC-67/00

⁴³⁰ GI-DEC-DP-11/00

⁴³¹ GI-DIS-81/00

osobie, której dane dotyczą pełnych informacji o procesie przetwarzania jej danych. Rozpatrzenie wniosku osoby, której dane dotyczą powinno odbyć się w formie zrozumiałej dla tej osoby i w ustawowo wskazanym terminie 30 dni. Również zakres udzielonych informacji nie może być węższy niż przewiduje ustawa. Tymczasem jak wynikało z sygnałów docierających do Generalnego Inspektora wielu administratorów pozostawiało bez rozpoznania wpływające do nich wnioski, uniemożliwiając tym samym wykonanie kontroli przetwarzania danych osób, których dane dotyczą. Zanotowano przypadki, w których *osoby uprawnione nie tylko nie zostały poinformowane o przetwarzaniu danych w zbiorze danych określonej firmy, ale również nie powiadomiono ich o przekazaniu danych, w celach marketingowych, innym administratorom danych, w tym podmiotom zagranicznym*.⁴³² W takich sytuacjach, oprócz wydawania decyzji nakazujących usunięcie uchybień, Generalny Inspektor uznając bezprawność przedmiotowych zachowań składał do właściwych organów ścigania zawiadomienie o popełnieniu przestępstwa z art. 54 ustawy.⁴³³

Zwrócono również uwagę na realizację przez podmioty zajmujące się marketingiem produktów i usług obowiązku zabezpieczenia zbioru danych znajdującego się w ich posiadaniu. Zgodnie z art. 36 ustawy, administrator danych jest zobowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, a w szczególności powinien zabezpieczyć dane przed ich udostępnianiem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem. Obowiązek zabezpieczenia danych osobowych obciąża administratora danych również w razie zawarcia pisemnej umowy powierzenia, o której mowa w art. 31 ustawy. Jak wielokrotnie podkreślano, w każdym wypadku spoczywa na nim odpowiedzialność za przestrzeganie przepisów ustawy i tylko administrator odpowiada za skuteczne zanonimizowanie danych, w sytuacji gdy przestają one służyć celowi dla którego zostały zebrane. Ponieważ ustawa o ochronie danych nie wskazuje w swoich regulacjach sposobu dokonania przedmiotowej anonimizacji pojawiło się na tym tle wiele pytań, szczególnie od firm marketingowych tworzących bazy danych na podstawie zebranych ankiet.⁴³⁴ Jak wynika z obserwacji Generalnego Inspektora w poszczególnych firmach istnieją różnorodne metody niszczenia dokumentów (np. w tzw. „niszczarce” lub poprzez spalenie dokumentów). Istotne jest przede wszystkim, aby niszczenie danych osobowych było efektywne i przeprowadzone w sposób uniemożliwiający udostępnienie ich osobom nieupoważnionym.

⁴³² GI-DIS-136/99/54/00, GI-DIS-97/00, GI-DIS-166/00

⁴³³ GI-DIS-97/00 (zawiadomienie nr 23/00)

⁴³⁴ GI-DP-024/1324/00

Uwzględniając szczególny charakter celów marketingowych, dla realizacji których prowadzony jest obrót danymi osobowymi Generalny Inspektor w licznych kontrolach prowadzonych przez swoich inspektorów badał stopień zabezpieczenia tych danych. Wyniki postępowań ujawniły, iż wiele firm dopuszcza się istotnych uchybień w procesie przetwarzania danych, np. w postaci braku nadzoru nad niszczeniem materiałów zawierających dane osobowe, braku ewidencji osób zatrudnionych przy przetwarzaniu danych, braku stosownych instrukcji wskazanych w przepisach wykonawczych. Uchybienia powodowane były najczęściej zarówno nieznaną ustawą o ochronie danych, jak i wydanego na jej podstawie rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 80, poz. 521). Z reguły w wyniku przedstawienia ustaleń pokontrolnych firmy usuwały stwierdzone naruszenia. Wobec podmiotów, które nie stosowały właściwych systemów zabezpieczeń i narażały tym samym zgromadzone dane na udostępnienie osobom nieupoważnionym wydawano decyzje administracyjne nakazujące usunięcie uchybień w procesie przetwarzania danych.⁴³⁵

Indywidualne skargi i zapytania, które wpłynęły do Biura Generalnego Inspektora Ochrony Danych Osobowych *dotyczyły legalności przysyłanych skarżącym przez firmy marketingowe bezimiennych ankiet i zakresu danych w nich wymaganych*. Generalny Inspektor zwrócił uwagę, iż ustawa określa zasady postępowania przy przetwarzaniu danych osobowych oraz prawa osób fizycznych, których dane są lub mogą być przetwarzane w zbiorach danych (art. 2 ust. 1). Informacją o charakterze osobowym będzie każda informacja dotycząca konkretnej osoby lub takiej osoby, którą można zidentyfikować. Cechą wyróżniającą dane osobowe od innych informacji dotyczących osób jest brak anonimowości. Informacja posiada charakter osobowy, dopóki jest możliwe ustalenie tożsamości osoby, której ona dotyczy (art. 6 ustawy). Jeżeli ankietę nie wymaga umieszczenia w niej danych osobowych ankietowanego i nie zawiera innych informacji, które pozwalałyby określić tożsamość ankietowanego, przepisy ustawy nie znajdują do niej zastosowania.⁴³⁶ Jednakże zarzuty, także pod adresem przesyłek bezadresowych, dotyczyły, np. szczegółowości pytań w ankietach wypełnianych dobrowolnie. Przykładem w tym zakresie może być sprawa firmy rozsyłającej ankietę, bez imiennego ich adresowania, jednakże formułujące szczegółowe

⁴³⁵ GI-DEC-DP-8/00

⁴³⁶ GI-DP-916/00/1078, GI-DIS-142/00

pytania dotyczące stanu rodzinnego, zainteresowań, stanu majątkowego, itp.⁴³⁷ Udzielenie tych informacji było warunkiem wzięcia udziału w konkursie i ewentualnego wygrania określonych w regulaminie tego konkursu nagród. Firma dopełniła jednak obowiązki nałożone przez ustawę na administratorów danych; m.in. poinformowała o dobrowolności podania danych. Generalny Inspektor uznał więc, iż nie zostały naruszone przepisy ustawy o ochronie danych osobowych, podkreślając przy tym, że fakt wzięcia udziału w konkursie wymaga podjęcia decyzji przez każdego zainteresowanego i ma ona charakter zgody na przetwarzanie danych osobowych. Skierowano jednakże do administratora danych żądanie umieszczenia w sposób widoczny, nie budzący wątpliwości pouczenia o zakresie i celu przetwarzania danych oraz o prawach przysługujących osobom podającym dane osobowe.⁴³⁸

Do Generalnego Inspektora wpływały również pisma, w których skarżący zwracali się o dokonanie analizy prawnej charakteru organizowanych konkursów i loterii, jak również domagali się usunięcia ich danych osobowych z bazy danych firm prowadzących konkursy. Swoje żądanie skarżący argumentowali faktem nieprawidłowego wywiązania się organizatora konkursu z zawartej z nimi umowy. Generalny Inspektor zauważył, iż przedmiotową sprawę należałoby raczej rozpatrywać w świetle reguł prawa cywilnego, z uwzględnieniem zasad autonomii woli stron i równorzędności stron stosunków cywilnoprawnych. Sam udział w loterii opiera się na zasadzie dobrowolności, z zachowaniem ograniczeń wynikających z art. 353 Kodeksu cywilnego. Charakter konkursu wskazuje na to, że udział w nim, odbiór nagrody i związane z tym faktem podawanie danych osobowych celem jej otrzymania są całkowicie dobrowolne. Organizator konkursu ma prawo ustalać warunki uczestnictwa w konkursie, jak i warunki wydania nagrody. Jeżeli wymogiem, jaki należy spełnić jest podanie imienia, nazwiska i adresu pod który należy przesłać nagrodę, to decyzja o przystąpieniu do konkursu i odbiorze nagrody, oznacza przyjęcie wszelkich reguł uczestnictwa, a więc i warunku podania swoich danych. W ocenie Generalnego Inspektora takie działanie nie narusza przepisów o ochronie danych osobowych.⁴³⁹

Generalny Inspektor zwrócił ponadto uwagę, że sprawy z zakresu nieuczciwych praktyk marketingowych, w tym przesyłania na koszt klienta niezamówionych towarów, obiecywania nagród w zamian za zamówienie, należą do właściwości Urzędu Ochrony Konkurencji i Konsumentów.⁴⁴⁰ Generalny Inspektor nie był również upoważniony do

⁴³⁷ GI-DP-235/00/337

⁴³⁸ GI-DP-GI-DIS-175/00

⁴³⁹ GI-DIS-175/00

⁴⁴⁰ GI-DIS-86/00, GI-DIS-128/00, GI-DIS-226/00, GI-DIS-279/00 – sprawa w toku, GI-DIS-350/00

rozpatrywania skarg dotyczących przedłużenia prenumeraty bez zgody osoby, której dane dotyczą, w związku z czym przekazywano je według właściwości Urzędowi Ochrony Konkurencji i Konsumentów, na podstawie art. 19 ust. 1 pkt 3a ustawy z dnia 24 lutego 1990 r. o przeciwdziałaniu praktykom monopolistycznym i ochronie interesów konsumentów (Dz. U. z 1999 r. Nr 52, poz. 547 z późn. zm.).⁴⁴¹

Niezależnie od konkretnego stanu faktycznego przedstawionego Generalnemu Inspektorowi Ochrony Danych Osobowych przez osoby skarżące (zarówno nabywców produktów i usług, jak i osoby nie będące klientami danej firmy), zostały one pouczone o przysługującym im prawie kontroli przetwarzania danych, polegającym w szczególności na prawie do żądania uzupełnienia, uaktualniania, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo stały się zbędne, do realizacji celu, dla którego zostały zebrane, a także o prawie do wniesienia pisemnego umotywowanego żądania zaprzestania przetwarzania danych ze względu na ich szczególną sytuację. Ponadto Generalny Inspektor przeprowadzał szeroką akcję informacyjną na łamach mediów, mającą na celu podniesienie poziomu wiedzy na temat ustawy o ochronie danych osobowych. Osoby, których przedmiotem skarg było przetwarzanie ich danych dla celów marketingowych, były informowane o prawie złożenia sprzeciwu wobec przetwarzania ich danych w tym celu, a w razie jego bezskuteczności, o dalszych przysługujących im środkach prawnych. Do odpowiedzi dołączano przykładowy wzór sprzeciwu.⁴⁴² W celu pełnej realizacji praw przysługujących osobom, których dane były przetwarzane, zostały one poinformowane o obowiązkach nałożonych przepisami ustawy na administratorów danych. Większość firm w wyniku wniesienia sprzeciwu określonego w art. 32 ust. 1 pkt. 8 ustawy zaprzestała przetwarzania kwestionowanych danych.⁴⁴³

K. PRZETWARZANIE DANYCH OSOBOWYCH PRZEZ ZAKŁADY UBEZPIECZENIOWE I FUNDUSZE EMERYTALNE

W 2000 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło blisko 80 spraw związanych z działalnością firm ubezpieczeniowych i funduszy emerytalnych. Sprawy dotyczyły zakresu danych przetwarzanych przez te podmioty, formy, w jakiej mogą występować do innych organów o udostępnienie danych, jak również realizacji

⁴⁴¹ GI-DIS-43/00

⁴⁴² GI-DP-1088/00/1634, GI-DP-430/1709/00

⁴⁴³ GI-DP-122/00/256

obowiązków administratora danych, wskazanych w przepisach ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.).

Uprawnienie firm ubezpieczeniowych do pozyskiwania danych osobowych wynika m.in. z ustawy z dnia 28 lipca 1990 r. o działalności ubezpieczeniowej (Dz. U. z 1996 r. Nr 11, poz. 62 z późn. zm.). Wśród przepisów dotyczących pozyskiwania danych, a stosowanych przez firmy, należy przede wszystkim wskazać art. 8a tej ustawy. Zgodnie z jego treścią na wniosek zakładu ubezpieczeń, Ubezpieczeniowego Funduszu Gwarancyjnego lub Polskiego Biura Ubezpieczeń Komunikacyjnych oraz w zakresie zadań wykonywanych przez te instytucje ubezpieczeniowe i w celu ich wykonania, w związku z wypadkiem lub zdarzeniem będącym podstawą ustalania odpowiedzialności, sądy, organy prokuratury, policji oraz inne organy i instytucje mają obowiązek udzielić informacji i udostępnić materiały niezbędne do ustalenia okoliczności tych wypadków i zdarzeń oraz do określenia wysokości odszkodowania lub świadczenia. W aktualnym stanie prawnym zakłady ubezpieczeń mogą zatem gromadzić dane osobowe na tej podstawie i wykorzystywać je w swojej działalności. Należy przy tym zaznaczyć, iż zakład ubezpieczeń powinien dokładnie określić, jakie dane i informacje są mu niezbędne do ustalenia okoliczności wypadków i wysokości odszkodowań. Zdarzały się przypadki, że zakład ubezpieczeń pozyskiwał i dysponował danymi przekraczającymi zakres danych niezbędnych do zawarcia i realizacji umowy.⁴⁴⁴

Do Generalnego Inspektora Ochrony Danych Osobowych wpłynęła skarga, z której wynikało, że *w związku ze zgłoszeniem szkody w pojeździe, zakład ubezpieczeń kopiował wybrane strony dowodu osobistego skarżącego, w ramach zawartej z nim umowy dobrowolnego ubezpieczenia komunikacyjnego autocasco.*⁴⁴⁵ Skarga okazała się zasadna. Przeprowadzone postępowanie wykazało, że zakład ubezpieczeń przetwarzał dane swoich klientów w zakresie szerszym, niż jest to konieczne do stwierdzenia, czy osoba występująca z roszczeniem jest uprawniona do wypłaty odszkodowania z tytułu zawartej umowy ubezpieczenia, nadto sporządzał kopie wybranych stron dowodu osobistego klienta, który zgłasza roszczenie, co prowadziło do pozyskania danych osobowych zbędnych dla realizacji celu, dla którego były gromadzone. Generalny Inspektor, podkreślając niedopuszczalność przedmiotowych działań, wskazywał na treść art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych, zgodnie z którym administrator przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były merytorycznie poprawne i

⁴⁴⁴ GI-DIS-320/00, GI-DIS-338/00

adekwatne do celów, w jakich są przetwarzane. Wskazano przy tym, iż administrator danych nie może w żaden sposób stawiać swego interesu ponad dobro osoby, której dane przetwarza. W decyzji administracyjnej Generalny Inspektor nakazał zatem przetwarzanie danych osobowych klientów, którzy zgłaszają roszczenia odszkodowawcze z tytułu dobrowolnego ubezpieczenia komunikacyjnego wyłącznie w zakresie obejmującym: imię, nazwisko, adres zamieszkania, numer PESEL lub datę urodzenia oraz zaprzestanie kopiowania dokumentów tożsamości klientów zawierających inne niż ww. dane osobowe wraz z usunięciem ze zbioru danych nieadekwatnych w stosunku do celów, w jakich są przetwarzane.⁴⁴⁶

Niezwykle istotne okazało się ustalenie kręgu podmiotów, którym zakłady ubezpieczeń mogą udostępniać dane osobowe. Z treści skargi, która wpłynęła do Biura GODO wynikało, iż *jeden z zakładów ubezpieczeniowych przekazywał dane osobowe skarżącego, bez jego zgody, firmie mającej swoją siedzibę w Holandii*. Przeprowadzone postępowanie wykazało, iż proceder ten dotyczył klientów zakładu, którzy chcieli kontynuować ubezpieczenie za granicą u innego ubezpieczyciela i polegał na przekazywaniu zagranicznemu zakładowi ubezpieczeń zaświadczeń o przebiegu ubezpieczenia komunikacyjnego w RP. Generalny Inspektor uznał, iż w przedmiotowej sprawie zostały naruszone przepisy ustawy o ochronie danych osobowych, a w szczególności art. 26 ust. 1 pkt 1. Zgodnie z art. 9 zakład ubezpieczeń nie może udzielać informacji dotyczących poszczególnych umów ubezpieczenia. Zakaz ten nie dotyczy informacji udzielanych po spełnieniu określonych przesłanek i na żądanie podmiotów ściśle wskazanych w tym przepisie, a więc sądu, prokuratora, organu nadzoru ubezpieczeniowego lub osoby trzeciej, na rzecz której została zawarta umowa ubezpieczenia, Ubezpieczeniowego Funduszu Gwarancyjnego, Najwyższej Izby Kontroli, Narodowego Banku Polskiego, Generalnego Inspektora Kontroli Skarbowej. Wyliczenie zawarte w tym przepisie jest wyczerpujące i nie można go interpretować rozszerzająco. Wskazany w skardze zakład ubezpieczeń nie miał zatem żadnej podstawy ku temu, by informacje dotyczące poszczególnych umów ubezpieczenia zawieranych ze swymi klientami, przekazywać firmie zagranicznej. W przekonaniu Generalnego Inspektora przekazywanie przez zakłady ubezpieczeń danych swych klientów za granicę powinno być dokonywane nie tylko w oparciu o art. 47 ustawy o ochronie danych osobowych (jak często argumentowały zakłady). W takich sytuacjach dane osobowe byłyby bez żadnej kontroli i nierzadko wbrew woli osoby, której dotyczą, bezpodstawnie przekazywane pomiędzy różnymi podmiotami. Dlatego każda z firm

⁴⁴⁵ GI-DIS-145/00

zamierzająca przetwarzać dane, powinna się wykazać podstawą prawną; może nią być w szczególności zgoda osoby, której dane dotyczą. Zgodnie z art. 5 ustawy o ochronie danych osobowych, w przypadku, gdy przepisy odrębnych ustaw dotyczące przetwarzania danych, przewidują dalej idącą ich ochronę niż to wynika z niniejszej ustawy, stosuje się przepisy tych ustaw. Zdaniem Generalnego Inspektora takimi przepisami są przepisy ustawy o działalności ubezpieczeniowej. Określają one zamknięty katalog podmiotów uprawnionych do otrzymywania danych z umów ubezpieczenia i nie może być on dowolnie rozszerzany przez zakłady ubezpieczeniowe. Mając powyższe na względzie Generalny Inspektor wydał decyzję nakazującą zaprzestanie przekazywania przedmiotowych danych podmiotom nieuprawnionym.⁴⁴⁷

Do Generalnego Inspektora zwróciło się jedno z towarzystw ubezpieczeniowych z wnioskiem o wykreślenie zbioru przetwarzanych przez siebie danych, z uwagi na fakt, że *zestaw danych prowadzony w formie papierowej uporządkowany był według jednego tylko kryterium dostępu*, co zdaniem wnioskodawcy wykluczało przyjęcie, że jest to zbiór danych w rozumieniu art. 7 pkt 2 ustawy o ochronie danych osobowych. Przyczyną nieporozumień jest w tym przypadku brzmienie art. 7 pkt 2 ustawy, zgodnie z którym zbiorem jest "zestaw danych (...) uporządkowany według określonych kryteriów". Użycie przez ustawodawcę terminu "kryterium" w liczbie mnogiej przesądzać miałyby o tym, że uporządkowany jedynie wg kryterium alfabetycznego zestaw nie podlega przepisom ustawy o ochronie danych osobowych.⁴⁴⁸ Zdaniem Generalnego Inspektora Ochrony Danych Osobowych użycie przez ustawodawcę liczby mnogiej oznacza jedynie, że mogą funkcjonować różne kryteria dostępu do danych w zestawach, ale aby dany zestaw mógł być uznany za zbiór wystarczy zastosowanie przynajmniej jednego.

Sygnalizowane były także przypadki *wykorzystywania danych osobowych przez osoby zatrudnione w jednej firmie na rzecz innych firm*, w których te osoby pracowały jako agenci ubezpieczeniowi.⁴⁴⁹ Generalny Inspektor podkreślał, iż charakter czynności wykonywanych przez agentów, którzy zawierają umowy z poszczególnymi klientami na rzecz zakładu ubezpieczeń i w związku z tym przetwarzają dane w imieniu tego zakładu i na jego rzecz wskazuje, iż administratorem w ten sposób pozyskanych danych osobowych jest wyłącznie zakład ubezpieczeniowy, natomiast działalność agentów ze względu na formę i

⁴⁴⁶ GI-DP-DEC-58/00

⁴⁴⁷ GI-DP-DEC-31/00

⁴⁴⁸ GI-DP-403/00, GI-DP-1172/00

⁴⁴⁹ GI-DIS-37/00

treść stosunku prawnego łączącego ich z administratorem danych należy uznać za działanie podmiotu, któremu dane jedynie powierzono do przetwarzania, na podstawie art. 31 ustawy.

Administrator danych powinien podjąć wszelkie środki zapobiegające ewentualnemu naruszeniu przepisów ustawy o ochronie danych osobowych przez podmiot, z którym zawarł umowę powierzenia. Prawidłowa realizacja powyższego obowiązku powinna wyrażać się m.in. w dbałości o staranny dobór osób, którym dane zostają powierzone do przetwarzania, jak również w dbałości o to, aby osoby, którym dane zostały powierzone obowiązane były do zachowania ich w tajemnicy również po ustaniu zatrudnienia. Wprawdzie obowiązek sprawowania kontroli nad tym, jakie dane osobowe, kiedy i przez kogo, są pozyskiwane oraz komu przekazywane obciąża również podmiot przetwarzający dane z mocy art. 31 ustawy, jednakże okoliczność ta nie może zwolnić administratora danych od odpowiedzialności za naruszenie przepisów ustawy, np. za przetwarzanie danych niezgodne z celem, dla którego zostały udostępnione, za naruszanie praw osób, których dane dotyczą, czy za niedostateczne zabezpieczenie zbiorów danych osobowych. W konsekwencji, Generalny Inspektor, korzystając z nadanych mu w art. 19 ustawy o ochronie danych osobowych uprawnień, kierował zawiadomienia o popełnieniu przestępstwa z art. 51 ustawy wobec administratorów danych.

Do Generalnego Inspektora Ochrony Danych Osobowych zwracano się również z pytaniami, czy agent, który chciałby „wyręczyć” swojego klienta w załatwianiu formalności związanych ze zmianą ubezpieczyciela ma prawo *uzyskiwać informacje o przebiegu umowy ubezpieczenia*, w szczególności o przysługujących klientowi zniżkach z tytułu bezszkodowej jazdy.⁴⁵⁰ W odpowiedzi stwierdzano, iż wśród podmiotów upoważnionych do otrzymywania przedmiotowych informacji nie znajdują się agenci ubezpieczeniowi, wobec czego odmowa udostępnienia tego rodzaju informacji jest w pełni uzasadniona. Podkreślono jednak, że jeżeli ubezpieczony upoważni agenta do dokonywania odpowiednich czynności, ubezpieczyciel nie może odmówić wydania przedmiotowych informacji.

Wiele pism dotyczyło bardzo szczegółowego zbierania przez firmy ubezpieczeniowe danych klientów dotyczących stanu majątkowego, stanu cywilnego (pełnych odpisów aktów urodzenia) w postępowaniu o wypłatę odszkodowania.⁴⁵¹ W odpowiedzi Generalny Inspektor stwierdził, że podstawą żądania tego rodzaju danych są przepisy prawa cywilnego, dotyczące wypłaty odszkodowania i renty sieroczej, które obligują poszkodowanych do przedstawienia wyczerpującego materiału dowodowego. Z powyższych względów, jako podstawę

⁴⁵⁰ GI-DP-1115/00

przetwarzania tych danych wskazano art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych.

Liczne wątpliwości wzbudzało zagadnienie *przetwarzania przez zakłady ubezpieczeń informacji o stanie zdrowia*.⁴⁵² Generalny Inspektor wskazał art. 18 ust. 3 ustawy z dnia 30 jako przepis uprawniający zakłady ubezpieczeń do pozyskiwania danych zawartych w dokumentacji medycznej. Przepis ten zawiera katalog odstępstw od zasady tajemnicy dokumentacji medycznej pacjenta i zgodnie z jego treścią zakład opieki zdrowotnej udostępnia dokumentację medyczną osób korzystających ze świadczeń zdrowotnych zakładu organom rentowym, zakładom ubezpieczeniowym oraz zespołom do spraw orzekania o stopniu niepełnosprawności, w związku z prowadzonym przez nie postępowaniem. Generalny Inspektor podkreślił, iż niezbędnym warunkiem skutecznego powoływania się na zawarte w art. 18 ust. 3 pkt 6 uprawnienie, jest prowadzenie przez zakład stosownego postępowania po zaistnieniu określonego zdarzenia losowego. Z tego też powodu nieuprawnione jest spotykane wciąż w praktyce żądanie firmy udostępnienia jej dokumentacji medycznej na etapie oceny ryzyka ubezpieczeniowego w toku zawierania umowy.⁴⁵³ Podstawą zbierania danych o stanie zdrowia klienta – pacjenta, na tym etapie, może być wyłącznie udzielona na piśmie zgoda podmiotu danych. Z sygnałów napływających do Generalnego Inspektora wynika jednak, iż przypadki udostępniania dokumentacji medycznej, bez zgody pacjenta, dla celów „underwritingu”⁴⁵⁴ są bardzo częste.

Podobne pytania kierowano do GODO w związku z *obowiązkiem przekazywania zakładom ubezpieczeniowym faktur za wykupione lekarstwa*. Zdaniem skarżących nazwy zalecanych leków ujawniają w sposób pośredni określone schorzenia i wobec tego naruszona została ustawa o ochronie danych osobowych.⁴⁵⁵ W tym zakresie przetwarzanie danych osobowych przez zakłady ubezpieczeniowe znajduje podstawę w art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych. Generalny Inspektor Ochrony Danych Osobowych zwracał przy tym uwagę, że udostępnianie danych zakładom ubezpieczeniowym na podstawie art. 18 ust. 3 pkt 6 może nastąpić wyłącznie w związku z postępowaniem likwidacyjnym.

W jednej ze spraw zakład ubezpieczeniowy zwrócił się do osoby starającej się o wypłatę odszkodowania o *przedstawienie pełnego odpisu aktu urodzenia*.⁴⁵⁶ Generalny

⁴⁵¹ GI-DIS-320/00, GI-DIS-338/00

⁴⁵² GI-DIS-359/00

⁴⁵³ Ibidem

⁴⁵⁴ tj. dla oceny ryzyka ubezpieczeniowego

⁴⁵⁵ GI-DP-973/00

⁴⁵⁶ GI-DIS-320/00

Inspektor zwrócił uwagę, że zasady wydawania odpisów aktów stanu cywilnego i zaświadczeń są uregulowane w ustawie z dnia 29 września 1986 r. Prawo o aktach stanu cywilnego (Dz. U. Nr 36, poz. 180 z późn. zm.). Art. 83 ust. 1 stanowi, że odpisy oraz zaświadczenia określone w art. 79 wydaje się na wniosek sądu lub innego organu państwowego, osoby której stan cywilny został w akcie stwierdzony, jej wstępnego, zstępnego, rodzeństwa, małżonka lub przedstawiciela ustawowego. Ponadto, stosownie do art. 83 ust. 2 odpisy aktów stanu cywilnego i zaświadczenia o dokonanych w księgach stanu cywilnego wpisach lub o ich braku mogą być również wydane na wniosek innych osób niż wymienione w ust. 1, które wykażą w tym interes prawny, oraz na wniosek organizacji społecznej, jeżeli jest to uzasadnione celami statutowymi takiej organizacji i gdy przemawia za tym interes społeczny. Zaświadczenie o zaginięciu lub zniszczeniu księgi stanu cywilnego może być także wydane na wniosek innych zainteresowanych osób. Ze względu na to Generalny Inspektor stwierdził, że podstawę prawną przetwarzania danych w tej sytuacji przez ubezpieczyciela stanowi art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych stanowiący, że przetwarzanie danych osobowych jest dopuszczalne, gdy zezwalają na to przepisy prawa.

Generalny Inspektor zajmował się sprawą dotyczącą uzależnienia przez zakład ubezpieczeń zawarcia grupowego ubezpieczenia pracowniczego od *przedstawienia imion i nazwisk wszystkich żołnierzy, którzy mieliby zostać objęci ubezpieczeniem*. W szczególności nie chciano się zgodzić na przekazanie danych ze względu na to, że wskazany w skardze zakład jest podmiotem z udziałem kapitału zagranicznego. Zdaniem skarżącego, gdyby we władzach spółki zasiadały osoby z obcym obywatelstwem, doszłoby do ujawnienia tym osobom zbyt szczegółowych informacji i naruszenia przepisów o ochronie informacji niejawnych. Generalny Inspektor nie podzielił powyższego stanowiska i wyjaśnił, że zawarcie jakiegokolwiek umowy wiąże się ze zidentyfikowaniem i określeniem jej stron. Nie jest możliwe takie zawarcie ubezpieczenia, zgodnie z którym zakład ubezpieczeń pozbawiony byłby informacji o tym, kto jest uprawniony z tytułu określonego zdarzenia ubezpieczeniowego, na rzecz kogo zakład ten jest obowiązany spełnić określone świadczenie. Zakład musi być uprawniony do dysponowania danymi osobowymi ubezpieczonych. W zakresie tajemnicy państwowej ustawa o ochronie danych osobowych w żaden sposób nie koliduje z przepisami ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95 z późn. zm.), ponieważ stosownie do art. 5 ustawy o ochronie danych osobowych, jeżeli przepisy innych ustaw, które odnoszą się do przetwarzania danych przewidują dalej idącą ochronę niż ustawa o ochronie danych osobowych, stosuje się przepisy

tych ustaw. W sytuacji istnienia dwóch ustaw odnoszących się do przetwarzania danych, np. ustawy o ochronie informacji niejawnych i ustawy o ochronie danych osobowych, stosuje się przepisy tej pierwszej w zakresie, w jakim przewiduje ona wyższe standardy ochrony danych osobowych. Zgodnie art. 2 pkt 1 ustawy o ochronie informacji niejawnych, tajemnicą państwową jest informacja niejawna określona w wykazie rodzajów informacji niejawnych, stanowiącym załącznik nr 1 do ustawy, której nieuprawnione ujawnienie mogłoby spowodować istotne zagrożenie dla podstawowych interesów Rzeczypospolitej Polskiej albo narazić te interesy na co najmniej znaczną szkodę. W załączniku nr 1 do ustawy o ochronie informacji niejawnych wśród informacji kwalifikowanych, jako informacje niejawne oznaczone klauzulą "tajne" ze względu na obronność i bezpieczeństwo państwa oraz porządek publiczny wymieniony został system ewidencji danych o osobach zajmujących stanowiska związane z obronnością kraju. Stanowiska te określone zostały w rozporządzeniu Prezesa Rady Ministrów z dnia 26 września 1997 r. w sprawie określenia stanowisk pracy związanych z obronnością kraju (Dz. U. Nr 124, poz. 787).

Problemy ze stosowaniem przepisów ustawy o ochronie danych osobowych przez zakłady ubezpieczeniowe pojawiały się także w innym kontekście. Podobnie bowiem, jak w ubiegłym okresie sprawozdawczym wątpliwości budziła *kwestia udostępniania danych osobowych sprawców wypadków przez Policję*. Generalny Inspektor Ochrony Danych Osobowych pismem z dnia 2 czerwca 2000 r. zwrócił się do Rzecznika Ubezpieczonych,⁴⁵⁷ w którym stwierdził, że jednym z przepisów regulujących przetwarzanie danych osoby kierującej pojazdem, właściciela lub posiadacza pojazdu jest art. 44 ust. 1 pkt 4 ustawy z dnia 20 czerwca 1997 r. Prawo o ruchu drogowym (Dz. U. Nr 98, poz. 602 z późn. zm.). Stanowi on, że kierujący pojazdem w razie uczestniczenia w wypadku drogowym jest obowiązany, na żądanie osoby uczestniczącej w wypadku, podać swoje dane oraz dane dotyczące zakładu ubezpieczeń, z którym zawarta została umowa obowiązkowego ubezpieczenia odpowiedzialności cywilnej. W niektórych przypadkach sprawcy zdarzenia odmawiali podania tych informacji twierdząc, że nie są sprawcami wypadku a jedynie kolizji drogowej. Generalny Inspektor wskazał zatem, że pojęcie wypadku drogowego występuje w ustawie prawo o ruchu drogowym w bardzo szerokim znaczeniu. Pod pojęciem tym ustawa rozumie wszystkie zdarzenia związane z ruchem drogowym, które:

- zaistniały na drodze publicznej,

⁴⁵⁷ GI/529/00

- spowodowały uszkodzenie ciała, rozstrój zdrowia, śmierć albo jakąkolwiek szkodę w mieniu,
- zostały spowodowane przez działanie lub zaniechanie sprawcy (kierującego, pieszego lub innego uczestnika drogi).

Z uwagi na to wszelkie tego rodzaju zdarzenia związane z ruchem drogowym są wypadkami w rozumieniu ustawy Prawo o ruchu drogowym i ich uczestnicy mają obowiązek podać określone w art. 44 ust. 1 pkt 4 tej ustawy dane osobowe. Natomiast odmowa ich udzielenia, z powołaniem się na ustawę o ochronie danych osobowych stanowi nadużycie i wynika z niezrozumienia jej uregulowań.

Skargi dotyczyły również działalności Policji w kwestii *żądania od ubezpieczycieli wniosku o udostępnienie danych osobowych*, o którym mowa jest w art. 29 ustawy o ochronie danych osobowych.⁴⁵⁸ Generalny Inspektor poinformował, że postanowienia art. 8a ustawy o działalności ubezpieczeniowej stanowiąc, że sądy, organy prokuratury, policji oraz inne organy i instytucje ustalające okoliczności wypadków i zdarzeń mają obowiązek, na wniosek zakładu ubezpieczeń lub Ubezpieczeniowego Funduszu Gwarancyjnego, udzielać informacji oraz udostępniać materiały niezbędne do ustalenia okoliczności tych wypadków i zdarzeń oraz do określenia wysokości odszkodowania lub świadczenia, dają wystarczającą podstawę do zwracania się o udostępnienie tych informacji. Jednocześnie zaznaczono, że zakłady ubezpieczeniowe nie są zobowiązane do stosowania wniosku, o którym mowa w art. 29 ustawy, z uwagi na to, że gromadzone przez nie dane zostają włączone do zbioru, wobec czego art. 29 nie znajduje w ogóle zastosowania.⁴⁵⁹

Wątpliwości pojawiały się również w przypadku stosowania przepisów nakładających na administratora danych obowiązek poinformowania osób uprawnionych o przetwarzaniu dotyczących ich danych osobowych.

Z prośbą o wyjaśnienie niektórych wątpliwości do Generalnego Inspektora zwrócił się Prezes Państwowego Urzędu Nadzoru Ubezpieczeń. Art. 37 b ust. 1 ustawy o działalności ubezpieczeniowej stanowi, że aktuariuszem może być osoba, która spełni wymogi określone w tym przepisie. Takim wymogiem jest m.in. wpis na listę aktuariuszy. Wpis dokonywany jest z urzędu, po zdaniu egzaminu przed Komisją Egzaminacyjną dla Aktuariuszy. Na liście tej znajdują się określone dane, takie jak adres zamieszkania, numer dowodu, imiona

⁴⁵⁸ GI-DP-1177/00/1455

⁴⁵⁹ GI-DP-024/1482/00

rodziców oraz inne, które uzyskiwane są od osoby, której one dotyczą, samo zaś imię i nazwisko osoby, która zdała egzamin, przekazywane są przez komisję egzaminacyjną. Z uwagi na to, że obowiązek prowadzenia listy został przewidziany przepisami wcześniejszymi niż ustawa o ochronie danych osobowych PUNU powziął wątpliwość, czy w stosunku do aktuariuszy konieczne jest spełnienie obowiązku informacyjnego.⁴⁶⁰ Generalny Inspektor uznał, że w omawianym przypadku nie zachodzi żadna z przesłanek zwalniających administratora danych z obowiązku informacyjnego. Zgodnie z przepisem art. 25 ust. 2 obowiązek informacyjny nie istnieje, gdy ustawa zezwala na przetwarzanie danych bez ujawniania faktycznego celu gromadzenia tych danych. Zwrócono przy tym uwagę, że obowiązek informowania jest regułą w systemie ochrony danych osobowych, oraz jednym z najważniejszych środków ochrony tych danych. Jakikolwiek zatem odstępstwa od tej zasady powinny jasno wynikać z przepisów ustawy. Przykładem wyraźnego upoważnienia do przetwarzania danych osobowych bez wiedzy osoby, której dane dotyczą jest, np. art. 20 ustawy o Policji. Stanowi on, że Policja może gromadzić i przetwarzać dane osobowe w tym sposób tajny i poufny. Analogiczne postanowienia zawierają: ustawa z dnia 26 kwietnia 1996 r. o Służbie Więziennej (Dz. U. Nr 61, poz. 283 z późn. zm.) oraz ustawa z dnia 6 kwietnia 1990 r. o Urzędzie Ochrony Państwa (Dz. U. z 1999 r. Nr 51, poz. 526 z późn. zm.). Za takim stanowiskiem przemawia również konieczność przyjęcia tezy o racjonalnym ustawodawcy, który w chwili uchwalania ustawy zdawał sobie sprawę ze stanu ustawodawstwa. Ponieważ przepisy ustawy o działalności ubezpieczeniowej nie zawierają wyraźnego upoważnienia dla jakiegokolwiek podmiotu do przetwarzania danych bez wiedzy osoby, której dane dotyczą, a także w sposób jednoznaczny nie zwalniają administratora danych od obowiązku informacyjnego należy przyjąć, że na Państwowym Urzędzie Nadzoru Ubezpieczeń ciąży obowiązek poinformowania aktuariuszy o przetwarzaniu danych ich dotyczących oraz o innych okolicznościach wymienionych w art. 25 ustawy o ochronie danych osobowych.

Generalny Inspektor podjął sprawę jednego z towarzystw ubezpieczeniowych, które w treści formularzy „Wniosek o ubezpieczenie na życie” zamieściło zapis o wyrażeniu przez wnioskodawcę zgody na *zasięganie przez towarzystwo informacji o treści medycznej od każdego lekarza*, który się nim opiekował lub opiekuje, dotyczących fizycznego lub psychicznego stanu zdrowia.⁴⁶¹ Po przeprowadzeniu postępowania stwierdzono, że zgoda

⁴⁶⁰ GI-DP-489/00

wyrażona w sposób powyżej opisany spełnia wymogi z art. 27 ust. 2 pkt 1 ustawy z dnia 30 sierpnia 1991 r. o zakładach opieki zdrowotnej (Dz. U. Nr 91, poz. 408 z późn. zm.). Zgoda taka nie będzie jednak przesłanką uprawniającą do żądania danych o stanie zdrowia psychicznego, z uwagi na to, że nie zezwalają na to przepisy ustawy z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego (Dz. U. Nr 111, poz. 535 z późn. zm.). Przepis art. 50 ust. 2 tej ustawy zwalnia osoby wykonujące czynności wynikające z tej ustawy od obowiązku zachowania tajemnicy w stosunku do:

- lekarza sprawującego opiekę,
- właściwych organów administracji rządowej lub samorządowej, co do okoliczności, których ujawnienie jest niezbędne do wykonywania zadań z zakresu pomocy społecznej,
- osób współpracujących w wykonywaniu czynności w ramach pomocy społecznej, w zakresie, w jakim jest to niezbędne,
- służb ochrony państwa i ich upoważnionym na piśmie funkcjonariuszom lub żołnierzom w zakresie niezbędnym do przeprowadzenia postępowania sprawdzającego na podstawie przepisów o ochronie informacji niejawnych.

W wyniku podjętych przez Generalnego Inspektora czynności towarzystwo jeszcze w trakcie postępowania zmodyfikowało klauzulę wyrażenia zgody, w ten sposób, że zgoda odnosiła się tylko do informacji o stanie zdrowia fizycznego, a nie psychicznego. W trakcie przeprowadzonego postępowania kontrolnego stwierdzono jednakże również istotne uchybienia pozostałym postanowieniom ustawy o ochronie danych osobowych polegające w szczególności na braku odpowiednich zabezpieczeń przetwarzanych danych osobowych, niewywiązywaniu się administratora danych z obowiązku informacyjnego, a także niespełnienia odpowiednich wymogów technicznych i organizacyjnych, jakie powinny spełniać systemy informatyczne w myśl przepisów wykonawczych do ustawy o ochronie danych osobowych. Towarzystwo wskazywało, że dane osób ubezpieczonych nie są w zasadzie udostępniane, a jedynie wyjątkowo sądom i prokuratorom, wobec czego nie zachodzi potrzeba odnotowywania w systemie informacji, czy i komu dane zostały udostępnione. Zdaniem Generalnego Inspektora stwierdzenie, że incydentalny charakter i poufność udostępnień są przyczyną, dla której przypadki udostępnienia nie są odnotowywane, stoi w sprzeczności z obowiązkiem wynikającym z § 16 pkt 4 rozporządzenia Ministra Spraw

Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. W związku ze stwierdzonymi uchybieniami Generalny Inspektor w wydanej decyzji nakazał ich usunięcie.

Jedna ze skarg dotyczyła umieszczenia danych skarżącego na druku polecenie przelewu i wezwania go do zapłaty na rzecz towarzystwa ubezpieczeniowego kwoty z tytułu opłaty za wpis do rejestru osób uprawnionych do wykonywania czynności akwizycyjnych na rzecz otwartych funduszy emerytalnych.⁴⁶² W toku czynności wyjaśniających ustalono, iż towarzystwo przetwarzało dane skarżącego w oparciu o art. 23 ust. 1 pkt 3 ustawy o ochronie danych osobowych, w związku z zawarciem umowy o wykonanie czynności akwizycyjnych.

W praktyce pojawiła się ponadto kwestia okresu, przez który mogłyby być przechowywane dane o osobach ubezpieczonych.⁴⁶³ Generalny Inspektor zwrócił uwagę, że zarówno przechowywanie danych osób ubezpieczonych przez okres lat 50, jak proponowało towarzystwo ubezpieczeniowe, jak i uzależnienie długości tego okresu wyłącznie od woli administratora danych nie byłoby zgodne z zasadą adekwatności przewidzianą w ustawie o ochronie danych osobowych.

Wprowadzenie reformy systemu emerytalnego spowodowało, że do Biura Generalnego Inspektora Ochrony Danych Osobowych kierowanych było ponadto wiele spraw związanych z działalnością funduszy emerytalnych.

Zmiana ustawy o systemie ubezpieczeń społecznych spowodowała, że otwarte fundusze emerytalne do dnia 30 czerwca 2000 r. miały obowiązek uzupełnić dane osobowe w rejestrach członków funduszu o numer identyfikacji podatkowej (NIP). W związku z tym do Generalnego Inspektora napływały pytania, czy *Zakład Ubezpieczeń Społecznych będący w posiadaniu tych danych, może je przekazać otwartemu funduszowi emerytalnemu* nie naruszając przy tym ustawy o ochronie danych osobowych.⁴⁶⁴ Generalny Inspektor wskazał, że mimo iż art. 89 tej ustawy daje funduszowi podstawę do przetwarzania danych członków funduszu, to nie stanowi jednak przesłanki umożliwiającej Zakładowi Ubezpieczeń Społecznych udostępnienie danych innemu podmiotowi. Na podstawie art. 50 ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz. U. Nr 137, poz. 887 z późn. zm.) dane zgromadzone na koncie ubezpieczonego (wymienione w art. 40) i na koncie

⁴⁶² GI-DIS-359/00

płatnika składek, mogą być udostępniane sądom, prokuratorom, organom kontroli skarbowej oraz Urzędowi Nadzoru nad Funduszami Emerytalnymi a także osobom fizycznym i płatnikom składek, których dotyczą informacje zawarte na kontach. Z uwagi na to, że brak jest wyraźnego przepisu dającemu funduszowi emerytalnemu uprawnienie do żądania numerów identyfikacji podatkowej Generalny Inspektor uznał, że ZUS nie jest zobowiązany do udostępnienia żądanych danych osobowych.

Skarżono się na naruszenia art. 26 ust. 1 ustawy o ochronie danych osobowych. Pisma dotyczyły *odmowy skorygowania danych lub przewlekłych i niezwykle sformalizowanych procedur poprawiania danych*.⁴⁶⁵ Jako przyczyny zwłoki w przypadku uaktualniania danych podawano obowiązującą u administratora danych procedurę, w przypadku zmiany stanu cywilnego oraz dokumentu tożsamości wymagane było złożenie odpowiednich dokumentów poświadczających te zmiany. Procedura taka miała na celu wyeliminowanie niebezpieczeństwa przyjęcia przez Towarzystwo zarządzające funduszem sfałszowanego „formularza zmiany dotychczasowych danych członka funduszu”. W wyniku interwencji Generalnego Inspektora Ochrony Danych Osobowych procedura uaktualniania danych została znacznie uproszczona, w ten sposób, że zrezygnowano z wymogu składania przez członków funduszu potwierdzonych za zgodność z oryginałem kopii dokumentów stwierdzających fakt zawarcia małżeństwa i związanej z tym zmiany danych osobowych.

W 2000 r. zanotowano liczną grupę spraw związanych z fałszowaniem umów przystąpienia do otwartych funduszy emerytalnych. W takich sytuacjach Generalny Inspektor Ochrony Danych Osobowych przekazywał sprawy do rozpoznania, zgodnie z właściwością, Urzędowi Nadzoru nad Funduszami Emerytalnymi, jak również właściwym organom ścigania.⁴⁶⁶

Część II. KONTROLE

⁴⁶⁴ GI-DP-351/00

⁴⁶⁵ GI-DIS-336/00

⁴⁶⁶ GI-DP-351/00, GI-DIS-23/00, GI-DIS-70/00

W okresie sprawozdawczym, upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych, inspektorzy przeprowadzili 102 kontrole zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Kontrole były przeprowadzane w różnym zakresie: polegały bądź na sprawdzeniu wszystkich zbiorów danych prowadzonych przez jednostkę kontrolowaną, bądź tylko niektórych zbiorów. Kontrolowano również wykonanie decyzji Generalnego Inspektora Ochrony Danych Osobowych.⁴⁶⁷

W prowadzonych kontrolach brali udział prawnicy – pracownicy Departamentu Inspekcji Biura GODO oraz informatycy, pracownicy Departamentu Informatyki.

I. Ocena zabezpieczeń organizacyjnych i technicznych systemów informatycznych przez administratorów danych osobowych

Kontrole przeprowadzane były zarówno w małych jednostkach organizacyjnych, mieszczących się niekiedy w pojedynczym lokalu i dysponujących jednym stanowiskiem komputerowym, na którym przetwarzano dane osobowe, np. Woryed S-ka z o.o. w Warszawie, jak też dużych, często wielooddziałowych firmach działających na terenie całego kraju, połączonych rozbudowanymi sieciami komputerowymi typu WAN i ośrodkami komputerowymi o dużej mocy obliczeniowej, jak np. Telekomunikacja Polska S.A., Najwyższa Izba Kontroli, operatorzy telefonii komórkowej, czy też niektóre banki.

Pomimo, iż ustawa o ochronie danych osobowych, jak i rozporządzenie w wymaganiach określających warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy służące do przetwarzania danych osobowych nie bierze pod uwagę wielkości podmiotów, to w rzeczywistości w niektórych małych jednostkach wiele elementów nie występuje lub ich wielkość powoduje, iż stawianie im wymagań określonych w rozporządzeniu staje się wprost bezprzedmiotowe. Tak, np. zbędne wydaje się, aby od jednostki zajmującej pojedynczy lokal o powierzchni rzędu 10 m² i zatrudniającej jednego pracownika jak w Spółce Woryed S.A. żądać zgodnie z wymaganiami § 7 punkt 1 rozporządzenia wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe skoro dane te wskazane są wprost poprzez adres siedziby jednostki. Trudno również wymagać, aby jednostka przetwarzająca dane osobowe na wyizolowanym, pojedynczym stanowisku komputerowym przeprowadzała jakieś zaawansowane badania w celu wypełnienia obowiązku, o którym mowa w § 2 rozporządzenia i tworzyła w tym zakresie odrębny dokument określający, tzw. politykę bezpieczeństwa.

⁴⁶⁷ Wykaz kontroli zamieszczony został w załączniku na końcu Sprawozdania

Całkowicie odmiennie do wymienionych wyżej wymagań, należy się jednak odnieść w przypadku dużych jednostek organizacyjnych mieszczących się często w wielu różnych budynkach zlokalizowanych na terenie całej Polski i nie tylko. Dla zarządzania bezpieczeństwem dużych systemów informatycznych oraz nadzorowania ochrony danych osobowych, posiadanie odpowiednich wykazów i ewidencji jest niezbędne.

Stąd też szczególnie trudne i pracochłonne były kontrole w dużych jednostkach organizacyjnych przetwarzających niekiedy dane osobowe kilku milionów osób. Zbiory danych osobowych oraz systemy informatyczne wykorzystywane do ich przetwarzania zlokalizowane były często na wielu różnych serwerach. Systemy informatyczne przetwarzające tak duże zbiory danych oraz same zbiory danych zainstalowane były często na kilku lub kilkadziesiąt współpracujących ze sobą maszynach. W przypadku bardzo dużych systemów, ich budowa była najczęściej modułowa, a same bazy danych podzielone funkcjonalnie i/lub tematycznie. Do przetwarzania danych w dużych systemach informatycznych wykorzystywane były najczęściej profesjonalne systemy baz danych typu Oracle, Informix, Sybase itp.

I.1 Warunki techniczne i organizacyjne w jakich przetwarzane były dane osobowe w dużych i średnich jednostkach organizacyjnych.

Z przeprowadzonych kontroli wynika, że w dużych jednostkach organizacyjnych w celu wykonania zadań organizacyjno technicznych jakim powinny odpowiadać systemy informatyczne do przetwarzania danych wymienionych w rozporządzeniu powołano najczęściej odpowiednią komórkę organizacyjną. Dotyczy to szczególnie organizacji komercyjnych, działających na podstawie uzyskanych koncesji lub zezwoleń typu operatorzy usług telekomunikacyjnych, towarzystwa ubezpieczeniowe, itp. W organizacjach tych można było zauważyć, że do zagadnień związanych z ochroną danych, w tym także danych osobowych, podchodzi się poważnie i z dość dużą odpowiedzialnością. Do jednostek takich można, np. zaliczyć T.U.n.Ž. Nationale - Nederlanden, które wypełniło w najszerszym zakresie większość z wymagań zarówno organizacyjnych jak i technicznych wskazanych w rozporządzeniu. Jedyne uchybienia, które ustalono tam podczas kontroli dotyczyły odnotowywania informacji o udostępnieniach. Uchybienia te nie dotyczyły jednak głównego systemu, gdzie przetwarzane były dane osób ubezpieczonych.

I.2 Polityka bezpieczeństwa, techniczne warunki przetwarzania

Na uwagę zasługuje fakt, że administratorzy danych będący dużymi jednostkami organizacyjnymi, nie mieli na ogół kłopotów z realizacją podstawowych wymagań technicznych i organizacyjnych stawianych urządzeniom i systemom informatycznym przetwarzającym dane osobowe w zakresie bezpieczeństwa przetwarzania. Duże jednostki organizacyjne, zwłaszcza te związane z sektorem finansowym (banki, Towarzystwa Ubezpieczeniowe) dysponowały najczęściej odpowiednim dokumentem określającym tzw. politykę bezpieczeństwa, który zawierał elementy, o których mowa w § 2 rozporządzenia. W przypadku banków dokument ten składał się na ogół z części dotyczącej bezpieczeństwa fizycznego oraz z części dotyczącej bezpieczeństwa systemów informatycznych uwzględniając różne rodzaje ryzyka i zagrożeń, na jakie ich systemy mogą być narażone. Należy przypuszczać, iż fakt zwracania dużej uwagi na bezpieczeństwo fizyczne oraz bezpieczeństwo systemów informatycznych zarówno pod kątem niezawodności ich funkcjonowania, jak i pod kątem ochrony zawartych w nich informacji, wynika z budowanej w tych instytucjach od wielu kultur ochrony zarówno aktywów materialnych, jak i informacyjnych. Do stosowania pewnych standardów w zakresie bezpieczeństwa niektóre jednostki obligowane są również innymi przepisami prawa krajowego, np. przepisami wynikającymi z ustawy o ochronie informacji niejawnych. Ponadto, w przypadku organizacji finansowych pewne standardy dotyczące bezpieczeństwa narzucane są przez ich przepisy wewnętrzne. Jako przykład można wymienić PolCard S.A. w Warszawie, gdzie przed rozpoczęciem przetwarzania danych osobowych w systemie personalizacji kart magnetycznych Visa, system ten, procedury jego użytkowania oraz zastosowane środki ochrony fizycznej musiały uzyskać akredytację organizacji finansowej Visa, która przeprowadziła w tym celu odpowiednią kontrolę.

Ważne jest również to, że wymienione instytucje określając politykę bezpieczeństwa, odpowiednią wagę przykładają na ogół nie tylko do ochrony przetwarzanych tam danych przed zniszczeniem lub utratą, ale przede wszystkim do ochrony przed ich nieautoryzowanym przetwarzaniem oraz ujawnieniem, wypełniając tym samym jeden z głównych warunków jakim zgodnie z wymaganiami rozporządzenia powinny spełniać systemy informatyczne przetwarzające dane osobowe.

Nieco inna sytuację zaobserwowano w jednostkach organizacyjnych, zwłaszcza tych, które należą do organów władzy publicznej oraz tych będących pod kontrolą państwa. W wielu takich jednostkach, działania mające na celu właściwe zabezpieczenie danych osobowych przetwarzanych w systemach informatycznych rozpoczęto dopiero po wejściu w życie ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2000 r.

Nr 12, poz. 136). Przepisy wymienionej ustawy, w przeciwieństwie do rozporządzenia, nakazują w art. 60 ust. 3 wprost obowiązek zastosowanej polityki bezpieczeństwa. Przykładem jest Najwyższa Izba Kontroli, w której administratora bezpieczeństwa informacji powołano dopiero w dniu 8 marca 2000 r. Dopiero po tym terminie rozpoczęto również działania organizacyjne, zmierzające do wykonania obowiązków określonych w rozporządzeniu.

Należy jednak z dużym niepokojem stwierdzić, że wśród dużych jednostek organizacyjnych skontrolowanych w 2000 r. znacznie większą grupę stanowiły jednostki, w których nie dokonano czynności określonych w § 2 rozporządzenia, nie wspominając już o ich udokumentowaniu. Niechlubnym przykładem jest KPRM, w której podczas czynności kontrolnych przeprowadzanych w dniach 7-18.04.2000 r. stwierdzono brak jakichkolwiek działań formalnych podjętych w powyższej sprawie. Do obowiązku wykonania zadań określonych w rozporządzeniu nie poczuwał się również powołany tam Dyrektor Biura Ochrony.

I.3 Instrukcje i procedury

Na bezpieczeństwo przetwarzania danych osobowych, poza jakością użytego sprzętu i oprogramowania, duży wpływ ma dyscyplina organizacyjna, do wymuszenia której niezbędne są odpowiednie instrukcje i procedury. Stąd też dużą uwagę w czasie kontroli zwracano na takie elementy, jak:

- wyznaczenie osób odpowiedzialnych za eksploatację i monitorowanie wdrożonych systemów zabezpieczeń,
- ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych oraz ich indywidualne zakresy czynności,
- instrukcje postępowania w sytuacji naruszenia ochrony danych osobowych oraz
- instrukcję zarządzania systemem informatycznym, w którym przetwarzane są dane osobowe.

Pozytywnym zjawiskiem obserwowanym podczas czynności kontrolnych w dużych jednostkach organizacyjnych takich, jak towarzystwa emerytalne, banki, telekomunikacja, itp. jest to, że w większości z tych jednostek, wyznaczony był administrator bezpieczeństwa informacji oraz sporządzone były odpowiednie instrukcje, o których mowa w § 6 i § 11 rozporządzenia.

Istotne zastrzeżenia inspektorów budziła często jednak jakość merytoryczna sporządzonych instrukcji. Według interpretacji Departamentu Informatyki instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych, przeznaczona dla osób zatrudnionych przy przetwarzaniu danych osobowych powinna zawierać między innymi:

- wyjaśnienia dotyczące opisu sytuacji oraz zachowania się programu i/lub bazy danych wskazujących na wystąpienia naruszenia ochrony danych,
- wyjaśnienia dotyczące zachowania się sprzętu, mogące wskazywać na naruszenie lub próby naruszenia danych (np. nieuzasadniona intensywna praca dysków komputera),
- opisu sytuacji wskazujących na wystąpienia nieautoryzowanego dostępu do danych lub próby takiego dostępu,
- opisu sytuacji, które w danym środowisku mogą wskazywać na naruszenie zabezpieczenia danych,
- opisu zdarzeń i zjawisk mogących potencjalnie spowodować naruszenie ochrony, np. wystąpienie wirusów komputerowych lub pojawienie się nieznanego procesu obliczeniowego,
- kolejność powiadamiania osób o zaistniałym zdarzeniu (informatyka odpowiedzialnego za nadzór nad systemem, administratora sieci czy też administratora bezpieczeństwa informacji),
- czynności, jakie obowiązany jest wykonać użytkownik w celu utrwalenia zaistniałego stanu oraz
- czynności, jakich użytkownik nie powinien podejmować z uwagi na możliwość spowodowania dalszych niepożądanych działań i/lub zatarcia dowodów.

Za nie wystarczające natomiast uznaje się instrukcje, których treść zawiera niemal wyłącznie sformułowania zawarte w § 6.2 rozporządzenia nie zawierające żadnych indywidualnych elementów odzwierciedlających stan rzeczywiście występujących w danej jednostce zagrożeń czy też charakterystyki pojawienia się potencjalnie możliwych, niebezpiecznych dla ochrony informacji zdarzeń.

Podobne zastrzeżenia odnotowano również w odniesieniu do instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji. Instrukcja taka powinna być przygotowana stosownie do skali problemów, jakie występują w zarządzaniu poszczególnymi

systemami informatycznymi. Za nie wystarczające uznawano instrukcje, w których stwierdzano jedynie, że np.:

- określono sposób przydziału haseł,
- opracowano procedury rozpoczęcia i zakończenia pracy,
- określono metodę i częstotliwość tworzenia kopii awaryjnych, itp. nie rozwijając szerzej poszczególnych zagadnień.

Od instrukcji tych wymagano natomiast, aby wskazywały one jak dla danego systemu rozwiązano konkretny problem, tj. np. kto jest odpowiedzialny za przydzielanie hasła, jakie przyjęto w tym zakresie procedury, jakie czynności należy wykonać, ewentualnie co należy sprawdzić, na co zwrócić uwagę podczas rozpoczynania i kończenia pracy, itp. W przypadku, gdy dane osobowe przetwarzane są w kilku różnych systemach posiadających, np. odmienne mechanizmy autoryzacji użytkownika, inne potrzeby w zakresie wykonywania kopii, itp. wówczas dla każdego z nich powinna być odpowiednia instrukcja zarządzania lub jedna instrukcja wspólna obejmująca zagadnienia ogólne z odpowiednimi załącznikami. W załącznikach takich dla każdego systemu powinny być wyjaśnione te elementy zarządzania i te procedury, które nie zostały ujęte w instrukcji ogólnej. Rozwiązania takie mają zastosowanie głównie w takich jednostkach, które eksploatują wiele różnych systemów informatycznych administrowanych często przez niezależne zespoły.

Oceniając przekrojowo jakość wymienionych wyżej instrukcji, należy stwierdzić, że w dużych jednostkach organizacyjnych poza nielicznymi wyjątkami jak, np. w KPRM, były one na ogół dość dobre. Jako wyróżniające się można by wskazać instrukcje przygotowane między innymi przez Towarzystwo Ubezpieczeń na Życie Nationale-Nederlanden Polska S.A., Centertel Sp. z o.o., AsterCity Sp. z o.o. czy też mniejsze jednostki jak KKKK Sp. z o.o. Instrukcje zarządzania systemami informatycznymi w wymienionych jednostkach opracowane były na wysokim poziomie merytorycznym. Odzwierciedlały one rzeczywiście występujące tam problemy związane z zarządzaniem eksploatowanymi systemami informatycznymi wraz ze wskazaniem konkretnych procedur eksploatacyjnych i naprawczych. Ponadto, co jest najważniejsze, instrukcje te w wymienionych jednostkach były rzeczywiście wdrożone. Tak, np. instrukcja zarządzania systemem informatycznym w T.U.n.Ż. Nationale-Nederlanden Polska S.A. składa się z dwóch części: ogólnej - obejmującej całokształt zagadnień związanych z ogólnymi zasadami użytkowania i zabezpieczania zasobów w systemach informatycznych oraz instrukcji szczegółowych – określających

szczegółowe procedury regulujące zasady dostępu i ochrony poszczególnych segmentów sieci informatycznej oraz konkretnych systemów informatycznych. Ich wdrożenie polega natomiast na zapoznaniu poszczególnych pracowników, stosownie do zajmowanego stanowiska i zakresu obowiązków z procedurami za stosowanie których są odpowiedzialni. Procedury te udostępnione były w formie dokumentów papierowych oraz zapisów we wskazanym katalogu systemu informatycznego.

Za pozytywne skutki przeprowadzonych w 2000 r. inspekcji należy uznać również to, iż wiele z kontrolowanych jednostek, w których odnotowano w czasie kontroli liczne uchybienia, przedstawione zalecenia potraktowało bardzo poważnie i poczyniły wiele wysiłku, aby sprostać postawionym wymagom. W grupie tej są zarówno jednostki organizacyjne typu Naczelna Izba Kontroli, jak i jednostki gospodarcze jak, np. Stołeczne Przedsiębiorstwo Energetyki Ciepłej, ul. Batorego 2 w Warszawie.

I.4 Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych.

Wiele zastrzeżeń zarówno w dużych, jak i małych jednostkach organizacyjnych stawianych administratorom danych podczas kontroli odnosiło się do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych pomimo, że w nielicznych tylko przypadkach odnotowano całkowity jej brak. Według wymagań określonych w rozporządzeniu, ewidencja taka powinna zawierać imię i nazwisko upoważnionego do przetwarzania danych osobowych pracownika wraz z odpowiadającym mu w systemie informatycznym identyfikatorem. Ewidencja taka powinna nadto zawierać datę nadania oraz dla pracowników, którym uprawnienie takie cofnięto, datę utraty uprawnień. Zgodnie bowiem z sensem znaczeniowym samego słowa „ewidencja”, odpowiedni spis wymienionych danych powinien być prowadzony w sposób odzwierciedlający kolejność następujących po sobie zdarzeń. Ewidencja, o której mowa powinna zawierać zatem nie tylko spis aktualnie zatrudnionych przy przetwarzaniu danych osób, ale również spis osób i przypisanych im identyfikatorów, które w przeszłości pracowały w danej jednostce przy przetwarzaniu danych osobowych. Brak w ewidencji zapisów dla osób, które aktualnie nie są już zatrudnione przy przetwarzaniu danych osobowych, a tym samym brak informacji o przyznanym mu identyfikatorze uniemożliwiał by administratorowi realizację wymogu stawianego w § 14 punkt 7 rozporządzenia. Wymóg ten stanowi, że identyfikator użytkownika nie powinien być zmieniany, a po jego wyrejestrowaniu z systemu informatycznego nie powinien być przydzielany innej osobie.

Zasadniczymi uchybieniami odnotowanymi w kontrolowanych jednostkach odnoszącymi się do sposobu prowadzenia ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych były:

- brak identyfikatora użytkownika (dla osób przetwarzających dane osobowe w systemach informatycznych),
- brak daty nadania/odebrania uprawnień do przetwarzania danych,
- niekompletność i brak koordynacji przy jej prowadzeniu.

Ostatnie z wymienionych uchybień w zakresie prowadzenia ewidencji wynikało najczęściej z faktu, że w jednostce nie było wyznaczonej osoby, która odpowiedzialna byłaby za te czynności lub faktu rozłożenia tej odpowiedzialności na wiele osób, najczęściej administratorów poszczególnych systemów informatycznych. Skutkiem takich działań było to, że każdy z administratorów ograniczał się do utworzenia jedynie listy aktualnych użytkowników swojego systemu w dowolnej wymyślonej przez siebie formie, czego przykładem mogą być ewidencje prowadzone w takich jednostkach jak PolCard S.A. w Warszawie, KPRM, NIK i wielu innych jednostkach.

Niewskazane są również rozwiązania skrajne jak, np. w Telekomunikacji Polskiej S.A., gdzie jak się okazało podczas kontroli w Zakładzie Telekomunikacyjnym w Łodzi, prowadzeniem ewidencji zajmuje się nie Zakład Telekomunikacyjny w Łodzi lecz Wydział Ochrony Danych utworzony w Pionie Systemów Informatycznych Dyrekcji Spółki. Procedura dokonania wpisu do takiej ewidencji trwa jak się okazało w praktyce około 2 tygodni, a w ogóle nie wiadomo tak naprawdę w jakim stopniu taka ewidencja jest wiarygodna i komu tak naprawdę ma służyć.

1.5 Warunki techniczne i organizacyjne w jakich przetwarzane były dane osobowe w małych jednostkach organizacyjnych.

O ile generalnie można stwierdzić, iż niektóre większe jednostki podejmowały nieudolne, co prawda, ale zawsze jakieś próby stworzenia dokumentu określającego politykę bezpieczeństwa, to w mniejszych jednostkach nie stwierdzono nawet takich prób. Nie mówiąc już o pełnowartościowym, zawierającym całościowe spojrzenie na sprawy związane z ochroną danych, dokumentem, utworzonym zgodnie z jedną z powszechnie stosowanych metodyk. Przyczyna tego zjawiska tkwi najczęściej w tym, że:

- niektóre podmioty nie dostrzegają rzeczywistych potrzeb i korzyści z wdrożenia polityki bezpieczeństwa, a rozporządzenie nie wymaga wprost, aby fakt jej opracowania udokumentowany był w postaci odpowiedniego dokumentu,
- w kontrolowanych jednostkach dał się zauważyć brak specjalistów będących w stanie stworzyć, stosowną dla potrzeb firmy, politykę bezpieczeństwa, a zlecenie tego typu usług na zewnątrz postrzegane jest jako niewskazane ze względu na ujawnianie tym samym rozwiązań, które powinny być chronione,
- w niektórych jednostkach organizacyjnych całkowicie zignorowano ustawowe obowiązki ochrony prawnie chronionych danych w tym również obowiązki ochrony danych osobowych.

W odniesieniu do pierwszej z wymienionych grup podmiotów, t.j. tych, które rozważały elementy wskazane w § 2 rozporządzenia, ale nie opracowały ich w formie dokumentu z uwagi na ich zdaniem brak takiej potrzeby, trudno nie przyznać im racji. Zwłaszcza, jeśli przetwarzany przez nich zbiór danych osobowych był nieliczny, zlokalizowany na pojedynczym komputerze typu PC lub w kilkustanowiskowej sieci lokalnej. Za uzasadnione wydaje się wówczas rozumowanie, iż dokument taki nie jest konieczny, zwłaszcza jeżeli najistotniejsze elementy, o których mowa w § 2 rozporządzenia włączone zostaną do instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji, o której mówi § 11 punkt 1 rozporządzenia. Sytuacja taka wystąpiła, jak już wspomniano, w Spółce Woryed S.A.

W wielu jednak przypadkach Generalny Inspektor ustalił, że jednostka nie dysponowała w ogóle żadną z wymienionych dokumentacji jak, np. w Biurze Pośrednictwa Nieruchomościami „STOLICA” w Warszawie, czy MIDAS Sp. z o.o. w Łodzi. W innych jednostkach jak, np. w Euroglob Sp. z o.o w Gdyni, w Agencja Nieruchomości Poreda Sp. z o.o w Warszawie, czy też w COID System Sp. z o.o w Warszawie, przedstawione do wglądu instrukcje były „anonimowe”, to jest ich zawartość ograniczała się praktycznie do przepisanej z niewielkimi zmianami, treści odpowiednio § 6 punkt 2 rozporządzenia oraz § 11 punkt 2 rozporządzenia i nie stanowiła rzeczywiście przyjętych ustaleń i procedur dotyczących sposobu zarządzania eksploatowanym systemem.

Charakterystycznym dla małych jednostek organizacyjnych było również to, iż pomimo posiadanej często wiedzy na temat wymagań, jakie nakłada na administratorów ustawa o ochronie danych osobowych, jednostki takie nie posiadały na ogół instrukcji

zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, o której mówi § 11 rozporządzenia. W wielu przypadkach wynikało to z faktu, że w małych jednostkach organizacyjnych administracją systemów informatycznych zajmują się firmy zewnętrzne na podstawie umowy outsorsingu. Firmy te na ogół nie dostarczają swoim klientom żadnych dokumentacji zarządzania administrowanym systemem. Wymagań takich nie zawarto w zawieranych umowach outsorsingowych. Same jednostki korzystające z usług outsorsingowych, będące formalnie administratorem przetwarzanych danych osobowych, nie przyłożyły należytej uwagi do wymaganych przez ustawę warunków techniczno - organizacyjnych. Jak wynika z przeprowadzonych kontroli, tylko w nielicznych przypadkach sporządzono aneksy do zawartych umów outsorsingowych, w których dookreślono zakres przetwarzania danych osobowych i czynności, jakie zobowiązany jest dopełnić zleceniobiorca w związku z wejściem w życie ustawy.

I.6 Uchybienia w zakresie wymagań funkcjonalnych stawianych systemom informatycznym przetwarzającym dane osobowe

Bardzo niepokojącym faktem, który zaobserwowano podczas prowadzonych kontroli zarówno w dużych jak i małych jednostkach organizacyjnych jest to, że pomimo upływu 2 lat od wejścia w życie rozporządzenia, nadal tylko w nielicznych przypadkach systemy służące do przetwarzania danych w pełni odpowiadają przyjętym w nim wymogom.

Wiele z kontrolowanych w 2000 r. systemów informatycznych, nie spełniało warunków określonych w § 16 punkt 1, 2 i 3 odnoszących się odpowiednio do obowiązku: odnotowania daty pierwszego wprowadzenia danych, obowiązku odnotowania źródła pochodzenia danych oraz obowiązku odnotowania identyfikatora użytkownika wprowadzającego dane.

Nadal tylko nieliczne systemy dostosowane są do realizacji wymogów określonych w § 16 punkt 4 i 5 Rozporządzenia. Należą do nich między innymi system „Zorba” użytkowany w PKO BP co ustalono w czasie kontroli PKO BP S.A. IV Oddział Centrum we Wrocławiu oraz niektóre egzemplarze systemu Kadrowo-Płacowego autorstwa firmy PROKOM co odnotowano podczas kontroli w Zakładzie Telekomunikacji w Łodzi oraz kontroli sprawdzającej wykonanie zaleceń pokontrolnych w Najwyższej Izbie Kontroli.

Podobne zastrzeżenia odnoszą się do realizacji wymogów określonych w § 17 Rozporządzenia, który mówi że *„system informatyczny służący do przetwarzania danych osobowych powinien umożliwiać udostępnienie na piśmie, w powszechnie zrozumiałej formie,*

treści danych o każdej osobie, której dane są przetwarzane, wraz z informacjami, o których mowa w § 16.”

Optymistycznym akcentem, jaki można zaobserwować w działalności administratorów bezpieczeństwa informacji w dużych jednostkach organizacyjnych, jest podejmowanie działań zmierzających do dostosowania systemów informatycznych do pełnej realizacji wymagań określonych w § 16 i 17 rozporządzenia. Sposób ich realizacji jest różny. W niektórych jednostkach wymienia się stare systemy informatyczne na nowe, spełniające wymagania ustawy o ochronie danych osobowych, w innych natomiast do eksploatowanych obecnie systemów dobudowuje się specjalne moduły. Czas jaki rezerwują sobie jednak administratorzy danych na wykonanie wspomnianych czynności naprawczych jest w niektórych przypadkach zbyt długi. Nie do zaakceptowania jest, np. okres 2-3 lat w jakim zadeklarował się czynności takie przeprowadzić Zakład Ubezpieczeń Społecznych.

II. Omówienie zakresu kontroli w poszczególnych jednostkach organizacyjnych

DIS-K-1/00

Firma Medyczno – Farmaceutyczna Pulsmed w Łodzi

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek informacji o znalezieniu na śmietniku kart szczepień zawierających dane osobowe, zamieszczonej w „Dzienniku Łódzkim”. Kontrolą objęto sposób zabezpieczenia zbiorów danych osobowych prowadzonych przez Firmę Medyczno – Farmaceutyczną Pulsmed w Łodzi. W jej toku stwierdzono uchybienia organizacyjno – techniczne, w postaci m.in. nieusuwania lub poddawania anonimizacji danych ze zbioru doraźnego, braku ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych, niezastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, nie wypełnienie obowiązków o charakterze personalnym i formalnym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W związku z dokonanymi ustaleniami Generalny Inspektor Ochrony Danych Osobowych wydał decyzję GI-DEC-DP-32/00, nakazującą administratorowi danych usunięcie uchybień w procesie przetwarzania danych osobowych. Po złożeniu przez Firmę Medyczno – Farmaceutyczną Pulsmed w Łodzi wniosku o ponowne rozpatrzenie sprawy,

Generalny Inspektor Ochrony Danych Osobowych wydał decyzję GI-DEC-DP-51/00 utrzymującą w mocy zaskarżoną decyzję.

Ponadto, w przedmiotowej sprawie skierowano do prokuratury zawiadomienie o popełnieniu przez Firmę Medyczno – Farmaceutyczną Pulsmed w Łodzi przestępstwa określonego w art. 52 ustawy o ochronie danych osobowych.

DIS-K-2/00

Powszechne Towarzystwo Emerytalne Pioneer S.A. z siedzibą w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek skargi GI-DIS-464/99. Kontrolą objęto marketingową bazę danych prowadzoną przez Powszechne Towarzystwo Emerytalne Pioneer S.A. z siedzibą w Warszawie, zgłoszoną do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych. W jej toku stwierdzono uchybienia w zakresie nie zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

W związku z powyższym, Generalny Inspektor wysłał pismo informujące kontrolowanego administratora danych o uchybieniach stwierdzonych w toku kontroli oraz wystąpienie z żądaniem wszczęcia postępowania dyscyplinarnego wobec osoby odpowiedzialnej za zabezpieczenie danych osobowych i poinformowania w określonym terminie o wynikach tego postępowania i podjętych działaniach.

Wobec usunięcia przez jednostkę kontrolowaną stwierdzonych nieprawidłowości, w przedmiotowej sprawie nie wszczęto postępowania administracyjnego.

DIS-K-3/00

Stowarzyszenie Finlandia Arctic Club w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na wniosek Departamentu Rejestracji Zbiorów Danych Osobowych. Kontrolą objęto zbiór danych osobowych prowadzony przez Stowarzyszenie Finlandia Arctic Club w Warszawie o nazwie „Baza Finlandia Arctic Club” (zgłoszenie Nr R 000597/99). W jej toku ustalono, że Stowarzyszenie Finlandia Arctic Club w Warszawie nie pozyskiwało danych do zbioru zgłoszonego do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych i nie zamierza czynić tego w przyszłości. Ponadto, w trakcie kontroli Prezes Stowarzyszenia złożył oświadczenie o wycofaniu wniosku rejestracyjnego.

Wnioski z kontroli zostały przekazane do Departamentu Rejestracji Zbiorów Danych Osobowych.

DIS-K-4/00

Solidum Sp. z o.o. z siedzibą w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na wniosek Departamentu Rejestracji Zbiorów Danych Osobowych. Kontrolą objęto zbiór danych osobowych prowadzony przez Solidum Sp. z o.o. z siedzibą w Warszawie o nazwie „Kandydaci” (zgłoszenie Nr R 006398/99). W jej toku stwierdzono uchybienia w następującym zakresie: niedopełnienia obowiązku informacyjnego, niezastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, braku ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych, niewypełnienia obowiązków o charakterze personalnym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Wnioski z kontroli przekazano Departamentowi Rejestracji Zbiorów Danych Osobowych.

DIS-K-5/00 i DIS-K-65/00

PolCard S.A. z siedzibą w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek skargi GI-DP-796/99. Kontrolą objęto zbiory danych osobowych prowadzone przez PolCard S.A. w Warszawie. W jej toku stwierdzono uchybienia w zakresie niedopełnienia obowiązku informacyjnego oraz niewypełnienia obowiązków o charakterze personalnym i technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W związku z tym, że w toku postępowania wyjaśniającego jednostka kontrolowana usunęła stwierdzone w trakcie kontroli uchybienia, w przedmiotowej sprawie nie wszczęto postępowania administracyjnego.

DIS-K-6/00

Polsko – Amerykańskie Przedsiębiorstwo Produkcyjno – Handlowe KOSS Sp. z o.o. z siedzibą w Nadarzynie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na wniosek Państwowej Inspekcji Pracy w Łodzi. Kontrolą objęto zbiór danych osobowych kandydatów do pracy oraz pracowników prowadzony przez Polsko – Amerykańskie Przedsiębiorstwo Produkcyjno – Handlowe KOSS Sp. z o.o. z siedzibą w Nadarzynie. W jej toku stwierdzono uchybienia w zakresie braku podstawy prawnej do przetwarzania danych osobowych szczególnie chronionych w odniesieniu do pracowników i kandydatów do pracy oraz nieadekwatności przetwarzanych danych w stosunku do celów, dla których zostały zebrane.

W związku z powyższym, Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne. Decyzją GI-DP-DEC-29/00 Generalny Inspektor nakazał Polsko – Amerykańskiemu Przedsiębiorstwu Produkcyjno – Handlowemu KOSS Sp. z o.o. z siedzibą w Nadarzynie usunięcie uchybień w procesie przetwarzania danych osobowych.

DIS-K-7/00

Reader's Digest Przegląd Sp. z o.o. z siedzibą w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek licznych skarg dotyczących przetwarzania danych osobowych skarżących bez ich zgody. Kontrolą objęto zbiory danych osobowych prowadzone przez Reader's Digest Przegląd Sp. z o.o. z siedzibą w Warszawie o nazwach „Baza klientów – RDP – CDMS” (zgłoszenie nr R 015867/99) oraz „Baza klientów – RDP – IFS” (zgłoszenie nr R 015864/99). W jej toku stwierdzono uchybienia w zakresie niedopełniania obowiązku informacyjnego oraz braku procedury uwzględniania sprzeciwów.

W związku z tym, że Reader's Digest Przegląd Sp. z o.o. z siedzibą w Warszawie w toku postępowania wyjaśniającego usunęła stwierdzone w trakcie kontroli uchybienia, w przedmiotowej sprawie nie wszczęto postępowania administracyjnego.

DIS-K-8/00

ABN – AMRO Bank (Polska) S.A. z siedzibą w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek skargi GI-DIS-6/00. Kontrolą objęto zbiory

danych osobowych prowadzone przez ABN – AMRO Bank (Polska) S.A. w Warszawie. W jej toku stwierdzono uchybienia w zakresie niedopełniania obowiązku informacyjnego oraz braku ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych.

W związku z tym, że w toku postępowania wyjaśniającego jednostka kontrolowana usunęła stwierdzone w trakcie kontroli uchybienia, w przedmiotowej sprawie nie wszczęto postępowania administracyjnego.

DIS-K-9/00

Komitet Ochrony Praw Dziecka z siedzibą w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek skargi GI-DIS-244/99. Kontrolą objęto zbiory danych osobowych prowadzone przez Komitet Ochrony Praw Dziecka w Warszawie. W jej toku stwierdzono uchybienia w zakresie niedopełnienia obowiązku informacyjnego.

W związku z tym, że w toku postępowania wyjaśniającego Komitet Ochrony Praw Dziecka w Warszawie usunął stwierdzone w trakcie kontroli uchybienia, w przedmiotowej sprawie nie wszczęto postępowania administracyjnego.

GI-DIS-10/00

SMG / KRC Poland Human Resources Sp. z o.o. z siedzibą w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na wniosek Departamentu Rejestracji Zbiorów Danych Osobowych. Kontrolą objęto zbiór danych osobowych prowadzony przez SMG / KRC Poland Human Resources Sp. z o.o. z siedzibą w Warszawie o nazwie „Baza danych SMG / KRC Poland Human Resources Sp. z o.o.” (zgłoszenie Nr R 010305/99). W jej toku stwierdzono uchybienia w zakresie braku ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych oraz niewypełnienia obowiązków o charakterze personalnym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Wnioski z kontroli zostały przekazane do Departamentu Rejestracji Zbiorów Danych Osobowych.

DIS-K-11/00

Korporacja Nieruchomości LDM Sp. z o.o. z siedzibą w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na wniosek Departamentu Rejestracji Zbiorów Danych Osobowych. Kontrolą objęto zbiór danych osobowych prowadzony przez. Korporację Nieruchomości LDM Sp. z o.o. z siedzibą w Warszawie pod nazwą „Baza danych klientów biura obrotu nieruchomościami LDM” (zgłoszenie Nr R 008053/99). W jej toku stwierdzono uchybienia w zakresie braku podstaw prawnych przetwarzania danych objętych szczególną ochroną, niedopełniania obowiązku informacyjnego oraz niezastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

Wnioski pokontrolne przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych.

DIS-K-12/00

Polska Korporacja Telewizyjna Sp. z o.o. z siedzibą w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na wniosek Departamentu Rejestracji Zbiorów Danych Osobowych. Kontrolą objęto zbiór danych o nazwie „SMS WEB – System Zarządzania Abonamentem Canal +/Cyfra +” (zgłoszenie nr R 010510/99). W jej toku stwierdzono uchybienia w zakresie łączenia zgody na przetwarzanie danych abonenta w celach marketingowych, badań statystycznych oraz na udostępnianie danych osobom trzecim w momencie podpisywania umowy, bez możliwości rezygnacji z wyrażenia zgody przez abonenta na przetwarzanie danych w którymś ze wskazanych celów, nieudokumentowania, że pracownikom dopuszczonym do obsługi systemu informatycznego służącego do przetwarzania danych osobowych zostały wydane stosowne upoważnienia oraz niewypełnienia obowiązków o charakterze personalnym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Wnioski pokontrolne zostały przekazane do Departamentu Rejestracji Zbiorów Danych Osobowych.

DIS-K-13/00

Dargo Pośrednictwo Ubezpieczeniowe S.C. Grażyna Rosińska, Agata Rosińska z siedzibą w Łodzi

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na wniosek Departamentu Rejestracji Zbiorów Danych Osobowych. Kontrolą objęto zbiory danych osobowych prowadzone przez Dargo Pośrednictwo Ubezpieczeniowe S.C. Grażyna Rosińska, Agata Rosińska z siedzibą w Łodzi, w tym zbiór o nazwie „Zbiór danych osobowych ubezpieczanych, ubezpieczających, uposażonych” (zgłoszenie nr R 011392/99). W jej toku stwierdzono uchybienia w zakresie niezastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

Wnioski z kontroli przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych. Ponadto, w związku z usunięciem przez jednostkę kontrolowaną w toku postępowania wyjaśniającego uchybień w zakresie zabezpieczenia danych osobowych, w przedmiotowej sprawie nie wszczęto postępowania administracyjnego.

DIS-K-14/00

Midas Sp. z o.o. z siedzibą w Łodzi

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na wniosek Departamentu Rejestracji Zbiorów Danych Osobowych. Kontrolą objęto zbiory danych osobowych prowadzone przez Midas Sp. z o.o. z siedzibą w Łodzi, w tym zbiór danych o nazwie „Midas Sp. z o.o.” (zgłoszenie Nr R 006989/99). W jej toku stwierdzono uchybienia w zakresie niedopełnienia obowiązku informacyjnego, braku ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych, niezastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych oraz niewypełnienia obowiązków o charakterze personalnym, organizacyjnym i technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Wnioski z kontroli przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych.

DIS-K-15/00

Zakład Telekomunikacji Polskiej S.A. w Łodzi

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek informacji prasowej o kradzieży bazy danych.

Kontrolą objęto zbiór danych osobowych prowadzony przez Zakład Telekomunikacji Polskiej S.A. w Łodzi. W jej toku stwierdzono uchybienia w zakresie braku podstawy prawnej do przetwarzania danych osobowych w celach marketingowych, niedopełnienia obowiązku informacyjnego oraz niewypełnienia obowiązków o charakterze formalnym i technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W okresie sprawozdawczym sprawa w toku, ze względu na konieczność przeprowadzenia kontroli w innych jednostkach organizacyjnych Telekomunikacji Polskiej S.A., a w szczególności w siedzibie zarządu Spółki.

DIS-K-16/00

SMG / KRC Poland Media S.A. z siedzibą w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek skargi GI-DIS-372/99. Kontrolą objęto zbiory danych osobowych prowadzone przez SMG / KRC Poland Media S.A. z siedzibą w Warszawie. W jej toku stwierdzono uchybienia w zakresie niedopełnienia obowiązku informacyjnego oraz niewypełnienia obowiązków o charakterze formalnym i technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Wnioski z kontroli zostały przekazane do Departamentu Rejestracji Zbiorów Danych Osobowych.

DIS-K-17/00

Agencja Poreda – Nieruchomości w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na wniosek Departamentu Rejestracji Zbiorów Danych Osobowych. Kontrolą objęto zbiory danych osobowych prowadzone przez Agencję Poreda – Nieruchomości w Warszawie, w tym zbiór danych o nazwie „Baza danych klientów Agencja Poreda – Nieruchomości” (zgłoszenie Nr R 006674/99). W jej toku stwierdzono uchybienia, co do braku podstawy prawnej do przetwarzania danych osobowych objętych szczególną

ochroną, niedopełnienia obowiązku informacyjnego, niezastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, braku ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych oraz niewypełnienia obowiązków o charakterze formalnym, personalnym i technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Wnioski pokontrolne przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych.

DIS-K-18/00

Firma Kodeks – Mirosława Krzyczkowska w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na wniosek Departamentu Rejestracji Zbiorów Danych Osobowych. Kontrolą objęto zbiory danych osobowych prowadzone przez Firmę Kodeks – Mirosława Krzyczkowska w Warszawie, w tym zbiór o nazwie „Baza danych klientów biura obrotu nieruchomościami Kodeks” (zgłoszenie Nr R 003503/99). W jej toku stwierdzono uchybienia w zakresie braku podstawy prawnej do przetwarzania danych osobowych objętych szczególną ochroną oraz niezastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

Wnioski z kontroli przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych.

DIS-K-19/00

Bols Sports & Travel Sp. z o.o. z siedzibą w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek skargi GI-DIS-430/99. Kontrolą objęto zbiory danych osobowych prowadzone przez Bols Sports & Travel Sp. z o.o. w Warszawie, w tym zbiór o nazwie „Baza danych rozmówców bezpłatnej infolinii BOLS & TRAVEL” – Nr KR 000064. W jej toku stwierdzono uchybienia w zakresie niedopełnienia obowiązku zgłoszenia zmian w zbiorze danych oraz niewypełnienia obowiązków o charakterze formalnym i technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim

powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W związku z tym, że w toku postępowania wyjaśniającego jednostka kontrolowana usunęła stwierdzone w trakcie kontroli uchybienia, w przedmiotowej sprawie nie wszczęto postępowania administracyjnego.

DIS-K-20/00

Lukas S.A. z siedzibą we Wrocławiu

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek skargi GI-DIS-425/99. Kontrolą objęto zbiory danych osobowych prowadzone przez Lukas S.A. z siedzibą we Wrocławiu, w tym zbiory o nazwach „Zbiór osób, którym został udzielony kredyt na zakup towarów, usług lub samochodów za pośrednictwem Lukas S.A. – służący celom marketingowym” (nr księgi 007228), „Zbiór osób, którym został udzielony kredyt na zakup towarów, usług lub samochodów za pośrednictwem Lukas S.A.” (zgłoszenie nr R 011980/99), „Kandydaci do pracy w Lukas S.A.” (zgłoszenie nr R 011977/99) i „Kontrahenci Lukas S.A.” (zgłoszenie nr R 011978/99). W jej toku stwierdzono uchybienia w zakresie braku podstawy prawnej do przetwarzania danych osobowych szczególnie chronionych w odniesieniu do pracowników, niedopełnienia obowiązku informacyjnego, nieadekwatności zakresu przetwarzanych danych w stosunku do celów, dla których zostały zebrane, w związku z kserowaniem stron dowodu osobistego oraz niewypełnienia obowiązków o charakterze formalnym i technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. W trakcie kontroli zakwestionowana została również praktyka kontrolowanego podmiotu polegająca na tym, iż zawarcie umowy jest uzależnione od wyrażenia zgody na przetwarzanie danych w celach marketingowych.

W związku z dokonanymi ustaleniami Generalny Inspektor Ochrony Danych Osobowych wydał decyzję GI-DP-DEC-5/01, nakazującą Lukas S.A. z siedzibą we Wrocławiu przywrócić w procesie przetwarzania danych osobowych stan zgodny z prawem.

DIS-K-21/00

Centrala Banku Polska Kasa Opieki S.A. – Grupa Pekao S.A. z siedzibą w Warszawie

Kontrolą objęto zbiór danych osobowych potencjalnych klientów Banku Polska Kasa Opieki S.A. – Grupa Pekao S.A. z siedzibą w Warszawie prowadzony przez Centralę Banku Polska Kasa Opieki S.A. – Grupa Pekao S.A. z siedzibą w Warszawie. W jej toku stwierdzono uchybienia w zakresie braku podstawy prawnej do przetwarzania danych osobowych potencjalnych klientów, niedopełniania obowiązku informacyjnego, niedopełnienia obowiązku zgłoszenia do rejestracji zbioru danych potencjalnych klientów, braku ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych oraz niewypełnienia obowiązków o charakterze organizacyjnym i technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Wobec usunięcia przez jednostkę kontrolowaną w toku postępowania wyjaśniającego uchybień stwierdzonych w trakcie kontroli, w przedmiotowej sprawie nie wszczęto postępowania administracyjnego.

DIS-K-22/00

Centrum Muzyczno – Rozrywkowe Digital Sp. z o.o. z siedzibą w Warszawie

Kontrolę przeprowadzono w celu sprawdzenia wykonania decyzji Generalnego Inspektora Ochrony Danych Osobowych, nr GI-DP-DEC-68/99, nakazującej usunięcie uchybień stwierdzonych podczas kontroli DIS-K-32/99. Kontrolą objęto zbiór danych osobowych prowadzony przez Centrum Muzyczno – Rozrywkowe Digital Sp. z o.o. z siedzibą w Warszawie, w którym przetwarzane są dane osobowe klientów. W jej toku stwierdzono uchybienia w zakresie niewypełnienia obowiązków o charakterze formalnym i personalnym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W związku z usunięciem przez jednostkę kontrolowaną w toku postępowaniu wyjaśniającego stwierdzonych w trakcie kontroli uchybień, uznano, że Centrum Muzyczno – Rozrywkowe Digital Sp. z o.o. z siedzibą w Warszawie wykonała zalecenia zawarte w decyzji Generalnego Inspektora Ochrony Danych Osobowych, nr GI-DP-DEC-68/99.

DIS-K-23/00

Euroglob Sp. z o.o. z siedzibą w Sopocie

Kontrolę przeprowadzono w celu sprawdzenia wykonania wniosków z kontroli DIS-K-45/99. Kontrolą objęto zbiór danych osobowych o nazwie „Euroglob” prowadzony przez Euroglob Sp. z o.o. z siedzibą w Sopocie, zgłoszony do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (zgłoszenie Nr R 018040/99). W jej toku stwierdzono uchybienia w zakresie niedopełniania obowiązku informacyjnego, braku ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych oraz niewypełnienia obowiązków o charakterze technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W związku z dokonanymi ustaleniami Generalny Inspektor Ochrony Danych Osobowych wydał decyzję GI-DP-DEC-22/00, nakazującą Euroglob Sp. z o.o. z siedzibą w Sopocie usunięcie uchybień w procesie przetwarzania danych osobowych.

Ponadto, Generalny Inspektor Ochrony Danych Osobowych skierował do prokuratury zawiadomienie o popełnieniu przez osoby odpowiedzialne za przetwarzanie danych osobowych w zbiorach danych osobowych prowadzonych przez Euroglob Sp. z o.o. z siedzibą w Sopocie przestępstwa z art. 54 ustawy o ochronie danych osobowych. Prokurator Prokuratury Rejonowej w Gdyni odmówił wszczęcia dochodzenia w przedmiotowej sprawie. Na ww. postanowienie Generalny Inspektor Ochrony Danych Osobowych wniósł zażalenie do Prokuratora Okręgowego w Gdańsku, który uwzględnił zażalenie, uchylił postanowienie o odmowie wszczęcia dochodzenia i wszczął dochodzenie.

DIS-K-24/00

Bank Polska Kasa Opieki S.A. – Grupa Pekao S.A. Oddział V w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono w związku z kontrolą DIS-K-21/00. Kontrolą objęto zbiór danych osobowych potencjalnych klientów Banku Polska Kasa Opieki S.A. – Grupa Pekao S.A. z siedzibą w Warszawie, prowadzony przez V Oddział Banku Polska Kasa Opieki S.A. – Grupa Pekao S.A. z siedzibą w Warszawie. Wnioski i sposób zakończenia sprawy przedstawione zostały przy omawianiu kontroli DIS-K-21/00.

DIS-K-25/00

Wydawnictwo Verlag Dashöfer Sp. z o.o. z siedzibą w Warszawie

Kontrolę przeprowadzono w celu sprawdzenia wykonania decyzji Generalnego Inspektora Ochrony Danych Osobowych, sygn. GI-DP-DEC-64/99. Kontrolą objęto zbiór danych osobowych prowadzony przez Wydawnictwo Verlag Dashöfer Sp. z o.o. z siedzibą w Warszawie. Materiał dowodowy zebrany w jej toku stanowił podstawę do uznania, że Wydawnictwo Verlag Dashöfer Sp. z o.o. z siedzibą w Warszawie wykonało zalecenia zawarte w decyzji Generalnego Inspektora Ochrony Danych Osobowych, sygn. GI-DP-DEC-64/99.

DIS-K-26/00

Aster City Cable Sp. z o.o. z siedzibą w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek skargi GI-DIS-14/00. Kontrolą objęto zbiory danych osobowych prowadzone przez Aster City Cable Sp. z o.o. w Warszawie, w tym zbiór o nazwie „Baza abonentów Aster City Cable” (Nr KR 007400). W jej toku stwierdzono uchybienia w zakresie niedopełnienia obowiązku informacyjnego oraz niewypełnienia obowiązków o charakterze personalnym, formalnym i technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Ponadto, w trakcie kontroli stwierdzono, iż formularze umów abonenckich zawierają informację, iż abonent wyraża zgodę na przetwarzanie jego danych osobowych między innymi w celach marketingowych, reklamowych oraz informacyjnych. Formularze zawierają także informację o wyrażeniu zgody przez abonenta na przesyłanie materiałów promocyjnych i reklamowych innych podmiotów, rozpowszechnionych przez Operatora. Informacje te ujęte zostały w formie postanowień umowy. Abonent podpisując umowę wyraża jednocześnie zgodę na wszystkie zawarte w niej postanowienia.

W związku z dokonanymi ustaleniami, Generalny Inspektor Ochrony Danych Osobowych wydał decyzję GI-DP-DEC-44/00, nakazującą usunięcie uchybień w procesie przetwarzania danych.

DIS-K-27/00

Conrad Electronic Sp. z o.o. z siedzibą w Skierniewicach

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek skargi GI-DIS-80/00. Kontrolą objęto zbiory danych osobowych prowadzone przez Conrad Electronic Sp. z o.o., w tym zbiór o nazwie „COFI” (nr KR 000080). W jej toku stwierdzono uchybienia w zakresie niedopełnienia obowiązku informacyjnego oraz niewypełnienia obowiązków o charakterze technicznym, organizacyjnym i formalnym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W związku z tym, że jednostka kontrolowana nie usunęła wszystkich stwierdzonych w trakcie kontroli uchybień, Generalny Inspektor Ochrony Danych Osobowych wydał decyzję GI-DP-DEC-67/00, nakazującą usunięcie uchybień w procesie przetwarzania danych osobowych.

DIS-K-28/00

Niepubliczny Zakład Opieki Zdrowotnej Poradnia Medycyny Rodzinnej S.C. z siedzibą w Markach

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek skargi GI-DIS-139/00. Kontrolą objęto zbiory danych osobowych prowadzone przez Niepubliczny Zakład Opieki Zdrowotnej Poradnia Medycyny Rodzinnej S.C. z siedzibą w Markach. W jej toku stwierdzono uchybienia w zakresie braku podstawy prawnej pozyskania dokumentacji medycznej, niedopełniania obowiązku informacyjnego oraz niewypełnienia obowiązków o charakterze personalnym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W związku z tym, że w toku postępowania wyjaśniającego jednostka kontrolowana usunęła stwierdzone w trakcie kontroli uchybienia, w przedmiotowej sprawie nie wszczęto postępowania administracyjnego.

DIS-K-29/00

Niepubliczny Zakład Opieki Zdrowotnej Eskulap S.C. z siedzibą w Markach

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek skargi GI-DIS-139/00. Kontrolą objęto zbiory danych osobowych prowadzone przez Niepubliczny Zakład Opieki Zdrowotnej Eskulap S.C. z siedzibą w Markach. W jej toku stwierdzono uchybienia w zakresie braku podstawy prawnej do udostępniania dokumentacji medycznej, niedopełniania obowiązku informacyjnego, niezastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych oraz niewypełnienia obowiązków o charakterze personalnym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W związku z tym, że w toku postępowania wyjaśniającego jednostka kontrolowana usunęła stwierdzone w trakcie kontroli uchybienia, w przedmiotowej sprawie nie wszczęto postępowania administracyjnego.

DIS-K-30/00

Najwyższa Izba Kontroli w Warszawie

Kontrolą objęto zbiory danych osobowych prowadzone przez Najwyższą Izbę Kontroli w Warszawie. W jej toku stwierdzono uchybienia w zakresie niedopełnienia obowiązku zgłoszenia do rejestracji zbioru danych osób wnoszących skargi i wnioski oraz niewypełnienia obowiązków o charakterze formalnym, personalnym i technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Wobec usunięcia przez jednostkę kontrolowaną w toku postępowania wyjaśniającego uchybień stwierdzonych w trakcie kontroli, także w postaci zgłoszenia do zarejestrowania zbioru osób zgłaszających skargi i wnioski, w przedmiotowej sprawie nie wszczęto postępowania administracyjnego. Ponadto, na podstawie art. 17 ust. 2 ustawy o ochronie danych osobowych, zażądano wszczęcia postępowania dyscyplinarnego wobec osoby (bądź osób), odpowiedzialnej za realizację obowiązku zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi.

DIS-K-31/00

Najwyższa Izba Kontroli Delegatura w Katowicach

Kontrolą objęto zbiory danych osobowych prowadzone przez Najwyższą Izbę Kontroli Delegatura w Katowicach. W jej toku stwierdzono uchybienia w zakresie niewypełnienia obowiązków o charakterze personalnym i technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Wobec usunięcia przez jednostkę kontrolowaną w toku postępowania wyjaśniającego uchybień stwierdzonych w trakcie kontroli, w przedmiotowej sprawie Generalny Inspektor nie wszczął postępowania administracyjnego.

Ponadto, na podstawie art. 17 ust. 2 ustawy o ochronie danych osobowych, zażądał wszczęcia postępowania dyscyplinarnego wobec osoby (bądź osób) odpowiedzialnej za realizację wymogów określonych w rozporządzeniu, z uwagi na znaczne opóźnienie w stosunku do terminu wskazanego w art. 62 ust. 1 ustawy.

DIS-K-32/00

Volkswagen Bank Polska S.A. z siedzibą w Warszawie

Kontrolę przeprowadzono w celu sprawdzenia wykonania decyzji GI-DEC-DP-3/00. Kontrolą objęto zbiór danych osobowych prowadzony przez Volkswagen Bank Polska S.A. z siedzibą w Warszawie o nazwie „Dane Naszych Klientów”, zgłoszony do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (zgłoszenie Nr 000009/98). W jej toku stwierdzono uchybienia w zakresie niewypełnienia obowiązków o charakterze technicznym, określonych w rozporządzeniu ministra spraw wewnętrznych i administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Wobec usunięcia przez jednostkę kontrolowaną w toku postępowania wyjaśniającego uchybień stwierdzonych w trakcie kontroli, w przedmiotowej sprawie nie wszczęto postępowania administracyjnego.

DIS-K-33/00

Kancelaria Prezesa Rady Ministrów w Warszawie

Kontrolą objęto zbiory danych osobowych prowadzone przez Kancelarię Prezesa Rady Ministrów w Warszawie. W jej toku stwierdzono uchybienia w zakresie niedopełnienia

obowiązku zgłoszenia do rejestracji zbioru danych osób wnoszących skargi, braku ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych oraz niewypełnienia obowiązków o charakterze formalnym, organizacyjnym, technicznym i personalnym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W związku z dokonanymi ustaleniami, Generalny Inspektor Ochrony Danych Osobowych wydał decyzję GI-DEC-DIS-72/01, nakazującą usunięcie uchybień w procesie przetwarzania danych osobowych.

DIS-K-34/00

Przedsiębiorstwo Handlowe Bela Vita Sp. z o.o. z siedzibą we Wrocławiu

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek skargi GI-DIS-86/00. Kontrolą objęto zbiory danych osobowych prowadzone przez Przedsiębiorstwo Handlowe Bela Vita Sp. z o.o. we Wrocławiu, w tym zbiór o nazwie „Klienci Przedsiębiorstwa Handlowego Bela Vita” – Nr KR 000087. W jej toku stwierdzono uchybienia w zakresie niedopełnienia obowiązku informacyjnego oraz niewypełnienia obowiązków o charakterze technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W celu sprawdzenia wykonania zaleceń pokontrolnych w Przedsiębiorstwie Handlowym Bela Vita Sp. z o.o. z siedzibą we Wrocławiu przeprowadzono kontrolę DIS-K-89/00. W związku z nie usunięciem przez jednostkę kontrolowaną wszystkich stwierdzonych uchybień, Generalny Inspektor Ochrony Danych Osobowych wydał decyzję GI-DEC-DP-100/00, nakazującą jednostce kontrolowanej usunięcie uchybień w procesie przetwarzania danych osobowych.

DIS-K-35/00

Bankowy Fundusz Gwarancyjny w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na wniosek Departamentu Rejestracji Zbiorów Danych Osobowych. Kontrolą objęto zbiór danych osobowych prowadzony przez Bankowy Fundusz Gwarancyjny o nazwie „Lista deponentów”. W jej toku stwierdzono uchybienia w zakresie

niedopełnienia obowiązku zgłoszenia do rejestracji zbioru danych osobowych o nazwie „Lista deponentów” oraz niedopełniania obowiązku informacyjnego.

Ustalenia z kontroli przekazane zostały do Departamentu Rejestracji Zbiorów Danych Osobowych.

DIS-K-36/00

Telemark Sp. z o.o. w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek skargi. Kontrolą objęto zbiory danych osobowych prowadzone przez Telemark Sp. z o.o. z siedzibą w Warszawie, w tym zbiór o nazwie „Marketingowa baza danych Telemark” (nr zgłoszenia R 035550/99). W jej toku stwierdzono uchybienia w zakresie niedopełniania obowiązku informacyjnego, nie zgłoszenia zmian w zbiorze danych, braku określenia w umowie zawartej z podmiotem, któremu udostępniono zbiór danych osobowych do jednorazowego wykorzystania, celu, w jakim dane mogą zostać wykorzystane oraz braku ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych.

W okresie sprawozdawczym sprawa w toku, ze względu na konieczność przeprowadzenia kontroli sprawdzającej wykonanie zaleceń Generalnego Inspektora.

DIS-K-37/00

The Communications Bridge Sp. z o.o. z siedzibą w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek skargi. Kontrolą objęto zbiory danych osobowych prowadzone przez The Communications Bridge Sp. z o.o. w Warszawie, w tym zbiór o nazwie „Baza Danych – Margaryna” (Nr KR 001744). W jej toku stwierdzono uchybienia w zakresie niedopełniania obowiązku informacyjnego oraz niewypełnienia obowiązków o charakterze technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Ponadto stwierdzono, iż w umowie zawartej między jednostką kontrolowaną a podmiotem powierzającym przetwarzanie danych osobowych nie została uregulowana kwestia związana z przechowywaniem, zabezpieczaniem i niszczeniem materiałów pochodzących z akcji marketingowych.

W związku z ogłoszeniem upadłości The Communications Bridge Sp. z o.o. z siedzibą w Warszawie w przedmiotowej sprawie Generalny Inspektor nie wszczął postępowania administracyjnego.

DIS-K-38/00

MediAdress Polonia Sp. z o.o. z siedzibą w Skierniewicach

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek licznych skarg dotyczących przetwarzania danych osobowych skarżących bez ich zgody. Kontrolą objęte zostały zbiory danych osobowych prowadzone przez MediAdress Sp. z o.o. z siedzibą w Skierniewicach, której, zgodnie z art. 31 ustawy o ochronie danych osobowych, Dom Wysyłkowy Home Shopping Wereagentur Thomas Lowe powierzył zbiór o nazwie „Klienci Domu Wysyłkowego Home Shopping” (zgłoszenie Nr R 019649/99). W jej toku stwierdzono uchybienia w zakresie niezastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, niewypełnienia obowiązków o charakterze formalnym i technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Wnioski z kontroli przekazane zostały do Departamentu Rejestracji Zbiorów Danych Osobowych.

DIS-K-39/00

Lek Polska Sp. z o.o. z siedzibą w Pruszkowie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na wniosek Departamentu Rejestracji Zbiorów Danych Osobowych. Kontrolą objęto zbiory danych osobowych prowadzone przez Lek Polska Sp. z o.o. z siedzibą w Pruszkowie, w tym zbiór o nazwie „MEGAJEAN” (zgłoszenie nr R 020407/99). W jej toku stwierdzono uchybienia w zakresie braku ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych oraz niewypełnienia obowiązków o charakterze formalnym, organizacyjnym, technicznym i personalnym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W związku z tym, że w toku postępowania wyjaśniającego jednostka kontrolowana usunęła stwierdzone w trakcie kontroli uchybienia, w przedmiotowej sprawie nie wszczęto postępowania administracyjnego.

DIS-K-40/00

Bankowe Towarzystwo Ubezpieczeń i Reasekuracji Heros S.A. z siedzibą w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek zamieszczonej w „Rzeczpospolitej” informacji o zamiarze przekazania przez Towarzystwo Ubezpieczeniowe Winterthur S.A. z siedzibą w Warszawie portfela polis majątkowych Towarzystwu Ubezpieczeń i Reasekuracji Heros S.A. z siedzibą w Warszawie. Kontrolą objęto zbiór danych osobowych prowadzony przez Bankowe Towarzystwo Ubezpieczeń i Reasekuracji Heros S.A. z siedzibą w Warszawie o nazwie „Baza danych zintegrowanego systemu obsługi Towarzystwa Ubezpieczeniowego” – zgłoszenie nr R 010997/99 oraz zbiór danych osobowych posiadaczy polis majątkowych, przekazany przez Winterthur S.A. z siedzibą w Warszawie. W toku kontroli stwierdzono uchybienia w zakresie przetwarzania danych osób, których wnioski o ubezpieczenie zostały odrzucone, niedopełnienia obowiązku informacyjnego, niezastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych oraz braku ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych.

Ponadto ustalono, że Spółka nie przetwarza danych osobowych ubezpieczających pojazdy marki Renault w Towarzystwie Ubezpieczeniowego Winterthur S.A. z siedzibą w Warszawie przy ul. Puławskiej 15; umowa o przeniesienie portfela ubezpieczeniowego nie doszła do skutku ze względu na stanowisko Państwowego Urzędu Nadzoru Ubezpieczeń w kwestii sposobu pokrycia rezerw techniczno – ubezpieczeniowych, przekazywanych w ramach portfela ubezpieczeń.

W związku z dokonanymi ustaleniami, Generalny Inspektor Ochrony Danych Osobowych wydał decyzję GI-DEC-DP-33/01, nakazującą usunięcie uchybień w procesie przetwarzania danych osobowych.

DIS-K-41/00

Aeroklub Warszawski

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek skargi GI-DIS-208/00. Kontrolą objęto zbiór

danych osobowych członków Aeroklubu Warszawskiego. W jej toku stwierdzono uchybienia w zakresie braku ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych, niewypełnienia obowiązków o charakterze personalnym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych oraz niezastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

W związku z usunięciem przez jednostkę kontrolowaną w toku postępowania wyjaśniającego uchybień stwierdzonych w trakcie kontroli, w przedmiotowej sprawie nie wszczęto postępowania administracyjnego.

Ponadto, zwrócono się do Dyrektora Aeroklubu Warszawskiego o wszczęcie postępowania dyscyplinarnego w stosunku do Kierownika Sekcji Spadochronowej, odpowiedzialnego za prawidłowe zabezpieczenie dokumentacji kandydatów oraz członków Sekcji Spadochronowej.

DIS-K-42/00

Towarzystwo Ubezpieczeniowe Winterthur S.A. z siedzibą w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek zamieszczonej w „Rzeczpospolitej” informacji o zamiarze przekazania przez Towarzystwo Ubezpieczeniowe Winterthur S.A. z siedzibą w Warszawie portfela polis majątkowych Towarzystwu Ubezpieczeń i Reasekuracji Heros S.A. z siedzibą w Warszawie. Kontrolą objęto zbiór danych osobowych posiadaczy polis majątkowych, przekazany przez Winterthur S.A. z siedzibą w Warszawie do Bankowego Towarzystwa Ubezpieczeń i Reasekuracji Heros S.A. z siedzibą w Warszawie. W toku kontroli ustalono, że zbiór danych osobowych posiadaczy polis ubezpieczeniowych nie został przekazany do TUiR Heros S.A. z siedzibą w Warszawie.

W związku z powyższym, w przedmiotowej sprawie brak było podstaw do wszczęcia postępowania administracyjnego.

DIS-K-43/00

Netmarkets S.C. z siedzibą w Nowej Wsi Warszawskiej

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na wniosek Departamentu Rejestracji Zbiorów Danych Osobowych. Kontrolą objęto zbiory danych osobowych prowadzone przez Netmarkets S.C. z

siedzibą w Nowej Wsi Warszawskiej, w tym zbiór o nazwie „Zapytania ofertowe NM” (zgłoszenie nr R 019161/99). W jej toku ustalono, że ww. zbiór nie został utworzony, a prowadzona przez Netmarkets S.C. działalność gospodarcza została decyzją Wójta Gminy Niepołomice wykreślona z ewidencji działalności gospodarczej.

Wnioski z kontroli przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych.

DIS-K-44/00

Stella Sp. z o.o. z siedzibą w Gdyni

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek skargi GI-DIS-56/00. Kontrolą objęto zbiory danych osobowych prowadzone przez Stella Sp. z o.o. z siedzibą w Gdyni, w tym zbiór o nazwie „Stella” – zgłoszenie Nr R 069659/99. W jej toku stwierdzono uchybienia w zakresie niedopełniania obowiązku informacyjnego, nieuwzględnienia w ewidencji wszystkich osób zatrudnionych przy przetwarzaniu danych osobowych, braku określenia w umowie o przetwarzanie danych zakresu i celu przetwarzania danych, a w umowach licencyjnych czasu obowiązywania licencji oraz niewykonania obowiązków o charakterze formalnym, technicznym i personalnym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W związku z tym, że w toku postępowania wyjaśniającego jednostka kontrolowana usunęła stwierdzone w trakcie kontroli uchybienia, w przedmiotowej sprawie Generalny Inspektor nie wszczął postępowania administracyjnego.

DIS-K-45/00

Krajowa Rada Radiofonii i Telewizji z siedzibą w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek skargi GI-DIS-216/00. Kontrolą objęto zbiory danych osobowych, w których przetwarzane są dane wrażliwe członków zarządów mediów publicznych, prowadzone przez Krajową Radę Radiofonii i Telewizji w Warszawie. W jej toku stwierdzono uchybienia w zakresie braku podstawy prawnej do przetwarzania danych szczególnie chronionych członków zarządów mediów publicznych, niedopełniania obowiązku

informacyjnego, braku ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych oraz braku upoważnień do przetwarzania danych w systemie informatycznym.

W związku z dokonanymi ustaleniami, Generalny Inspektor Ochrony Danych Osobowych wydał decyzję GI-DEC-DP-53/00, nakazującą przywrócenie stanu zgodnego z prawem.

DIS-K-46/00

Przedsiębiorstwo Państwowe Polskie Koleje Państwowe w Rudzie Śląskiej

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono w związku ze złożonym wnioskiem o ponowne rozpatrzenie sprawy zakończonej decyzją Generalnego Inspektora Ochrony Danych Osobowych, nr GI-DEC-DP-13/00. Kontrolą objęto zbiór danych osobowych stałych klientów Przedsiębiorstwa Państwowego Polskie Koleje Państwowe w Rudzie Śląskiej. W związku z dokonanymi ustaleniami, Generalny Inspektor Ochrony Danych Osobowych wydał decyzję GI-DEC-DP-34/00 utrzymującą w mocy zaskarżoną decyzję.

DIS-K-47/00

Wspólnota Chleb Życia w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek skargi GI-DIS-63/00. Kontrolą objęto zbiory danych osobowych prowadzone przez Wspólnotę Chleb Życia w Warszawie. W jej toku ustalono, że Wspólnota Chleb Życia w Warszawie przetwarza dane osobowe w postaci imienia i nazwiska, które zapisywane są w zeszycie bez zastosowania określonego kryterium i nie tworzących zbioru w rozumieniu art. 7 pkt 1 ustawy o ochronie danych osobowych, tym samym przetwarzanie tych danych nie podlega przepisom wskazanej ustawy. W związku z powyższym, w przedmiotowej sprawie nie wszczęto postępowania administracyjnego.

DIS-K-48/00

Zakład Usług Komunalnych Sp. z o.o. z siedzibą w Mikołajkach

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na wniosek Departamentu Rejestracji Zbiorów Danych Osobowych. Kontrolą objęto zbiory danych osobowych prowadzone przez Zakład Usług Komunalnych Sp. z o.o. z siedzibą w Mikołajkach, w tym zbiór o nazwie „Kadry” (zgłoszenie Nr R 022490/99). W jej toku stwierdzono uchybienia w zakresie braku podstawy prawnej do

przetwarzania danych osobowych szczególnie chronionych w odniesieniu do pracowników, niedopełniania obowiązku informacyjnego, braku pisemnych upoważnień do obsługi systemu informatycznego, służącego do przetwarzania danych osobowych oraz niewypełnienie obowiązków o charakterze formalnym, technicznym i personalnym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W związku z usunięciem przez jednostkę kontrolowaną w toku postępowania wyjaśniającego stwierdzonych w trakcie kontroli uchybień, w przedmiotowej sprawie nie wszczęto postępowania administracyjnego.

DIS-K-49/00

Aqua – Pol Serwis w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na wniosek Departamentu Prawnego. Kontrolą objęto zbiory danych osobowych prowadzone przez Aqua – Pol Serwis w Warszawie. W jej toku stwierdzono uchybienia w zakresie niedopełniania obowiązku informacyjnego, nieadekwatności zakresu przetwarzanych danych osobowych w stosunku do celu, dla którego zostały zebrane, niezastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, niewypełnienia obowiązków o charakterze personalnym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, braku ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych oraz braku w umowie zawartej z podmiotem, któremu powierzono przetwarzanie danych osobowych pracowników, postanowień dotyczących powierzenia przetwarzania ww. danych.

W związku z tym, że w toku postępowania wyjaśniającego jednostka kontrolowana usunęła stwierdzone w trakcie kontroli uchybienia, w przedmiotowej sprawie Generalny Inspektor nie wszczął postępowania administracyjnego.

DIS-K-50/00

Centrum Operacyjne Informacji i Dystrybucji w Gdańsku

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na wniosek Departamentu Rejestracji Zbiorów Danych

osobowych. Kontrolą objęto zbiory danych osobowych prowadzone przez Centrum Operacyjne Informacji i Dystrybucji w Gdańsku, w tym zbiór o nazwie „Europejski Bank Pojazdów – European Vehicle Register” (zgłoszenie nr R 008049/99). W jej toku stwierdzono uchybienia w zakresie niedopełniania obowiązku informacyjnego oraz niewypełnienia obowiązków o charakterze formalnym, personalnym i technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Wnioski z kontroli przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych.

DIS-K-51/00

Vevay – Evita Poland Sp. z o.o. z siedzibą w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek skargi GI-DIS-243/00. Kontrolą objęto zbiory danych osobowych prowadzone przez Vevay – Evita Poland Sp. z o.o. z siedzibą w Warszawie. W jej toku stwierdzono uchybienia w zakresie niedopełnienia obowiązku zgłoszenia do rejestracji zbioru danych osobowych klientów, niedopełnienia obowiązku informacyjnego, braku ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych oraz niewypełnienia obowiązków o charakterze personalnym, formalnym, organizacyjnym i technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W związku z dokonanymi ustaleniami, Generalny Inspektor Ochrony Danych Osobowych wydał decyzję GI-DP-DEC-2/01, nakazującą Vevay – Evita Poland Sp. z o.o. z siedzibą w Warszawie usunięcie uchybień w procesie przetwarzania danych osobowych.

DIS-K-52/00

Ernst & Young Usługi Księgowe Sp. z o.o. z siedzibą w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono w związku z kontrolą w Bols Sports & Travel Sp. z o.o. z siedzibą w Warszawie (kontrola DIS-K-19/00). Kontrolą objęto zbiory danych osobowych prowadzone przez Ernst & Young Usługi Księgowe Sp. z o.o. z siedzibą w Warszawie na

podstawie zawartych z Bols Sports & Travel Sp. z o.o. z siedzibą w Warszawie umów powierzenia przetwarzania danych. W jej toku stwierdzono uchybienia w zakresie niewykonania obowiązków o charakterze personalnym, organizacyjnym i technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych oraz braku ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych.

W związku z tym, że w toku postępowania wyjaśniającego jednostka kontrolowana usunęła stwierdzone w trakcie kontroli uchybienia, w przedmiotowej sprawie Generalny Inspektor nie wszczął postępowania administracyjnego.

DIS-K-53/00

Biuro Rzeczoznawstwa Majątkowego i Obrotu Nieruchomościami EFEKT Wiesława i Janusz Kaptur w Bydgoszczy.

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na wniosek Departamentu Rejestracji Zbiorów Danych Osobowych. Kontrolą objęto zbiór danych osobowych o nazwie „Baza Danych Klientów Biura Rzeczoznawstwa i Obrotu Nieruchomościami EFEKT” (zgłoszenie nr R 0094557/99). W jej toku stwierdzono uchybienia w zakresie niedopełniania obowiązku informacyjnego, nieuwzględnienia w ewidencji wszystkich osób zatrudnionych przy przetwarzaniu danych osobowych, przetwarzania danych osób, z którymi rozwiązana została umowa zlecenia pośrednictwa oraz niewypelnienia obowiązków o charakterze personalnym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W związku z usunięciem przez jednostkę kontrolowaną w toku postępowania wyjaśniającego stwierdzonych w trakcie kontroli uchybień, w przedmiotowej sprawie Generalny Inspektor nie wszczął postępowania administracyjnego.

DIS-K-54/00

Generalny Inspektorat Celny w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek skargi GI-DIS-30/00. Kontrolą objęto zbiory danych osobowych prowadzone przez Generalny Inspektorat Celny w Warszawie. W jej toku

stwierdzono uchybienia w zakresie niewykonania obowiązków o charakterze personalnym, formalnym i technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, niedopełnienia obowiązku zgłoszenia do rejestracji zbioru danych osobowych kandydatów do pracy oraz braku podstawy prawnej do przetwarzania danych osobowych szczególnie chronionych w odniesieniu do pracowników. Ponadto stwierdzono, iż pracownikom dopuszczonym do obsługi systemu informatycznego służącego do przetwarzania danych osobowych nie zostały wydane stosowne upoważnienia.

W związku z usunięciem przez jednostkę kontrolowaną w toku postępowania wyjaśniającego stwierdzonych w trakcie kontroli uchybień, w przedmiotowej sprawie Generalny Inspektor nie wszczął postępowania administracyjnego.

DIS-K-55/00

Krakowska Fabryka Kabli S.A. z siedzibą w Krakowie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na wniosek Państwowej Inspekcji Pracy Inspektorat w Krakowie. Kontrolą objęto zbiory danych osobowych dotyczących pracowników prowadzone przez Krakowską Fabrykę Kabli S.A. z siedzibą w Krakowie. W jej toku stwierdzono uchybienia w zakresie braku podstawy prawnej do przetwarzania danych osobowych szczególnie chronionych w odniesieniu do pracowników, braku ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych oraz niewypełnienia obowiązków o charakterze organizacyjnym, personalnym, formalnym i technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. W toku kontroli stwierdzono ponadto, iż pracownikom dopuszczonym do obsługi systemu informatycznego służącego do przetwarzania danych osobowych nie zostały wydane stosowne upoważnienia.

W związku z usunięciem przez jednostkę kontrolowaną w toku postępowania wyjaśniającego stwierdzonych w trakcie kontroli uchybień, w przedmiotowej sprawie Generalny Inspektor nie wszczął postępowania administracyjnego.

DIS-K-56/00

Haring Project Support Sp. z o.o. z siedzibą w Krakowie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono w związku z kontrolą DIS-K-36/00. Kontrolą objęto zbiory danych osobowych prowadzone przez Haring Project Support Sp. z o.o. z siedzibą w Krakowie, w tym zbiór o nazwie „Mail Order”. W jej toku stwierdzono uchybienia w zakresie braku ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych oraz niewypełnienia obowiązków o charakterze formalnym, technicznym i personalnym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W związku z otwartym procesem likwidacji Haring Project Support Sp. z o.o. z siedzibą w Krakowie w przedmiotowej sprawie Generalny Inspektor nie wszczął postępowania administracyjnego.

DIS-K-57/00

Spółdzielnia Mieszkaniowa Ksawerów w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek skargi GI-DIS-135/00. Kontrolą objęto zbiory danych osobowych prowadzone przez Spółdzielnię Mieszkaniową Ksawerów w Warszawie, ze szczególnym uwzględnieniem ich zabezpieczenia. W jej toku stwierdzono uchybienia w zakresie niedopełnienia obowiązku informacyjnego, braku podstawy prawnej do przetwarzania danych osobowych szczególnie chronionych w odniesieniu do pracowników, niewypełnienie obowiązków o charakterze personalnym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych oraz braku ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych. W toku kontroli stwierdzono również, iż zakres przetwarzanych danych osobowych członków spółdzielni jest niezgodny z zakresem danych określonym w art. 30 prawa spółdzielczego.

W związku z usunięciem przez jednostkę kontrolowaną w toku postępowania wyjaśniającego stwierdzonych w trakcie kontroli uchybień, w przedmiotowej sprawie Generalny Inspektor nie wszczął postępowania administracyjnego.

DIS-K-58/00

Przedsiębiorstwo Państwowe Polskie Koleje Państwowe Zakład Infrastruktury Kolejowej we Wrocławiu

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek skargi GI-DIS-207/00. Kontrolą objęto zbiory danych osobowych pracowników prowadzone przez Przedsiębiorstwo Państwowe Polskie Koleje Państwowe Zakład Infrastruktury Kolejowej we Wrocławiu, ze szczególnym uwzględnieniem ich archiwizowania. W jej toku stwierdzono uchybienia w zakresie niedopełnienia obowiązku informacyjnego, braku podstawy prawnej do przetwarzania danych osobowych szczególnie chronionych w odniesieniu do pracowników, niezastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, braku ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych oraz niewypełnienia obowiązków o charakterze formalnym, personalnym i technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Ponadto stwierdzono, że pracownikom dopuszczonym do obsługi systemu informatycznego służącego do przetwarzania danych osobowych nie zostały wydane stosowne upoważnienia.

W okresie sprawozdawczym sprawa w toku, ze względu na konieczność przeprowadzenia kontroli w siedzibie zarządu Polskich Kolei Państwowych S.A.

DIS-K-59/00

Przedsiębiorstwo Państwowe Polskie Koleje Państwowe Zakład Teleinformatyki Kolejowej we Wrocławiu

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek skargi GI-DIS-207/00. Kontrolą objęto zbiory danych osobowych pracowników prowadzone przez Przedsiębiorstwo Państwowe Polskie Koleje Państwowe Zakład Teleinformatyki Kolejowej we Wrocławiu. W jej toku stwierdzono uchybienia w zakresie niedopełnienia obowiązku informacyjnego, braku podstawy prawnej do przetwarzania danych osobowych szczególnie chronionych w odniesieniu do pracowników, braku ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych oraz niewypełnienia obowiązków o charakterze formalnym, personalnym i technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny

odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Ponadto pracownikom dopuszczonym do obsługi systemu informatycznego służącego do przetwarzania danych osobowych nie zostały wydane stosowne upoważnienia.

W okresie sprawozdawczym sprawa w toku, ze względu na konieczność przeprowadzenia kontroli w siedzibie zarządu Polskich Kolei Państwowych S.A.

DIS-K-60/00

Dolnośląska Regionalna Kasa Chorych we Wrocławiu

Kontrolą objęto zbiory danych osobowych prowadzone przez Dolnośląską Regionalną Kasę Chorych z siedzibą we Wrocławiu, w tym zbiór o nazwie „Ubezpieczeni w Dolnośląskiej Regionalnej Kasie Chorych” (nr księgi rejestrowej 015870). W jej toku stwierdzono uchybienia w zakresie niedopełnienia obowiązku zgłoszenia do rejestracji zbioru danych osobowych kandydatów do pracy oraz niewykonania obowiązków o charakterze technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Ponadto, w toku kontroli stwierdzono, iż zakres żądanych od świadczeniodawców danych osobowych, w związku z zawartą umową, wykracza poza zakres określony w § 3 rozporządzenia Ministra Zdrowia i Opieki Społecznej w sprawie ustalenia zakresu niezbędnych danych gromadzonych przez świadczeniodawców oraz w systemach informatycznych Kas Chorych, a także zakresu i procedury wymiany danych pomiędzy Kasami Chorych oraz Kasami Chorych a świadczeniodawcami, Urzędem Nadzoru Ubezpieczeń Zdrowotnych i Krajowym Związkiem Kas Chorych oraz, że zakres zbieranych przez DRKCh danych w związku z rozpatrywaniem skierowań na leczenie uzdrowiskowe wykracza poza zakres określony w załączniku do rozporządzenia Ministra Zdrowia i Opieki Społecznej w sprawie sposobu i warunków wystawiania skierowania na leczenie uzdrowiskowe przez lekarza ubezpieczenia zdrowotnego oraz potwierdzania tego skierowania przez Kasę Chorych.

W związku z dokonanymi ustaleniami, Generalny Inspektor Ochrony Danych Osobowych wydał decyzję GI-DIS-DEC-61/01, nakazującą usunięcie uchybień w procesie przetwarzania danych osobowych.

DIS-K-62/00

Stołeczne Przedsiębiorstwo Energetyki Ciepłej w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na wniosek Powiatowego Rzecznika Konsumentów w Warszawie w związku z prowadzonym przez Generalnego Inspektora Ochrony Danych Osobowych postępowaniem administracyjnym. Kontrolą objęto zbiory danych osobowych prowadzone przez Stołeczne Przedsiębiorstwo Energetyki Ciepłej w Warszawie. W jej toku stwierdzono uchybienia w zakresie niedopełnienia obowiązku zgłoszenia do rejestracji zbioru danych osobowych odbiorców energii ciepłej, niedopełniania obowiązku informacyjnego, nieadekwatności zakresu przetwarzanych danych osobowych w stosunku do celu, dla którego zostały zebrane, w związku z kierowaniem stron dowodu osobistego, braku podstawy prawnej do przetwarzania danych osobowych szczególnie chronionych w odniesieniu do pracowników, braku ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych oraz niedopełnienia obowiązków o charakterze formalnym, organizacyjnym, technicznym i personalnym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. W toku kontroli stwierdzono ponadto, iż pracownikom dopuszczonym do obsługi systemu informatycznego służącego do przetwarzania danych osobowych nie zostały wydane stosowne upoważnienia.

W celu sprawdzenia wykonania zaleceń pokontrolnych w Stołecznym Przedsiębiorstwie Energetyki Ciepłej w Warszawie przeprowadzono kontrolę DIS-K-94/00. W związku z dokonanymi ustaleniami Generalny Inspektor Ochrony Danych Osobowych wydał decyzję GI-DEC-DP-101/00, nakazującą usunięcie uchybień w procesie przetwarzania danych osobowych.

DIS-K-63/00

Woreyd Sp. z o.o. z siedzibą w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek skargi GI-DIS-262/00. W jej toku stwierdzono uchybienia w zakresie niedopełniania obowiązku informacyjnego, nieuwzględnienia w ewidencji wszystkich osób zatrudnionych przy przetwarzaniu danych osobowych oraz niewypełnienia obowiązków o charakterze technicznym i personalnym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W związku z tym, że w toku postępowania wyjaśniającego jednostka kontrolowana usunęła stwierdzone w trakcie kontroli uchybienia, w przedmiotowej sprawie Generalny Inspektor nie wszczął postępowania administracyjnego.

DIS-K-64/00

Samodzielny Publiczny Szpital Kliniczny Akademii Medycznej w Białymstoku

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na wniosek Prokuratury Rejonowej dla m. Białegostoku. Kontrolą objęto zbiory danych osobowych prowadzone przez Samodzielny Publiczny Szpital Kliniczny Akademii Medycznej w Białymstoku. W jej toku stwierdzono uchybienia w zakresie braku podstawy prawnej do przetwarzania danych osobowych szczególnie chronionych w odniesieniu do pracowników, niezastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, braku ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych oraz niewypełnienia obowiązków o charakterze formalnym, organizacyjnym, technicznym i personalnym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Ponadto, nie wszystkim pracownikom dopuszczonym do obsługi systemu informatycznego służącego do przetwarzania danych osobowych zostały wydane stosowne upoważnienia.

W okresie sprawozdawczym sprawa w toku, ze względu na konieczność przeprowadzenia kontroli sprawdzającej wykonanie zaleceń Generalnego Inspektora.

DIS-K-66/00

Andersen Consulting Sp. z o.o. z siedzibą w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na wniosek Departamentu Prawnego. Kontrolą objęto zbiory danych osobowych prowadzone przez Andersen Consulting Sp. z o.o. z siedzibą w Warszawie, w tym zbiory o nazwach „MIDAS” (zgłoszenie nr R 011850/99) oraz „Potencjalni pracownicy Andersen Consulting Sp. z o.o.” (zgłoszenie nr R 011851/99). W jej toku stwierdzono uchybienia w zakresie braku podstawy prawnej do przetwarzania danych osobowych szczególnie chronionych w odniesieniu do pracowników i kandydatów do pracy, niedopełnienia obowiązku informacyjnego, nieadekwatności zakresu przetwarzanych danych

osobowych pracowników w stosunku do celu, dla którego zostały zebrane oraz niewypełnienia obowiązków o charakterze personalnym i technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Wnioski z kontroli przekazane zostały do Departamentu Prawnego.

DIS-K-67/00

Biuro Turystyczno – Marketingowe Paradis Holiday w Toruniu

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na wniosek Głównego Inspektora Inspekcji Handlowej. Kontrolą objęto zbiory danych osobowych prowadzone przez Biuro Turystyczno – Marketingowe Paradis Holiday w Toruniu. W jej toku stwierdzono uchybienia w zakresie niedopełnienia obowiązku informacyjnego, braku w umowach o współpracę regulacji dotyczących zakresu przekazywanych danych osobowych, sposobu ich przekazywania oraz ochrony, a także niewypełnienia obowiązków o charakterze formalnym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W związku z tym, że w toku postępowania wyjaśniającego jednostka kontrolowana usunęła stwierdzone w trakcie kontroli uchybienia, w przedmiotowej sprawie Generalny Inspektor nie wszczął postępowania administracyjnego.

DIS-K-68/00

Lubelska Regionalna Kasa Chorych w Lublinie

Kontrolą objęto zbiory danych osobowych prowadzone przez Lubelską Regionalną Kasę Chorych w Lublinie. W jej toku stwierdzono uchybienia w zakresie niedopełnienia obowiązku zgłoszenia do rejestracji zbioru danych osobowych kandydatów do pracy, braku podstawy prawnej do przetwarzania danych osobowych szczególnie chronionych w odniesieniu do pracowników, nieuwzględnienia w ewidencji wszystkich osób zatrudnionych przy przetwarzaniu danych osobowych, niezastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych oraz niewypełnienia obowiązków o charakterze technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych

warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. W toku kontroli stwierdzono ponadto, iż zakres żądanych od świadczeniodawców danych osobowych, w związku z zawartą umową, wykracza poza zakres określony w § 3 rozporządzenia Ministra Zdrowia i Opieki Społecznej w sprawie ustalenia zakresu niezbędnych danych gromadzonych przez świadczeniodawców oraz w systemach informatycznych Kas Chorych, a także zakresu i procedury wymiany danych pomiędzy Kasami Chorych oraz Kasami Chorych a świadczeniodawcami, Urzędem Nadzoru Ubezpieczeń Zdrowotnych i Krajowym Związkiem Kas Chorych.

W związku z tym, że w toku postępowania wyjaśniającego jednostka kontrolowana usunęła stwierdzone w trakcie kontroli uchybienia, w przedmiotowej sprawie Generalny Inspektor nie wszczął postępowania administracyjnego.

DIS-K-69/00

Świętokrzyska Regionalna Kasa Chorych w Kielcach

Kontrolą objęto zbiory danych osobowych prowadzone przez Świętokrzyską Regionalną Kasę Chorych w Kielcach. W jej toku stwierdzono, że zakres żądanych od świadczeniodawców danych osobowych, w związku z zawartą umową, wykracza poza zakres określony w § 3 rozporządzenia Ministra Zdrowia i Opieki Społecznej w sprawie ustalenia zakresu niezbędnych danych gromadzonych przez świadczeniodawców oraz w systemach informatycznych Kas Chorych, a także zakresu i procedury wymiany danych pomiędzy Kasami Chorych oraz Kasami Chorych a świadczeniodawcami, Urzędem Nadzoru Ubezpieczeń Zdrowotnych i Krajowym Związkiem Kas Chorych, oraz, że zakres zbieranych danych w związku z rozpatrywaniem skierowań na leczenie uzdrowiskowe wykracza poza zakres określony w załączniku do rozporządzenia Ministra Zdrowia i Opieki Społecznej w sprawie sposobu i warunków wystawiania skierowania na leczenie uzdrowiskowe przez lekarza ubezpieczenia zdrowotnego oraz potwierdzania tego skierowania przez Kasę Chorych. Ponadto, nie uwzględniono w ewidencji wszystkich osób zatrudnionych przy przetwarzaniu danych osobowych, a także nie wypełniono obowiązków o charakterze formalnym i technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. W trakcie inspekcji stwierdzono ponadto brak podstawy

prawnej do przetwarzania danych osobowych szczególnie chronionych w odniesieniu do pracowników.

W okresie sprawozdawczym sprawa w toku.

DIS-K-70/00

Gminny Ośrodek Pomocy Społecznej w Kołobrzegu

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na wniosek Departamentu Rejestracji Zbiorów Danych Osobowych. Kontrolą objęto zbiór danych osobowych pod nazwą „Skrócona kartoteka mieszkańców” prowadzony przez Gminny Ośrodek Pomocy Społecznej w Kołobrzegu (zgłoszenie do rejestracji nr R 065144/99). W jej toku stwierdzono uchybienia w zakresie braku podstawy prawnej do przetwarzania danych osobowych wszystkich mieszkańców gminy, a także naruszenia organizacyjne i techniczne w postaci niezastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych oraz niewypełnienia obowiązków o charakterze technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Wnioski z kontroli przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych.

DIS-K-71/00

Gminny Ośrodek Pomocy Społecznej w Ustroniu Morskim

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na wniosek Departamentu Rejestracji Zbiorów Danych Osobowych. Kontrolą objęto zbiór danych osobowych pod nazwą „Skrócona kartoteka mieszkańców” prowadzony przez Gminny Ośrodek Pomocy Społecznej w Ustroniu Morskim (zgłoszenie do rejestracji nr R 046380/99). W jej toku stwierdzono uchybienia w zakresie braku podstawy prawnej do przetwarzania danych osobowych wszystkich mieszkańców gminy, niezastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych oraz niewypełnienia obowiązków o charakterze technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim

powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Wnioski z kontroli przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych.

DIS-K-72/00

Polska Telefonía Komórkowa Centertel Sp. z o.o. z siedzibą w Warszawie

Kontrolę przeprowadzono w celu sprawdzenia wykonania decyzji Generalnego Inspektora Ochrony Danych Osobowych, sygn. GI-DP-DEC-28/00. Kontrolą objęto zbiory danych osobowych prowadzone przez Polską Telefonią Komórkową Centertel Sp. z o.o. z siedzibą w Warszawie.

Materiał dowodowy zebrany w jej toku stanowił podstawę do stwierdzenia, że Polska Telefonía Komórkowa Centertel Sp. z o.o. z siedzibą w Warszawie wykonała zalecenia zawarte w decyzji Generalnego Inspektora Ochrony Danych Osobowych, sygn. GI-DP-DEC-28/00.

DIS-K-73/00

Zakład Ubezpieczeń Społecznych Oddział w Tarnowskich Górach

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek skargi GI-DIS-265/00. Kontrolą objęto zbiory danych osobowych prowadzone przez Oddział Zakładu Ubezpieczeń Społecznych w Tarnowskich Górach, w tym zbiór o nazwie „Zbiór danych zawierający dane o osobach pobierających emerytury i renty, świadczenia otrzymywane lub przekazywane za granicę, zasiłki chorobowe lub alimentacyjne, dodatki rodzinne, pielęgnacyjne i wychowawcze, dane o płatnikach składek przetwarzany w Zakładzie Ubezpieczeń Społecznych” – księga numer 012888 , zbiór o nazwie „Centralne rejestry oraz rozproszony system plików Kompleksowego Systemu Informatycznego Zakładu Ubezpieczeń Społecznych” – księga numer 000053. W jej toku stwierdzono uchybienia w zakresie braku podstawy prawnej do przetwarzania danych osobowych szczególnie chronionych w odniesieniu do pracowników, nieadekwatności zakresu przetwarzanych danych osobowych pracowników firm zewnętrznych w stosunku do celu, dla którego zostały zebrane oraz niewypełnienia obowiązków o charakterze technicznym, organizacyjnym i personalnym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i

organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W okresie sprawozdawczym sprawa w toku, ze względu na konieczność przeprowadzenia kontroli sprawdzającej wykonanie zaleceń Generalnego Inspektora.

DIS-K-74/00

Zurich Handlowy Towarzystwo Ubezpieczeń na Życie S.A. z siedzibą w Warszawie

Kontrolą objęto zbiory danych osobowych prowadzone przez Zurich Handlowy Towarzystwo Ubezpieczeń na Życie S.A. z siedzibą w Warszawie, w tym zbiory danych osobowych o nazwach: „Baza Danych Agentów i Brokerów” (Nr księgi rejestrowej 000021), „Baza Klientów Systemu Komputerowej Obsługi Ubezpieczeń na Życie” (Nr księgi rejestrowej 000008), „Baza Danych Akwizytorów” (Nr zgłoszenia R 000061/99) oraz „Baza Kandydatów Do Pracy” (Nr księgi rejestrowej 000022). W jej toku stwierdzono uchybienia w zakresie braku podstawy prawnej do przetwarzania danych szczególnie chronionych w odniesieniu do pracowników.

W toku kontroli stwierdzono również, iż formularz oświadczenia o stanie zdrowia wypełniany przez osobę podpisującą umowę ubezpieczenia zawiera klauzulę o upoważnieniu lekarzy, szpitali, innych placówek opieki medycznej, a także zakładów ubezpieczeń lub osoby, które posiadają jej dane osobowe oraz dane dotyczące stanu zdrowia, do udzielenia w każdym czasie, na wniosek Zurich Towarzystwo Ubezpieczeń na Życie S.A., pełnej informacji związanej z przebytymi chorobami, fizycznym i psychicznym stanem zdrowia, pobytami w szpitalu, udzielonymi poradami lub diagnostyką medyczną oraz leczeniem.

W okresie sprawozdawczym sprawa w toku.

DIS-K-75/00

Towarzystwo Ubezpieczeniowe Allianz Życie Polska S.A. z siedzibą w Warszawie

Kontrolą objęto zbiory danych osobowych prowadzone przez Towarzystwo Ubezpieczeniowe Allianz Życie Polska S.A. z siedzibą w Warszawie, w tym zbiory o nazwach „Umowy ubezpieczenia Towarzystwa Ubezpieczeniowego Allianz Życie Polska S.A.” (nr KR 000013), „Agenci ubezpieczeniowi Towarzystwa Ubezpieczeniowego Allianz Życie Polska S.A.” (nr KR 000014) i „Rozmówcy infolinii Towarzystwa Ubezpieczeniowego Allianz Życie Polska Spółka Akcyjna” (zgłoszenie nr R 001340/00). W jej toku stwierdzono

uchybień w zakresie niedopełnienia obowiązku informacyjnego, nieadekwatności zakresu przetwarzanych danych osobowych w stosunku do celów, dla których zostały zebrane, w związku z kierowaniem stron dowodu osobistego, przetwarzania danych osób, których wnioski o zawarcie umowy ubezpieczenia zostały odrzucone, braku podstawy prawnej do przetwarzania danych osobowych szczególnie chronionych w odniesieniu do pracowników oraz niewypełnienia obowiązków o charakterze formalnym, organizacyjnym, technicznym i personalnym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W okresie sprawozdawczym sprawa w toku, ze względu na konieczność przeprowadzenia kontroli sprawdzającej wykonanie zaleceń Generalnego Inspektora.

DIS-K-76/00

Daewoo – Życie Towarzystwo Ubezpieczeniowe S.A. z siedzibą w Warszawie

Kontrolą objęto zbiory danych osobowych prowadzone przez Daewoo – Życie Towarzystwo Ubezpieczeniowe S.A. z siedzibą w Warszawie, w tym zbiór o nazwie „Ubezpieczony, Ubezpieczający, Uposażony” (nr KR 003495). W jej toku stwierdzono uchybień co do nieadekwatności zakresu przetwarzanych danych osobowych w stosunku do celu, dla którego zostały zebrane, w związku z kierowaniem stron dowodu osobistego, przetwarzania danych osób, których wnioski o zawarcie umowy ubezpieczenia zostały odrzucone oraz niewypełnienia obowiązków o charakterze personalnym i technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W okresie sprawozdawczym sprawa w toku.

DIS-K-77/00

Bestfoods Polska Sp. z o.o. z siedzibą w Poznaniu

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek skargi GI-DIS-187/00. W jej toku stwierdzono uchybień w zakresie nieadekwatności zakresu przetwarzanych danych osobowych w stosunku do celu, dla którego zostały zebrane, braku podstawy prawnej do przetwarzania

danych osobowych szczególnie chronionych w odniesieniu do pracowników, braku ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych oraz niewypełnienia obowiązków o charakterze formalnym, organizacyjnym, technicznym i personalnym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W związku z dokonanymi ustaleniami, Generalny Inspektor Ochrony Danych Osobowych wydał decyzję GI-DEC-DIS-73/01, nakazującą usunięcie uchybień w procesie przetwarzania danych osobowych.

DIS-K-78/00

Powszechna Kasa Oszczędności Bank Polski S.A. IV Oddział we Wrocławiu

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek informacji prasowej. Kontrolą objęto zbiory danych osobowych prowadzone przez Powszechną Kasę Oszczędności Bank Polski S.A. IV Oddział we Wrocławiu, w tym zbiory o nazwach „Faktoring” (zgłoszenie nr R 006619/99) oraz „Polisa 2000” (zgłoszenie nr R 008188/99). W jej toku stwierdzono uchybienia w zakresie nieadekwatności zakresu przetwarzanych danych osobowych w stosunku do celu, dla którego zostały zebrane, w związku z kserowaniem stron dowodu osobistego, braku podstawy prawnej do przetwarzania danych osobowych szczególnie chronionych w odniesieniu do pracowników oraz niezastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych i niewypełnienia obowiązków o charakterze technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. W toku inspekcji stwierdzono ponadto, iż zgłoszony do rejestracji zbiór danych o nazwie „Faktoring”, zawiera dane przedsiębiorców.

W okresie sprawozdawczym sprawa w toku.

DIS-K-79/00

Mega Music Sp. z o.o. z siedzibą w Sopocie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na wniosek Departamentu Rejestracji Zbiorów Danych Osobowych. Kontrolą objęto zbiory danych osobowych prowadzone przez Mega Music Sp. z

o.o. z siedzibą w Sopocie, w tym zbiory o nazwie „Lista Subskrybentów” (zgłoszenie Nr R 000406/99) i „Ewidencja Kart Gwarancyjnych” (zgłoszenie Nr 060809/99). W jej toku stwierdzono uchybienia w zakresie niedopełnienia obowiązku informacyjnego, nieuwzględnienia w ewidencji wszystkich osób zatrudnionych przy przetwarzaniu danych osobowych oraz niewypełnienia obowiązków o charakterze formalnym, technicznym i personalnym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Ponadto, w toku kontroli ustalono, że podstawą prawną przetwarzania danych osobowych przez Spółkę jest art. 23 ust. 1 pkt 1 ustawy o ochronie danych osobowych, tj. zgoda osoby, której dane osobowe są przetwarzane. Karta Rejestracyjna nie zawiera jednak klauzuli zgody w rozumieniu art. 7 pkt 5 powołanej ustawy.

W okresie sprawozdawczym sprawa w toku, ze względu na konieczność przeprowadzenia kontroli sprawdzającej wykonanie zaleceń Generalnego Inspektora.

DIS-K-80/00

COID – System Sp. z o.o. z siedzibą w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na wniosek Departamentu Rejestracji Zbiorów Danych Osobowych. W jej toku stwierdzono uchybienia w zakresie niedopełnienia obowiązku informacyjnego, niezastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych oraz niewypełnienia obowiązków o charakterze formalnym, personalnym, organizacyjnym i technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Wnioski z kontroli przekazane zostały do Departamentu Rejestracji Zbiorów Danych Osobowych.

DIS-K-81/00

Samodzielny Wojewódzki Zespół Publicznych Zakładów Psychiatrycznej Opieki Zdrowotnej w Warszawie.

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek skargi GI-DIS-229/00. Kontrolą objęto zbiory

danych osobowych stażystów Poradni i Oddziału Terapii i Rozwoju Osobowości w Warszawie, przekazanych po jej likwidacji do Samodzielnego Wojewódzkiego Zespołu Publicznych Zakładów Psychiatrycznej Opieki Zdrowotnej w Warszawie. W jej toku stwierdzono uchybienia w zakresie przetwarzania danych osobowych studentów odbywających praktyki zawodowe w zbiorze pacjentów oraz przetwarzania danych osobowych objętych szczególną ochroną w odniesieniu do studentów.

W związku z dokonanymi ustaleniami, Generalny Inspektor Ochrony Danych Osobowych wydał decyzję GI-DEC-DP-92/00, nakazującą Samodzielnemu Wojewódzkiemu Zespołowi Publicznych Zakładów Psychiatrycznej Opieki Zdrowotnej w Warszawie przywrócić w procesie przetwarzania danych osobowych stanu zgodnego z prawem.

DIS-K-82/00

Urząd Gminy Jabłonna

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek informacji Mazowieckiego Urzędu Wojewódzkiego w Warszawie dotyczącej kradzieży bazy danych z Urzędu Gminy Jabłonna. Kontrolą objęto zbiory danych osobowych prowadzone przez ww. Urząd. W jej toku stwierdzono uchybienia w zakresie braku podstawy prawnej do przetwarzania danych osobowych szczególnie chronionych w odniesieniu do pracowników, braku ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych, niezastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych oraz niewypełnienia obowiązków o charakterze technicznym, personalnym i organizacyjnym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W okresie sprawozdawczym sprawa w toku, ze względu na kompleksową zmianę systemów informatycznych, służących do przetwarzania danych osobowych.

DIS-K-83/00

Miejski Ośrodek Pomocy Społecznej w Łodzi

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek skarg GI-DIS-252/00 i GI-DIS-254/00, na potrzeby toczącego się postępowania administracyjnego. Zakresem kontroli objęto

przetwarzanie przez Miejski Ośrodek Pomocy Społecznej w Łodzi danych osobowych córki skarżących. W związku z dokonаныmi ustaleniami, Generalny Inspektor Ochrony Danych Osobowych wydał decyzję GI-DEC-DP-99/00, nakazującą Miejskiemu Ośrodkowi Pomocy Społecznej w Łodzi przywrócenie stanu zgodnego z prawem.

DIS-K-84/00

ABB Centrum Automatyki Sp. z o.o. z siedzibą we Wrocławiu

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na wniosek Departamentu Rejestracji Zbiorów Danych Osobowych. Kontrolą objęto zbiory danych osobowych prowadzone przez ABB Centrum Automatyki Sp. z o.o. z siedzibą we Wrocławiu, w tym zbiór danych o nazwie „System informacji marketingowej” (zgłoszenie numer R 043614/99).

W jej toku stwierdzono uchybienia w zakresie niedopełniania obowiązku informacyjnego, braku podstawy prawnej do przetwarzania danych osobowych szczególnie chronionych w odniesieniu do pracowników oraz niewypełnienia obowiązków o charakterze personalnym i technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W okresie sprawozdawczym sprawa w toku, ze względu na konieczność przeprowadzenia kontroli sprawdzającej wykonanie zaleceń Generalnego Inspektora.

DIS-K-85/00

HPS Direct Marketing Sp. z o.o. z siedzibą w Krakowie

Kontrolą objęto zbiory danych osobowych prowadzone przez HPS Direct Marketing Sp. z o.o. z siedzibą w Krakowie. W jej toku stwierdzono uchybienia w zakresie nie zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, nieuwzględnienia w ewidencji wszystkich osób zatrudnionych przy przetwarzaniu danych osobowych oraz niewypełnienia obowiązków o charakterze organizacyjnym i technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. W trakcie kontroli stwierdzono ponadto, iż pracownikom

dopuszczonym do obsługi systemu informatycznego służącego do przetwarzania danych osobowych nie zostały wydane stosowne upoważnienia.

W związku z tym, że w toku postępowania wyjaśniającego jednostka kontrolowana usunęła stwierdzone w trakcie kontroli uchybienia, w przedmiotowej sprawie Generalny Inspektor nie wszczął postępowania administracyjnego.

DIS-K-86/00

Uniwersyteckie Przedsiębiorstwo Turystyczno – Usługowe Almatulist S.A. z siedzibą we Wrocławiu

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na wniosek Departamentu Rejestracji Zbiorów Danych Osobowych. Kontrolą objęto zbiory danych osobowych prowadzone przez Uniwersyteckie Przedsiębiorstwo Turystyczno – Usługowe Almatulist S.A. we Wrocławiu, w tym zbiór danych o nazwie „Marketingowa baza danych Almatulist S.A.” (zgłoszenie numer R 045584/99). W jej toku stwierdzono brak ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych oraz nie wypełnienie obowiązków o charakterze personalnym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W związku z tym, że w toku postępowania wyjaśniającego jednostka kontrolowana usunęła stwierdzone w trakcie kontroli uchybienia, w przedmiotowej sprawie Generalny Inspektor nie wszczął postępowania administracyjnego.

DIS-K-87/00

Bertelsmann Media Sp. z o.o. z siedzibą w Warszawie, Bertelsmann Media Sp. z o.o. II Oddział w Warszawie Bertelsmann Music Group Poland z siedzibą w Warszawie i Bertelsmann Media Sp. z o.o. X Oddział w Warszawie Bertelsmann Wydawnictwa Fachowe z siedzibą w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na wniosek Prokuratury Rejonowej Warszawa Mokotów. Kontrolą objęto zbiory danych osobowych prowadzone przez:

- Bertelsmann Media Sp. z o.o. - zbiór danych osobowych o nazwie „Klienci Klubu Świat Książki” - (numer księgi rejestrowej 002161/99),

- Bertelsmann Media Sp. z o.o. II Oddział w Warszawie BMG Poland - zbiór o nazwie „Korespondenci BMG Poland” - (numer księgi rejestrowej 000022/00),
- Bertelsmann Media Sp. z o.o. X Oddział w Warszawie Bertelsmann Wydawnictwa Fachowe – zbiór o nazwie „Baza Prenumeratorów Czasopism” - (numer księgi rejestrowej 034675/99).

W jej toku stwierdzono uchybienia w postaci niedopełnienia obowiązku informacyjnego, braku podstawy prawnej udostępniania danych osobowych klientów innym podmiotom, braku podstawy prawnej do przetwarzania danych osobowych szczególnie chronionych w odniesieniu do pracowników oraz braku ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych, a także niewypełnienia obowiązków o charakterze formalnym, personalnym, organizacyjnym i technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W związku z tym, że w toku postępowania wyjaśniającego jednostka kontrolowana usunęła stwierdzone w trakcie kontroli uchybienia, w przedmiotowej sprawie Generalny Inspektor nie wszczął postępowania administracyjnego.

DIS-K-90/00

Holiday Travel Center Sp. z o.o. z siedzibą w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek skargi GI-DIS-326/00. Kontrolą objęto zbiory danych osobowych prowadzone przez Holiday Travel Center Sp. z o.o. z siedzibą w Warszawie. W jej toku stwierdzono uchybienia w zakresie niedopełnienia obowiązku informacyjnego, nieadekwatności zakresu przetwarzanych danych osobowych w stosunku do celu, dla którego zostały zebrane, w związku z kserowaniem stron dowodu osobistego, niezastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, braku ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych oraz niewypełnienia obowiązków o charakterze formalnym, technicznym i personalnym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Ponadto, pracownikom dopuszczonym do obsługi systemu informatycznego służącego do przetwarzania danych osobowych nie zostały wydane stosowne upoważnienia.

W okresie sprawozdawczym sprawa w toku, ze względu na konieczność przeprowadzenia kontroli sprawdzającej wykonanie zaleceń Generalnego Inspektora.

DIS-K-91/00

Polkomtel S.A. z siedzibą w Warszawie

Kontrolę przeprowadzono w celu sprawdzenia wykonania stwierdzonych w trakcie kontroli DIS-K-46/99 uchybień. W jej toku stwierdzono uchybienia w zakresie niedopełnienia obowiązku informacyjnego, nieadekwatności zakresu przetwarzanych danych osobowych w stosunku do celu, dla którego zostały zebrane, w związku z kserowaniem stron dowodu osobistego oraz niewypełnienia obowiązków o charakterze formalnym i technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W związku z dokonanymi ustaleniami, Generalny Inspektor Ochrony Danych Osobowych wydał decyzję GI-DP-DEC-15/01, nakazującą usunięcie uchybień w procesie przetwarzania danych osobowych.

DIS-K-92/00

Towarzystwo Ubezpieczeń na Życie Nationale – Nederlanden Polska S.A. z siedzibą w Warszawie

Kontrolą objęto zbiory danych osobowych prowadzone przez Towarzystwo Ubezpieczeń na Życie Nationale – Nederlanden Polska S.A. z siedzibą w Warszawie, w tym zbiory o nazwach „Ubezpieczeni NNP” (KR nr 008179), „Ubezpieczeni NNP – Ubezpieczenia Grupowe” (KR nr 008153), „Ubezpieczający NNP” (KR nr 008174), „Uposażeni NNP” (KR nr 008211), „Uposażeni NNP – Ubezpieczenia grupowe” (KR nr 008214), „Baza danych osób zatrudnionych przez podmioty wchodzące w skład grupy ING w Polsce” (KR nr 000760), „Kandydaci do pracy w NNP” (KR nr 008213), „Agenci ubezpieczeniowi NNP” (zgłoszenie nr R 013660/99), „Osoby zainteresowane ubezpieczeniem w NNP” (zgłoszenie nr R 043274/99), „Osoby zarekomendowane NNP” (zgłoszenie nr R 043269/99), „Klienci internetowi NNP” (zgłoszenie nr R 070419/99). W jej toku stwierdzono uchybienia w zakresie nieadekwatności zakresu przetwarzanych danych osobowych w stosunku do celu, dla którego zostały zebrane, braku podstawy prawnej do przetwarzania danych osób korzystających z infolinii administrowanej przez Powszechne Towarzystwo

Emerytalne Nationale – Nederlanden Polska S.A. z siedzibą w Warszawie oraz daty urodzenia i danych o wykształceniu pracowników podmiotów należących do grupy ING w Polsce oraz niewypełnienia obowiązków o charakterze organizacyjnym i technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W okresie sprawozdawczym sprawa w toku, ze względu na konieczność przeprowadzenia kontroli sprawdzającej wykonanie zaleceń Generalnego Inspektora.

DIS-K-93/00

Klub Książki Księgarni Krajowej Sp. z o.o. z siedzibą w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na wniosek Prokuratury Rejonowej Warszawa Mokotów. Kontrolą objęto zbiory danych osobowych prowadzone przez Klub Książki Księgarni Krajowej Sp. z o.o. z siedzibą w Warszawie, w tym zbiory o nazwach: „Klienci Firmy KKKK Sp. z o.o. – Sklep Internetowy” (KR Nr 008916) oraz „Klienci Firmy KKKK Sp. z o.o.” (KR Nr 008921). W jej toku stwierdzono uchybienia w zakresie wykonywania obowiązku informacyjnego, niezastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, nieuwzględnienia w ewidencji wszystkich osób zatrudnionych przy przetwarzaniu danych osobowych oraz niewykonania obowiązków o charakterze personalnym, technicznym i organizacyjnym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. W okresie sprawozdawczym sprawa w toku.

DIS-K-95/00

Wydawnictwo Naukowe PWN S.A. z siedzibą w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na wniosek Prokuratury Rejonowej Warszawa Mokotów. Kontrolą objęto zbiory danych osobowych prowadzone przez Wydawnictwo Naukowe PWN S.A. z siedzibą w Warszawie, w tym zbiór o nazwie „Klienci PWN” (zgłoszenie nr R 047660/99). W jej toku stwierdzono uchybienia dotyczące niedopełnienia obowiązku

informatycznego, niezastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, przetwarzania danych osobowych kandydatów do pracy, mimo iż nie na wszystkich ofertach zamieszczone zostało oświadczenie o wyrażeniu zgody na przetwarzanie danych w celach rekrutacyjnych oraz niewypełnienia obowiązków o charakterze organizacyjnym, technicznym i personalnym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Także pracownikom dopuszczonym do obsługi systemu informatycznego służącego do przetwarzania danych osobowych nie zostały wydane stosowne upoważnienia.

W okresie sprawozdawczym sprawa w toku.

DIS-K-96/00

Hand – Prod Sp. z o.o. z siedzibą w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na wniosek Komendy Powiatowej Policji w Bytowie. W jej toku stwierdzono uchybienia w zakresie braku podstawy prawnej do przetwarzania danych osobowych szczególnie chronionych w odniesieniu do pracowników, braku ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych oraz niewypełnienia obowiązków o charakterze formalnym, technicznym i personalnym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W okresie sprawozdawczym sprawa w toku.

DIS-K-98/00

Biuro Obrotu Nieruchomościami Stolica S.C. z siedzibą w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na wniosek Departamentu Rejestracji Zbiorów Danych Osobowych. Kontrolą objęto zbiory danych osobowych prowadzone przez Biuro Obrotu Nieruchomościami Stolica S.C. z siedzibą w Warszawie, w tym zbiór o nazwie „Pośrednictwo w obrocie nieruchomościami, doradztwo personalne - BON Stolica S.C.” (zgłoszenie Nr R 006488/99).

W jej toku stwierdzono nieadekwatność zakresu przetwarzanych danych osobowych w stosunku do celu, dla którego zostały zebrane oraz niewypełnienie obowiązków o charakterze formalnym, technicznym i personalnym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W związku z wykreśleniem z ewidencji działalności gospodarczej Biura Obrotu Nieruchomościami Stolica S.C. z siedzibą w Warszawie w przedmiotowej sprawie generalny Inspektor nie wszczął postępowania administracyjnego.

DIS-K-99/00

A. D. Dragowski S.A. z siedzibą w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek skargi GI-DIS-257/00. W jej toku stwierdzono uchybienia w zakresie niewykonywania obowiązku informacyjnego, braku podstawy prawnej do przetwarzania danych osobowych szczególnie chronionych w odniesieniu do pracowników, nieuwzględnienia w ewidencji wszystkich osób zatrudnionych przy przetwarzaniu danych osobowych oraz niewypełnienia obowiązków o charakterze organizacyjnym, personalnym, technicznym i formalnym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W związku z dokonanymi ustaleniami, Generalny Inspektor Ochrony Danych Osobowych wydał decyzję GI-DIS-DEC-69/01, nakazującą usunięcie uchybień w procesie przetwarzania danych osobowych.

DIS-K-100/00

Expertus w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek skargi GI-DIS-430/409/00. Kontrolą objęto zbiory danych osobowych prowadzone przez Expertus w Warszawie. W jej toku stwierdzono brak dopełniania obowiązku informacyjnego, brak ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych oraz nie wykonywanie obowiązków o charakterze formalnym, personalnym i technicznym, określonych w rozporządzeniu Ministra Spraw

Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W okresie sprawozdawczym sprawa w toku.

DIS-K-101/00

Wydawnictwo C. H. Beck Sp. z o.o. z siedzibą w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek skargi GI-DIS-430/430/00. Kontrolą objęto zbiory danych osobowych prowadzone przez Wydawnictwo C. H. Beck Sp. z o.o. z siedzibą w Warszawie. W jej toku stwierdzono brak dopełniania obowiązku informacyjnego, brak zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych oraz niewykonanie obowiązków o charakterze personalnym, organizacyjnym i technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W okresie sprawozdawczym sprawa w toku.

DIS-K-102/00

Ministerstwo Spraw Wewnętrznych i Administracji w Warszawie

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono zgodnie z planem kontroli Departamentu Inspekcji. Kontrolą objęto zbiory danych osobowych prowadzone przez Ministerstwo Spraw Wewnętrznych i Administracji w Warszawie, w tym zbiory danych o nazwach „Rejestr PESEL i podsystemy tematyczne” (zgłoszenie nr R 008975/99), „Centralny rejestr metryczek wydanych dokumentów tożsamości od 1952 r. do 1997 r.” (zgłoszenie nr R 008976/99), „Centralny rejestr uprawnionych” (zgłoszenie nr R 008977/99), „Katalog utraconych paszportów” (zgłoszenie nr R 008978/99), „Spis fundacji, dla których Minister Spraw Wewnętrznych i Administracji jest ministrem właściwym, ze względu na zakres i rodzaj działalności” (zgłoszenie nr R 010511/99), „Rejestr złożonych do Prezydenta Rzeczypospolitej Polskiej wniosków o nadanie obywatelstwa polskiego” (zgłoszenie nr R 010512/99), „Rejestr złożonych do Prezydenta Rzeczypospolitej Polskiej wniosków o nadanie

obywatelstwa polskiego” (zgłoszenie nr R 010513/99), „Centralny rejestr wniosków o odmowę wydania lub unieważnienia paszportu” (zgłoszenie nr R 008978/99).

W okresie sprawozdawczym sprawa w toku.

DIS-K-103/00

Stoen Biuro Obsługi Klienta Warszawa – Ursynów

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek skargi GI-DIS-430/473/00. W jej toku stwierdzono nie wykonywanie obowiązków o charakterze technicznym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W związku z tym, że w toku postępowania wyjaśniającego jednostka kontrolowana usunęła stwierdzone w trakcie kontroli uchybienia, w przedmiotowej sprawie Generalny Inspektor nie wszczął postępowania administracyjnego.

DIS-K-104/00

Telekomunikacja Polska S.A. Biuro Obsługi Klienta w Warszawie przy ul. Irysowej

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono na skutek skargi GI-DIS-430/473/00. W jej toku stwierdzono nieadekwatność zakresu przetwarzanych danych osobowych w stosunku do celu, dla którego zostały zebrane, nie zastosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, brak ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych oraz nie wykonywanie obowiązków o charakterze personalnym, określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W związku z tym, że w toku postępowania wyjaśniającego jednostka kontrolowana usunęła stwierdzone w trakcie kontroli uchybienia, w przedmiotowej sprawie Generalny Inspektor nie wszczął postępowania administracyjnego.

Część III. REJESTRACJA ZBIORÓW DANYCH OSOBOWYCH

I. Zagadnienia wstępne dotyczące procesu rejestracyjnego

Do ustawowych zadań Departamentu Rejestracji Zbiorów Danych Osobowych należy:

- 1) przyjmowanie zgłoszeń zbiorów danych osobowych do rejestru danych osobowych,
- 2) prowadzenie rejestru zbiorów danych osobowych,
- 3) przygotowywanie projektów decyzji o odmowie zarejestrowania zbioru,
- 4) wydawanie zaświadczeń o zarejestrowaniu zbioru,
- 5) udostępnianie danych zawartych w rejestrze.

Ustawa o ochronie danych osobowych w art. 40 nakłada na administratora danych obowiązek zgłoszenia prowadzonego zbioru danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.

W rozumieniu ustawy daną osobową jest każda informacja dotycząca osoby fizycznej, która pozwala na określenie tożsamości tej osoby. Zbiorem danych osobowych jest natomiast każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielny funkcjonalnie. Administratorem danych, zaś jest „organ, instytucja, jednostka organizacyjna, podmiot lub osoba, (...) decydujące o celach i środkach przetwarzania danych osobowych”. Administratorami danych w sferze publicznej są organy państwowe oraz samorządu terytorialnego, a także inne państwowe i komunalne jednostki organizacyjne oraz podmioty niepaństwowe realizujące zadania publiczne.

Administratorami danych w sferze prywatnej są osoby fizyczne i prawne oraz jednostki organizacyjne nie mające osobowości prawnej, które przetwarzają dane w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych.

W omawianym okresie sprawozdawczym kwestia zgłaszania zbiorów do rejestracji nadal wywoływała wiele kontrowersji. Zdarzały się z jednej sytuacji, gdy administratorzy danych starali się uniknąć obowiązku rejestracji, z drugiej jednak (dotyczyło to niektórych podmiotów ze sfery prywatnej) zarejestrowanie zbioru w pewnym sensie uwiarygodniało administratorów danych w oczach ich klientów.

Działalność Generalnego Inspektora Ochrony Danych Osobowych w roku 2000 w zakresie rejestracji zbiorów danych polegała głównie na rozpatrywaniu zgłoszeń zbiorów danych, które wpłynęły do Biura Generalnego Inspektora Ochrony Danych Osobowych jeszcze w roku 1999. Spowodowane to było zgłoszeniem do rejestracji 70 910 zbiorów danych osobowych. Mimo, iż ustawodawca przewidział w art. 61 ustawy 18 miesięczny termin od dnia wejścia w życie ustawy na dopełnienie obowiązku rejestracyjnego przez „podmioty (...) prowadzące w dniu wejścia w życie ustawy zbiory danych osobowych w systemach informatycznych”, tj. do dnia 30 października 1999 r., to jednak zdecydowana większość podmiotów zgłosiła zbiory danych w ostatnich dniach powyższego terminu.

Liczba wpływających do Biura Generalnego Inspektora Ochrony Danych Osobowych zgłoszeń zwiększała się wraz z upływem okresu przejściowego i wynosiła:

- w dniu 1 marca 1999 r. - 172 zgłoszenia,
- w dniu 1 czerwca 1999 r. - 524 zgłoszenia,
- w dniu 15 października 1999 r. - 18 755 zgłoszeń.

Tylko w jednym dniu 2 listopada 1999 r. dokonano 22 335 zgłoszeń zbiorów danych. W sumie do końca 1999 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych trafiło 70 910 wniosków rejestracyjnych.

W 2000 r. do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zostało zgłoszonych 2801 zbiorów danych osobowych.

Podmioty określone w art. 3 ust. 1 ustawy, tj. organy państwowe oraz samorządu terytorialnego, inne państwowe i komunalne jednostki organizacyjne oraz podmioty niepaństwowe realizujące zadania publiczne, zgłosiły 1712 zbiorów danych, natomiast podmioty określone w art. 3 ust. 2 ustawy, tj. osoby fizyczne i prawne oraz jednostki organizacyjne nie posiadające osobowości prawnej, które przetwarzają dane w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych – 1089 zbiorów danych.

Gminy zgłosiły do rejestracji 567 zbiorów danych osobowych, powiaty natomiast 168 zbiorów. Jednostki organizacyjne, czyli np.:

- ośrodki pomocy społecznej - 71 zgłoszeń zbiorów danych osobowych,

- powiatowe centra pomocy rodzinie - 93 zgłoszenia zbiorów danych osobowych,
- biblioteki - 109 zgłoszeń zbiorów danych osobowych,
- powiatowe urzędy pracy - 9 zgłoszeń zbiorów danych osobowych do rejestracji.

Organy i instytucje centralne zgłosiły 55 zbiorów danych osobowych. Wykaz zgłoszeniodawców stanowi załącznik nr 1.

Organy administracji rządowej i samorządowej województw zgłosiły 64 zbiory danych osobowych. Szczegółowe zestawienie przedstawiono w załączniku nr 2.

W roku 2000 zostało zarejestrowanych 35675 zbiorów danych osobowych, tj. ponad 5 - krotnie więcej niż w 1999 r. Na dzień 31 grudnia 2000 r. ogólna liczba zarejestrowanych zbiorów danych wyniosła 42325. Natomiast w stosunku do 4031 zgłoszeń przeprowadzono postępowanie wyjaśniające (dla porównania w 1999 r. przeprowadzono 1604 takie postępowania).

Do rejestracji zgłaszane także były zbiory danych osobowych, które nie podlegały temu obowiązkowi, gdyż niektórzy administratorzy danych na podstawie art. 43 ust 1 ustawy są zwolnieni z obowiązku zgłoszenia zbioru danych osobowych do rejestracji.

Spośród rozpatrzonych w roku 2000 wniosków rejestracyjnych taka sytuacja miała miejsce w 853 przypadkach. Szczegółowe zestawienie wyłączeń z punktu widzenia poszczególnych przesłanek, o których mowa w art. 43 ust. 1 ustawy, opisano w załączniku nr 3.

Zgłoszeń dokonywały podmioty nie będące administratorami danych osobowych w rozumieniu art. 7 ust. 4 w związku z art. 3 ustawy o ochronie danych osobowych - wysłano do nich 4035 pism zawiadamiających, iż zgłoszenie zostało dokonane przez podmiot nieuprawniony (w roku 1999 takich pism wysłano 221). Do podmiotów tych należy w szczególności zaliczyć agentów ubezpieczeniowych lub osoby reprezentujące otwarte fundusze emerytalne. Generalny Inspektor Ochrony Danych Osobowych uznał, że agenci ubezpieczeniowi przetwarzający dane osobowe w ramach czynności wykonywanych na rzecz towarzystw ubezpieczeniowych lub otwartych funduszy emerytalnych nie mają statusu administratora danych, ale jedynie podmiotu, któremu administrator danych powierzył przetwarzanie danych osobowych na podstawie art. 31 ustawy o ochronie danych osobowych (szczegółowe omówienie w punkcie II. 2).

II. Zawiadomienia o zwolnieniach i zgłoszeniach przez podmioty nieuprawnione

II.1 Zwolnienia z obowiązku zgłoszenia zbioru danych osobowych do rejestracji

Zwolnienia z obowiązku rejestracyjnego określone zostały w art. 43 ust. 1 ustawy. Mają one charakter przedmiotowy i stanowią listę numerus clausus. Z obowiązku rejestracji zwolnieni są administratorzy danych:

- 1) objętych tajemnicą państwową ze względu na obronność lub bezpieczeństwo państwa, ochronę życia i zdrowia ludzi, mienia lub bezpieczeństwa i porządku publicznego,
- 2) przetwarzanych przez właściwe organy dla potrzeb postępowania sądowego,
- 3) dotyczących członków kościoła lub innego związku wyznaniowego, o uregulowanej sytuacji prawnej,
- 4) dotyczących osób u nich zatrudnionych, zrzeszonych lub uczących się,
- 5) dotyczących osób korzystających z ich usług medycznych, obsługi notarialnej, adwokackiej lub radcy prawnego,
- 6) tworzonych na podstawie ordynacji wyborczych do Sejmu, Senatu, rad gmin, rad powiatów i sejmików województw, ustawy o wyborze Prezydenta Rzeczypospolitej Polskiej oraz ustaw o referendum i ustawy o referendum gminnym,
- 7) dotyczących osób pozbawionych wolności na podstawie ustawy, w zakresie niezbędnym do wykonania tymczasowego aresztowania lub kary pozbawienia wolności,
- 8) przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej,
- 9) powszechnie dostępnych,
- 10) przetwarzanych w celu przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego,
- 11) przetwarzanych w zakresie drobnych bieżących spraw życia codziennego.

Administratorzy zgłaszający Generalnemu Inspektorowi zbiory danych osobowych nie podlegające rejestracji, są zawiadamiani, że z mocy ustawy zwolnieni są z obowiązku rejestracyjnego.

Poniżej przedstawiono przykładowe zgłoszenia zbiorów danych osobowych do rejestracji, w stosunku do których zastosowano tego typu procedurę.

1) Zbiory danych osobowych przetwarzanych przez właściwe organy dla potrzeb postępowania sądowego (art. 43 ust. 1 pkt 2)

np. zbiory danych osobowych dotyczące spraw karno - skarbowych

Generalnemu Inspektorowi Ochrony Danych Osobowych urzędy skarbowe zgłaszały zbiory danych osobowych powstające w związku z prowadzeniem dochodzeń w sprawach

o przestępstwa i wykroczenia skarbowe.

Zgodnie z art. 133 § 1 pkt 2 w związku z art. 155 § 1 ustawy z dnia 10 września 1999 r. Kodeks karny skarbowy (Dz. U. Nr 83, poz. 930) urzędy skarbowe prowadzą dochodzenia w sprawach o przestępstwa i wykroczenia skarbowe, a także w przypadku istnienia podstaw do wniesienia aktu oskarżenia sporządzają go i wnoszą do właściwego sądu oraz popierają go przed tym sądem (np. zgłoszenie nr R 012088/99).

2) Zbiory danych osobowych dotyczących osób zatrudnionych, zrzeszonych lub uczących się (art. 43 ust. 1 pkt 4)

np. - zbiory danych osobowych dotyczących osób zatrudnionych

Wyłączenie to odnosi się do danych przetwarzanych w związku z najszerzej rozumianym pojęciem zatrudnienia, mieszczącym w sobie zarówno pracownicze, jak i niepracownicze (np. administracyjnoprawne lub cywilnoprawne) stosunki zatrudnienia. (np. zgłoszenia nr R 037009/99, nr R 070897/99).

- zbiory danych osobowych dotyczących osób uczących się

Generalnemu Inspektorowi Ochrony Danych Osobowych zgłoszone zostały do rejestracji zbiory danych osobowych dotyczące dzieci uczących się w ramach szkół i placówek systemu oświaty (np. zgłoszenia nr: R 007321/99, R 016642/99).

Wyłączeniem tym objęte są także zbiory danych osobowych dotyczące rodziców dzieci uczących się, gdyż zgodnie z rozporządzeniem Ministra Edukacji Narodowej z dnia 19 kwietnia 1999 r w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. Nr 41, poz. 414) dane rodziców, jako opiekunów prawnych, są przyporządkowane danym dzieci, mają wobec nich charakter wtórny i są

przetwarzane jedynie na potrzeby edukacji dzieci (np. zgłoszenia nr: R 022439/99, R 039348/99).

- zbiory danych osobowych dotyczące osób zrzeszonych

Generalnemu Inspektorowi Ochrony Danych Osobowych zgłaszane były do rejestracji przez spółdzielnie, izby oraz stowarzyszenia zbiory danych osobowych dotyczące ich członków.

1. Zgodnie z art. 1 § 1 ustawy z dnia 16 września 1982 r. Prawo spółdzielcze (Dz. U. z 1995 r. Nr 54, poz. 288 z późn. zm) „spółdzielnia jest dobrowolnym zrzeszeniem nieograniczonej liczby osób, o zmiennym składzie osobowym i zmiennym funduszu udziałowym, która w interesie swoich członków prowadzi wspólną działalność gospodarczą” (np. zgłoszenia nr: R 048299/99, R 055615/99).

2. Zgodnie z art. 1 ust. 3 w związku z art. 12 ust. 1 ustawy z dnia 17 maja 1989 r. o izbach lekarskich (Dz. U. Nr 30, poz. 158 z późn. zm.), okręgowa izba lekarska jest jednostką organizacyjną samorządu lekarzy posiadającą osobowość prawną, zrzeszającą z mocy prawa osoby posiadające prawo wykonywania zawodu lekarza, które zamierzają wykonywać lub wykonują zawód na obszarze działania izby (np. zgłoszenie nr R 010864/99)

3. Analogiczna sytuacja dotyczy członków izb rolniczych, gdyż zgodnie z art. 3 ust. 1 w związku z art. 1 ust. 1 ustawy z dnia 14 grudnia 1995 r. o izbach rolniczych (Dz. U z 1996 r. Nr 1, poz. 3 z późn. zm.) izba rolnicza jest jednostką organizacyjną samorządu rolniczego działającego na rzecz rozwiązywania problemów rolnictwa i reprezentującego interesy zrzeszonych w nim podmiotów. Członkostwo w izbie nabywają z mocy prawa podmioty określone w art. 1 ust. 2 wyżej powołanej ustawy. Uznać zatem należy, iż zbiór danych dotyczących członków izby rolniczej nie podlega obowiązkowi zgłoszenia do rejestracji (np. zgłoszenie nr R 000657/99).

4. Zgodnie z art. 2 ust. 1 ustawy z dnia 7 kwietnia 1989 r. Prawo o stowarzyszeniach (Dz. U. Nr 20, poz. 104 z późn. zm.) stowarzyszenie jest dobrowolnym, samorządnym i trwałym zrzeszeniem o celach niezarobkowych (np. zgłoszenia nr: R 011299/99, R 029113/99).

3) Zbiory danych osobowych dotyczące osób korzystających z usług medycznych, obsługi notarialnej, adwokackiej lub radcy prawnego (art. 43 ust. 1 pkt 5)

np. - zbiory danych osobowych prowadzone przez zakłady opieki zdrowotnej

Zgłoszenia w tym zakresie dokonywane były przez zakłady opieki zdrowotnej. Zgodnie z ustawą z dnia 30 sierpnia 1991 r. o zakładach opieki zdrowotnej (Dz. U. Nr 91, poz. 408 z późn. zm.) zakład opieki zdrowotnej jest wyodrębnionym organizacyjnie zespołem osób i środków majątkowych utworzonym w celu udzielania świadczeń zdrowotnych i promocji zdrowia, a świadczeniami zdrowotnymi są działania służące zachowaniu, ratowaniu, przywracaniu i poprawie zdrowia i inne działania medyczne wynikające z procesu leczenia, w szczególności związane m.in. z: leczeniem, badaniem i poradą lekarską, rehabilitacją leczniczą, pielęgnacją chorych (np. zgłoszenia nr: R 026259/99, nr R 051575/99).

- zbiory danych osobowych prowadzone przez poradnie psychologiczno - pedagogiczne

Zgodnie z art. 2 ust. 1 pkt 2 ustawy z dnia 30 sierpnia 1991 r. o zakładach opieki zdrowotnej (Dz. U. Nr 91, poz. 408 z późn. zm.) zakładem opieki zdrowotnej jest przychodnia, ośrodek zdrowia, poradnia. Art. 27 ust. 1 powołanej ustawy stanowi, iż poradnia udziela świadczeń zdrowotnych, które mogą swym zakresem obejmować świadczenia podstawowej i specjalistycznej opieki zdrowotnej. Natomiast, stosownie do postanowień art. 3 powołanej ustawy świadczeniem zdrowotnym są działania służące zachowaniu, ratowaniu, przywracaniu i poprawie zdrowia oraz inne działania medyczne wynikające z procesu leczenia lub przepisów odrębnych regulujących zasady ich wykonywania, w szczególności związane z badaniem i terapią psychologiczną (np. zgłoszenia nr: R 010867/99, nr R 13424/99).

- zbiory danych osobowych dotyczących osób korzystających z obsługi notarialnej, adwokackiej lub radcy prawnego

Generalnie, administratorzy takich danych nie zgłaszali do rejestracji prowadzonych w tym zakresie zbiorów. Odsobnionym przypadkiem było zgłoszenie zbioru o nazwie „Klienci radcy prawnego” (zgłoszenie nr R 050792/99).

4) Zbiory danych osobowych tworzonych na podstawie ordynacji wyborczych do Sejmu, Senatu, rad gmin, rad powiatów i sejmików województw, ustawy o wyborze Prezydenta Rzeczypospolitej Polskiej oraz ustaw o referendum gminnym (art. 43 ust. 1 pkt 6)

Generalnemu Inspektorowi Ochrony Danych Osobowych gminy zgłaszały rejestry wyborców. Zgodnie z art. 15 ust. 1 ustawy z dnia 28 maja 1993 r. Ordynacja wyborcza do Sejmu Rzeczypospolitej Polskiej (Dz. U. Nr 45, poz. 205 z późn. zm.) „gmina prowadzi, jako zadanie zlecone, stały rejestr wyborców”. Służy on, na podstawie art. 15 ust. 2 tejże ustawy, do sporządzania spisów wyborców dla wyboru Prezydenta RP, dla wyborów do Sejmu i do Senatu oraz do rad gmin, a także do sporządzania spisów osób uprawnionych do udziału w referendum ogólnokrajowym oraz lokalnym.

Wobec powyższego, przedmiotowe zbiory danych, jako tworzone na podstawie ordynacji wyborczej do Sejmu, nie podlegają obowiązkowi zgłoszenia do rejestracji na podstawie art. 43 ust. 1 pkt 6 ustawy o ochronie danych osobowych (np. zgłoszenia nr: R 017732/99, R 031224/99).

5) Zbiory danych osobowych przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub sprawozdawczości finansowej (art. 43 ust. 1 pkt 8)

Z obowiązku rejestracji zwolnione są zbiory danych prowadzone wyłącznie w tym celu. Tak więc istnienie jakiegokolwiek innego celu przetwarzania danych uniemożliwia zastosowanie omawianego zwolnienia. Było ono stosowane tylko wówczas, gdy zgłoszeniodawca oświadczał, że przetwarza dane osobowe wyłącznie w celu wystawienia rachunku, faktury lub sprawozdawczości finansowej (np. zgłoszenia nr: R020529/99, R 021571/99). Wątpliwości wzbudzała rejestracja zbiorów danych osobowych użytkowników wodociągu gminnego oraz oczyszczalni ścieków.⁴⁶⁸ W odpowiedzi stwierdzono, że o ile zbiór taki wykorzystywany będzie wyłącznie w celu wystawiania faktur i rachunków, podlegać będzie zwolnieniu z obowiązku rejestracji. Jeżeli jednak byłby on wykorzystywany do innych celów (np. dochodzenia roszczeń wynikających z niewykonania zobowiązań) wówczas niezbędne jest zarejestrowanie takiego zbioru.

Jednocześnie podkreślono, że zwolnienie z obowiązku rejestracji nie jest równoznaczne ze zwolnieniem z innych obowiązków określonych w ustawie o ochronie danych osobowych.

6) Zbiory danych osobowych powszechnie dostępnych (art. 43 ust. 1 pkt 9)

np. - zbiory kar pieniężnych

Zgodnie z § 13 ust. 5 rozporządzenia Rady Ministrów z dnia 22 grudnia 1998 r. w sprawie kar pieniężnych za naruszanie wymagań ochrony środowiska oraz rejestru decyzji dotyczących tych kar (Dz. U. Nr 162, poz. 1138), wydanego na podstawie art. 110 ust. 1c ustawy o ochronie i kształtowaniu środowiska (Dz. U. z 1994 r. Nr 49, poz. 196 z późn. zm.) przedmiotowy rejestr jest powszechnie dostępny (np. zgłoszenia nr: R 024579/99, R 029172/99).

- zbiory danych osobowych udziałowców spółek z ograniczoną odpowiedzialnością

Zgodnie z art. 188 rozporządzeniem Prezydenta Rzeczypospolitej z dnia 27 czerwca 1934 r. – Kodeks handlowy (Dz. U. Nr 502, poz. 502 z późn. zm.) zarząd spółki z o.o. zobowiązany jest do prowadzenia księgi udziałów, do której należy wpisywać imię i nazwisko (firmę) każdego wspólnika, adres (siedzibę) oraz ilość i wysokość jego udziałów oraz wszelkie zmiany w osobach wspólników i posiadaniu udziałów. Po każdym wpisaniu zmiany zarząd przedkłada sądowi rejestrowemu aktualną listę wspólników i składa ją do zbioru dokumentów rejestrowych, który na mocy art. 13 ust. 2 Kodeksu handlowego, jest jawny. W związku z tym księga udziałów spółki z ograniczoną odpowiedzialnością, jako zbiór danych wspólników jest powszechnie dostępna (np. zgłoszenia nr: R 040055/99, R 043591/99)

- zbiory danych osobowych dotyczących osób reprezentujących podmioty prowadzące działalność gospodarczą

Zbiory te zawierają dane osób reprezentujących firmy, służą kontaktom służbowym i przetwarzane są wyłącznie w zakresie pozwalającym na realizację tego celu (zgłoszenia nr: R 008698/99, R 037380/99).

7) Zbiory danych osobowych przetwarzanych w zakresie drobnych bieżących spraw życia codziennego (art. 43 ust. 1 pkt 11)

Wyłączeniem tym objęte zostały zgłoszone do rejestracji zbiory danych osobowych będące rejestrami przepustek jednorazowych, prowadzone zarówno przez podmioty sfery prywatnej, jak i publicznej (np. zgłoszenie nr: R 07526/99, R 024805/99).

II.2 Zgłoszenia zbiorów danych osobowych do rejestracji dokonane przez podmioty nieuprawnione

W 2000 r. wysłano 3993 pisma zawiadamiające o zgłoszeniu zbioru danych przez podmiot nie będący administratorem danych. Były to m.in.:

1. Agenci ubezpieczeniowi.

Z charakteru czynności wykonywanych przez agentów ubezpieczeniowych (zawieranie umów z poszczególnymi klientami i w związku z tym przetwarzanie danych osobowych na rzecz towarzystwa ubezpieczeniowego lub otwartego funduszu emerytalnego) wynika, iż są to jedynie podmioty, którym zgodnie z 31 ustawy o ochronie danych osobowych, powierzono przetwarzanie danych osobowych. Administratorem danych jest natomiast towarzystwo ubezpieczeniowe lub otwarty fundusz emerytalny. Wysłanych zostało 3912 takich pism (np. zgłoszenie nr R 060253/99).

2. Gminy zgłaszające zbiory danych związane z obrotem nieruchomościami rolnymi Skarbu Państwa.

Administratorem przedmiotowych zbiorów jest Agencja Własności Rolnej Skarbu Państwa, która przetwarza dane osobowe dla wykonania prawa własności i innych praw rzeczowych w stosunku do mienia wchodzącego w skład Zasobu Własności Rolnej Skarbu Państwa (art. 5 ust. 1 w zw. z art. 12 ust. 3 ustawy z dnia 19 października 1991 r. o gospodarowaniu nieruchomościami rolnymi Skarbu Państwa, tj. Dz. U. z 1995 r. Nr 57, poz. 299 z późn. zm.) Zgodnie z art. 27 tejże ustawy, sprzedaż i nabywanie nieruchomości może w szczególności prowadzić upoważniony przez Agencję w drodze umowy zlecenia inny podmiot, w tym gmina. W związku z tym uznać należy, iż gminy są jedynie podmiotami, którym administrator danych, zgodnie z art. 31 ustawy o ochronie danych osobowych, powierzył w drodze umowy przetwarzanie danych osobowych. Odpowiedzialność za przestrzeganie przepisów ustawy o ochronie danych osobowych spoczywa na administratorze danych, który w szczególności powinien dopełnić

obowiązku zgłoszenia zbioru danych do rejestracji. Nie wyłącza to odpowiedzialności podmiotu, o którym mowa w art. 31 ustawy, za przetwarzanie danych niezgodnie z umową powierzenia. Jest on również zobowiązany do zastosowania środków, o których mowa w art. 36 – 39 ustawy, zabezpieczających zbiór danych osobowych. Generalny Inspektor Ochrony Danych Osobowych zawiadamiał w takich przypadkach, że wnioskodawcy nie są administratorami danych i w związku z tym nie ciąży na nich obowiązek rejestracyjny. Wysłanych zostało 81 takich pism (np. zgłoszenie nr R 043907/99).

III. Postępowania wyjaśniające

III.1 Postępowania wyjaśniające zakończone rejestracją zbioru danych osobowych

Z uwagi na to, że w roku 1999 zgłoszono ponad 70910 zgłoszeń, w roku 2000 postępowania wyjaśniające były prowadzone głównie w odniesieniu do zgłoszeń zbiorów danych złożonych w roku poprzednim.

Ustawa o ochronie danych osobowych w art. 44 ust. 1 określa przesłanki, których zaistnienie skutkuje wydaniem przez Generalnego Inspektora Ochrony Danych Osobowych decyzji o odmowie rejestracji zbioru danych osobowych. Odmawiając rejestracji zbioru danych osobowych Generalny Inspektor nakazuje wstrzymanie dalszego przetwarzania danych w tym zbiorze lub ich usunięcie ze zbioru (art. 44 ust. 2). Nakaz ten podlega natychmiastowemu wykonaniu (art. 44 ust. 3).

W każdym przypadku zgłoszeń zbiorów danych osobowych do rejestracji, wywołujących wątpliwości dotyczące stanu prawnego lub faktycznego Generalny Inspektor Ochrony Danych Osobowych przeprowadza postępowania wyjaśniające. Prowadzenie tego rodzaju postępowań jest praktyczną realizacją zasad: pozyskiwania zaufania obywateli do organów prowadzących postępowanie administracyjne (art. 8 K.p.a.), oraz udzielania pomocy prawnej (art. 9 K.p.a.), które w kontekście nowatorskiego charakteru regulacji dotyczących ochrony danych osobowych na gruncie polskiego prawa nabierają szczególnego znaczenia.

W roku 2000 przeprowadzono 3983 postępowania wyjaśniające. Występujące nieprawidłowości można podzielić na:

- 1) wady formalne

2) wady merytoryczne

Ad 1) Zgłoszenie zbioru danych osobowych zgodnie z art. 63 Kodeksu postępowania administracyjnego powinno w szczególności zawierać elementy, o których mowa w §§ 2 i 3 powołanego przepisu. Do podstawowych kodeksowych wad formalnych należy zaliczyć brak podpisu, bądź podpis nie pozwalający na ustalenie, czy zbiór został zgłoszony przez osobę uprawnioną do reprezentowania administratora danych (np. zgłoszenia nr: R 010876/99, R 043211/99).

Elementy zgłoszenia zbioru danych osobowych zostały określone w art. 41 ust. 1 ustawy o ochronie danych osobowych, natomiast obowiązujący wzór zgłoszenia stanowi załącznik nr 2 do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia wniosku o udostępnienie danych osobowych, zgłoszenia zbioru danych do rejestracji oraz imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. Nr 80, poz. 522 z późn. zm.). Zgłoszenia nie były dokonywane na obowiązującym wzorze, tj. administrator danych składał jedynie podanie zawierające żądanie zarejestrowania zbioru danych osobowych (np. zgłoszenia nr: R 005290/99, R 013949/99), bądź też zgłaszano zbiór do rejestracji na druku niezgodnym z obowiązującym wzorem, najczęściej opracowanym przez wnioskodawcę (np. zgłoszenia nr: R 028131/99, R 056064/99). Zbiory danych osobowych zgłaszano też na niekompletnym formularzu, tzn. zgłoszenia nie zawierały jednej lub kilku stron wzoru (np. zgłoszenia nr: R 026872/99, R 027841/99), lub w zgłoszeniu nie wypełniono poszczególnych części formularza (np. zgłoszenia nr: R 033361/99, R 046566/99).

W opisanej sytuacji wnioskodawca był wzywany do uzupełnienia zgłoszenia pomimo, że niespełnienie wymogów formalnych stanowi przesłankę do wydania przez Generalnego Inspektora Ochrony Danych Osobowych, na podstawie art. 44 ust. 1 pkt 1 ustawy, decyzji o odmowie rejestracji zbioru danych osobowych.

Ad 2) Podobne działania były podejmowane w przypadku spełnienia przesłanki z art. 44 ust. 1 pkt 2 ustawy o ochronie danych osobowych. Generalny Inspektor Ochrony Danych Osobowych odmawia rejestracji zbioru danych, jeżeli przetwarzanie danych w przedmiotowym zbiorze naruszałoby zasady określone w art. 23-30 ustawy, np.:

- w przypadku braku podstawy prawnej legalności przetwarzania danych osobowych - art. 23 ust. 1 ustawy o ochronie danych osobowych (zgłoszenia nr: R 024424/99, R 058904/99),
- w przypadku naruszenia zasady zachowania szczególnej staranności przy przetwarzaniu danych osobowych w celu ochrony interesów osób, których dane dotyczą - art. 26 ust. 1 ustawy (zgłoszenia nr: R 026072/99, R 035982/99),
- w przypadku przetwarzania bez podstawy prawnej tzw. „danych wrażliwych” - art. 27 ust. 2 ustawy (zgłoszenia nr: R 021041/99, R 026100/99, R 028479/99),
- naruszenie zasady legalności przetwarzania danych dotyczących skazań, orzeczeń o ukaraniu, mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym - art. 28 ust. 1 ustawy (zgłoszenia nr: R 017141/99, R 026451/99, R 031144/99).

Znaczna liczba zgłoszeń zbiorów danych spełniało przesłankę odmowy, o której mowa w art. 44 ust. 1 pkt 3, tj. urządzenia i systemy informatyczne służące do przetwarzania zbioru danych zgłoszonego do rejestracji nie spełniają wymogów technicznych i organizacyjnych wskazanych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 80, poz. 521).

Przyczyn takiej sytuacji można przede wszystkim upatrywać w redakcji wzoru zgłoszenia, który w częściach dotyczących technicznych i organizacyjnych aspektów przetwarzania danych osobowych (części E i F) miał charakter opisowy, podczas gdy pozostałe części skonstruowane zostały na zasadzie pól do wypełniania lub zakreslania właściwych odpowiedzi. Od dnia 5 grudnia 1999 r. obowiązuje nowy wzór zgłoszenia zbioru danych osobowych do rejestracji. Zrezygnowano w nim z opisowej części F, która została uproszczona poprzez podzielenie jej na odpowiednie pola do zakreslania lub wypełnienia. Drugim powodem, dla którego administratorzy danych pozostawiali pustą część F zgłoszenia, było rzeczywiste niedopełnianie wymogów wynikających z rozporządzenia. W trakcie postępowań wyjaśniających administratorzy danych przywracali, w zakresie wskazanym przez Generalnego Inspektora, stan zgodny z prawem, czego konsekwencją było uznanie zgłoszeń za prawidłowe i ich rejestracja (np. zgłoszenia nr: R 015329/99, R025933/99, R 040813/99).

Szczególne trudności związane z rozpatrywaniem zgłoszeń do rejestracji jednostek administracji publicznej spowodowane są faktem, iż administratorzy danych w sposób samodzielny decydują o tym, czy określone w szczegółowych przepisach prawa zadanie jest realizowane poprzez prowadzenie jednego bądź kilku odrębnych zbiorów danych osobowych. Następstwem takiej sytuacji są trudności w ustaleniu standardowej liczby zgłoszeń, jakie powinny zostać nadesłane przez jednostki administracji publicznej poszczególnych szczebli.

III.2 Postępowania wyjaśniające zakończone wydaniem decyzji odmawiającej rejestracji

Generalny Inspektor Ochrony Danych Osobowych w 2000 roku wydał 14 decyzji administracyjnych odmawiających rejestracji zbioru danych osobowych dotyczących:

1. Zgłoszenia zbioru danych o nazwie „Alcatel/Rekrutacja”, złożonego przez Alcatel Polska S.A. Ze zgłoszenia wynikało, iż przetwarzanie danych w tym zbiorze spełniało przesłanki wydania decyzji odmownej wymienione w:
 - art. 44 ust. 1 pkt 2 ustawy, tj. przetwarzanie w zgłoszonym zbiorze danych osobowych dotyczących skazań naruszałoby zasadę, o której mowa w art. 28 ust. 1 ustawy, zgodnie z którą przetwarzanie tego typu danych może odbywać się wyłącznie na podstawie ustawy (wnioskodawca nie wskazał takiej ustawowej podstawy);
 - art. 44 ust. 1 pkt 3 ustawy, tj. urządzenia i systemy służące do przetwarzania danych osobowych w zgłoszonym zbiorze nie spełniały podstawowych warunków organizacyjnych i technicznych, o których mowa w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji.

W związku z tym, zwrócono się do Alcatel Polska S.A. o złożenie pisemnych wyjaśnień w tej sprawie. W odpowiedzi strona nie odniosła się do przedstawionych wad zgłoszenia.

Wobec powyższego, Generalny Inspektor Ochrony Danych Osobowych, w drodze decyzji administracyjnej, odmówił rejestracji przedmiotowego zbioru danych osobowych i nakazał usunięcie danych ze zbioru.⁴⁶⁹

2. Zgłoszenia zbioru danych o nazwie <”Posesja” Biuro Obrotu Nieruchomościami - Baza Danych Klientów>, złożonego przez Biuro Obrotu Nieruchomościami „Posesja”.

⁴⁶⁹ GI/DRZDO/DEC/5/00

Ze zgłoszenia wynikało, iż przetwarzanie danych w tym zbiorze spełniało przesłanki wydania decyzji odmownej wymienione w:

- art. 44 ust. 1 pkt 2 ustawy, tj. przetwarzanie danych w zgłoszonym zbiorze danych naruszałoby zasadę art. 28 ust. 1 ustawy, ponieważ bez podstawy ustawowej przetwarzane są orzeczenia wydane w postępowaniu sądowym (postanowienia o stwierdzeniu nabycia spadku),
- art. 44 ust. 1 pkt 3 ustawy, tj. urządzenia i system informatyczny służące do przetwarzania danych osobowych w przedmiotowym zbiorze nie spełniały podstawowych warunków technicznych i organizacyjnych, o których mowa w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji.

W związku z tym, zwrócono się do Biura Obrotu Nieruchomościami „Posesja” o złożenie pisemnych wyjaśnień w tej sprawie. Ze złożonych wyjaśnień wynikało, iż wnioskodawca nie spełnił wymogów określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji, a tym samym spełniona została przesłanka odmowy rejestracji, o której mowa w art. 44 ust. 1 pkt 3 ustawy o ochronie danych osobowych.

Wobec powyższego, Generalny Inspektor Ochrony Danych Osobowych, w drodze decyzji administracyjnej, odmówił rejestracji przedmiotowego zbioru danych osobowych i nakazał usunięcie danych ze zbioru.⁴⁷⁰

3. Zgłoszenia zbioru danych o nazwie <Baza danych klientów agencji nieruchomości „TARA”>, złożonego przez Agencję Nieruchomości „TARA” z siedzibą w Krakowie. Ze zgłoszenia wynikało, iż przetwarzanie danych w tym zbiorze spełniało przesłanki wydania decyzji odmownej wymienione w:
 - art. 44 ust. 1 pkt 2 ustawy, tj. przetwarzanie danych w zgłoszonym zbiorze danych naruszałoby zasadę art. 28 ust. 1 ustawy, ponieważ bez podstawy ustawowej przetwarzane były orzeczenia wydane w postępowaniu sądowym (postanowienia o stwierdzeniu nabycia spadku),
 - art. 44 ust. 1 pkt 3 ustawy, tj. urządzenia i system informatyczny służące do przetwarzania danych osobowych w przedmiotowym zbiorze nie spełniały podstawowych warunków technicznych i organizacyjnych, o których mowa w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji.

⁴⁷⁰ GI/DRZDO/DEC/36/00

W związku z tym zwrócono się do Agencji Nieruchomości „TARA” o złożenie pisemnych wyjaśnień w tej sprawie.

Ze złożonych wyjaśnień wynikało, iż zgłoszeniodawca nie spełnił wymogów określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji, a tym samym spełniona została przesłanka odmowy rejestracji, o której mowa w art. 44 ust. 1 pkt 3 ustawy o ochronie danych osobowych.

Jednocześnie w złożonych wyjaśnieniach Agencja Nieruchomości „TARA” potwierdziła, iż przetwarza w przedmiotowym zbiorze dane dotyczące orzeczeń wydanych w postępowaniu sądowym (postanowienia o stwierdzeniu nabycia spadku). Strona nie podała w wyjaśnieniach ustawowej podstawy przetwarzania tego typu danych.

Tym samym spełniona więc została przesłanka odmowy rejestracji wymieniona w art. 44 ust. 1 pkt 2 ustawy o ochronie danych osobowych.

Wobec powyższego, Generalny Inspektor Ochrony Danych Osobowych, w drodze decyzji administracyjnej, odmówił rejestracji przedmiotowego zbioru danych osobowych i nakazał wstrzymanie przetwarzania danych w zgłoszonym zbiorze, za wyjątkiem przechowywania danych.⁴⁷¹

4. Zgłoszenia zbioru danych o nazwie „JBK”, złożonego przez „Medim” Sp. z o.o

Zgłoszenie to nie spełniało wymogów, o których mowa w art. 41 pkt 6 ustawy, tj. nie zawierało informacji o sposobie wypełnienia wymagań technicznych i organizacyjnych, o których mowa w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji. Tym samym została spełniona przesłanka odmowy rejestracji zbioru danych określona w art. 44 ust. 1 pkt 1 ustawy o ochronie danych osobowych.

W związku z tym zwrócono się do „Medim” Sp. z o. o. o złożenie pisemnych wyjaśnień w tej sprawie. Mimo poinformowania strony, jaka zdaniem organu rejestracyjnego przesłanka odmowy rejestracji przedmiotowego zbioru została spełniona, a także pouczenia, iż w przypadku nie złożenia wymaganych wyjaśnień, Generalny Inspektor Ochrony Danych Osobowych odmówi rejestracji przedmiotowego zbioru danych, „Medim” Sp. z o. o. w odpowiedzi ograniczyła się jedynie do ogólnych wyjaśnień dotyczących kategorii osób, których dane są przetwarzane oraz pojedynczej metody zabezpieczenia, a także deklaracji spełnienia w przyszłości obowiązków wynikających z ustawy. Jednocześnie w wyznaczonym terminie w żaden sposób nie doszło do uzupełnienia braków zgłoszenia.

⁴⁷¹ GI/DRZO/DEC/24/00

Wobec powyższego, Generalny Inspektor Ochrony Danych Osobowych, w drodze decyzji administracyjnej, odmówił rejestracji przedmiotowego zbioru danych osobowych i nakazał wstrzymanie przetwarzania danych w zgłoszonym zbiorze, za wyjątkiem przechowywania danych.⁴⁷²

5. Zgłoszeń dziewięciu zbiorów danych dotyczących kartotek osobowo-adresowych złożonych przez ośrodki pomocy społecznej. Zgłoszenia te spełniały przesłankę odmowy rejestracji, o której mowa w art. 44 ust. 1 pkt 2 w związku z art. 23 ust. 1 ustawy – zgłoszeniodawcy oświadczyli, iż prowadzenie przedmiotowych zbiorów jest niezbędne do wykonywania określonych prawem zadań realizowanych dla dobra publicznego, tj. weryfikacji wniosków o przyznanie pomocy z ośrodka pomocy społecznej oraz wywiadów środowiskowych. Przeprowadzone postępowania wyjaśniające wykazały, iż zbiory danych dotyczące kartotek osobowo-adresowych dotyczą wszystkich mieszkańców gminy, nie tylko klientów ośrodków i osób ubiegających się o pomoc w ośrodkach pomocy społecznej. Dane te są pozyskiwane z ewidencji ludności prowadzonej przez gminy, regularnie aktualizowane i brak jest podstaw prawnych do ich przetwarzania. W związku z tym przetwarzanie danych osobowych w zgłoszonych zbiorach naruszało zasadę, o której mowa w art. 23 ust. 1 ustawy, a tym samym została spełniona przesłanka odmowy rejestracji określona w art. 44 ust. 1 pkt 2 ustawy o ochronie danych osobowych.

Wobec powyższego, Generalny Inspektor Ochrony Danych Osobowych, w drodze decyzji administracyjnej, odmówił rejestracji przedmiotowych zbiorów danych osobowych i nakazał usunięcie danych ze zbiorów.⁴⁷³

6. Zgłoszenia zbioru danych o nazwie „Regionalna baza danych o wierzytelnościach” złożonego przez Beskidzką Izbę Kapitałową Sp. z o.o. z siedzibą w Bielsku-Białej.

Ze zgłoszenia wynikało, iż spełniona została przesłanka odmowy rejestracji, o której mowa w art. 44 ust. 1 pkt 3 ustawy, tj. urządzenia i systemy informatyczne służące do przetwarzania danych w przedmiotowym zbiorze nie spełniają wymogów, o których mowa w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji. Ponadto, w związku z oświadczeniem wnioskodawcy, iż podstawę prawną upoważniającą do prowadzenia przedmiotowego zbioru danych stanowi art. 105 ust. 4 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. Nr 140, poz. 939 z późn. zm.) należało wyjaśnić, czy wnioskodawca

⁴⁷² GI/DRZDO/DEC/26/00

⁴⁷³ GI/DRZDO/DEC/14/00

GI/DRZDO/DEC/18/00

GI/DRZDO/DEC/23/00

GI/DRZDO/DEC/47/00

spełnia warunki dotyczące instytucji, o której mowa w tym przepisie, tj. utworzonej przez banki wspólnie z bankowymi izbami gospodarczymi instytucji do zbierania i udostępniania bankom informacji o wierzytelnościach oraz o obrotach i stanach rachunków bankowych w zakresie, w jakim informacje te są potrzebne w związku z udzielaniem kredytów, pożyczek pieniężnych, gwarancji bankowych i poręczeń.

W związku z powyższym zwrócono się do wnioskodawcy o złożenie pisemnych wyjaśnień w tej sprawie.

Ze złożonych przez wnioskodawcę wyjaśnień wynikało, iż administrator danych spełnił wymogi określone w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji. Tym samym nie zachodziła przesłanka wydania decyzji o odmowie rejestracji, o której mowa w art. 44 ust. 1 pkt 3 ustawy. Wobec wątpliwości, jakie zrodziły się na gruncie interpretacji art. 105 ust. 4 Prawa bankowego, który przesądzał o podstawach prawnych (legalności) prowadzenia zbioru danych, Generalny Inspektor Ochrony Danych Osobowych zwrócił się do Przewodniczącego Komisji Nadzoru Bankowego o przedstawienie opinii prawnej w niniejszej sprawie. Uzyskana opinia potwierdziła stanowisko wyrażone przez Generalnego Inspektora Ochrony Danych Osobowych. Wskazano w niej, iż uprawnione do utworzenia instytucji, są banki wspólnie z bankowymi izbami gospodarczymi; zarówno literalna, jak i celowościowa wykładania przepisu art. 105 ust. 4 Prawa bankowego wskazuje na dopuszczalność istnienia jedynie jednej instytucji tego rodzaju w skali kraju. Nadto wskazano, iż utworzenie jednej instytucji wynika z faktu, że chronionym dobrem jest tajemnica bankowa, zaś rozszerzenie listy podmiotów uprawnionych do dysponowania danymi objętymi tajemnicą bankową mogłoby stanowić zagrożenie bezpieczeństwa tych danych.⁴⁷⁴

Jednocześnie z wyjaśnień wynikało, iż Beskidzka Izba Kapitałowa Sp. z o.o. nie spełnia warunków instytucji, o której mowa w art. 105 ust. 4 ustawy Prawo Bankowe. Zatem przepis ten, ani żaden inny ze wskazanych przez wnioskodawcę przepisów ustawy Prawo bankowe, nie stanowi podstawy prawnej do przetwarzania danych w zgłoszonym zbiorze.

Tym samym spełniona więc została przesłanka odmowy rejestracji wymieniona w art. 44 ust. 1 pkt 2 ustawy o ochronie danych osobowych, tj. dane osobowe w zgłoszonym zbiorze przetwarzane są z naruszeniem zasady art. 23 ust. 1 ustawy, bez podstawy prawnej upoważniającej wnioskodawcę do prowadzenia zgłoszonego zbioru danych

⁴⁷⁴ DPZRP-11-5-258/01

Wobec powyższego, Generalny Inspektor Ochrony Danych Osobowych, w drodze decyzji administracyjnej, odmówił rejestracji przedmiotowego zbioru danych osobowych i nakazał usunięcie danych ze zbioru.⁴⁷⁵

IV. Zaświadczenia

Zgodnie z art. 42 ust. 3 ustawy o ochronie danych osobowych, na wniosek osoby zainteresowanej może zostać wydane zaświadczenie o zarejestrowaniu zbioru danych.

W 2000 r. wydanych zostało 1890 zaświadczeń, z czego 1456 potwierdzało zarejestrowanie zbiorów danych zgłoszonych przez administratorów, o których mowa w art. 3 ust. 1 ustawy o ochronie danych osobowych, natomiast 434 - zgłoszonych przez podmioty określone w art. 3 ust. 2 ustawy. Żaden wniosek o wydanie zaświadczenia nie został załatwiony odmownie.

V. Wnioski

W roku 2000 Generalny Inspektor Ochrony Danych Osobowych dokonywał rejestracji zbiorów danych pochodzących z roku 1999. Zdecydowana ich większość została rozpatrzona. Wprowadzony przez ustawę termin (18 miesięcy od dnia wejścia w życie ustawy) na dopełnienie obowiązku rejestracyjnego przez podmioty prowadzące w dniu wejścia w życie ustawy zbiory danych osobowych, z jednej strony doprowadził do napływu w krótkim okresie czasu ogromnej liczby zgłoszeń do rejestracji, z drugiej zaś zmobilizował podmioty do szybkiego składania wniosków rejestracyjnych. Wnioskodawcami zgłoszeń były przede wszystkim podmioty określone w art. 3 ust. 1 ustawy, czyli szeroko rozumiana tzw. sfera publiczna. Mimo realizowania takich samych obowiązków nałożonych przepisami prawa, liczba zgłaszanych zbiorów danych przez analogiczne podmioty (np. gminy czy powiaty) była różna. Można domniemywać, że w kolejnych latach działalności Generalnego Inspektora Ochrony Danych Osobowych większość zgłaszanych do rejestracji zbiorów danych będzie pochodziła od podmiotów określonych w art. 3 ust. 2 ustawy, tj. od podmiotów należących do sektora prywatnego.

W odniesieniu do administratorów zbiorów danych podlegających rejestracji wyjaśniano, iż obowiązek rejestracji zbiorów danych powinien być dopełniony przed rozpoczęciem procesu przetwarzania danych w zbiorze (art. 46 ustawy).

⁴⁷⁵ GI/DRZDO/DEC/44/00; w 2001 r. strona złożyła w niniejszej sprawie skargę do Naczelnego Sądu Administracyjnego.

Zauważyć należy, iż w omawianym okresie sprawozdawczym szczególnie wiele wątpliwości wywoływała kwestia zasadności rejestracji zbiorów danych, których administratorem były, np. apteki, poradnie psychologiczno – pedagogiczne, czy lekarze prowadzący prywatne gabinety lekarskie i laboratoria medyczne. Administrator danych, zobowiązany z mocy art. 40 ustawy o ochronie danych osobowych do rejestracji zbioru danych, jest jednak zwolniony od spoczywającego na nim obowiązku rejestracji w sytuacjach określonych w art. 43 ust. 1 ustawy. Podmioty o których mowa w art. 2 ustawy o zakładach opieki zdrowotnej (tj. zakłady opieki zdrowotnej), jak również inny zakład, spełniający warunki określone w cytowanej ustawie, zwolnione są z rejestracji danych osób korzystających z ich usług medycznych na podstawie art. 43 ust. 1 pkt 5 ustawy o ochronie danych.⁴⁷⁶ Z obowiązku rejestracji zbiorów danych osobowych wyłączone są również poradnie psychologiczno – pedagogiczne oraz inne poradnie specjalistyczne.⁴⁷⁷ Wprawdzie przepisy, wskazujące zakres przedmiotowy świadczonych przez poradnie usług nie obowiązują od 1 lipca 2000 r., nie zmienia to faktu, iż wskazane poradnie świadczą usługi medyczne w rozumieniu ustawy o zakładach opieki zdrowotnej, zgodnie z którą świadczeniem zdrowotnym są działania służące zachowaniu, ratowaniu, przywracaniu i poprawie zdrowia oraz inne działania medyczne wynikające z procesu leczenia lub przepisów odrębnych regulujących zasady ich wykonywania, w szczególności związane z badaniem i terapią psychologiczną (art. 3 pkt 3).⁴⁷⁸ Zwolnienie obejmuje także administratorów prywatnych praktyk lekarskich, jak również osoby wykonujące zawód medyczny lub przez grupową praktykę lekarską,⁴⁷⁹ grupową praktykę pielęgniarek, położnych na zasadach określonych w odrębnych przepisach.⁴⁸⁰ W udzielanych odpowiedziach wielokrotnie podkreślano, iż zwolnienie z obowiązku rejestracji nie oznacza zwolnienia z pozostałych obowiązków nałożonych na administratora zbioru danych przez ustawę o ochronie danych osobowych, np. obowiązku informacyjnego czy obowiązku właściwego zabezpieczenia

⁴⁷⁶ Np. GI-DP-4/00/75, GI-DP-024/1283/00

⁴⁷⁷ GI-DP-724/00/904, GI-DP-403/1253/00

⁴⁷⁸ Na podstawie art. 74 w związku z art. 25 pkt 22 ustawy z dnia 21 stycznia 2000 r. o zmianie niektórych ustaw związanych z funkcjonowaniem administracji publicznej (Dz. U. Nr 12, poz. 136) rozporządzenie z dnia 11 czerwca 1993 r. w sprawie organizacji i zasad działania publicznych poradni psychologiczno – pedagogicznych oraz innych poradni specjalistycznych (Dz. U. Nr 67, poz. 322) utraciło moc prawną z dniem 1 lipca 2000 r. Minister właściwy do spraw oświaty i wychowania został upoważniony do wydania nowego rozporządzenia

⁴⁷⁹ GI-DP-024/1283/00, GI-DP-174/00/185

⁴⁸⁰ Zob. np. ustawa z dnia 5 lipca 1996 r. o zawodach pielęgniarki i położnej (Dz. U. Nr 91, poz. 410 z późn. zm.) oraz przepisy wykonawcze wydane na jej podstawie.

zbiorów danych.⁴⁸¹ Zasada ta dotyczy wszystkich podmiotów świadczących usługi medyczne.

W omawianym okresie sprawozdawczym do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło ponadto wiele zapytań dotyczących sposobu i warunków rejestracji zbiorów danych osobowych, które administratorzy danych przetwarzali w celach marketingowych. Generalny Inspektor wyjaśniał, iż obowiązkowi powyższemu podlegają zbiory danych prowadzonych zarówno w systemach informatycznych, jak i manualnych. W ocenie Generalnego Inspektora bez znaczenia z punktu prawnego jest fakt, czy administrator pozyskał dane jako gotową bazę danych, czy też sam zgromadził posiadany zbiór. Istotne jest natomiast, aby zbiór zgłoszony został do rejestracji przed przystąpieniem do przetwarzania danych. Rejestracja zbioru danych jest czynnością jednorazową. Po dokonaniu zgłoszenia, zgodnie z art. 41 ust. 2 ustawy, Generalny Inspektor powinien zostać poinformowany o ewentualnych zmianach, jakie nastąpiły w zakresie zgłoszonych informacji, np. oznaczenia podmiotu, zakresu i celu przetwarzanych danych.

W zakresie realizacji obowiązku rejestracji zbiorów danych mieściły się również pytania dotyczące *zbiorów doraźnych*.⁴⁸² Ustawa o ochronie danych osobowych zwolniła niektóre kategorie zbiorów z obowiązku rejestracji. Nie będzie podlegał rejestracji zbiór sporządzony doraźnie, a po wykorzystaniu niezwłocznie usuwany (art. 2 ust. 3 cytowanej ustawy). Do takiej kategorii zbiorów w zasadzie nie mają zastosowania przepisy ustawy o ochronie danych osobowych za wyjątkiem przepisów rozdziału 5 ustawy, dotyczących zabezpieczenia zbiorów danych. Generalny Inspektor podkreślił, iż warunkiem umożliwiającym zastosowanie dyspozycji art. 2 ust. 3 ustawy jest to, aby taki zbiór był utworzony z założenia doraźnie, a więc dla chwilowej potrzeby, a po wykorzystaniu dane osobowe w nim zawarte zostały usunięte lub poddane anonimizacji. Oznacza to, że można pozostawić tylko takie dane, których wykorzystanie nie umożliwi identyfikacji osób, co do ich tożsamości. Samo fizyczne wyeliminowanie danych ze zbioru nie czyni zadość wymogom ustawy – w żadnym bowiem wypadku nie mogą one zostać udostępnione osobom nieupoważnionym. Usuwanie danych powinno być efektywne, tzn. uniemożliwiać do nich wgląd w każdych okolicznościach, nawet po zakończeniu przechowywania w zbiorze.⁴⁸³ W przypadku przewidywania możliwości dalszego przetwarzania danych, zbiór taki należy zgłosić do rejestracji. I tak w przypadku, gdy firma wykorzystuje jednorazowo dane osobowe

⁴⁸¹ Zob. GI-DP-024/1311/00

⁴⁸² Np. GI-DP-90/00/27, GI-DIS-248/00

⁴⁸³ GI-DP-487/00/485

dla potrzeb, np. zorganizowanego konkursu i niezwłocznie po jego zakończeniu efektywnie dane usuwa czy anonimizuje, to działanie takie w ocenie Generalnego Inspektora nie stanowi naruszenia ustawy o ochronie danych osobowych.⁴⁸⁴ Jednakże byłoby niedopuszczalne przetwarzanie danych znajdujących się w tym zbiorze, także w innym celu (np. marketingowym). Stosownie do art. 49 ustawy, przetwarzanie w zbiorze danych, do których przetwarzania nie jest się uprawnionym podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Zgodnie z art. 50 ustawy, kto administrując zbiorem danych przechowuje w zbiorze dane osobowe niezgodnie z celem utworzenia zbioru, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Analiza spraw w roku sprawozdawczym wykazała, iż Kasy Chorych przetwarzały dane zawarte w prowadzonych przez siebie zbiorach danych, nie zgłaszając uprzednio zbiorów do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych. Kasy Chorych wprawdzie nie udzielają usług medycznych, ale zarządzają udzielanie przedmiotowych usług i w związku z tym w szerokim zakresie przetwarzają dane o stanie zdrowia osób ubezpieczonych. Z mocy art. 72 pkt 1 ustawy o powszechnym ubezpieczeniu zdrowotnym Kasy Chorych zostały zobligowane do prowadzenia ewidencji osób objętych ubezpieczeniem zdrowotnym. Ponadto, zgodnie z art. 16 ust. 2 ustawy z dnia 20 czerwca 1997 r. o zmianie ustawy o zakładach opieki zdrowotnej oraz o zmianie niektórych ustaw (Dz. U. Nr 104, poz. 661 z późn. zm.), Kasy Chorych prowadzą rejestr usług medycznych. W związku z powyższym na Kasach Chorych, jako administratorach danych od dnia ich powstania (tj. od 1 stycznia 1999 r.) spoczął obowiązek prowadzenia oraz zarejestrowania przedmiotowych zbiorów danych. Przez okres ponad 1,5 roku funkcjonowania Kas Chorych wiele Kas nie zgłosiło zbiorów danych znajdujących się w ich posiadaniu, wskutek czego Generalny Inspektor Ochrony Danych Osobowych złożył zawiadomienia o popełnieniu przestępstwa określonego w art. 53 ustawy o ochronie danych osobowych przez osoby sprawujące zarząd w poszczególnych Kasach Chorych do prokuratur właściwych ze względu na siedzibę danej Kasy.⁴⁸⁵ Większość spraw wszczętych wskutek złożenia przedmiotowych zawiadomień została zakończona umorzeniem postępowania uzasadnianym brakiem znamion czynu zabronionego (art. 17 § 1 pkt 2 K.p.k.) lub znikomą szkodliwością społeczną czynu (art. 17 § 1 pkt 3 K.p.k.).⁴⁸⁶ W takich sytuacjach Generalny Inspektor zwracając się do

⁴⁸⁴ Ibidem

⁴⁸⁵ GI/527/00, GI/443/00, GI/444/00, GI/442/00

⁴⁸⁶ Np. w sprawie o sygn. 4 Ds. 111/00/Św (GI-DP-1171/00)

Prokuratora Generalnego wnosił o podjęcie na nowo umorzonego postępowania przygotowawczego.⁴⁸⁷ Ponadto Generalny Inspektor w piśmie skierowanym do Prezesa Urzędu Nadzoru Ubezpieczeń Zdrowotnych przedstawił skargi dotyczące nieprawidłowego funkcjonowania Kas Chorych, w szczególności uchybienia Kas związane z niewykonywaniem obowiązku rejestracyjnego.⁴⁸⁸ Powyższe działania skutkowały zgłoszeniem do rejestracji przez wszystkie Kasy Chorych ww. zbiorów danych.⁴⁸⁹

Generalnemu Inspektorowi Ochrony Danych Osobowych zgłoszono ponadto do rejestracji zbiorów danych osobowych, które to *dane na podstawie umowy z firmą marketingową zostały wykorzystane jednorazowo, dla celów własnej akcji promocyjnej*.⁴⁹⁰ Generalny Inspektor uznał wówczas, że zgodnie z art. 2 ust. 3 ustawy o ochronie danych osobowych obowiązek rejestracji nie obciąża administratorów danych przetwarzanych w zbiorach danych sporządzanych doraźnie, wyłącznie ze względów technicznych, a po ich wykorzystaniu niezwłocznie usuwanych albo poddawanych anonimizacji.

W roku 2000 zbiory danych osobowych składane były przede wszystkim na nowym wzorze zgłoszenia. Charakteryzuje się on większym uproszczeniem w porównaniu ze wzorem obowiązującym do 4 grudnia 1999 r. W nowym wzorze zrezygnowano z opisowej części F stanowiącej informację o sposobie wypełnienia podstawowych wymagań technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Została ona podzielona na pola do zakreslenia lub wypełnienia. Zmiana ta wraz z korektami pozostałej części zgłoszenia zapewnia szybsze rejestrowanie wpływających zgłoszeń. W związku z tym, biorąc pod uwagę mniejszą w porównaniu z 1999 r. liczbę zgłoszonych do rejestracji zbiorów danych w roku 2000, można się spodziewać, że w roku 2001 zgłaszane zbiory danych osobowych będą rejestrowane na bieżąco.

Pomimo obowiązywania ustawy o ochronie danych osobowych od dnia 30 kwietnia 1998 r., wielu administratorów danych nie dopełniło wynikającego z przepisów ustawy obowiązku zgłoszenia do rejestracji posiadanych zbiorów danych osobowych. Zaniechanie tego obowiązku dotyczy także organów państwowych. Wykaz zbiorów danych osobowych,

⁴⁸⁷ Np. GI/894/00,

⁴⁸⁸ Pismo z dnia 10 listopada 2000 r., sygn. GI-DP-10/45

⁴⁸⁹ Szerzej w części Sprawozdania ... dotyczącej rejestracji zbiorów danych osobowych

⁴⁹⁰ GI-DP-403/1473/00

które powinny zostać zgłoszone do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych np. przez centralne organy państwowe zawarty jest w załączniku numer 4.

Część IV. ZAWIADOMIENIA O POPEŁNIENIU PRZESTĘPSTWA

W 2000 r. Generalny Inspektor Ochrony Danych Osobowych skierował w 46 przypadkach zawiadomienia o popełnieniu przestępstwa do organów ścigania. Przedmiotowe omówienie nie dotyczy przypadków wszczynania postępowania w sprawach o ochronę danych osobowych przez Policję i prokuraturę z urzędu, w związku ze stwierdzonymi bezpośrednio przez te organy naruszeniami prawa.

Uprawnienie Generalnego Inspektora do inicjowania postępowania przed organami ścigania w sprawach związanych z realizacją ustawy o ochronie danych osobowych jest realizacją ustawowego obowiązku nałożonego na organ powołany do badania przestrzegania przepisów o ochronie danych osobowych. Zgodnie z art. 19 ustawy o ochronie danych osobowych, w razie stwierdzenia, że działanie lub zaniechanie kierownika jednostki organizacyjnej, jej pracownika lub innej osoby fizycznej będącej administratorem danych wyczerpuje znamiona przestępstwa określonego w ustawie, Generalny Inspektor kieruje do organu powołanego do ścigania przestępstw zawiadomienie o popełnieniu przestępstwa, dołączając dowody dokumentujące podejrzenie.

Zawiadomienia skierowane do organów ścigania dotyczyły: bezprawnego przetwarzania danych - przetwarzania danych przez osoby nieuprawnione, tj. popełnienia przestępstwa z art. 49 ustawy o ochronie danych osobowych (16 spraw), niedopełnienia obowiązku informacyjnego, tj. popełnienia przestępstwa określonego w art. 54 ustawy (10 spraw), niedopełnienia obowiązku rejestracyjnego, tj. przestępstwa z art. 53 ustawy (8 spraw), nieodpowiedniego zabezpieczenia danych osobowych pochodzących ze zbioru danych, tj. popełnienia przestępstwa określonego w art. 51 ustawy (8 spraw), jak również przestępstwa określonego w art. 52 ustawy, tj. nieumyślnego naruszenia obowiązku zabezpieczenia danych (2 sprawy), przetwarzania niezgodnego z celem utworzenia zbioru, tj. przestępstwa z art. 50 ustawy (1 przypadek).

W dwóch przypadkach postępowania prowadzone przed organami ścigania w sprawie naruszenia przepisów ustawy o ochronie danych osobowych zostały zakończone przez prokuraturę skierowaniem do sądu aktu oskarżenia.

W pozostałych sprawach, po przeprowadzeniu postępowania przygotowawczego, wydawano postanowienia o odmowie wszczęcia postępowania (7 przypadki), bądź umarzono sprawy, wskazując jako podstawę umorzenia znikomą szkodliwość czynu (5 przypadków), albo brak ustawowych znamion czynu zabronionego (25 przypadków). W trzech przypadkach

nie stwierdzono popełnienia przestępstwa z uwagi na to, iż czynu nie popełniono. W innych przypadkach postępowanie zawieszano lub nie informowano Generalnego Inspektora o prowadzonym (lub umorzonym) postępowaniu.

W związku z powyższymi rozstrzygnięciami Generalny Inspektor zwracał się do Prokuratora Generalnego o uchylenie postanowienia (w 16 przypadkach), ale jedynie w 6 przypadkach wnioski te zostały uwzględnione i organy prokuratury przeprowadziły ponowne postępowanie sprawdzające zasadność złożonych zażaleń. Przedmiotowe postępowania w większości przypadków zostały zakończone wydaniem postanowienia o umorzeniu postępowania ze względu na przesłanki określone w art. 17 § 1 pkt 1 – 3 K.p.k. Należy przy tym zaznaczyć, że u podstaw umorzenia postępowania przez organy ścigania wielokrotnie znajdowała się niekonsekwentna postawa skarżących, którzy z jednej strony w postępowaniu przygotowawczym składali zeznania potwierdzające zasadność zawiadomienia o popełnieniu przestępstwa, a następnie stwierdzali, iż nie są zainteresowani prowadzeniem postępowania karnego w danej sprawie (w 7 przypadkach).⁴⁹¹ Uzasadnione wątpliwości budziły rozstrzygnięcia o umorzeniu postępowania z uwagi, iż czynu nie popełniono, w sytuacji istnienia dowodów wskazujących na naruszenie ustawy o ochronie danych osobowych.⁴⁹²

1. Sprawy rozpatrywane przez sąd

- 1.1. W związku ze skargami kierowanymi do Biura GODO, Generalny Inspektor Ochrony Danych Osobowych wszczął postępowanie wyjaśniające w sprawie udostępnienia przez zarządcę komisarycznego osobom nieupoważnionym listy uczestników wyjazdu studyjnego do Finlandii, zawierającą dane osobowe skarżących i osób trzecich. Jak wskazywali skarżący, w wydaniu Super Ekspresu opublikowano zdjęcie zarządcy komisarycznego, trzymającego w ręku przedmiotową listę w sposób umożliwiający odczytanie umieszczonych na niej danych osobowych w postaci: imienia, nazwiska, daty i miejsca urodzenia, miejsca pracy, adresu zamieszkania oraz numeru paszportu. W trakcie postępowania ustalono, iż ww. podmiot udostępnił listę uczestników wyjazdu studyjnego do Finlandii autorom materiału prasowego w celu opublikowania i w ten sposób umożliwił dostęp do danych szerokiemu kręgowi osób nieupoważnionych. W związku z powyższym, Generalny Inspektor zawiadomił prokuraturę o popełnieniu przestępstwa stypizowanego w art. 51 ustawy o ochronie danych osobowych. Prokuratura uznając

⁴⁹¹ Np. w sprawie prowadzonej przez Prokuraturę Rejonową Warszawa Wola, nr 6 Ds. 625/00, jak również w sprawie prowadzonej przez Prokuraturę Rejonową w Otwocku, nr 1 Ds. 527/00.

⁴⁹² Np. postanowienie Prokuratury Rejonowej Łódź Śródmieście Ds. 10048/00.

przedstawioną argumentację wszczęła postępowanie i skierowała akt oskarżenia do sądu.⁴⁹³

- 1.2. Generalny Inspektor przeprowadził postępowanie wyjaśniające w sprawie przetwarzania danych osobowych skarżącej przez firmę Euroglob Sp. z o. o. i Stella Sp. z o. o. Prezesi wskazanych Spółek oświadczyli, iż sporne dane osobowe pozyskali od BelaVita Sp. z o. o. W związku z faktem, że powyższa okoliczność nie znalazła potwierdzenia w wyjaśnieniach złożonych przez BelaVita, jak również wobec braku zgody osoby, której dane dotyczą na przetwarzanie jej danych przez Spółkę Euroglob i Stella GODO skierował do prokuratury zawiadomienie o popełnieniu przez wskazane podmioty przestępstwa określonego w art. 49 ust. 1 i art. 54 ustawy o ochronie danych osobowych. Ponadto w świetle zebranego materiału dowodowego Generalny Inspektor stwierdził, iż zarówno Prezes Euroglob Sp. z o. o., jak i Prezes Spółki Stella poświadczyli nieprawdę, tj. popełnili przestępstwo określone w art. 271 § k.k.⁴⁹⁴ W zakresie dotyczącym bezprawnego przetwarzania danych osobowych skarżącej i poświadczenia nieprawdy przez Prezesa Zarządu Euroglob Sp. z o. o., prokuratura, uwzględniając stanowisko Generalnego Inspektora, skierowała do sądu akt oskarżenia.⁴⁹⁵ W tym samym stanie faktycznym wobec Stella Sp. z o. o. prokuratura postępowanie umorzyła ze względu na brak znamion czynu zabronionego.⁴⁹⁶ W uzasadnieniu postanowienia prowadzący sprawę prokurator nie tylko nie odniósł się do argumentacji Generalnego Inspektora przedstawionej w zawiadomieniu, ale również błędnie określił czyn zabroniony, który był przedmiotem postępowania przygotowawczego. Na skutek pisma GODO skierowanego do Prokuratora Generalnego sprawa jest rozpatrywana ponownie.
- 1.3. W związku ze skargami dotyczącymi bezprawnego przetwarzania danych osobowych przez MediAdress Polonia Sp. z o. o., tj. przetwarzania danych osobowych skarżących pozyskanych od podmiotu mającego swoją siedzibę w Niemczech (MediAdress GmbH), pomimo wniesionego uprzednio sprzeciwu osoby, której dane dotyczą, Generalny Inspektor Ochrony Danych Osobowych złożył zawiadomienie o popełnieniu przestępstwa przez ww. Spółkę, tj. o naruszenie art. 49 ust. 1 ustawy o ochronie danych osobowych.⁴⁹⁷ Pomimo istnienia dowodów wskazujących bezspornie na fakt naruszenia przepisów ustawy, prokuratura w przedmiotowej sprawie wydała postanowienie o odmowie

⁴⁹³ Sprawa prowadzona przez Prokuraturę Rejonową w Giżycku, nr 1 Ds. 813/00.

⁴⁹⁴ GI-DIS-56/00/7000

⁴⁹⁵ Sprawa prowadzona przez Prokuraturę Rejonową w Sopocie, nr Ds. 1186/00.

⁴⁹⁶ Postanowienie Prokuratury Rejonowej w Gdyni, nr 4 Ds. 1799/00.

⁴⁹⁷ Postanowienie Prokuratury Rejonowej w Skierniewicach, nr Ds. 1682/00.

wszczęcia dochodzenia, uzasadniając swoje stanowisko faktem dwukrotnego nadesłania na adres zamieszkania skarżącej informacji o wykreśleniu jej ze zbioru danych przez administratora. W piśmie do prokuratury rejonowej GODO zarzucił prokuraturze niezrozumienie przepisów ustawy o ochronie danych osobowych, a w szczególności błędną interpretację pojęcia przetwarzania danych osobowych. Generalny Inspektor podkreślił, iż dwukrotne nadesłanie informacji po sprzeciwie i żądaniu usunięcia danych ze zbioru jest niezaprzeczalnym dowodem świadczącym o pozostawianiu danych w zbiorze i dalszym ich przetwarzaniu. Ponadto prokurator dowolnie interpretował wnioski pokontrolne, nie przedstawiając żadnych dowodów uzasadniających zajęte w sprawie stanowisko. Przedmiotowe zażalenie prokuratura okręgowa skierowała do rozpoznania przez sąd. Sprawa jest w toku.⁴⁹⁸

2. Pozostałe sprawy zakończone umorzeniem postępowań przez prokuraturę oraz odmową wszczęcia postępowania.

Liczna grupa zawiadomień o popełnieniu przestępstwa dotyczyła niewykonania przez administratora danych obowiązku informacyjnego określonego w ustawie o ochronie danych osobowych (10 przypadków). We wszystkich tych przypadkach podstawą umorzenia było stwierdzenie braku ustawowych znamion czynu zabronionego⁴⁹⁹ lub znikomej społecznej szkodliwości czynu,⁵⁰⁰ jak również stwierdzenie, iż zarzucanego czynu nie popełniono.⁵⁰¹

Administrator danych, który nie wykonuje spoczywającego na nim obowiązku informacyjnego względem osoby, której dane dotyczą, podlega sankcjom karnym określonym w art. 54 ustawy o ochronie danych osobowych. Zgodnie z treścią wskazanego przepisu, kto administrując zbiorem danych nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w niniejszej ustawie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Przepisy ustawy o ochronie danych osobowych nakładają na administratora danych obowiązek poinformowania osoby, której dane dotyczą – w momencie zbierania danych (art. 24 ustawy), bądź bezpośrednio po utrwaleniu danych, jeśli są one zbierane nie od osoby,

⁴⁹⁸ Pismo Sądu Rejonowego w Skierniewicach, sygn. akt. II KOI 124/00.

⁴⁹⁹ Sprawa prowadzona przez Prokuraturę w Otwocku, nr 1 Ds. 97/2000, nr 1 Ds. 839/00.

⁵⁰⁰ Postanowienie Prokuratury Rejonowej Warszawa Mokotów, nr 2 Ds. 173/00V.

⁵⁰¹ Postanowienie Prokuratury Rejonowej w Otwocku, nr 1 Ds. 536/00, nr 1 Ds. 527/00, nr 1Ds. 1017/00.

której dane dotyczą (art. 25 ustawy) – o nazwie i siedzibie administratora danych, celu i zakresie zbierania, źródle danych oraz uprawnieniach wynikających z ustawy o ochronie danych osobowych. Zarówno prawny obowiązek poinformowania, jak i sankcje karne mają zagwarantować osobom, których dane dotyczą, realizację przysługujących im konstytucyjnie praw.

W przekonaniu wielu organów ścigania częściowe wykonanie obowiązku informacyjnego ekskulowało administratorów danych, a konsekwencją takiego stanowiska było umarzanie spraw z uwagi na znikomą społeczną szkodliwość czynu.⁵⁰² Jak wykazało jedno z postępowań wyjaśniających prowadzonych wobec Telewizji Kablowej TVM S.A. na formularzu umowy abonenckiej umieszczano jedynie adres siedziby i pełną nazwę Spółki. Brakowało natomiast pozostałych informacji określonych w art. 24 ustawy, które nie były udzielane ani odrębnym pismem, ani ustnie przy zawieraniu umowy. W niniejszej sprawie, w postanowieniu o odmowie wszczęcia dochodzenia, prokuratura wyraźnie potwierdziła, iż obowiązek z art. 24 ustawy nie jest realizowany, lecz jednocześnie stwierdzono, że nie zachodzi uzasadnione podejrzenie popełnienia przestępstwa.⁵⁰³ Interwencja Generalnego Inspektora Ochrony Danych Osobowych doprowadziła do uchylecia powyższego postanowienia. Obecnie sprawa podlega dalszemu rozpoznaniu.⁵⁰⁴

W uzasadnieniu postanowienia o umorzeniu postępowania wobec Art File Sp. z o. o. wskazano, iż poprzez jednokrotne wykorzystanie danych skarżącego za pośrednictwem osób trzecich (tj. Reader's Digest Przegląd Sp. z o. o.), administrator danych nie ma obowiązku informowania osoby, której dane dotyczą, o uprawnieniach wskazanych w art. 25 ust. 1 ustawy o ochronie danych osobowych.⁵⁰⁵ Generalny Inspektor w piśmie do prokuratury apelacyjnej podkreślił, że samo przechowywanie danych - zgodnie z treścią art. 7 pkt 2 ustawy - jest przetwarzaniem, jak również wykazał, że Spółka przetwarzała dane kwestionowane przez skarżącego przed ich udostępnieniem Reader's Digest Przegląd Sp. z o. o., podczas udostępnienia, jak i po fakcie udostępnienia. Argumentacja Generalnego Inspektora została podzielona przez prokuraturę apelacyjną i w konsekwencji prokurator rejonowy, w trybie nadzoru służbowego, został zobligowany do podjęcia na nowo umorzonego postępowania.

⁵⁰² Np. w postanowieniu Prokuratury Rejonowej Warszawa Mokotów, nr 2 Ds. 2223/00/II.

⁵⁰³ Postanowienie Prokuratury Rejonowej Warszawa Śródmieście, nr 6 Ds. 433/00/VIII.

⁵⁰⁴ Zawiadomienie Prokuratury Okręgowej z dnia 26 czerwca 2000 r., nr I 4 Dsn 465/00Śr.

⁵⁰⁵ Sprawa prowadzona przez Prokuraturę Rejonową Warszawa Mokotów, nr 3 Ds. 483/00/VII.

W omawianym okresie sprawozdawczym administratorem danych dokonującym najczęstszych naruszeń art. 24 i 25 ustawy o ochronie danych osobowych była ZXY Sp. z o. o. Firma ta w ramach prowadzonej działalności marketingowej rozsyłała ulotki reklamowe do wszystkich osób, których dane znajdowały się w bazach danych zakupionych przez nią od innych podmiotów, np. od Salonu Nowości Sp. z o. o. i od Willemse Ogrody Sp. z o. o. Przeprowadzone postępowania wyjaśniające wykazały, iż bezpośrednio po zgromadzeniu danych osobowych skarżących, tj. przed wysłaniem ofert promocyjnych, Spółka nie wykonała obowiązku informacyjnego określonego w art. 25 ustawy. W wyniku powyższych ustaleń Generalny Inspektor skierował do organów ścigania 5 zawiadomień o popełnieniu przestępstwa przez ww. Spółkę. Prokuratura nie podzieliła stanowiska Generalnego Inspektora i uznała, że w przesłanych pokrzywdzonym ofertach promocyjnych został wykonany obowiązek informacyjny. W konsekwencji prowadzone postępowania przygotowawcze zostały umorzone wobec braku ustawowych znamion czynu zabronionego.⁵⁰⁶ Składając zażalenia na powyższe postanowienia, Generalny Inspektor zwracał uwagę organom ścigania na niezrozumienie istoty przepisu art. 25 ustawy, którego treść wskazuje, iż osoby, której dane są przetwarzane w celach marketingowych powinny mieć możliwość skorzystania z uprawnień przyznanych im przez ustawę, m.in. prawo złożenia sprzeciwu na podstawie art. 32 ust. 1 pkt 8 ustawy. ZXY Sp. z o. o. wykonując obowiązek informacyjny dopiero z chwilą przesłania oferty reklamowej, pozbawiła tym samym osoby, których dane dotyczą, realizacji ustawowych uprawnień.⁵⁰⁷

Uzasadnienia postanowień o umorzeniu postępowania wielokrotnie nacechowane były wewnętrzną sprzecznością i brakiem konsekwencji w podnoszonej argumentacji. W sprawie dotyczącej niedopełnienia obowiązku informacyjnego przez Fiat Auto Poland S.A. prokurator oceniając zebrany materiał dowodowy uznał, że osoby odpowiedzialne za przetwarzanie danych osobowych w zbiorach prowadzonych przez ww. firmę wyczerpały znamiona przestępstwa z art. 54 ustawy o ochronie danych osobowych, albowiem nie informowały skarżących o możliwości wniesienia sprzeciwu wobec przetwarzania ich danych w celach marketingowych, jak również nie podzielił argumentacji Fiat Auto Poland S.A. w przedmiocie jednorazowego wykorzystania danych osobowych pokrzywdzonego. W dalszej części wskazanego uzasadnienia prokurator wywodził, iż dla bytu przestępstwa z art. 54 ustawy niewystarczającym jest wypełnienie znamion określonych w tym przepisie i

⁵⁰⁶ Sprawy prowadzone pod sygn. 1 Ds. 536/00, 1 Ds. 527/00, 1 Ds. 97/00, 1 Ds. 1017/00, 1 ds. 839/00.

⁵⁰⁷ Sprawa prowadzona przez Prokuraturę Apelacyjną w Warszawie, sygn. Ap I Dsn 141/01/W-wa, Ap I Dsn 142/01/W-wa.

podkreślił, iż przetwarzanie danych przez Spółkę miało charakter jednorazowy i było zgodne z przepisami ustawy o ochronie danych osobowych.⁵⁰⁸ W konsekwencji wydane zostało postanowienie o odmowie wszczęcia postępowania. Generalny Inspektor Ochrony Danych Osobowych zauważył, iż odmowa wszczęcia postępowania karnego z powodu jego znikomej społecznej szkodliwości, mimo że administrator danych wypełnił swym działaniem znamiona czynu przestępczego, może prowadzić do powszechnego przekonania, że przepisy karne ustawy o ochronie danych osobowych można bezkarnie naruszać. W piśmie do prokuratury wskazano ponadto na coraz powszechniejszą praktykę firm, które prowadząc akcje marketingowe, nastawione na przynoszenie zysków, z pełną świadomością nie wykonują obowiązku informacyjnego. Działania takie budzą uzasadniony społeczny sprzeciw i z tego względu nieuzasadnionym jest twierdzenie o ich znikomej społecznej szkodliwości.

Zaskarżając wydane na podstawie art. 17 § 1 pkt 3 K.p.k. orzeczenia organów ścigania, Generalny Inspektor wielokrotnie podkreślał, iż oceny społecznej szkodliwości czynu dokonał sam ustawodawca decydując się na penalizację tego rodzaju zachowania. O ile zatem nie zachodzą żadne szczególne okoliczności podmiotowe lub przedmiotowe czynu, jest on według oceny ustawodawcy społecznie szkodliwy w stopniu wystarczającym do penalizacji takiego zachowania. Ponieważ w sprawach rozpatrywanych przez prokuraturę takie okoliczności zwykle nie zachodziły, często wydawane w I instancji rozstrzygnięcia nosiły cechy arbitralnych, nie popartych żadnymi dowodami, twierdzeń.

Liczna grupa umorzeń postępowań przygotowawczych związana była z niekonsekwentną postawą samych pokrzywdzonych (7 przypadków). Np. w sprawie związanej z przetwarzaniem danych osobowych skarżącej przez Medstar Sp. z o. o. prokuratura argumentując umorzenie postępowania wobec znikomego stopnia społecznej szkodliwości podkreśliła, że do takiej oceny sprawy uprawnia ją m.in. poczucie szkody pokrzywdzonej, która nie jest zainteresowana prowadzeniem postępowania karnego w tej sprawie.⁵⁰⁹

W 16 przypadkach Generalny Inspektor Ochrony Danych Osobowych zawiadamiał organy ścigania o wypełnieniu przez administratorów danych dyspozycji art. 49 ustawy o ochronie danych osobowych. Zgodnie z treścią ust. 1 wskazanego przepisu, kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch. W przypadku, gdy ww. działania dotyczą danych

⁵⁰⁸ Postanowienie Prokuratury Rejonowej Warszawa Mokotów, nr 2 Ds. 2223/00/II.

szczególnie chronionych (tj. określonych w art. 27 ust. 1 ustawy), sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech (art. 49 ust. 2 ustawy). Przykładem administratora danych realizującego proces przetwarzania danych, w sytuacji gdy przetwarzanie należy uznać za niedopuszczalne jest firma Reader's Digest Przegląd Sp. z o. o., która pomimo wniesienia przez skarżących sprzeciwu określonego w art. 32 ust. 1 pkt 8 ustawy, przetwarzała w dalszym ciągu zakwestionowane dane osobowe.⁵¹⁰ Obecnie w prokuraturze toczą się postępowania przygotowawcze mające na celu wyjaśnienie zasadności czterech złożonych przez Generalnego Inspektora zawiadomień o popełnieniu przestępstwa z art. 49 ust. 1 ustawy przez ww. Spółkę.⁵¹¹

Zagadnienie nieuprawnionego przetwarzania danych osobowych organy ścigania rozstrzygały najczęściej poprzez umorzenie postępowania ze względu na brak znamion czynu zabronionego, albo poprzez odmowę wszczęcia postępowania.⁵¹² W jednym tylko przypadku ocena zasadności przypisania sprawcy czynu znamion przestępstwa określonego w art. 49 ustawy została poddana ostatecznej kontroli sądu.

Podobne rozstrzygnięcia zapadały w związku z zawiadamianiem organów ścigania o udostępnieniu danych osobom nieupoważnionym. Naruszenie obowiązku właściwego zabezpieczenia danych osobowych zostało spenalizowane w art. 51 ustawy o ochronie danych osobowych, zgodnie z którym, kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności lub pozbawienia wolności do lat dwóch. W związku z wypełnieniem przez administratorów danych znamion określonych w cytowanym przepisie, Generalny Inspektor Ochrony Danych Osobowych skierował 8 zawiadomień o popełnieniu przestępstwa.

Z treści jednej ze skarg, zakończonej skierowaniem zawiadomienia o popełnieniu przestępstwa określonego w art. 51 ustawy, wynikało, że Główny Urząd Cel bezprawnie udostępnił dane skarżącego z akt sprawy karno – skarbowej prowadzonej przez jeden z oddziałów, Związku Żołnierzy Armii Krajowej. Przeprowadzone przez GODO postępowanie potwierdziło okoliczności przytoczone w skardze – orzeczenie karne uznające skarżącego za winnego popełnienia przestępstwa skarbowego zostało udostępnione podmiotowi wskazanemu w skardze, który żądanie udostępnienia wnioskowanych danych

⁵⁰⁹ Postanowienie Prokuratury Rejonowej Warszawa Wola, nr 6 Ds. 625/00.

⁵¹⁰ Sprawa prowadzona przez Prokuraturę Rejonową Warszawa Wola, nr 6 Ds. 524/99, nr 6 Ds. 226/2000, nr 6 Ds. 179/2000, nr 6 Ds. 134/2000.

⁵¹¹ Ibidem

⁵¹² Np. Postanowienie Prokuratury w Sopocie, nr Ds. 361/00.

uzasadniał przesłanką określoną w art. 23 ust. 1 pkt 4 ustawy o ochronie danych osobowych (tj. realizacją własnych zadań statutowych). Podkreślając rygoryzm art. 28 ust. 1 ustawy w zawiadomieniu o popełnieniu przestępstwa Generalny Inspektor wskazał, że dane o karalności skarżącego mogą być przetwarzane wyłącznie w oparciu o przesłankę ustawową. Tym samym udostępnienie Związkowi danych skarżącego na innej podstawie prawnej niż ustawa uznano za działanie nieuprawnione. Analiza przedstawionej sprawy dokonana przez organy ścigania doprowadziła do wydania postanowienia o odmowie wszczęcia dochodzenia.⁵¹³ W sporządzonym lakonicznie uzasadnieniu przedmiotowego postanowienia nie wykazano, z jakich powodów przyjęto brak naruszenia przepisów ustawy, jak i nie odniesiono się do argumentacji zawartej w zawiadomieniu o przestępstwie. W związku z powyższym Generalny Inspektor, zwrócił się o uchylenie postanowienia i ponowne rozpatrzenie sprawy. Powyższe zażalenie zostało uwzględnione i obecnie sprawa podlega dalszemu rozpoznaniu.

Zawiadomienia o popełnieniu przestępstwa dotyczyły ponadto przetwarzania danych osobowych niezgodnie z celem utworzenia zbioru, tj. przestępstwa określonego w art. 50 ustawy o ochronie danych osobowych. Wskutek skargi klienta Banku Śląskiego S.A. skierowanej do Biura GODO zostało wszczęte postępowanie wyjaśniające, które doprowadziło do ustalenia, iż wskazany Bank przetwarza dane osobowe byłych klientów w celach marketingowych, pomimo braku wyraźnej zgody na przetwarzanie danych osobowych w celach innych, niż realizacja umowy z Bankiem. Prokuratura nie podzieliła stanowiska Generalnego Inspektora w przedmiotowej sprawie i umorzyła postępowanie ze względu na brak znamion czynu zabronionego.⁵¹⁴ Stanowisko zajęte w sprawie prokurator umotywował lapidarnie brakiem umyślności po stronie administratora danych.

Należy zaznaczyć, iż w sześciu przypadkach organy nadzorujące pracę organów ścigania (np. prokuratury okręgowe, apelacyjne, Prokurator Generalny), uznając argumenty Generalnego Inspektora, uwzględniały wnioski o uchylenie postanowień I instancji, jednakże żadne z zapadłych następnie rozstrzygnięć nie doprowadziło do skierowania aktu oskarżenia do sądu wobec podmiotów winnych naruszeń ustawy o ochronie danych osobowych.

Przykładem sprawy wielokrotnie rozpatrywanej przez organy ścigania, która do tej pory nie zakończyła się sformułowaniem aktu oskarżenia jest sprawa dotycząca umieszczenia na śmietniku za budynkiem Sądu Rejonowego we Włocławku – Roki Sądowe w Aleksandrowie Kujawskim, akt sądowych, dowodów rzeczowych, wypisów aktów notarialnych i innych dokumentów zawierających dane osobowe stron i uczestników

⁵¹³ Postanowienie Prokuratury Rejonowej Warszawa Śródmieście, nr 6 Ds. 1841/00/V.

postępowania przed organami sprawiedliwości. Informacja o udostępnieniu przedmiotowej dokumentacji osobom nieupoważnionym dotarła do Generalnego Inspektora Ochrony Danych Osobowych za pośrednictwem środków masowego przekazu w roku 1999 i od tego momentu Generalny Inspektor podejmował działania w celu ustalenia osób winnych naruszeń ustawy o ochronie danych osobowych. Pomimo trzykrotnie wszczynanych postępowań, w których zebrano materiał dowodowy, wskazujący na naruszenie art. 51 i 52 ustawy o ochronie danych osobowych, jak również art. 231 § 1 K.k., organy ścigania umarzały postępowanie z uwagi na brak ustawowych znamion czynu zabronionego. Należy przy tym zaznaczyć, że uzasadnienia tych postanowień stały w rażącej sprzeczności z ich sentencją. Cechowała je niekonsekwencja wywodów, wewnętrzna sprzeczność, a miejscami całkowity brak logiki.

Z treści uzasadnienia Prokuratury Okręgowej we Włocławku wynikało, że dokumenty pozostawione na śmietniku, w większości dokumenty zawierające dane o skazaniu, były materiałami, za których zniszczenie odpowiadała powołana do tego specjalna komisja likwidacyjna. Ustalono ponadto, że członkowie wskazanej komisji podpisali protokoły zniszczenia przedmiotów przed dokonaniem czynności całkowitego ich zniszczenia, a następnie dokumenty umieszczono w pomieszczeniu gospodarczym używanym przez osoby zajmujące się sprzątaniami budynku sądu, które w ramach swoich obowiązków wyniosły materiały na śmietnik w przekonaniu o ich zbędności. Z ustalonego przez prokuraturę stanu faktycznego wynikało również, że członkowie komisji pozostawiając niezabezpieczone dokumenty w pomieszczeniu gospodarczym nie uczynili żadnej wzmianki (np. w protokole dokumentów już zlikwidowanych) o ilości i rodzaju dokumentów nie zniszczonych, nie uprzedzili też w żadnej formie osób ewentualnie korzystających z ww. pomieszczenia o niedopuszczalności dokonywania jakichkolwiek czynności z nimi związanych. W świetle powyższego niezrozumiała wydawała się argumentacja prokuratora okręgowego, który w dalszej części uzasadnienia umorzenia postępowania wywodził, iż działanie członków komisji było postępowaniem z uwzględnieniem należytej staranności i sumienności oraz logicznego zachowania wynikającego z nabytego doświadczenia. Uznając postępowanie członków Komisji za działania nie wypełniające znamion art. 51 i 52 ustawy o ochronie danych osobowych, prokuratura wykazała nieznaną sobie podstawowych pojęć tej ustawy, a przede wszystkim pojęcia administratora danych, przetwarzania danych oraz zakresu obowiązku zabezpieczenia danych osobowych. W opinii prokuratury, skoro działania osób odpowiedzialnych za zniszczenie dokumentów zmierzały do ich zniszczenia i w

⁵¹⁴ Postanowienie Prokuratury Rejonowej Katowice Centrum Zachód, nr 1 Ds. 410/00/ Z.

znacznej mierze czynności te zostały dokonane, to tym samym nie doszło do naruszenia obowiązku właściwego zabezpieczenia danych.⁵¹⁵

Generalny Inspektor w zażaleniu na przedmiotowe postanowienie podkreślił, że podmiotem odpowiedzialnym ustawowo za właściwe zabezpieczenie danych osobowych pozostawał administrator zbioru, tj. Sąd Rejonowy we Włocławku – Roki Sądowe w Aleksandrowie Kujawskim, reprezentowany przez Prezesa Sądu. Organowi II instancji wykazano ponadto wiele sprzeczności w strukturze uzasadnienia Prokuratury Okręgowej we Włocławku, która z jednej strony twierdziła, że przeprowadzone dowody nie pozwoliły na wskazanie okoliczności, w jakich pisma zawierające dane osobowe znalazły się na śmietniku, jak również nie pozwoliły na ustalenie osób odpowiedzialnych za zniszczenie tych pism, a następnie stwierdzono, że umieszczenie na śmietniku przedmiotów zbędnych dla postępowania sądowego było samowolnym działaniem sprzątaczek, podjętym bez wiedzy osób odpowiedzialnych za zniszczenie dokumentów. Generalny Inspektor odnosząc się do ustalonego przez organy ścigania stanu faktycznego wskazał ponadto na naganność praktyki stosowanej przez członków komisji likwidacyjnej (w skład której wchodził również sędziowie), polegającej na podpisywaniu protokołów zniszczenia przedmiotów przed dokonaniem tej czynności.

Pomimo uwzględnienia zażalenia przez organ odwoławczy i ponownego rozpatrzenia sprawy przez Prokuraturę Okręgową w Bydgoszczy, postępowanie ponownie umorzono ze względu na brak znamion czynu zabronionego, przy czym argumentacja stojąca u podłoża tego rozstrzygnięcia była tożsama z twierdzeniami przytaczanymi we wcześniej wydanych orzeczeniach organów ścigania.⁵¹⁶ Interpretacja poglądów Prokuratury prowadziła do wniosku, iż brak przepisów szczególnych regulujących tryb i sposób niszczenia dokumentacji o skazaniach, jak również luka prawna w obowiązujących przepisach odnośnie zasad i formy dokumentowania czynności niszczenia może być usprawiedliwieniem dla wykształcenia i stosowania praktyki podpisywania dokumentów potwierdzających nieprawdziwy stan faktyczny. Po raz kolejny treść umorzenia wskazywała na niezrozumienie istoty przepisów ustawy o ochronie danych osobowych. Zamiar zniszczenia całości dokumentacji utożsamiono z należytym wywiązaniem się z obowiązku zabezpieczenia danych niezanonimizowanych. Uzasadnienie umorzenia było niespójne i nielogiczne. Z jednej strony przedstawiony stan faktyczny prokuratura określiła jako pozwalający na przypisanie członkom komisji czynu niedopełnienia obowiązków w zakresie zabezpieczenia danych

⁵¹⁵ Postanowienie Prokuratury Okręgowej we Włocławku, nr I Ds. 21/99.

osobowych, a następnie w sentencji postanowienia postępowanie umorzono z uwagi na brak znamion czynu zabronionego.

Należy podkreślić, iż w żadnym z postanowień wydanych w opisywanej sprawie w sposób bezpośredni nie wskazano osób odpowiedzialnych za umieszczenie na śmietniku danych osobowych zawartych w aktach sądowych, do których dostęp miały osoby nieupoważnione. Dotychczasowe ustalenia organów ścigania prowadzą do bezskarności administratora danych. Obecnie wskutek kolejnego wniosku Generalnego Inspektora Ochrony Danych Osobowych o ponowne podjęcie sprawy Prokurator Generalny zobowiązał Prokuratora Apelacyjnego w Gdańsku do ponownego przeprowadzenia postępowania.⁵¹⁷

W ośmiu przypadkach umorzeń postępowań, zawiadomienie ze strony Generalnego Inspektora Ochrony Danych Osobowych dotyczyło niedopełnienia obowiązku rejestracji zbioru danych osobowych, w tym cztery spośród nich dotyczyły niezgłoszenia do rejestracji zbiorów danych przez Kasy Chorych, tj. Lubuską Regionalną Kasę Chorych, Warmińsko - Mazurską Regionalną Kasę Chorych, Podlaską Regionalną Kasę Chorych oraz Kujawsko - Pomorską Regionalną Kasę Chorych. Biorąc pod uwagę tożsamość stanów faktycznych i prawnych znajdujących się u podłoża przedmiotowych zawiadomień wydawano rozstrzygnięcia o umorzeniu postępowania ze względu na znikomą społeczną szkodliwość czynu, brak znamion czynu zabronionego, albo też z uwagi na brak danych dostatecznie uzasadniających popełnienie przestępstwa. Rozstrzygnięcia organów ścigania opierały się głównie na przyjęciu błędnej wykładni przepisów ustawy o ochronie danych osobowych, a w szczególności na niezrozumieniu istoty obowiązku rejestracyjnego, którego wykonanie obciąża administratora danych przed rozpoczęciem procesu przetwarzania danych w zbiorze. Powyższy obowiązek nie może być zatem realizowany w trakcie lub po zakończeniu przetwarzania danych osobowych. W umorzeniu postępowania wobec osób sprawujących zarząd w Lubuskiej Regionalnej Kasie Chorych, prokurator pomimo potwierdzenia okoliczności niewypełnienia obowiązku rejestracji zbiorów danych, w konkluzji uzasadnienia przyjął twierdzenie przeciwne i uznał, że postępowanie osób odpowiedzialnych za zarejestrowanie danych nie wykazuje lekceważącego stosunku do dyrektyw ustawodawcy i nie może być uznane za naganne. Dla przekreślenia bytu przestępstwa określonego w art. 53 ustawy o ochronie danych osobowych, prokurator uznał za wystarczający fakt zaistnienia czynników zewnętrznych, determinujących zachowanie dyrektorów Lubuskiej Kasy Chorych. Do takich czynników zaliczył, np. zmiany w strukturze organizacyjnej Kasy (tj. częste rotacje

⁵¹⁶ Postanowienie Prokuratury Okręgowej w Bydgoszczy, nr V Ds. 24/00.

na stanowisku dyrektora Kasy), brak całości zbioru danych osób ubezpieczonych, problemy techniczne, zbyt krótki okres na sporządzenie wniosku o rejestrację. W zażaleniu na przedmiotowe postanowienie Generalny Inspektor wskazał na nieprawidłowość powyższej interpretacji i wyjaśnił, iż rejestracja zbioru danych nie polega na zgłoszeniu wszystkich zgromadzonych danych, ale na zgłoszeniu pewnej struktury, która nie zależy od ilości danych. Ocena przytoczonych przez prokuratora okoliczności mogłaby zatem wpływać na stopień społecznej szkodliwości, ewentualnie wymiar kary. Nie może być natomiast podstawą ustalenia braku znamion czynu opisanego w art. 53 ustawy o ochronie danych osobowych.⁵¹⁸ Argumentacja Generalnego Inspektora została w pełni podzielona przez organ odwoławczy i w konsekwencji sprawa została podjęta na nowo.⁵¹⁹

W analogicznej sprawie wobec osób sprawujących zarząd w Warmińsko – Mazurskiej Regionalnej Kasie Chorych, które nie dopełniły obowiązku zgłoszenia do rejestracji zbiorów danych Kasy, postępowanie umorzono ze względu na brak danych dostatecznie uzasadniających podejrzenie popełnienia przestępstwa.⁵²⁰ Również i w tej sprawie rozstrzygnięcie zagadnienia niezarejestrowania zbiorów danych osobowych przez Kasę Chorych oparto na błędnym przekonaniu, iż zbiorem danych podlegającym obowiązkowi rejestracji jest jedynie zbiór o stałej strukturze i niezmiennym składzie osób ubezpieczonych. Podobną nieznajomością przepisów ustawy o ochronie danych osobowych wykazała się prokuratura okręgowa, która rozpatrując wniosek Generalnego Inspektora o ponowne podjęcie sprawy zaakcentowała wprawdzie nietrafność orzeczenia wydanego przez organ I instancji, jednakże ze względu na bliżej nieokreślone przesłanki odmówiła podjęcia postępowania w sprawie. Odmowa wszczęcia postępowania w sprawie niedopełnienia obowiązku rejestracyjnego przez Warmińsko – Mazurską Kasę Chorych wydaje się tym bardziej niezrozumiała, iż w ocenie prokuratora okręgowego poczynione ustalenia i zebrany materiał dowodowy przemawiały za zmianą sentencji orzeczenia prokuratury rejonowej.⁵²¹

W sprawach związanych z umorzeniem postępowania z art. 53 ustawy w jednym tylko przypadku zostało wydane polecenie ponownego rozpatrzenia zasadności rozstrzygnięcia zapadłego w pierwszej instancji i zbadania akt dochodzenia.⁵²² Natomiast w sprawie niedopełnienia obowiązku rejestracji zbioru przez osoby sprawujące zarząd w

⁵¹⁷ Pismo z dnia 21 czerwca 2000 r., znak: PR II Dsn 238/99

⁵¹⁸ GI/894/00

⁵¹⁹ Pismo z dnia 15 listopada 2000 r., znak I Dsn 254/00/ZG

⁵²⁰ Postanowienie Prokuratury Rejonowej Olsztyn - Południe, nr 1 Ds. 394/00

⁵²¹ Ap. I Dsn 254/01/OL

⁵²² Pismo z dnia 7 listopada 2000 r., znak Ap.I-Dsn-296/00/ZG

Polskich Kolejach Państwowych do tej pory Generalny Inspektor nie został poinformowany o jakichkolwiek podjętych przez organy ścigania czynnościach wyjaśniających.⁵²³

Podkreślić należy, iż w niektórych sprawach Generalnego Inspektora zawiadamiano o wynikach prowadzonego postępowania po 8-10 miesiącach, przy czym wielokrotnie organy rozpatrujące sprawę ograniczały się do przesłania krótkiej informacji o umorzeniu postępowania bez przesłania treści uzasadnienia rozstrzygnięcia.⁵²⁴ W jednym tylko przypadku Generalnego Inspektora powiadomiono, iż z uwagi na obszerność czynności procesowych postępowanie zostanie zakończone po upływie 6-miesięcznego terminu wskazanego w przepisach procedury karnej.⁵²⁵ W kilku przypadkach Generalny Inspektor nie został w ogóle poinformowany, czy sprawa dotycząca naruszenia przepisów ustawy o ochronie danych osobowych pozostaje przedmiotem zainteresowania organów ścigania.⁵²⁶

W wielu postanowieniach prokuratorzy wskazywali błędne podstawy prawne umorzeń. Reakcją organów nadrzędnych nadzorujących proces orzekania w I instancji było wówczas stwierdzenie, iż okoliczność powołania niewłaściwej podstawy prawnej, np. umorzenia wobec zaistnienia art. 17 § 1 pkt 1 K.p.k. zamiast art. 17 § 1 pkt 2 K.p.k., nie uzasadnia podjęcia na nowo umorzonych w sprawie dochodzeń.⁵²⁷

Doświadczenia z trzech lat działalności Generalnego Inspektora Ochrony Danych Osobowych wskazują, że mimo powtarzających się przypadków stwierdzenia naruszenia przepisów ustawy o ochronie danych osobowych, zebrania materiału dowodowego i przekazania sprawy wraz z zawiadomieniem do stosownych organów ścigania, organy te rzadko kierują sprawy na drogę sądową. O ile w roku 1999 w trzech przypadkach doszło do rozpatrzenia przez sądy spraw z zakresu ochrony danych osobowych, w roku 2000 skierowano do sądu dwa akty oskarżenia potwierdzające zasadność argumentacji przytoczonej przez Generalnego Inspektora w zawiadomieniu o popełnieniu przestępstwa.

Wewnętrzna niespójność twierdzeń zawartych w rozstrzygnięciach organów ścigania, sprzeczność sentencji z uzasadnieniami postanowień, przywoływanie błędnych przepisów karnych ustawy o ochronie danych osobowych wskazują jednoznacznie na brak zrozumienia istoty tej ustawy oraz często powierzchowne i zbyt łagodne traktowanie podmiotów odpowiedzialnych za dokonanie naruszeń. W świetle powyższego, aktualna jest

⁵²³ Zawiadomienie o popełnieniu przestępstwa przez osoby sprawujące zarząd PKP zostało skierowane do Prokuratury Rejonowej Warszawa Śródmieście w dniu 15 listopada 2000 r.

⁵²⁴ Np. zawiadomienie Prokuratury Rejonowej Łódź Śródmieście, nr Ds. 10048/00

⁵²⁵ Postanowienie Prokuratury Rejonowej w Gdyni, nr 4 Ds. 4526/00

⁵²⁶ Zawiadomienie o popełnieniu przestępstwa z dnia 26 czerwca 2000 r., sygn. GI-DIS-82/00

sformułowana wcześniej ocena, iż naruszenie ustawy o ochronie danych osobowych nie jest uznawane przez organy ścigania, jako zasługujące na uwagę i nie uznaje się za wskazane przeprowadzenie postępowania karnego, zakończonego aktem oskarżenia.

Działania prokuratury w większości przypadków potwierdzają iluzoryczność prawnokarnej ochrony danych osobowych.

⁵²⁷ Np. w sprawie rozpatrywanej przez Prokuraturę Apelacyjną w Warszawie, sygn. Ap I Dsn 141/01 W-wa, Ap I Dsn 142/01/W-wa

Część V. WYSTĄPIENIA GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH

Wystąpienia o charakterze ogólnym

Obok innych form działania, Generalny Inspektor Ochrony Danych Osobowych kierował wystąpienia do naczelnych i centralnych organów administracji państwowej oraz organów samorządów gospodarczych, w celu poinformowania o nieprawidłowościach w działaniu organów i podmiotów gospodarczych, bądź zasygnalizowania niespójności w obowiązujących przepisach prawa.

W 2000 r. Generalny Inspektor Ochrony Danych Osobowych występował do następujących organów:

Ministra Zdrowia (GI – 609/00 z dnia 30 czerwca 2000 r.)

- w sprawie braku podstaw prawnych tworzenia i prowadzenia Regionalnych Rejestrów Nowotworów wskutek uchylenia dotychczas obowiązujących przepisów oraz konieczności uregulowania tej kwestii przepisami prawa (...)

Wystąpienie skierowane zostało do MZ w związku wpływającymi do Generalnego Inspektora Ochrony Danych Osobowych pytaniami dotyczącymi podstawy prawnej funkcjonowania Regionalnych Rejestrów Nowotworów i zakresu przetwarzania przez nich danych osobowych osób chorujących na raka, jak również podejmowania działań profilaktycznych wobec członków rodzin tych osób.

Z kierowanych do GODO pytań wynika, że w Polsce istnieją Regionalne Rejestry Nowotworów, zbierające informacje o zachorowaniach na nowotwory złośliwe. Dane z Rejestrów są następnie przekazywane do Centrum Onkologii, gdzie na ich podstawie publikowane są informacje dotyczące skuteczności walki z rakiem. Regionalne Rejestry Nowotworów wskazują jako podstawę prawną przepisy Instrukcji Ministrów Zdrowia i Opieki Społecznej, Obrony Narodowej, Spraw Wewnętrznych, Komunikacji oraz Sprawiedliwości z dnia 28 marca 1962 r. w sprawie zgłaszania przypadków nowotworów złośliwych i podejrzanych jako złośliwe (Monitor Polski Nr 30, poz. 141). W rzeczywistości Instrukcja ta obecnie nie obowiązuje. Nie został też stworzony żaden inny akt regulujący kwestie przetwarzania danych o osobach chorych na nowotwory złośliwe, co budzi poważne zaniepokojenie.

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883, z późn. zm.), w art. 27 ust. 1 ustanowiła zakaz przetwarzania pewnych kategorii danych, szczególnie ważnych dla ochrony prywatności każdego człowieka (danych szczególnie chronionych). Wśród tych informacji znajdują się m.in. dane o stanie zdrowia. Przetwarzanie takich danych jest jednak dopuszczalne za pisemną zgodą osoby, której dane dotyczą, gdy przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą i stwarza pełne gwarancje ich ochrony oraz gdy przetwarzanie jest niezbędne w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych (art. 27 ust. 2 pkt 1, 2 i 7 ustawy). Tak więc z chwilą wejścia w życie ustawy o ochronie danych osobowych, tj. od dnia 30 kwietnia 1998 r. – jeśli nie są spełnione inne przesłanki przetwarzania - przetwarzanie danych o stanie zdrowia powinno odbywać się tylko na podstawie aktu prawnego o randze ustawy.

Społecznie uzasadnione wydaje się również objęcie zapisem ustawowym kwestii przetwarzania przedmiotowych danych dla celów profilaktyki. Wystąpienie w jednej rodzinie kombinacji nowotworów stwarza wysokie prawdopodobieństwo ich genetycznego pochodzenia i powoduje konieczność objęcia badaniem i poddania obserwacji członków takiej rodziny. W tym celu zasadne wydaje się stworzenie regulacji prawnej umożliwiającej poradnikom profilaktycznym dostęp do takich danych w celu wczesnego wykrycia choroby i podjęcia jej leczenia.

Uwzględniając szczególny charakter danych osobowych dotyczących stanu zdrowia oraz faktyczną potrzebę szczegółowego uregulowania przedmiotowych kwestii, w ocenie Generalnego Inspektora koniecznym jest wprowadzenie - w miejsce obecnej luki prawnej - normy rangi ustawowej, stanowiącej podstawę gromadzenia i wykorzystywania powyższych danych, a także tworzącej gwarancję ochrony danych osób dotkniętych chorobą. Generalny Inspektor Ochrony Danych Osobowych zwrócił się do Ministra Zdrowia z prośbą o podjęcie działań mających na celu uchwalenie przez Parlament ustawy, regulującej przedmiotowe kwestie, z uwagi na to, że sam takiej inicjatywy nie posiada.

Ministra Zdrowia (GI – 407/00 z dnia 8 maja 2000 r.)

- w sprawie podstaw prawnych oraz zasadności powiadamiania przez szpital zakładu pracy o fakcie hospitalizacji pracownika (...). Pytanie powstało w związku z pismem, jakie wpłynęło od Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Sokołowie

Podlaskim, w którym zakład opieki zdrowotnej sygnalizował wynikający z przepisów prawa obowiązek szpitali powiadamiania o fakcie hospitalizacji pracownika jego zakładu pracy. Samodzielny Publiczny Zakład Opieki Zdrowotnej podał jako podstawę prawną takiego działania § 11 ust. 2 rozporządzenia Ministra Zdrowia i Opieki Społecznej z dnia 17 maja 1996 r. w sprawie orzekania o czasowej niezdolności do pracy (Dz. U. Nr 63, poz. 302 z późn. zm.).

Powołane rozporządzenie zostało wydane na podstawie art. 50 ust. 2 ustawy z dnia 17 grudnia 1974 r. o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa (Dz. U. z 1983 r. Nr 30, poz. 143 z późn. zm.), która już nie obowiązuje. Natomiast na podstawie art. 59 ust. 14 aktualnie obowiązującej ustawy z dnia 25 czerwca 1999 r. o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa (Dz. U. Nr 60, poz. 636) zostało wydane rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 27 lipca 1999 r. w sprawie szczegółowych zasad i trybu wystawiania zaświadczeń lekarskich, wzoru zaświadczenia lekarskiego i zaświadczenia lekarskiego wydanego w wyniku kontroli lekarza orzecznika Zakładu Ubezpieczeń Społecznych (Dz. U. Nr 65, poz. 741). W zakresie dotyczącym zasad i trybu wystawiania zaświadczeń lekarskich, zgodnie z § 8 tegoż rozporządzenia, straciło moc rozporządzenie Ministra Zdrowia i Opieki Społecznej z dnia 17 maja 1996 r. w sprawie orzekania o czasowej niezdolności do pracy (Dz. U. Nr 63, poz. 302 z późn. zm.).

Taki sposób uchylecia przepisów rozporządzenia z dnia 17 maja 1996 r. w sprawie orzekania o czasowej niezdolności do pracy (Dz. U. Nr 63, poz. 302 z późn. zm.) powoduje błędną praktykę szpitala, który wysyła zawiadomienia o hospitalizacji pracownika jego zakładowi pracy.

Tymczasem dane dotyczące stanu zdrowia, stosownie do art. 27 ust. 2 pkt 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.), mogą być przetwarzane bez zgody osoby, której one dotyczą, jedynie w sytuacji, gdy przepis szczególny innej ustawy zezwala na przetwarzanie takich danych, a ponadto stwarza pełne gwarancje ich ochrony.

Nawet gdyby § 11 rozporządzenia Ministra Zdrowia i Opieki Społecznej z dnia 17 maja 1996 r., w części dotyczącej powiadamiania zakładu pracy o pobycie w szpitalu jego pracownika, nie został uchylony, pozostawałby niewątpliwie w sprzeczności z art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych, bowiem do przetwarzania danych dotyczących stanu zdrowia, jak wyżej wskazano, niezbędne jest umocowanie ustawowe.

Ministra Zdrowia i Opieki Społecznej (GI-DP-606/00 z dnia 24 sierpnia 2000 r.)

- w sprawie nie mającej podstawy prawnej praktyki żądania przez świadczeniobiorców usług medycznych innych dokumentów weryfikujących fakt ubezpieczenia zdrowotnego, niż dokumenty określone w obowiązujących przepisach prawa oraz ewentualnej konieczności zmiany przepisów, jeśli obowiązujące dokumenty nie dają dostatecznych podstaw weryfikacji prawa do świadczenia zdrowotnego w ramach ubezpieczenia zdrowotnego.

Generalny Inspektor wskazywał, iż art. 51 ust. 1 ustawy z dnia 6 lutego 1997 r. o powszechnym ubezpieczeniu zdrowotnym (Dz. U. Nr 28, poz. 153 z późn. zm.) stanowi, że ubezpieczony ubiegający się o świadczenie z ubezpieczenia zdrowotnego jest obowiązany przedstawić kartę ubezpieczenia. Intencją tego przepisu jest weryfikacja uprawnienia ubezpieczonego do świadczenia. Rozporządzenie Rady Ministrów z dnia 18 marca 1999 r. w sprawie karty ubezpieczenia zdrowotnego, trybu jej wydawania i unieważniania (Dz. U. Nr 30, poz. 289) przewiduje w § 1 następujące formy karty ubezpieczenia: 1) kartę ubezpieczenia z układem elektronicznym, 2) kartę ubezpieczenia bez układu elektronicznego, 3) książeczkę usług medycznych.

Ustawa o powszechnym ubezpieczeniu zdrowotnym stanowi w art. 169f, że do dnia wydania ubezpieczonemu karty ubezpieczenia, dowodem ubezpieczenia jest każdy dokument, który do dnia 31 grudnia 1998 r. potwierdzał uprawnienia do świadczeń, oraz książeczka rejestru usług medycznych.

Tymczasem świadczeniodawcy (często na żądanie kasy chorych) wymagają takiego dokumentu ubezpieczenia, który jednoznacznie wykaże, że karta ubezpieczenia (książeczka usług medycznych) jest aktualna. Zakłady świadczące usługi medyczne żądają w szczególności legitymacji ubezpieczeniowej wraz z ostatnim dowodem wpłat na ubezpieczenie lub z ostatnim odcinkiem renty bądź emerytury. Te dokumenty informują o dochodach świadczeniobiorcy, a jeśli pacjent prowadzi działalność gospodarczą, informują także o jego pracownikach. Informacje takie wkraczają w sferę prywatności świadczeniobiorcy, zaś ich żądanie utrudnia dostęp do świadczeń medycznych, szczególnie w sytuacji, gdy pacjent odmawia ich podania. Świadczeniodawcy powołują się na fakt, że książeczka usług medycznych nie jest dostatecznym dowodem ubezpieczenia, ponieważ jest wydawana bezterminowo i w sytuacji, gdy ubezpieczony przestał płacić składki, nie ma obowiązku jej zwrotu.

Z art. 23 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.), zwanej dalej ustawą, wynika, że przetwarzanie danych, w tym ich

udostępnianie, jest dopuszczalne wyłącznie po spełnieniu jednej z przesłanek enumeratywnie wymienionych w tym przepisie. Przetwarzanie danych jest - między innymi - dopuszczalne, jeśli zezwala na to przepis prawa (art. 23 ust. 1 pkt 2 ustawy). W związku z tym zapisem, wymaganie innych dokumentów niż wskazane w art. 169 f ustawy o powszechnym ubezpieczeniu zdrowotnym, jest niezgodne z prawem, jako że nie ma odpowiedniej podstawy prawnej do formułowania przez świadczeniodawców takiego żądania.

W związku z powyższym Generalny Inspektor zwrócił się do MZ z wnioskiem o rozważenie możliwości przygotowania projektu nowelizacji przepisów w taki sposób, aby karta ubezpieczenia jednoznacznie wykazywała fakt uprawnień do świadczeń zdrowotnych. Jest bowiem uzasadnione, aby świadczeniodawcy mogli zweryfikować uprawnienie świadczeniobiorców do bezpłatnych świadczeń, jednakże w sposób gwarantujący nieujawnianie informacji nie mających znaczenia dla świadczenia usług zdrowotnych.

Ministra Zdrowia i Opieki Społecznej (GI-486/00 z dnia 26 maja 2000 r.)

- w sprawie interpretacji przepisów rozporządzenia Ministra Zdrowia z dnia 27 października 1999 r. w sprawie zasad i trybu finansowania z budżetu państwa świadczeń zdrowotnych udzielanych bezpłatnie przez publiczne zakłady opieki zdrowotnej (Dz. U. Nr 91, poz. 1040), w części dotyczącej danych pacjentów przekazywanych do MZiOS oraz Pełnomocnikowi Wojewody ds. Zdrowia oraz ewentualnej nowelizacji rozporządzenia (...).

Publiczne jednostki opieki zdrowotnej udzielające, na podstawie art. 165 ust. 1 i 2 ustawy z dnia 6 lutego 1997 r. o powszechnym ubezpieczeniu zdrowotnym (Dz. U. Nr 28, poz. 153), bezpłatnych świadczeń zdrowotnych na rzecz osób nieubezpieczonych, zostały zobowiązane przez Ministerstwo Zdrowia (na mocy pisma skierowanego przez Podsekretarza Stanu w Ministerstwie Zdrowia do wszystkich wojewodów) do przedstawienia Departamentowi Budżetu i Finansów Ministerstwa oraz Pełnomocnikowi Wojewody ds. Zdrowia zestawień, które mają zawierać m.in. dane pacjentów oraz tytuł uprawnienia do bezpłatnych świadczeń. W załączonym do pisma skierowanego do wszystkich wojewodów, formularzu zestawienia świadczeń zdrowotnych udzielanych na rzecz osób nieposiadających uprawnień z tytułu ubezpieczenia zdrowotnego, udzielonych w 1999 r., wymagane jest podanie imienia i nazwiska osoby, której udzielono świadczenia.

Ustawodawca nie określił wzoru formularza zestawienia w postaci załącznika do ww. rozporządzenia, ani też wzór taki nie stanowi integralnej części rozporządzenia. Ustawodawca posłużył się w § 5 rozporządzenia sformułowaniem "dane osobowe umożliwiające identyfikację osoby", co jest jednoznacznie rozumiane jako konieczność

umieszczania imienia i nazwiska w zestawieniu, które ma być przedstawione Departamentowi Budżetu i Finansów Ministerstwa oraz Pełnomocnikowi Wojewody ds. Zdrowia. Ujawnienie imienia i nazwiska pacjenta jedynie w celu dokonania rozliczeń finansowych stoi w sprzeczności z przepisami ustawy o ochronie danych osobowych, która do przetwarzania danych szczególnie chronionych, do których należą dane o stanie zdrowia, wymaga umocowania ustawowego, dla zagwarantowania odpowiedniego poziomu zabezpieczenia informacji o osobie.

Wystarczającym dla celów identyfikacji jest podanie numeru PESEL, bez konieczności podawania imienia i nazwiska, co w sposób wystarczający pozwoli na identyfikację osoby korzystającej ze świadczenia.

Dla poparcia przedstawionych wyżej argumentów trafnym wydaje się przytoczenie przepisów § 3 rozporządzenia z dnia 15 stycznia 1999 r. w sprawie ustalenia zakresu niezbędnych danych gromadzonych przez świadczeniobiorców oraz w systemach informatycznych Kas Chorych, a także zakresu i procedury wymiany pomiędzy Kasami Chorych oraz Kasami Chorych a świadczeniodawcami, Urzędem Nadzoru Ubezpieczeń Zdrowotnych i Krajowym Związkiem Kas Chorych (Dz. U. Nr 7, poz. 66, z późn. zm.). Na podstawie tych przepisów świadczeniodawcy przekazują Kasom Chorych, z którymi mają zawarte umowy, dane dotyczące świadczeń wykonanych na rzecz ubezpieczonych w nich osób. Dla identyfikacji osoby nie jest wymagane podawanie jej imienia i nazwiska. Wystarczającym, zgodnie z przepisami tego rozporządzenia, jest podanie numeru ewidencyjnego PESEL pacjenta.

Uwzględniając szczególny charakter danych osobowych dotyczących stanu zdrowia, niezależnie od faktu, czy dane dotyczą pacjentów ubezpieczonych, czy nieubezpieczonych, w ocenie Generalnego Inspektora Ochrony Danych Osobowych celowym byłoby uregulowanie kwestii zakresu danych przekazywanych w zestawieniach na mocy rozporządzenia z dnia 27 października 1999 r. w sprawie zasad i trybu finansowania z budżetu państwa świadczeń zdrowotnych udzielanych bezpłatnie przez publiczne zakłady opieki zdrowotnej, analogicznie do zakresu danych przewidzianego w rozporządzeniu z dnia 15 stycznia 1999 r.

Celowym byłoby określenie przez ustawodawcę wzoru formularza zestawienia świadczeń zdrowotnych, o których mowa w art. 165 ust. 1 i 2 ustawy o powszechnym ubezpieczeniu zdrowotnym, udzielanych bezpłatnie przez publiczne zakłady opieki zdrowotnej, z wyraźnym wskazaniem konieczności podania numeru PESEL.

Ministra Zdrowia i Opieki Społecznej (GI – 100/00 z dnia 26 stycznia 2000 r.)

- w sprawie podjęcia działań mających na celu wyeliminowanie wewnętrznej niespójności przepisów ustawy z dnia 6 lutego 1997 r. o powszechnym ubezpieczeniu zdrowotnym (Dz. U. Nr 28, poz.153 z późn. zm.), w związku z problemami dotyczącymi ustalenia zakresu danych osobowych, które na podstawie ustawy z dnia 6 lutego 1997 r. (Dz. U. Nr 28, poz. 153 z późn. zm.) należy przekazywać Kasom Chorych (...).

Ustawa o powszechnym ubezpieczeniu zdrowotnym stanowi w art. 141a ust. 2, że:

„Dla realizacji zadań, o których mowa w ust. 1, Kasy Chorych mają prawo przetwarzania następujących danych osobowych:

1. imię i nazwisko,
2. numer PESEL,
3. data urodzenia,
4. płeć,
5. stopień pokrewieństwa z opłacającym składką,
6. adres zamieszkania,
7. stopień niepełnosprawności, jeżeli dziecko ukończyło 26 lat,
8. udzielone ubezpieczonemu świadczenia zdrowotne..."

Jest to zamknięty katalog danych, których przetwarzanie jest dopuszczalne bez zgody osoby, której one dotyczą.

Równocześnie art. 16 tejże ustawy, przewidując obowiązek zgłoszenia do ubezpieczenia zdrowotnego, w ust. 11 precyzuje dane, które powinno zawierać zgłoszenie. Są to: „wskazanie Kasy Chorych, nazwisko, pierwsze i drugie imię, nazwisko rodowe, płeć, adres zamieszkania, numer PESEL, datę urodzenia oraz numer NIP w przypadku osób, którym nadano ten numer. Gdy osoba zgłaszana do ubezpieczenia zdrowotnego nie ma nadanego numeru PESEL i numeru NIP, zgłoszenie powinno zawierać rodzaj i numer dowodu tożsamości. Zgłoszenie powinno zawierać również następujące dane dotyczące członków rodziny objętej ubezpieczeniem: nazwisko, pierwsze i drugie imię, nazwisko rodowe, płeć, stopień pokrewieństwa, datę urodzenia, adres zamieszkania, stopień niepełnosprawności, numer PESEL oraz numer NIP w przypadku osób, którym nadano ten numer.”

Ze zderzenia tych dwóch przepisów wynika, że zgłaszający jest obowiązany dostarczyć Kasie Chorych drugie imię, nazwisko rodowe oraz - w pewnych sytuacjach -

numer NIP lub rodzaj i numer dowodu tożsamości, zaś Kasa Chorych nie ma prawa tych danych przyjąć i przetwarzać, ponieważ art.141 a nie daje podstaw do przetwarzania takich danych. Niezbędne byłoby zatem podjęcie działań mających na celu wyeliminowanie wewnętrznej niespójności przepisów ustawy o powszechnym ubezpieczeniu zdrowotnym.

Ponadto ustawodawca nie przewidział sytuacji, gdy osoba zgłaszana do ubezpieczenia nie podaje całości danych osobowych i - w interesie tejże osoby -ZUS i KRUS powinny zweryfikować lub uzupełnić posiadane dane z danymi zawartymi w ewidencji ludności (dotyczy to, np. podania prawidłowego numeru PESEL, drugiego imienia czy nazwiska rodzowego osoby ubezpieczanej). Byłoby zatem celowe uwzględnienie w ewentualnej nowelizacji ustawy prawa tychże podmiotów do uzyskiwania stosownych informacji z rejestrów publicznych, bowiem w chwili obecnej organy rządowe i samorządowe kategorycznie odmawiają pomocy w weryfikacji danych osób ubezpieczonych.

Ministra Edukacji Narodowej (GGI-024-1/00 z dnia 5 października 2000r.)

- w sprawie *nieuprawnionego żądania podawania szczegółowych danych dotyczących ucznia i jego rodziców na pierwszej stronie dzienniczka ucznia (...).*

GIODO wskazał, iż nie ulega wątpliwości, iż na podstawie § 3 rozporządzenia Ministra Edukacji Narodowej z dnia 19 kwietnia 1999 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. Nr 41, poz. 414) szkoły podstawowe i gimnazja prowadzą księgi ewidencji dzieci podlegających obowiązkowi szkolnemu, zamieszkałych w obwodzie szkoły. Do księgi ewidencji wpisuje się imię (imiona) i nazwisko oraz datę, miejsce urodzenia i adres zamieszkania dziecka, a także imiona i nazwiska rodziców (opiekunów prawnych) oraz adresy ich zamieszkania. Także, stosownie do § 6 wymienionego wyżej rozporządzenia, szkoła prowadzi dla każdego oddziału dziennik lekcyjny, w którym dokumentuje się przebieg nauczania w danym roku szkolnym. Do dziennika wpisuje się nazwiska i imiona uczniów, daty, miejsca urodzenia i adresy ich zamieszkania, imiona i nazwiska rodziców (prawnych opiekunów) oraz adresy ich zamieszkania. Informacje te, gromadzone przez szkoły, są - czy powinny być - odpowiednio zabezpieczone i udostępniane jedynie uprawnionym osobom .

Przepisy wyżej powołanego rozporządzenia oraz pozostałe przepisy wykonawcze do ustawy z dnia 7 września 1991 r. o systemie oświaty (Dz. U. z 1996 r., Nr 67, poz. 329 z późn. zm.) nie wskazują, jakie dane winien uczeń podać do dzienniczka ucznia. Tymczasem w obowiązujących uczniów dzienniczkach, na pierwszej stronie, oprócz danych wpisywanych

do ewidencji i dzienników szkolnych, widnieją rubryki wymagające wpisania zawodu oraz miejsca pracy rodziców lub opiekunów ucznia. Oznacza to, iż dzienniczka, do którego dostęp mogą mieć różne osoby (także osoby postronne), wpisywana jest większa ilość danych, aniżeli wymagana wskazanymi wyżej przepisami.

W związku z powyższym, GODO zwrócił się o wskazanie podstawy prawnej żądania przez nauczycieli szkół tak szerokiego zakresu danych o uczniu oraz podstawy nakładania na uczniów obowiązku wypełniania pierwszej strony dzienniczka ucznia.

Ministra Edukacji Narodowej (GI – 733/00 z dnia 26 lipca 2000 r.)

- w sprawie wzoru „Karty Kwalifikacyjnej Uczestnika Wypoczynku” stanowiącej załącznik nr 2 do rozporządzenia Ministra Edukacji Narodowej z dnia 21 stycznia 1997 r. w sprawie warunków, jakie muszą spełniać organizatorzy wypoczynku dla dzieci i młodzieży szkolnej, a także zasad jego organizowania i nadzorowania (Dz. U. Nr 12, poz. 67 z późn. zm.) (...)

Generalny Inspektor Ochrony Danych Osobowych otrzymywał sygnały, w których podnoszono, że zgodnie z obowiązującymi przepisami rozporządzenia Ministra Edukacji Narodowej z dnia 21 stycznia 1997 r. w sprawie warunków, jakie muszą spełniać organizatorzy wypoczynku dla dzieci i młodzieży szkolnej, a także zasad jego organizowania i nadzorowania (Dz. U. Nr 12, poz. 67 z późn. zm.), zwanego dalej rozporządzeniem, dostęp do „Kart Kwalifikacyjnych Uczestnika Wypoczynku” ma znaczna liczba osób: wychowawca klasy, pielęgniarka szkolna, kadra kolonijna, organy uprawnione do kontroli placówek wypoczynku. Dlatego też iluzoryczna jest ochrona dostępu do zawartych w części II - wniosek rodziców, pkt 6 i 7 „Karty Kwalifikacyjnej Uczestnika Wypoczynku”, zwanej dalej Kartą, danych o dziecku i jego rodzinie, a dotyczących liczby osób na utrzymaniu rodziców, miejsc i stanowisk pracy rodziców oraz ich dochodów miesięcznych. Osoby uprawnione do wypełnienia Karty mają prawo wglądu we wszystkie zawarte w niej informacje, ponieważ stanowi ona jeden dokument. Z powyższych względów powstaje pytanie, czy nie byłoby celowym podzielenie Karty na odrębne części w ten sposób, aby poszczególne osoby miały dostęp jedynie do informacji potrzebnych do wykonania tylko ich obowiązków.

W dniu 14 czerwca 2000 r. (pismo znak: GI-DP-626/00/842) Generalny Inspektor Ochrony Danych Osobowych zwrócił się do Dyrektora Departamentu Prawnego Ministerstwa Edukacji Narodowej, z prośbą o zajęcie stanowiska w przedmiotowej sprawie.

W odpowiedzi na powyższe pytanie w dniu 10 lipca 2000 r. (pismo znak: DP-024-458/00/MF) Generalny Inspektor Ochrony Danych Osobowych został poinformowany, iż

Karta jest bardzo istotnym dokumentem, gdyż wszelkie informacje, które zawiera są potrzebne organizatorom wypoczynku, będącymi osobami biorącymi całkowitą odpowiedzialność za życie, zdrowie i bezpieczeństwo dzieci i młodzieży. Punkty 6-8 Karty odnoszą się tylko do publicznych placówek wypoczynku, a ich wypełnienie jest obowiązkowe jedynie wtedy, gdy pobyt dziecka jest częściowo lub całkowicie finansowany ze środków budżetu państwa. Ponadto w piśmie stwierdzono, iż tworzenie kilku wzorów kart nie jest uzasadnione, natomiast wskazano, że istnieje konieczność wprowadzenia do Karty klauzuli o wyrażeniu zgody na gromadzenie i przetwarzanie danych w niej zawartych. Niemniej jednak, po przeanalizowaniu uwag, Departament Prawny rozważy zmianę wzoru Karty.

W związku z powyższymi uwagami i odpowiedzią Departamentu Prawnego MEN, GODO zwrócił się do Ministra Edukacji Narodowej z wnioskiem o rozważenie możliwości nowelizacji przedmiotowego rozporządzenia w zakresie uwzględniającym następujące wyjaśnienia i uwagi:

Przetwarzanie danych osobowych jest dopuszczalne po spełnieniu co najmniej jednej z przesłanek enumeratywnie wymienionych w art. 23 ust. 1 pkt 1 - 5 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.), zwanej dalej ustawą. Oznacza to, iż zgodnie z przepisami ustawy, przetwarzanie danych osobowych jest możliwe m.in., gdy zezwalają na to przepisy prawa.

Zawierane w Karcie informacje o dzieciach i ich rodzicach stanowią dane osobowe, gdyż są informacjami pozwalającymi, w myśl art. 6 ustawy, na określenie tożsamości tych osób. Zgodnie z art. 36 ustawy, administrator danych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym.

Z uwagi na przywołane wyżej przepisy, uzasadniona wydaje się propozycja podzielenia Karty na odrębne formularze. Dostęp do odpowiedniej części Karty powinny mieć bowiem tylko te osoby, które są zobowiązane znać zawarte w niej informacje jedynie ze względu na wykonywane obowiązki służbowe. Nie jest bowiem uzasadnione, aby informacje np. o wysokości dochodów rodziców czy opiekunów dziecka były ujawnione innym osobom (np. pielęgniarki czy wychowawcy), niż organizator wypoczynku decydujący o dofinansowaniu wypoczynku ze środków budżetu państwa. Ponadto, z tych samych względów nie znajduje uzasadnienia ujawnianie informacji o zdrowiu dziecka organizatorowi wypoczynku czy wychowawcy klasy, albo osobie potwierdzającej pobyt dziecka w placówce wypoczynku. Dane o stanie zdrowia dziecka powinny być dostępne jedynie osobom, które w

trakcie wypoczynku są zobowiązane do sprawowania opieki nad dzieckiem. Osobami takimi mogą być pielęgniarka bądź lekarz oraz kadra placówki wypoczynku.

Zgodnie z przepisem art. 26 ust. 1 pkt 2 i 3 ustawy o ochronie danych osobowych, administrator danych powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane przetwarza. Aby wypełnić ten obowiązek administrator jest obowiązany zapewnić, żeby dane były zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami oraz aby dane były merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane. Podział Karty w wyżej zaproponowany sposób jest uzasadniony ze względu na konieczność wypełnienia przez administratora danych, tj. osobę decydującą o celach i środkach przetwarzania danych, obowiązków nałożonych na niego przepisami art. 26 ustawy.

GIODO wyjaśnił ponadto, iż nie jest konieczne zamieszczanie w formularzu Karty klauzuli wyrażenia zgody na przetwarzanie danych, jeśli na mocy przepisów przedmiotowego rozporządzenia w formularzu tym określone jest, jakie dane i informacje mogą być zbierane dla potrzeb kwalifikacji uczestników wypoczynku.

Ministra Finansów (GI – 518/00 z dnia 1 czerwca 2000 r.)

- w sprawie żądania przez urzędy skarbowe w związku z przeprowadzaną kontrolą zakładów pracy chronionej, dostępu do akt osobowych pracowników.

Przetwarzanie danych osobowych jest dopuszczalne wyłącznie w przypadkach określonych w art. 23 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.), w szczególności gdy zezwala na to przepis prawa. Ustawa wprowadza szczególne zasady przetwarzania danych szczególnie chronionych, m. in. danych o stanie zdrowia. Ich przetwarzanie jest co do zasady zabronione, a wyjątki w tym zakresie zostały ustalone w art. 27 ust. 2 ustawy. Zgodnie z pkt 2 powołanego przepisu, dopuszczalne jest przetwarzanie danych wskazanych w art. 27 ust. 1, gdy przepis ustawy tak stanowi i jednocześnie stwarza on pełne gwarancje ochrony tych danych.

Zasady przeprowadzania kontroli podatkowej określa ustawa z dnia 29 sierpnia 1997 r. Ordynacja podatkowa (Dz. U. Nr 137, poz. 926 z późn. zm.). Art. 281 tej ustawy stanowi, że organy podatkowe, celem sprawdzenia wywiązywania się podatników, płatników i inkasentów z obowiązków wynikających z przepisów prawa podatkowego, przeprowadzają kontrolę. Kontrolujący, zgodnie z art. 284 § 1, są w szczególności uprawnieni do żądania udostępnienia im akt, ksiąg i wszelkiego rodzaju dokumentów związanych z przedmiotem

kontroli oraz dokonywania z nich odpisów, wyciągów i notatek. Prawo przeprowadzenia kontroli jest więc ograniczone przedmiotem kontroli oraz przepisami innych ustaw.

Przedmiot kontroli w poruszanej sprawie związany był z informacjami o pracownikach zakładów pracy chronionej. W myśl art. 14 a ustawy z dnia 8 stycznia 1993 r., o podatku od towarów i usług oraz o podatku akcyzowym (Dz. U. Nr 11, poz. 50 z późn. zm.), zwanej dalej ustawą o VAT, prowadzący zakład pracy chronionej ma prawo, w zakresie działalności tego zakładu, do otrzymania częściowego lub całkowitego zwrotu wpłaconej kwoty podatku od towarów i usług.

Przez prowadzącego zakład pracy chronionej rozumie się podmiot spełniający warunki określone w art. 28 i 29 ustawy z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych (Dz. U. Nr 123, poz. 776 z późn. zm.).

Zgodnie z art. 28 ust. 1 powyższej ustawy, pracodawca prowadzący działalność gospodarczą przez okres co najmniej 12 miesięcy, zatrudniający nie mniej niż 20 pracowników w przeliczeniu na pełny wymiar czasu pracy i osiągający wskaźniki zatrudnienia osób niepełnosprawnych, o których mowa w pkt 1, przez okres co najmniej 6 miesięcy, uzyskuje status pracodawcy prowadzącego zakład pracy chronionej, jeżeli:

1. wskaźnik zatrudnienia osób niepełnosprawnych wynosi:
 - co najmniej 40%, a w tym co najmniej 10% ogółu zatrudnionych stanowią osoby zaliczone do znacznego lub umiarkowanego stopnia niepełnosprawności, albo
 - co najmniej 30% niewidomych lub psychicznie chorych, albo upośledzonych umysłowo zaliczonych do znacznego albo umiarkowanego stopnia niepełnosprawności,
2. obiekty i pomieszczenia użytkowane przez zakład pracy:
 - odpowiadają przepisom i zasadom bezpieczeństwa i higieny pracy,
 - uwzględniają potrzeby osób niepełnosprawnych w zakresie przystosowania stanowisk pracy, pomieszczeń higieniczno - sanitarnych i ciągów komunikacyjnych oraz spełniają wymagania dostępności do nich,
3. jest zapewniona doraźna i specjalistyczna opieka lekarska, poradnictwo i usługi rehabilitacyjne, a także wystąpi z wnioskiem o przyznanie statusu pracodawcy prowadzącego zakład pracy chronionej.

Kwalifikacji osób do poszczególnych stopni niepełnosprawności dokonują zespoły orzekające o stopniu niepełnosprawności. Zgodnie z art. 30 ust. 1 powyższej ustawy decyzję w sprawie przyznania statusu zakładu pracy chronionej wydaje wojewoda na okres 3 lat. Ordynacja podatkowa, a także ustawa o VAT nie przewidują natomiast prawa dostępu urzędników skarbowych do akt osobowych zawierających w tym wypadku również dane o stanie zdrowia pracowników zakładów pracy chronionej. Na gruncie obowiązujących przepisów (art. 14 a ustawy o VAT) znaczenie dla wymiaru podatku ma informacja o ilości zatrudnionych osób niepełnosprawnych w rozliczeniu na poszczególne stopnie niepełnosprawności.

Organ podatkowy nie może natomiast domagać się dostępu do akt osobowych konkretnych pracowników i przetwarzać ich danych o stanie zdrowia. Ocena niepełnosprawności należy bowiem do powołanych w tym celu zespołów, a fakt czy dany podmiot spełnia ustawowe wymogi do bycia zakładem pracy chronionej leży w sferze kompetencji wojewody.

Przetwarzanie danych pracowników, zawartych w aktach osobowych, przez kontrolerów skarbowych, bez podstawy ustawowej narusza więc ustawę o ochronie danych osobowych, w szczególności art. 27 tej ustawy.

W odpowiedzi na w/w wystąpienie, GIODO powtórnie skierował do **Ministra Finansów** pismo (GI-DP-1098/00 z dnia 3 listopada 2000 r.) polemizujące ze stanowiskiem Ministra Finansów, wskazujące, iż nie można zgodzić się z zaproponowaną przez Ministerstwo podstawą prawną dostępu kontrolerów skarbowych do przedmiotowych danych, którą stanowić miałby przepis art. 23 ust. 1 pkt 4 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.), zwanej dalej ustawą. Zgodnie z tym przepisem przetwarzanie danych osobowych jest dopuszczalne, gdy jest to niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego. Nie jest możliwe na gruncie ustawy zaakceptowanie stanowiska odnośnie możliwości przetwarzania danych o stanie zdrowia pracowników zakładów pracy chronionej na podstawie tego przepisu. Wynika to z faktu, iż ustawa wprowadza, jak to przedstawiono w wystąpieniu Generalnego Inspektora z dnia 1 czerwca 2000 r., odrębne normy, określające zasady przetwarzania danych wrażliwych, których katalog zawiera art. 27 ust. 1. Są to m.in. dane o stanie zdrowia, które mogą być przetwarzane jedynie w przypadkach określonych w art. 27 ust. 2 ustawy, m.in., gdy zezwala na to przepis ustawy, (nie może być to zatem zapis zawarty

w akcie niższej rangi), bez zgody osoby, której dane dotyczą i są stworzone pełne gwarancje ochrony tych danych.

Zatem przepis ustawy winien zawierać upoważnienie dla pracowników urzędów skarbowych do przetwarzania danych osobowych o stanie zdrowia zatrudnionych.

Nie kwestionując, co do zasady, potrzeby takiego dostępu w celu efektywnej kontroli przestrzegania przez zakłady pracy chronionej zapisów ustawy z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych (Dz. U. Nr 123, poz. 776 z późn. zm.), należy postulować ewentualną nowelizację odpowiednich przepisów ustaw, tak aby zapewnić zgodność tych przepisów z wymaganiami art. 47 i 51 ust. 2 Konstytucji oraz z art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych.

Ministra Finansów (GI – 857/00 z dnia 1 września 2000 r.)

- w sprawie niejednolitych praktyk stosowanych przez urzędy skarbowe w ramach przeprowadzanych kontroli poprawności dokonywanych przez podmioty prowadzące działalność gospodarczą, rozliczeń podatkowych .

Generalny Inspektor Ochrony Danych Osobowych w swojej praktyce spotkał się ze skargami klientów dotyczącymi konieczności podawania szczegółowych danych osobowych, a także numeru dowodu osobistego i numeru PESEL, w przypadku odbierania należności z tytułu uwzględnionej reklamacji. Dane te są utrwalane w systemie informatycznym sklepu.

W wyniku przeprowadzonych na podstawie art. 14 pkt 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.), postępowań wyjaśniających ustalono, że dane osobowe klientów przetwarzane są w związku ze zwrotem zakupionego wcześniej towaru. Zwrot towaru jest równoznaczny z odstąpieniem od umowy kupna-sprzedaży i wymaga od właściciela sklepu sporządzenia odpowiedniej dokumentacji. Przedsiębiorstwa handlowe wyjaśniały, że prowadzą ewidencję każdej sprzedaży na kasie fiskalnej i mają obowiązek rozliczać się z wysokości wykazanej tam sprzedaży przed urzędem skarbowym, a zwrot towaru ma niewątpliwie wpływ na obniżenie wysokości zobowiązania podatkowego firmy wobec Skarbu Państwa. Wynika to z uregulowań ustawy z dnia 8 stycznia 1993 r. o podatku od towarów i usług oraz o podatku akcyzowym (Dz. U. Nr 11, poz. 50 z późn. zm.). Z kolei, jako płatnik podatku od towarów i usług oraz podatku dochodowego, firma taka ma obowiązek umożliwić urzędowi skarbowemu kontrolę poprawności dokonywanych rozliczeń podatkowych. W przypadku uznania reklamacji towaru, kierownik sklepu odbiera od klienta oryginalny paragon fiskalny korygowanej sprzedaży i sporządza dokument zwrotu towaru od klienta, na którym znajdują się takie dane

jak: imię, nazwisko, adres, oraz dowolny numer identyfikacyjny: NIP, PESEL lub numer dowodu osobistego. Gromadzenie tych danych ma na celu umożliwienie urzędnikom kontroli skarbowej dotarcie do klienta i sprawdzenie, czy zwrot miał faktycznie miejsce. Kierownictwa sklepów wskazywały, że zwracały się z prośbą o wyjaśnienie do działu podatków pośrednich izby skarbowej, gdzie stwierdzano, że nie ma ogólnych uregulowań prawnych dotyczących zwrotów towarów i sporządzana dokumentacja powinna odpowiadać wymaganiom urzędu skarbowego, któremu podlega dany płatnik. Natomiast w praktyce urzędów skarbowych nie ma jednolitego stanowiska w tej kwestii. Jedne z nich honorują sam oryginalny paragon potwierdzający zakup, inne z kolei wymagają oprócz tego dokładnych danych osoby, która dokonuje zwrotu, co tłumaczy dużą ilością nadużyć, kiedy to sprzedawcy nie dawali klientowi paragonu fiskalnego i na jego podstawie samodzielnie dokonywali korekty sprzedaży, a w rezultacie zaniżali własną sprzedaż. W tej sytuacji, przy surowych sankcjach przewidzianych w Kodeksie karnym skarbowym za wykroczenia i przestępstwa skarbowe, podmioty będące płatnikami podatku dochodowego i podatku od towarów i usług sporządzają pełen dokument zwrotu towaru na ogólnie przyjętych drukach.

Takie stanowisko płatników ww. podatków można zrozumieć, biorąc pod uwagę dość szeroko określone uprawnienia urzędników kontroli skarbowej i przepis art. 180 § 1 ustawy z dnia 29 sierpnia 1997 r. Ordynacja podatkowa (Dz. U. Nr 137, poz. 926 z późn. zm.), który pozwala organom podatkowym dopuścić w charakterze dowodu w sprawie wszystko, co może przyczynić się do jej wyjaśnienia, a nie jest sprzeczne z prawem.

Praktyka urzędów skarbowych, jak się okazuje - różna, budzi w opinii Generalnego Inspektora Ochrony Danych Osobowych poważne wątpliwości. Powinien istnieć stosowny przepis prawa, który ujednoliciłby działania wszystkich urzędów i stanowił podstawę przetwarzania danych osobowych klientów, bądź przesądzał o żądaniu od klienta, w razie zwrotów towarów, jedynie paragonu fiskalnego. Na trafność tego drugiego rozwiązania zwraca uwagę fakt, iż część urzędów skarbowych wymaga tylko takiego udokumentowania dokonanego zwrotu towaru, co oznacza, że żądanie danych osobowych klienta nie jest niezbędne.

W związku z powyższym, GIODO zwrócił się do Ministra Finansów z prośbą o podjęcie działań zmierzających do zapewnienia jednolitej praktyki stosowanej przez pracowników urzędów skarbowych.

Ministra Sprawiedliwości (GI – 881/00 z dnia 8 września 2000 r.)

- w sprawie rozważenia zmian w przepisach kodeksów - postępowania karnego i karnego wykonawczego, w trakcie przygotowywanej nowelizacji tychże kodeksów, w celu dostosowania ich przepisów do przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (D.U. Nr 133, poz. 883 z późn. zm.) .

1. Zmiany wymaga art. 214 § 7 ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karny (Dz. U. Nr 89, poz. 555 z późn. zm.) i wydane na jej podstawie rozporządzenie Ministra Sprawiedliwości z dnia 12 sierpnia 1998 r. w sprawie regulaminu czynności kuratora sądowego w zakresie przeprowadzania wywiadu środowiskowego oraz wzoru kwestionariusza tego wywiadu (Dz. U. Nr 111, poz. 695).

Art. 213 Kodeksu postępowania karnego precyzyjnie określa, jakie dane dotyczące oskarżonego należy ustalić w toku postępowania. Są to tożsamość, wiek, stosunki rodzinne i majątkowe, wykształcenie, zawód i źródła dochodu oraz informacje o wcześniejszej karalności oskarżonego. Następnie art. 214 § 1 Kodeksu postępowania karnego stanowi, iż w razie potrzeby sąd, a w postępowaniu przygotowawczym prokurator lub Policja, zarządza w stosunku do oskarżonego przeprowadzenie wywiadu środowiskowego przez zawodowego kuratora sądowego. Art. 214 § 3 wymienia, jakie informacje powinien zawierać wynik wywiadu środowiskowego. Pkt. 3 i 4 tego przepisu stanowi, iż wywiad środowiskowy powinien zawierać zwięzły opis dotychczasowego życia oskarżonego oraz dokładne informacje o środowisku oskarżonego, w szczególności rodzinnym, szkolnym lub zawodowym oraz własne spostrzeżenia i konkluzje kuratora.

Jednocześnie rozporządzenie w sprawie regulaminu czynności kuratora sądowego w zakresie przeprowadzania wywiadu środowiskowego oraz wzoru kwestionariusza tego wywiadu stanowi, iż wywiad obejmuje również stwierdzenie faktu nadużywania alkoholu lub środków odurzających oraz informacje dotyczące stanu zdrowia oskarżonego, z uwzględnieniem znanej w jego środowisku informacji dotyczącej stanu zdrowia, w tym psychicznego, uzależnienia od alkoholu lub środków odurzających.

Tymczasem, zgodnie z art. 27 ustawy o ochronie danych osobowych, dane dotyczące stanu zdrowia, jak też dane o nałogach należą do danych szczególnie chronionych, których przetwarzanie może odbywać się wyłącznie wówczas, gdy przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą i stwarza pełne gwarancje ich ochrony. Tymczasem art. 214 Kodeksu postępowania karnego takiej podstawy do przetwarzania danych wrażliwych nie zawiera, a samo rozporządzenie nie jest wystarczającą podstawą do przetwarzania danych.

Oznacza to, iż organy opracowujące wywiady środowiskowe i gromadzące ww. dane osobowe swoimi działaniami naruszają przepisy ustawy o ochronie danych osobowych.

Z tego względu, jeśli dane te powinny być gromadzone w toku sporządzania wywiadu środowiskowego, niezbędna jest zmiana treści art. 214 § 3 Kodeksu postępowania karnego w taki sposób, aby zawierał on upoważnienie do gromadzenia informacji również o stanie zdrowia oraz nałogach oskarżonego.

2. Wątpliwości powstają również w odniesieniu do art. 320 § 3 Kodeksu postępowania karnego i wydanego na jego podstawie rozporządzenie Ministra Sprawiedliwości z dnia 14 sierpnia 1998 r. w sprawie warunków, jakim powinny odpowiadać instytucje i osoby uprawnione do przeprowadzania mediacji, zakresu i warunków udostępniania im akt sprawy oraz zasad i trybu sporządzania sprawozdania z przebiegu wyników postępowania mediacyjnego (Dz. U. Nr 111, poz. 701). § 2 tego rozporządzenia wymienia kryteria, jakie musi spełniać osoba godna zaufania, której można przekazać sprawę, w celu przeprowadzenia postępowania mediacyjnego. Z treści tego przepisu wynika, iż niezbędne jest m.in., aby mediator nie był skazany za popełnienie przestępstwa.

W praktyce oznacza to ustalanie karalności kandydatów na mediatorów w oparciu o upoważnienie zawarte w przepisach rozporządzenia, a tym samym naruszanie art. 28 ustawy o ochronie danych osobowych, z treści którego jednoznacznie wynika, iż przetwarzanie danych dotyczących m.in. skazań, można prowadzić wyłącznie na podstawie ustawy. Dla tej kategorii danych osobowych ustawodawca nie dopuszcza nawet takiej sytuacji, aby osoba, której dane dotyczą mogła wyrazić zgodę na ich przetwarzanie. Oznacza to, iż w świetle przepisów ustawy o ochronie danych osobowych ustalanie niekaralności osoby godnej zaufania w oparciu o upoważnienie zawarte w rozporządzeniu jest niedopuszczalne, a w Kodeksie postępowania karnego nie ma przepisu dającego takie upoważnienie. Z tego względu przepisy Kodeksu postępowania karnego winny zostać uzupełnione o zapis stanowiący podstawę do sprawdzania karalności kandydatów na mediatorów.

3. Wątpliwości co do zgodności z ustawą o ochronie danych osobowych budzi treść art. 198 § 1 Kodeksu postępowania karnego. Przepis ten stanowi, iż w miarę potrzeby udostępnia się biegłemu akta sprawy i wzywa się go do udziału w przeprowadzeniu dowodu.

Art. 26 ust. 1 pkt. 3 ustawy o ochronie danych osobowych stanowi, iż administrator przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są

przetwarzane. Analizując pojęcie „adekwatności danych” do realizowanego celu należy przyjąć, iż oznacza to przetwarzanie danych w zakresie takim, jaki jest niezbędny do realizowanego celu, a jednocześnie w zakresie wystarczającym do jego zrealizowania. Wątpliwym jest zatem, np. przekazywanie biegłemu ustalającemu przyczyny i przebieg wypadku drogowego całych akt sprawy, w tym opinię o stanie zdrowia psychicznego podejrzanego i jego wywiad środowiskowy. Opinia takiego biegłego ma charakter ściśle techniczny, zatem dla sporządzenia przez niego ekspertyzy niezbędna będzie nie całość akt sprawy, a jedynie część materiału dowodowego zgromadzonego w toku postępowania.

Z tego względu Generalny Inspektor zaproponował rozważenie możliwości takiego zmodyfikowania przepisu, aby upoważniał on do przekazania biegłemu akt jedynie w zakresie niezbędnym do wydania przez niego opinii.

4. Modyfikacji wymaga art. 11 ustawy z dnia 6 czerwca 1997 r. Kodeks karny wykonawczy (Dz. U. Nr 90, poz. 557 z późn. zm.), który reguluje kwestie związane z przekazaniem dyrektorowi Zakładu Karnego lub Aresztu Śledczego informacji o skazanym. Przepis ten wskazuje, iż dyrektorowi Zakładu Karnego lub Aresztu Śledczego przesyła się m.in. odpisy orzeczeń i opinii lekarskich oraz psychologicznych, a na wniosek dyrektora Zakładu lub Aresztu - również akta sądowe. Tymczasem załącznik do rozporządzenia Ministra Sprawiedliwości z dnia 18 sierpnia 1998 r. w sprawie zakresu informacji dotyczących osoby skazanego, przesyłanych przez sąd dyrektorowi Zakładu Karnego lub Aresztu Śledczego (Dz. U. Nr 111, poz. 702) w pkt. 12 i 15 wymienia, iż wykaz informacji dotyczący osoby skazanego zawiera m.in. informacje o uprzedniej karalności oraz zastosowanych środkach wychowawczych lub poprawczych oraz informacje o stwierdzonym uzależnieniu od alkoholu, środków psychotropowych i odurzających.

Jak zostało to wskazane wyżej, z treści art. 27 ust. 2 i 28 ust. 1 ustawy o ochronie danych osobowych wynika, iż jedyną podstawą zezwalającą na przetwarzanie danych szczególnie chronionych (m.in. o nałogach, czy też dotyczących m.in. skazań, orzeczeń o ukaraniu) jest upoważnienie zawarte w przepisach ustawowych.

Z tego względu najbardziej uzasadnionym rozwiązaniem byłoby uzupełnienie treści przepisu art. 11 § 1 Kodeksu karnego wykonawczego o upoważnienie do przekazania dyrektorowi Zakładu Karnego lub Aresztu Śledczego informacji o uprzedniej karalności oraz zastosowanych wobec skazanego środkach wychowawczych lub poprawczych oraz informacji o stwierdzonym u niego uzależnieniu od alkoholu, środków psychotropowych i odurzających.

5. Przepisy art. 38 - 43 Kodeksu karnego wykonawczego poświęcone są zagadnieniu uczestnictwa społeczeństwa w wykonywaniu orzeczeń oraz pomocy w społecznej readaptacji skazanych. Szczegółowy zakres i tryb podejmowania tego rodzaju działań określony został w rozporządzeniu Prezesa Rady Ministrów z dnia 26 sierpnia 1998 r. w sprawie określenia zakresu i trybu uczestnictwa podmiotów wymienionych w art. 38 § 1 Kodeksu karnego wykonawczego w wykonywaniu kar, środków karnych, zabezpieczających i zapobiegawczych, a także społecznej kontroli nad ich wykonywaniem (Dz. U. Nr 113, poz. 724). § 2 tego rozporządzenia wylicza warunki, jakie musi spełniać przedstawiciel stowarzyszenia, fundacji, organizacji i instytucji oraz kościołów i innych związków wyznaniowych, jak również osoby godne zaufania podejmujące działania, o których mowa w rozporządzeniu. Pkt. 2 i 3 stanowią, iż osoba taka nie może być karana za przestępstwo popełnione umyślnie oraz nie może być pozbawiona praw rodzicielskich lub opiekuńczych.

Jak wspomniano wcześniej, art. 28 § 1 ustawy o ochronie danych osobowych stanowi, iż przetwarzanie danych dotyczących skazań i orzeczeń o ukaraniu można prowadzić wyłącznie na podstawie ustawy. Oznacza to, iż § 2 pkt 2 i 3 rozporządzenia regulującego zakres i tryb sprawowania nadzoru penitencjarnego nie może stanowić podstawy do przetwarzania tych danych. Takie upoważnienie musi wynikać z przepisów rangi ustawowej.

Jest to problem analogiczny, jak omówiony wyżej odnoszący się do warunków, jakie musi spełniać mediator. Podtrzymując przytoczoną wcześniej argumentację, GODO zwrócił się o rozważenie możliwości zmiany przepisów Kodeksu karnego wykonawczego w takim zakresie, aby to jego przepisy, a nie przepisy aktu wykonawczego do ustawy, stanowiły podstawę do ustalania niekaralności osób podejmujących działania, o których mowa w rozporządzeniu.

6. Generalny Inspektor zwrócił się również o rozważenie możliwości zmiany art. 82 § 2 i 3 Kodeksu karnego wykonawczego. Przepis ten stanowi podstawę do dokonywania klasyfikacji skazanych. Zgodnie z jego brzmieniem podstawą klasyfikacji są m.in. uprzednie odbywanie kary pozbawienia wolności, stan zdrowia fizycznego i psychicznego, stopień demoralizacji i zagrożenia społecznego. Z treści przepisu art. 83 § 1 Kodeksu karnego wykonawczego wynika, iż skazanego poddaje się w miarę potrzeby, za jego zgodą, bądź bez zgody, badaniom psychologicznym, a także psychiatrycznym.

Na podstawie art. 83 § 3 Kodeksu karnego wykonawczego wydane zostało rozporządzenie Ministra Sprawiedliwości z dnia 14 marca 2000 r. w sprawie zasad

organizacji i warunków przeprowadzania badań psychologicznych i psychiatrycznych w ośrodkach diagnostycznych (Dz. U. Nr 29, póź. 369). § 5 ust. 1 rozporządzenia wymienia, jakie dane w powinna zawierać opinia psychiatryczna i wylicza m.in., iż powinna zawierać informacje o stwierdzonym uzależnieniu od alkoholu albo środków odurzających lub psychotropowych.

Z uwagi na wymogi art. 27 ustawy o ochronie danych osobowych, który to przepis wprowadził ogólny zakaz przetwarzania m.in. danych o nałogach, warunkując możliwość przetwarzania danych od upoważnienia wynikającego z ustawy, GODO zaproponował rozszerzenie treści art. 82 § 2 Kodeksu karnego wykonawczego w ten sposób, aby przepis wymieniał również dane dotyczące uzależnienia od alkoholu albo środków odurzających lub psychotropowych, jako stanowiące jedną z informacji zawartych w opinii psychiatrycznej.

Wprowadzenie tej zmiany spowoduje, iż będzie można uznać, że § 65 ust. 1 rozporządzenia Ministra Sprawiedliwości z dnia 12 sierpnia 1998 r. w sprawie regulaminu wykonywania kary pozbawienia wolności (Dz. U. Nr 111, poz. 699) oraz § 28 ust. 2 rozporządzenia Ministra Sprawiedliwości z dnia 26 sierpnia 1998 r. w sprawie regulaminu wykonywania tymczasowego aresztowania (Dz. U. Nr 111, poz. 700) nie naruszają art. 27 ustawy o ochronie danych osobowych. Z treści wymienionych przepisów wynika bowiem, iż powołują się one na fakt stwierdzenia u skazanego lub tymczasowo aresztowanego uzależnienia od alkoholu albo środków odurzających lub psychotropowych. Jeżeli zatem przepis rangi ustawowej zawarty w art. 82 § 2 Kodeksu karnego wykonawczego będzie zawierał ogólne upoważnienie do ustalania tych informacji, dopuszczalne będzie określenie w rozporządzeniach szczegółowych zasad ich wykorzystania.

Ministra Sprawiedliwości (GI – 746/00 z dnia 31 lipca 2000 r.)

- w sprawie rozważenia w trakcie przygotowywanej nowelizacji Kodeksu karnego, możliwości zmiany przepisu art., poprzez objęcie ochroną przed udaremnieniem lub utrudnianiem wykonania czynności służbowych także inspektorów ochrony danych osobowych oraz o rozważenie możliwości wprowadzenia zmian w postępowaniu karnym, umożliwiającym Generalnemu Inspektorowi Ochrony Danych Osobowych uczestniczenie w postępowaniu w charakterze pokrzywdzonego .

Jak wskazał GODO, zmiana pierwsza mogłaby zostać wprowadzona przez dodanie § 3 do art. 225, w brzmieniu „§ 3. tej samej karze podlega, kto osobie uprawnionej do kontroli

w zakresie ochrony danych osobowych udaremnia lub utrudnia wykonywanie czynności służbowych."

Ustawa z dnia 29 sierpnia 1997. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.) uprawnia Generalnego Inspektora Ochrony Danych Osobowych lub upoważnionych przez niego inspektorów do działań kontrolnych, w tym do wstępu do pomieszczeń, w których zlokalizowany jest zbiór danych, żądania złożenia pisemnych lub ustnych wyjaśnień, żądania okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli, żądania udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych. Uprawnieniu temu odpowiada obowiązek podmiotów kontrolowanych umożliwienia przeprowadzenia kontroli.

Obowiązek ten nie jest jednak opatrzony sankcją, ani w samej ustawie o ochronie danych osobowych, ani w Kodeksie karnym czy w Kodeksie wykroczeń. Wobec braku sankcji za niedopuszczenie do przeprowadzenia kontroli zdarza się, iż administratorzy danych uniemożliwiają lub utrudniają wykonanie kontroli, zwłaszcza wówczas, gdy w sposób rażący naruszają przepisy ustawy o ochronie danych osobowych, a kontrola mogłaby dostarczyć jednoznacznego materiału dowodowego przeciwko nim.

GIODO zwrócił się również do Ministra Sprawiedliwości o rozważenie możliwości wprowadzenia zmian w postępowaniu karnym, umożliwiających Generalnemu Inspektorowi Ochrony Danych Osobowych uczestniczenie w postępowaniu w charakterze pokrzywdzonego, poprzez wprowadzenie stosownego zapisu w kodeksie postępowania karnego lub zmiany art. 19 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.) przez dodanie ust. 2 w brzmieniu:

„2. W sprawach karnych Generalnemu Inspektorowi przysługują uprawnienia pokrzywdzonego określone w przepisach kodeksu postępowania karnego, w zakresie ochrony danych osobowych."

Generalny Inspektor Ochrony Danych Osobowych jest centralnym organem administracji publicznej, odpowiedzialnym za ochronę danych osobowych, działającym w interesie publicznym w celu ochrony konstytucyjnego prawa do prywatności (art. 47 Konstytucji RP) i ochrony danych osobowych (art. 51 Konstytucji RP). Art. 19 ustawy o ochronie danych osobowych zobowiązuje Generalnego Inspektora do kierowania do organu powołanego do ścigania przestępstw, zawiadomienia o popełnieniu przestępstwa. Po złożeniu zawiadomienia, prawa Generalnego Inspektora w postępowaniu karnym ograniczają się jednak wyłącznie do możliwości zaskarżenia postanowienia o odmowie wszczęcia

postępowania (art. 306 § 1 K.p.k.); brak jest możliwości prawnych korzystania ze środków przysługujących pokrzywdzonemu po wszczęciu postępowania karnego, np. zaskarżenia postanowienia o umorzeniu postępowania, czy do składania wniosków dowodowych mimo, że Generalny Inspektor występuje w interesie publicznym. W rezultacie, po niezasadnym - w ocenie Generalnego Inspektora - umorzeniu postępowania przez prokuraturę, Generalny Inspektor kieruje do Prokuratora Generalnego pismo o rozważenie możliwości podjęcia na nowo umorzonego postępowania. Dotychczas argumenty Generalnego Inspektora za podjęciem na nowo umorzonego postępowania były przez Prokuratora Generalnego uwzględniane.

Kodeks postępowania karnego dopuszcza możliwość korzystania z praw pokrzywdzonego także innym podmiotom, niż osoby fizyczne lub prawne, których dobro prawne zostało bezpośrednio naruszone lub zagrożone przez przestępstwo (art. 49 § 1 K.p.k.), mianowicie: zakładowi ubezpieczeń - w zakresie, w jakim pokrył szkodę wyrządzoną pokrzywdzonemu przez przestępstwo lub jest zobowiązany do jej pokrycia - (art. 49 § 3), organom kontroli państwowej, które w zakresie swego działania ujawniły przestępstwo lub wystąpiły o wszczęcie postępowania - (art. 49 § 4) - tylko w sprawach o przestępstwa, którymi wyrządzono szkodę w mieniu instytucji państwowej, samorządowej lub społecznej, jeżeli nie działa organ pokrzywdzonej instytucji.

Wydaje się, że byłoby celowe, aby z praw pokrzywdzonego korzystała także instytucja (organ) występujący w interesie publicznym w celu ochrony konstytucyjnie określonych praw i wolności obywateli, nie tylko instytucje ujawniające przestępstwa, którymi wyrządzono szkodę w mieniu.

Ministra Transportu i Gospodarki Morskiej (GI-DP-024/1580/00)

- w sprawie zgodności z przepisami o ochronie danych osobowych wzoru legitymacji potwierdzającej uprawnienie do niestosowania się do niektórych znaków drogowych, stanowiącego załącznik do rozporządzenia Ministra Transportu i Gospodarki Morskiej z dnia 29 czerwca 2000 r. w sprawie określenia wzoru i szczegółowych zasad wydawania przez starostę legitymacji potwierdzających uprawnienie do niestosowania się do niektórych znaków drogowych (Dz. U. Nr 65, poz. 781), zwane dalej rozporządzeniem, z prośbą o rozważenie możliwości nowelizacji przedmiotowego rozporządzenia w zakresie wzoru legitymacji.

Zgodnie z instrukcją wprowadzoną przez organy wydające legitymacje, tj. przez starostów, którym uprawnienie to przysługuje na mocy § 1 powołanego wyżej rozporządzenia,

w razie pozostawienia pojazdu na postoju legitymacja powinna być umieszczona od wewnętrznej strony przedniej szyby w taki sposób, aby symbol był widoczny z zewnątrz. Wymóg ten nie dotyczy osób niepełnosprawnych korzystających z wózków inwalidzkich lub pojazdów zaopatrzonych z tyłu w znak lub nalepkę z wymienionym symbolem.

Według § 2 ust. 1 pkt 2 rozporządzenia, legitymacja powinna zawierać m.in. dane osoby korzystającej z uprawnień przewidzianych rozporządzeniem, tj. jej imię i nazwisko, datę urodzenia oraz adres zamieszkania. Wzór legitymacji, określony w załączniku do rozporządzenia, przewiduje, że dokładne dane osobowe, łącznie z adresem, pozwalające na określenie tożsamości osoby uprawnionej, umieszczone są na stronie 1 legitymacji, obok symbolu wskazującego na niepełnosprawność. Taki sposób określenia wzoru legitymacji powoduje, że aby skorzystać z przysługujących uprawnień osoba niepełnosprawna ujawnić musi osobom postronnym swoje dokładne dane osobowe.

Należy podkreślić, iż projekt rozporządzenia był opiniowany przez Ogólnopolską Federację Organizacji Osób Niepełnosprawnych, która przekazała w dniu 6 czerwca 2000 r. Ministrowi Transportu i Gospodarki Morskiej swoje uwagi, łącznie z projektem wzoru legitymacji. We wzorze legitymacji, w wersji zaproponowanej przez Federację, symbol niepełnosprawności umieszczony został na 1 stronie, natomiast dane osobowe jej właściciela na stronie 2 legitymacji. Ten sposób określenia wzoru legitymacji eliminuje konieczność ujawniania danych umożliwiających stwierdzenie tożsamości właściciela samochodu i w opinii Generalnego Inspektora zasługuje na uwzględnienie.

W związku z powyższymi uwagami GIODO zwrócił się do Ministra Transportu i Gospodarki Morskiej o rozważenie możliwości nowelizacji przedmiotowego rozporządzenia w zakresie uwzględniającym uwagi Ogólnopolskiej Federacji Organizacji Osób Niepełnosprawnych Ruchowo.

Ministra Spraw Wewnętrznych i Administracji (GI – 265/00 z dnia 27 marca 2000 r.)

- w sprawie terminowości udzielania informacji adresowej przez Centralne Biuro Adresowe

W związku ze skargami dotyczącymi nieterminowości udzielania informacji przez CBA, GIODO zwrócił się do MSWiA wskazując, iż mimo prawidłowo skierowanego wniosku o udostępnienie danych ze zbioru danych osobowych, którego wzór stanowi załącznik nr 1 do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia wzorów wniosku udostępnienie danych osobowych,

zgłoszenia zbioru danych do rejestracji oraz imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. Nr 80, poz. 522 z późn. zm.), skarżący, pomimo upływu ponad dwóch miesięcy, nie otrzymywali żadnej odpowiedzi; nie poinformowano ich także, czy informacje takie zostaną im udzielone, czy też nie.

Zgodnie z treścią art. 29 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.) dane osobowe, z wyłączeniem tzw. danych wrażliwych, o których mowa w art. 27 ust. 1 ustawy, mogą być udostępnione w celach innych niż włączenie do zbioru, innym osobom i podmiotom, niż wymienione w ust. 1 tego artykułu, jeżeli w sposób wiarygodny uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą. Administrator danych winien udzielić informacji adresowej, jeżeli jest to potrzebne, np. do dochodzenia spraw przed sądem, a nie zachodzą przesłanki odmowy udostępnienia danych osobowych - opisane w art. 30 ustawy - podmiotom innym niż wymienione w art. 29 ust. 1. Zgodnie z treścią art. 30 ustawy odmowa udostępnienia danych mogłaby nastąpić, ze względu na: 1) ujawnienie wiadomości stanowiących tajemnicę państwową, 2) zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi, mienia lub bezpieczeństwa i porządku publicznego, 3) zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa, 4) istotne naruszenie dóbr osobistych osób, których dane dotyczą, lub innych osób.

Ministra Spraw Wewnętrznych i Administracji (GI – 633/00 z dnia 30 czerwca 2000 r.)

- w sprawie skarg dotyczących zbyt szerokiego zakresu przetwarzania danych osobowych umieszczanych na druku „Zgłoszenie pobytu stałego”, z prośbą o rozważenie ewentualnej zmiany przepisu § 7 ust. 1 pkt 10 i 11 rozporządzenia Ministra Spraw Wewnętrznych z dnia 28 czerwca 1984 r. w sprawie wykonywania obowiązku meldunkowego i prowadzenia ewidencji ludności (Dz. U. Nr 32, poz. 176 z późn. zm.).

Generalny Inspektor Ochrony Danych Osobowych poinformował, iż do Biura GODO wpływa szereg skarg od obywateli, dotyczących zbyt szerokiego zakresu przetwarzania danych osobowych w druku „Zgłoszenie pobytu stałego”. W świetle tych skarg, jak też w świetle analizy przepisów rozporządzenia Ministra Spraw Wewnętrznych z dnia 28 czerwca 1984 r. w sprawie wykonywania obowiązku meldunkowego i prowadzenia ewidencji ludności (Dz. U. Nr 32, poz. 176 z późn. zm.), wydaje się niezasadne - wynikające z § 7 ust. 1 pkt. 10 i 11 - zobowiązanie osób fizycznych, w ramach obowiązku

meldunkowego, do zgłoszenia danych o wykształceniu i zawodzie wyuczonym, miejscu pracy i zawodzie wykonywanym, imion i nazwisk rodowych rodziców, jak również nazwisk z poprzedniego małżeństwa.

Zgodnie z art. 1 ust. 2 ustawy z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych (Dz. U. z 1984 r. Nr 32, poz. 174 z późn. zm.), ewidencja ludności polega m.in. na rejestracji danych o miejscu pobytu. Każda osoba przebywająca na terytorium Polski, niezależnie od obywatelstwa, powinna wykonać obowiązek meldunkowy określony w ustawie. W myśl art. 4 cytowanej ustawy, obowiązek meldunkowy może polegać m.in. na zameldowaniu się w miejscu pobytu stałego lub czasowego, a także wymeldowaniu się z takiego miejsca.

Wydane na podstawie art. 51 ust. 1 i 3 ustawy o ewidencji ludności i dowodach osobistych, rozporządzenie Ministra Spraw Wewnętrznych z dnia 28 czerwca 1984 r. w sprawie wykonywania obowiązku meldunkowego i prowadzenia ewidencji ludności (Dz. U. z 1984 r. Nr 32, poz. 176 z późn. zm.) reguluje m.in. zakres danych zgłaszanych przy zameldowaniu na pobyt stały. Zgodnie z § 7 ust. 1 pkt 10 i 11 cytowanego rozporządzenia, przy zameldowaniu na pobyt stały należy zgłosić dane o wykształceniu i zawodzie wyuczonym, jak również dane o miejscu pracy i wykonywanym zawodzie.

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.), zwana dalej ustawą, w art. 23 ust. 1 określiła przesłanki dopuszczalności przetwarzania danych. Jednocześnie zobligowała administratora danych do zachowania szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności do tego, aby dane te były adekwatne do celów, w jakich są przetwarzane. Zgodnie z zasadą adekwatności wyrażoną w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych, wymienione dane wydają się nieadekwatne do celu, w jakim są przetwarzane.

Zmiany wymaga również zakres danych niezbędnych do wypełnienia druku „Zgłoszenie pobytu stałego”.

Ponadto § 7 rozporządzenia w sprawie wykonywania obowiązku meldunkowego i prowadzenia ewidencji ludności w ust. 1 pkt 4 wskazuje na obowiązek podania stanu cywilnego. Pod tym pojęciem powinno się rozumieć informację o tym, czy dana osoba pozostaje w związku małżeńskim, czy też jest osobą stanu wolnego. Nieuzasadnionym wydaje się zatem zgłoszenie informacji o tym, czy dana osoba jest rozwiedziona, czy też jest osobą wolną wskutek śmierci współmałżonka, jak też informacji o nazwisku małżonka, z którym się rozwiodła. Zakres takich danych nie tylko wykracza poza cel, jakim mają one służyć - a więc zameldowanie się w nowym miejscu pobytu - ale również ingeruje w sferę

prywatności. Podobnie, zbędne dla realizacji przedmiotowego celu, jest umieszczenie imion i nazwisk rodowych rodziców na druku „Zgłoszenie pobytu stałego.”

Przewodniczącego Sejmowej Komisji Transportu i Łączności (GI – 412/00 z dnia 10 maja 2000 r.)

- w sprawie ewentualnego uzupełnienia przepisów dyskutowanego w Sejmowej Komisji Transportu i Łączności projektu ustawy Prawo telekomunikacyjne o przepisy pozwalające na udzielanie abonentom – pokrzywdzonym w sprawach o wykroczenia przez operatorów telefonii stacjonarnej i komórkowej, informacji o numerach połączeń przychodzących na numer ich stacji abonenckiej.

Jak wynika z pism przychodzących do Generalnego Inspektora Ochrony Danych Osobowych, do Prokuratur zgłaszają się abonenci niepokojeni tzw. głuchymi telefonami. Abonenci zwracają się do operatorów sieci w celu uzyskania informacji o numerach telefonów osób ich niepokojących. Operatorzy sieci powołują się na ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.), oraz na rozporządzenie Ministra Łączności z dnia 8 lutego 1996 r. w sprawie ogólnych warunków świadczenia usług telekomunikacyjnych w sieci telekomunikacyjnej użytku publicznego (Dz. U. Nr 20, poz. 93 z późn. zm.). W przypadku czynu, polegającego na złośliwym niepokojeniu abonenta tzw. głuchymi telefonami, Prokuratura nie prowadzi postępowania karnego, czyn ten bowiem nie stanowi przestępstwa, lecz wykroczenie opisane w art. 107 Kodeksu wykroczeń. Pokrzywdzony, który sam nie jest w stanie uzyskać informacji o numerach telefonów przychodzących na jego numer z innych stacji abonenckich, nie ma w tej sytuacji możliwości obrony swych praw. Nie może bowiem złożyć wniosku o ukaranie do kolegium ds. wykroczeń, jeżeli nie zna tożsamości sprawcy przedmiotowego wykroczenia. Operatorzy sieci telekomunikacyjnej odmawiają mu informacji mogących doprowadzić do ustalenia sprawcy.

W rozumieniu ustawy o ochronie danych osobowych za dane osobowe uważa się każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby (art. 6). Informacja zawierająca wyłącznie numer telefonu osoby fizycznej bez bliższego jej dookreślenia (np. imienia, nazwiska, adresu zamieszkania), nie stanowi danej osobowej w rozumieniu cytowanej ustawy, choć w odniesieniu do pewnych stanów faktycznych za taką może być uważana.

Rozporządzenie Ministra Sprawiedliwości w sprawie ogólnych warunków świadczenia usług telekomunikacyjnych w sieci telekomunikacyjnej użytku publicznego

nakłada w § 4 ust. 1 pkt 6, na operatora sieci obowiązek zapewnienia własnym abonentom uzyskania informacji o numerach stacji abonenckich osiąganych z ich stacji abonenckiej. Tak sformułowany zapis utrudnia działanie pokrzywdzonych, jak i organów ścigania, podejmowane w celu wykrycia potencjalnych sprawców wykroczeń, albowiem nie nakłada na operatora sieci obowiązku ujawnienia informacji o numerach przychodzących na stację abonencką pokrzywdzonego. GODO zwrócił się z prośbą o rozważenie możliwości uwzględnienia w nowym prawie telekomunikacyjnym, obowiązku udzielania przez operatora sieci, osobie pokrzywdzonej przez popełnienie na niej wykroczenia, informacji o numerach telefonów przychodzących na numer jej stacji abonenckiej. Zapis taki nie będzie stać w sprzeczności z ustawą o ochronie danych osobowych i niewątpliwie przyczyniłby się w dużym stopniu do zwiększenia wykrywalności sprawców tzw. głuchych telefonów.

Pełnomocnika Rządu ds. Wprowadzenia Powszechnego Ubezpieczenia Zdrowotnego (GI-DIS-32/00 z dnia 30 czerwca 2000 r.)

- w sprawie żądania przez Kasy Chorych od oferentów (świadczeniodawców), przy składaniu ofert na zawieranie umów o udzielanie świadczeń zdrowotnych, list osób, które złożyły deklarację o korzystaniu z usług danej placówki podstawowej opieki zdrowotnej, zawierających dane osobowe pacjentów w postaci nazwiska, imienia, nr PESEL, daty urodzenia, płci oraz adresu.

Zgodnie z art. 23 ust. 1 pkt 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.), przetwarzanie danych jest dopuszczalne wtedy, gdy zezwalają na to przepisy prawa. Sposób i zakres przetwarzanych przez Kasy Chorych danych osób ubezpieczonych został określony w rozdziale 7a ustawy z dnia 6 lutego 1997 r. o powszechnym ubezpieczeniu zdrowotnym (Dz. U. Nr 28, poz. 153 z późn. zm.) oraz w rozporządzeniu Ministra Zdrowia i Opieki Społecznej z dnia 15 stycznia 1999 r. w sprawie ustalenia zakresu niezbędnych danych gromadzonych przez świadczeniodawców oraz w systemach informatycznych Kas Chorych, a także zakresu i procedury wymiany danych pomiędzy Kasami Chorych oraz Kasami Chorych a świadczeniodawcami, Urzędem Nadzoru Ubezpieczeń Zdrowotnych i Krajowym Związkiem Kas Chorych (Dz. U. Nr 7, poz. 66).

Obowiązek przeprowadzenia konkursu ofert na zawieranie przez Kasy Chorych umów o udzielanie świadczeń zdrowotnych został wprowadzony przepisem art. 54 ust. 1 ustawy o powszechnym ubezpieczeniu zdrowotnym. Natomiast tryb składania ofert oraz sposób przeprowadzania konkursu reguluje rozporządzenie Ministra Zdrowia i Opieki Społecznej z dnia 27 listopada 1998 r. w sprawie konkursu ofert na zawieranie przez Kasy

Chorych umów o udzielanie świadczeń zdrowotnych (Dz. U. Nr 148, poz. 978 z późn. zm.), wydane na podstawie art. 54 ust. 2 wskazanej ustawy. Przepisy powyższego rozporządzenia nie nakładają jednak na oferentów obowiązku dołączenia do oferty imiennej listy osób (wraz z dookreślającymi ich danymi osobowymi), które zadeklarowały chęć korzystania z usług danej placówki. Przedmiotowego obowiązku nie można w szczególności wyprowadzić z brzmienia § 6 pkt 3 wskazanego rozporządzenia, zgodnie z którym zamawiający, w ogłoszeniu o konkursie ofert, jest zobligowany określić warunki, jakie powinna spełniać oferta. Obowiązek taki powinien bowiem, aby nie pozostawać w sprzeczności z przytoczonym wyżej przepisem art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych, wynikać wprost z przepisów prawa; natomiast nie może zostać narzucony przez Kasy Chorych.

Podstawy prawnej do żądania przez Kasy Chorych przedmiotowej listy nie stanowi również art. 141 a ust. 1 ustawy o powszechnym ubezpieczeniu zdrowotnym. Wskazany przepis wylicza enumeratywnie cele, dla realizacji których Kasa Chorych może pozyskiwać i przetwarzać dane osób ubezpieczonych. Jednakże żaden z nich nie uprawnia Kasy Chorych do żądania danych osób, które złożyły deklarację o korzystaniu z usług danego ośrodka (oferenta).

Wymóg dołączania do oferty przedmiotowej listy nie znajduje także uzasadnienia w przepisach rozporządzenia Ministra Zdrowia i Opieki Społecznej w sprawie ustalenia zakresu niezbędnych danych gromadzonych przez świadczeniodawców (...). Przepisy powyższego rozporządzenia regulują bowiem przekazywanie Kasom Chorych przez świadczeniodawców, z którymi Kasy Chorych mają zawarte umowy, danych dotyczących świadczeń wykonanych na rzecz osób ubezpieczonych, w zakresie określonym w § 3 wskazanego rozporządzenia.

Wobec powyższego należy stwierdzić, iż żądanie od oferentów przez Kasy Chorych, przy składaniu ofert na zawieranie umów o udzielanie świadczeń zdrowotnych, list osób, które złożyły deklarację o korzystaniu z usług danej placówki podstawowej opieki zdrowotnej, zawierających dane osobowe pacjentów, jako nie znajdujące uzasadnienia w powołanych wyżej przepisach, pozostaje w sprzeczności z art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych. Z punktu widzenia zgodności z ustawą o ochronie danych osobowych za wystarczające do prawidłowego przeprowadzenia konkursu ofert należy uznać informowanie Kasy Chorych wyłącznie o liczbie pacjentów, którzy będą korzystać z usług danego ośrodka, bez przekazywania Kasie Chorych dotyczących ich danych osobowych.

Z tego też powodu GİODO zwrócił się do Ministra Zdrowia i Opieki Społecznej z prośbą o podjęcie działań zmierzających do wyeliminowania praktyki Kas Chorych, jako nie

znajdującej podstawy prawnej i w związku z tym naruszającej przepisy ustawy o ochronie danych osobowych.

Podobne w treści wystąpienie skierowane zostało do *Urzędu Nadzoru Ubezpieczeń Zdrowotnych*

Prezesa Urzędu Nadzoru Ubezpieczeń Zdrowotnych (GI-DP-1045/00 z dnia 10 listopada 2000 r.)

- w sprawie uchybień i nieprawidłowości w pracy Kas Chorych w zakresie przetwarzania danych osobowych, ujawnionych wskutek skarg obywateli oraz w toku przeprowadzanych inspekcji.

W związku z przeprowadzaną reformą służby zdrowia, do Generalnego Inspektora Ochrony Danych Osobowych wpłynęło wiele pism z prośbą o interpretację i skarg dotyczących funkcjonowania Kas Chorych. Pytania dotyczyły głównie przekazywania danych między Kasami Chorych, zakresu i sposobu ich przekazywania między świadczeniodawcami a Kasami Chorych. Większość skarg napływających do Biura Generalnego Inspektora Ochrony Danych Osobowych dotyczyła udostępniania Kasom Chorych danych osobowych pacjentów Zakładów Opieki Zdrowotnej.

Zakres danych osobowych, które mogą przetwarzać Kasy Chorych wskazany został w rozdziale 7 a ustawy z dnia 6 lutego 1997 r. o powszechnym ubezpieczeniu zdrowotnym (Dz. U. Nr 28, poz. 152 z późn. zm.). Na podstawie art. 141 a ust. 2 cytowanej ustawy, dla realizacji zadań wymienionych w ust. 1 tego przepisu. Kasy Chorych mają prawo przetwarzania następujących danych osobowych:

- 1) imię i nazwisko,
- 2) numer PESEL,
- 3) data urodzenia,
- 4) płeć,
- 5) stopień pokrewieństwa z opłacającym składkę,
- 6) adres zamieszkania,
- 7) stopień niepełnosprawności, jeżeli dziecko ukończyło 26 lat,
- 8) udzielone ubezpieczonemu świadczenia zdrowotne, których charakterystyka zawiera między innymi:
 - a. rodzaj udzielonego świadczenia

b. świadczeniodawcę wykonującego usługę,
świadczeniodawcę zlecającego usługę, d) rozpoznanie według międzynarodowej klasyfikacji chorób, urazów i zatruc związane z wykonaną usługą.

Na podstawie ustawy o powszechnym ubezpieczeniu zdrowotnym zostało wydane rozporządzenie Ministra Zdrowia i Opieki Społecznej z dnia 15 stycznia 1999 r. w sprawie ustalenia niezbędnych danych gromadzonych przez świadczeniodawców oraz w systemach informatycznych Kas Chorych, a także zakresu i procedury wymiany danych pomiędzy Kasami Chorych oraz Kasami Chorych a świadczeniodawcami, Urzędem Nadzoru Ubezpieczeń Zdrowotnych i Krajowym Związkiem Kas Chorych (Dz. U. Nr 7, poz. 66). Przepisy rozporządzenia szczegółowo określają jakie dane gromadzą w systemach informatycznych świadczeniodawcy oraz Kasy Chorych.

Stosownie do § 3 cytowanego rozporządzenia, świadczeniodawcy usług medycznych są zobowiązani do przekazywania Kasom Chorych, z którymi mają zawarte umowy, następujące dane dotyczące świadczeń wykonanych na rzecz ubezpieczonych w nich osób:

- 1) numer ewidencyjny PESEL pacjenta, jeżeli został nadany,
- 2) numer karty ubezpieczenia,
- 3) numer służący do potwierdzenia wykonania świadczenia, uzyskany z karty ubezpieczenia - w przypadku, gdy karta jest stosowana do potwierdzenia świadczeń,
- 4) kod rodzaju świadczenia,
- 5) kod rozpoznania medycznego związanego z udzielonym świadczeniem według międzynarodowej klasyfikacji chorób, urazów i zatruc,
- 6) opłata wniesiona przez pacjenta,
- 7) dopłata ze strony Kasy Chorych,
- 8) numer REGON świadczeniodawcy wykonującego,
- 9) typ komórki organizacyjnej świadczeniodawcy, w której wykonano świadczenie, 10) data początku wykonywania świadczenia,
- 10) data wykonania (końca wykonywania) świadczenia,
- 11) numer REGON świadczeniodawcy zlecającego,
- 12) typ komórki organizacyjnej świadczeniodawcy zlecającego,
- 13) numer prawa wykonywania zawodu lekarza zlecającego,
- 14) data zlecenia.

Świadczeniodawcy są zobowiązani przekazywać regionalnej Kasie Chorych, na obszarze której prowadzą działalność, wymienione wyżej dane oraz symbol Kasy Chorych, w

której pacjent jest ubezpieczony, dotyczące świadczeń wykonanych na rzecz ubezpieczonych w Kasach Chorych, z którymi nie mają zawartej umowy.

Tymczasem wysuwane przez Kasy Chorych żądania przekazywania danych wykraczały poza szczegółowe regulacje zawarte w powołanym rozporządzeniu.

W związku z nieuprawnionymi żądaniami Kas Chorych, dotyczącymi zakresu przekazywanych danych osobowych, Biuro Generalnego Inspektora Ochrony Danych Osobowych było informowane przez zakłady opieki zdrowotnej o następujących nieprawidłowościach:

1. Świętokrzyska Regionalna Kasa Chorych zobowiązała zakład opieki medycznej do prowadzenia dokumentacji medycznej, która wymaga od osób korzystających ze świadczeń zdrowotnych podania danych takich, jak: imię, nazwisko, data urodzenia, miejsce zamieszkania, numer ewidencyjny PESEL, twierdząc, że dane te są niezbędne w celu dokonania rozliczeń finansowych z Kasą Chorych (GI-DP-318/99, GI-DP-390/99);
2. Mazowiecka Regionalna Kasa Chorych oraz Branżowa Kasa Chorych zwróciły się do jednego z zakładów opieki zdrowotnej w Warszawie o przekazanie danych osobowych leczonych pacjentów: imię i nazwisko, data urodzenia, adres, PESEL, określenie głównej jednostki chorobowej według ICD-10, data przyjęcia do szpitala, data wypisania ze szpitala lub data zgonu (GI-DP-424/99);
3. Dolnośląska Regionalna Kasa Chorych wymaga od zakładów opieki zdrowotnej podawania imienia, nazwiska i miejsca zamieszkania pacjentów w postaci wydruków komputerowych (GI-DP-509/99);
4. Mazowiecka Regionalna Kasa Chorych wymaga od jednego z zakładów opieki zdrowotnej przekazania wydruku bazy danych z informacją o chorych. Do bazy należy wpisać imię, nazwisko, datę urodzenia, adres oraz rozpoznanie choroby pacjenta (GI-DP-1536/99);
5. Zachodniopomorska Regionalna Kasa Chorych zażądała od zakładu opieki zdrowotnej przekazywania wykazów chorych zawierających imiona i nazwiska pacjentów. Ponadto urzędnicy tej Kasy Chorych żądają możliwości kserowania dokumentacji medycznej leczonych pacjentów (GI-DP-1382/99);
6. Warmińsko - Mazurska Regionalna Kasa Chorych zwróciła się do zakładu opieki zdrowotnej z żądaniem przekazania danych osobowych pacjentów tego zakładu, takich jak: imię, nazwisko, adres zamieszkania (GI-DP-548/99).

Poza wymienionymi przypadkami nieuprawnionego żądania przekazywania danych osobowych pacjentów przez Kasy Chorych do Biura napływają liczne pytania pacjentów i personelu medycznego o zakres danych, których przekazania od zakładów opieki zdrowotnej mogą żądać Kasy Chorych.

Skargi zakładów opieki zdrowotnej dotyczą również żądań sporządzania, dla potrzeb Kas Chorych, dokładnych zestawień monitorujących zawarte kontrakty. Taką skargę złożył zakład opieki zdrowotnej na Zachodniopomorską Regionalną Kasę Chorych, która zobowiązała tenże ZOZ do sporządzania comiesięcznych zestawień zawierających: imię i nazwisko pacjenta, kod choroby, rodzaj usługi, data usługi, miejsce wykonania usługi oraz dane lekarza wykonującego usługę. Dane te w sposób jawny i bez kodowania są przekazywane Kasie Chorych na dyskietkach (GI-DP-487/99).

Zakład opieki zdrowotnej złożył protest wobec zobowiązania tego zakładu przez Branżową Kasę Chorych dla Służb Mundurowych do przedkładania w formie elektronicznej comiesięcznych sprawozdań zawierających dane personalne zatrudnionych lekarzy, takich jak: imię i nazwisko, adres, numer telefonu, płeć, PESESL, numer prawa wykonywania zawodu, numer identyfikacyjny ZUS do zwolnień lekarskich (GI-DP-361/00).

Zakład opieki zdrowotnej poinformował, że podczas kontroli tej placówki przedstawiciele Kujawsko-Pomorskiej Regionalnej Kasy Chorych przeglądali Księgę Główną chorych, w której zawarte są: nazwisko i imię chorego, imiona rodziców, numer PESEL, data i miejsce urodzenia, stan cywilny, miejsce zamieszkania chorego i najbliższej rodziny lub opiekunów, podstawa do bezpłatnego leczenia, nazwa i adres pracodawcy chorego, dokument uprawniający do świadczeń, data przyjęcia do szpitala, rozpoznanie lekarskie, data wypisu ze szpitala, data zgonu, liczba dni pobytu w szpitalu, numer Kasy Chorych, lekarz kierujący. Ponadto przedstawiciele Kasy Chorych sporządzali kserokopie Księgi Główniej (GI-DP-969/99).

Wielkopolska Regionalna Kasa Chorych zobowiązała jeden z zakładów opieki zdrowotnej do przedłożenia kopii umów o pracę, zawartych z osobami zatrudnianymi przez świadczeniodawcę, pod rygorem rozwiązania z nim umowy bez wypowiedzenia (GI-DP-1354/99). Kasa poinformowała także Zakład, że niedołączenie do oferty kopii umów o pracę z pracownikami zatrudnionymi przez świadczeniodawcę spowoduje odrzucenie oferty.

Wątpliwości wzbudzała również kwestia rozszerzenia zakresu danych udostępnianych Kasom Chorych w drodze umowy.

Zgodnie z art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych, podstawą dopuszczalności przetwarzania danych wrażliwych może być jedynie przepis szczególny

innej ustawy. Oznacza to, że nie jest dopuszczalne określanie w drodze umów, pomiędzy Kasami a świadczeniodawcami usług medycznych, szerszego zakresu danych, niż przewidziane w przepisach prawa.

Biuro Generalnego Inspektora Ochrony Danych Osobowych poinformowano o fakcie żądania przez Śląską Regionalną Kasę Chorych przekazywania, na podstawie umowy zawartej z zakładem opieki zdrowotnej, danych w zakresie szerszym aniżeli wynika to z przepisów rozporządzenia Ministra Zdrowia i Opieki Społecznej z dnia 15 stycznia 1999 r. w sprawie ustalenia niezbędnych danych gromadzonych przez świadczeniodawców oraz w systemach informatycznych Kas Chorych (GI-DP-281/00, GI-DP-334/00/656).

Do Biura GODO napływały także pytania dotyczące obowiązku informacyjnego spoczywającego na Kasach Chorych. Łódzka Regionalna Kasa Chorych zwróciła się z pytaniem, czy ma ona obowiązek poinformowania osób, których dane pozyskała w zbiorze od Terenowego Banku Danych (GI-DP-778/99). Kasa Chorych powinna wykazać podstawę prawną żądania przekazania jej danych przez Terenowy Bank Danych. Analiza przepisów ustawy z dnia 6 lutego 1997 r. o powszechnym ubezpieczeniu zdrowotnym nie pozwala na twierdzenie, że na mocy tych przepisów Kasy Chorych mogą zbierać dane osoby, której one dotyczą, bez jej zgody. W związku z powyższym Kasy Chorych nie są zwolnione z obowiązku informacyjnego.

Wątpliwości budzi także kwestia udostępniania danych przez Kasy Chorych ze swoich zbiorów.

Przewodnicząca Szczecińskiej Izby Pielęgniarek i Położnych złożyła skargę na odmowę udostępnienia przez Dyrektora Zachodniopomorskiej Regionalnej Kasy Chorych danych osobowych zatrudnionych w Kasie pielęgniarek i położnych. Dane te były niezbędne do wykonywania ustawowych czynności przez Szczecińską Izbę Pielęgniarek i Położnych (GI-DP-605/00/724).

Zgodnie z art. 29 ust. 1 ustawy o ochronie danych osobowych, administrator danych udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do tego na mocy przepisów prawa. Stosownie zaś do ust. 2 tego artykułu, dane te mogą być również udostępniane innym osobom lub podmiotom, jeżeli w sposób wiarygodny uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą. Dane te udostępnia się na pisemny, umotywowany wniosek, którego wzór został określony w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia wzorów wniosku o udostępnienie danych osobowych, zgłoszenia zbioru danych do rejestracji oraz imiennego upoważnienia i legitymacji służbowej

inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. Nr 80, poz. 522 z późn. zm.).

Przedmiotem zainteresowania Generalnego Inspektora była także poprawność oświadczenia zawartego w skierowaniu na leczenie uzdrowiskowe, wynikającego z przepisów z przepisów rozporządzenia Ministra Zdrowia i Opieki Społecznej z dnia 30 grudnia 1998 r. w sprawie sposobu i warunków wystawiania skierowania na leczenie uzdrowiskowe przez lekarza ubezpieczenia zdrowotnego oraz potwierdzania tego skierowania przez Kasę Chorych (Dz. U. Nr 166, poz. 1262). Powstały wątpliwości, czy zakres tego oświadczenia nie jest zbyt szeroki, bowiem zgoda („wyrażam zgodę na przetwarzanie danych osobowych dotyczących mojej osoby, polegających w szczególności na zbieraniu, utrwalaniu, przechowywaniu i udostępnianiu danych, ujawnionych w niniejszym skierowaniu”) nie jest ograniczona nawet stwierdzeniem „dla celów medycznych” (GI-DP-116/99).

W powyższej sprawie Generalny Inspektor skierował do Ministra Zdrowia i Opieki Społecznej pismo z dnia 21 czerwca 1999 r. (GI-644/99). Niepokój budzi zwłaszcza fakt, iż dane o stanie zdrowia mogą być ujawnione także osobom, w stosunku do których nie obowiązują przepisy o tajemnicy lekarskiej czy pielęgniarek lub położnych. W ocenie Generalnego Inspektora uzyskanie zgody na przetwarzanie tych danych przez podmioty medyczne jest zbędne, zaś gdyby dane te miałyby być ujawnione innym podmiotom winno to być szczegółowo określone. W związku z tym Generalny Inspektor wniósł w swoim piśmie - bezskutecznie - o rozważenie możliwości nowelizacji powołanego rozporządzenia Ministra Zdrowia i Opieki Społecznej z dnia 30 grudnia 1998 r.

Stosownie do art. 40 ustawy o ochronie danych osobowych, administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1 ustawy. Obowiązek ten powinien być dopełniony przed rozpoczęciem przetwarzania danych w zbiorze (art. 46).

Kasy Chorych, na podstawie art. 72 pkt 1 ustawy o powszechnym ubezpieczeniu zdrowotnym, prowadzą ewidencję osób objętych ubezpieczeniem zdrowotnym. W związku z powyższym na Kasach Chorych, jako na administratorach danych, ciąży obowiązek prowadzenia (od dnia 1 stycznia 1999 r.) oraz zarejestrowania przedmiotowych zbiorów danych w Biurze Generalnego Inspektora Ochrony Danych Osobowych.

Obowiązku zarejestrowania wymienionych wyżej zbiorów nie dopełniły następujące Kasy Chorych:

1. Kujawsko-Pomorska Regionalna Kasa Chorych do dnia 1 czerwca 2000 r. zgłosiła do rejestracji jedynie zbiór danych osób zatrudnionych w tej Kasie oraz zbiór danych osobowych osób skierowanych na leczenie sanatoryjne;
2. Lubuska Regionalna Kasa Chorych nie zgłosiła do rejestracji żadnego zbioru danych;
3. Warmińsko-Mazurska Regionalna Kasa Chorych nie zgłosiła do rejestracji żadnego zbioru danych;
4. Podlaska Regionalna Kasa Chorych nie zgłosiła do rejestracji żadnego zbioru danych.

Brak zgłoszenia prowadzonych przez Kasy zbiorów danych wypełnia znamiona przestępstwa określonego w art. 53 ustawy o ochronie danych osobowych. W związku z tym Generalny Inspektor Ochrony Danych Osobowych, pismami z dnia 15 maja i 2 czerwca 2000 r., skierował do właściwych prokuratur zawiadomienie o popełnieniu przestępstwa przez osoby sprawujące zarząd w poszczególnych Kasach Chorych (GI/527/00, GI/443/00, GI/444/00, GI/442/00).

Urzędu Nadzoru Ubezpieczeń Zdrowotnych (GI-DP-1097/00 z dnia 24 października 2000 r.)

- w sprawie przesłanek przetwarzania danych osobowych, określonych w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.)

Generalny Inspektor Ochrony Danych Osobowych skierował wystąpienie w związku z pytaniem skierowanym przez Urząd Nadzoru Ubezpieczeń Zdrowotnych, jak też w związku ze skargami na placówki opieki zdrowotnej i Kasy Chorych, wskazującymi na błędną interpretację ustawy o ochronie danych osobowych przez te podmioty. GODO wskazał, że przetwarzanie danych osobowych jest dopuszczalne wyłącznie po spełnieniu co najmniej jednej z przesłanek określonych w ustawie o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.), zwanej dalej ustawą.

Przesłanki te wymienia m.in. art. 23 oraz art. 27 ustawy. W myśl art. 23 ust. 1 pkt 2 przetwarzanie danych osobowych jest dopuszczalne, jeżeli zezwalają na to przepisy prawa. Art. 27 ust. 2 pkt 2 natomiast przewiduje, że dane wrażliwe (np. dane o stanie zdrowia) mogą być przetwarzane, jeżeli przepis innej ustawy tak stanowi i stworzone zostają pełne gwarancje ochrony danych.

Zgodnie z art. 6 ustawy za dane osobowe uważa się każdą informację, która pozwala na określenie tożsamości osoby fizycznej. Jeżeli przekazywane informacje dotyczyć mają wyłącznie zakładów opieki zdrowotnej, umów zawartych pomiędzy Kasami Chorych a

świadczeniodawcami, i nie stanowią danych osobowych w rozumieniu ustawy o ochronie danych osobowych, to zgodnie z art. 2 ust. 1 ustawa o ochronie danych osobowych nie znajduje zastosowania. Jeśli jednak dane takie uznać można za dane osobowe, wówczas konieczne jest spełnienie jednej z przesłanek określonych w ustawie o ochronie danych osobowych. Zakres danych i krąg podmiotów, którym Kasy Chorych mogą przekazywać dane określony został szczegółowo w rozporządzeniu Ministra Zdrowia i Opieki Społecznej z dnia 15 stycznia 1999 r. w sprawie ustalenia zakresu niezbędnych danych gromadzonych przez świadczeniodawców oraz w systemach informatycznych Kas Chorych, a także zakresu i procedury wymiany danych pomiędzy Kasami Chorych oraz Kasami Chorych a świadczeniodawcami, Urzędem Nadzoru Ubezpieczeń Zdrowotnych i Krajowym Związkiem Kas Chorych (Dz. U. Nr 7 poz. 66 z późn. zm.). Brak jest w przepisach prawa uzasadnienia dla tego rodzaju przetwarzania danych a krąg podmiotów uprawnionych został ściśle określony.

W konkluzji GİODO stwierdził, że Kasy Chorych mogą przekazywać dane osobowe wyłącznie pomiotom określonym w przepisach wymienionego wyżej rozporządzenia lub takim, które spełniają inną przesłankę legalności przetwarzania danych.

Prezesa Zakładu Ubezpieczeń Społecznych (GI – 528/00 z dnia 2 czerwca 2000 r.)

- z wnioskiem o zmianę praktyki oddziałów ZUS, w związku z żądaniami skierowanymi do osób ubiegających się o przyznanie emerytury, które pracowały przez pewien czas za granicą, o dostarczenie zaświadczeń o wysokości zarobków dwóch pracowników pracujących w tym czasie w kraju.

(Sprawa ta była już przedmiotem wystąpienia z dnia 16 sierpnia 1999 r., znak GI-DP-690/99/695, jednak wyjaśnienia udzielone przez ZUS, pismem z dnia 27 października 1999 r., znak Sen 022-161/99, nie dały odpowiedzi na wyrażone w wystąpieniu wątpliwości).

W świetle obowiązującego prawa brak jest podstaw, aby zaświadczenia, których żąda ZUS na podstawie § 10 rozporządzenia Rady Ministrów z dnia 1 kwietnia 1985 r. w sprawie szczegółowych zasad ustalania podstawy wymiaru emerytur i rent (Dz. U. z 1989 r., Nr 11, poz. 63 z późn. zm.), zwanego dalej rozporządzeniem, zawierały - oprócz informacji o wynagrodzeniu, których wymaga przepis § 1 rozporządzenia w celu ustalenia podstawy wymiaru emerytury wnioskodawcy - również dane osobowe osób trzecich. Nie wynika to bowiem z treści przepisu, który mówi o kwocie wynagrodzenia przysługującemu bliżej nie określonego pracownikowi. Powyższy przepis nie upoważnia również do żądania przez ZUS,

by zaświadczenie zawierało informacje o wysokości wynagrodzenia oraz dane osobowe dwóch pracowników. Brak podstawy prawnej powoduje, że przetwarzanie danych osobowych przez ZUS jest niezgodne z ustawą o ochronie danych osobowych. Pracodawca udostępniający takie informacje osobie ubiegającej się o przyznanie emerytury, w sposób pozwalający na zapoznanie się z nimi, łamie również przepisy dotyczące ochrony danych osobowych. W omawianej sprawie wystarczające byłoby podanie przez pracodawcę informacji o wynagrodzeniu w zestawieniu z określonym stanowiskiem, lecz bez podawania danych osobowych.

Zgodnie z art. 66 ustawy z dnia 13 października 1998 r. (Dz. U. Nr 137 późn. 887 z późn. zm.) o systemie ubezpieczeń społecznych, Zakład działa na podstawie tej ustawy oraz innych ustaw regulujących poszczególne zakresy jego działalności. W zakresie prowadzonej działalności Zakładowi przysługują środki prawne właściwe organom administracji państwowej. Zatem uzyskiwanie przez Zakład zgody osób trzecich na przetwarzanie ich danych nie jest konieczne, gdyż w przypadku organów administracji państwowej zakres uprawnień musi wynikać z przepisów prawa.

Przetwarzanie danych jest dopuszczalne jedynie na podstawie art. 23 ustawy o ochronie danych osobowych, musi zatem istnieć wyraźna podstawa prawna dopuszczająca takie działanie. Podstawy takiej nie może również stanowić ogólne uprawnienie ZUS-u do przeprowadzania kontroli dla potrzeb postępowania, mającego na celu ustalenie świadczenia emerytalnego. Cel ten decyduje o zakresie dopuszczalności przetwarzania danych, określonym w przepisie § 1 ww. rozporządzenia, który nie daje podstaw do zbierania danych osobowych osób trzecich w celu ustalenia podstawy wymiaru emerytury wnioskodawcy. ZUS powinien zatem zbierać jedynie informacje, które zgodnie z przepisami wymagane są dla przeprowadzenia postępowania emerytalnego i tylko w takim zakresie przetwarzanie danych będzie odbywać się zgodnie z prawem.

Prezesa Zakładu Ubezpieczeń Społecznych (GI – 713/00 z dnia 20 lipca 2000 r.)

- w sprawie zatrzymywania w dokumentach legitymacji ubezpieczeniowych, co powoduje przetwarzanie przez ZUS danych nieadekwatnych do celu, w tym danych o stanie zdrowia, osób występujących o ponowne naliczenie wysokości emerytury, poprzez, z wnioskiem o podjęcie działań zmierzających do zmiany praktyki w jednostkach ZUS, jako niezgodnej z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133 poz. 883 z późn. zm.).

Zakład Ubezpieczeń Społecznych w związku z postępowaniami o ponowne naliczenie wysokości emerytury żąda od wnioskodawców przedłożenia dowodów uzasadniających prawo do otrzymania świadczenia w nowej wysokości. Fakty mające znaczenie dla ustalenia nowej podstawy wymiaru emerytury mogą być udowodnione zgodnie z przepisami, m.in. wpisami w legitymacjach ubezpieczeniowych, których dostarczenia wymagają inspektoraty ZUS. Legitymacje ubezpieczeniowe, które jako dokumenty pozostają w aktach sprawy, zawierają informacje niezbędne do prawidłowego załatwienia sprawy, np. o okresach zatrudnienia i wysokości osiąganych zarobków, ale również dane, które w sposób bezpośredni lub pośredni określają stan zdrowia wnioskodawcy (informacje o leczeniu wnioskodawcy w różnych poradniach i szpitalach, niektórych badaniach, przebywaniu na zwolnieniach lekarskich). Włączenie legitymacji ubezpieczeniowej do dokumentacji spraw o ponowne naliczenie wysokości emerytury powoduje iż, ww. informacje są również przetwarzane przez ZUS.

Jedną z fundamentalnych zasad przetwarzania danych jest zasada adekwatności. Zgodnie z przepisem art. 26 ust. 1 pkt 3 ustawy, administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane. Stosownie do wskazanego przepisu, niezgodne z ustawą będzie przetwarzanie danych w zakresie wykraczającym poza konieczny dla realizacji celu, w jakim są wykorzystywane.

Organ emerytalny powinien zebrać jedynie takie dane, które są niezbędne do prawidłowego przeprowadzenia postępowania, a ich zakres powinien być adekwatny w stosunku do celu, w jakim będą przetwarzane. Zbieranie danych o stanie zdrowia w istotny sposób narusza zasadę adekwatności przetwarzania danych wprowadzoną przez ustawę, bowiem dla realizacji celu, jakim jest naliczenie nowej wysokości emerytury nie jest konieczne przetwarzanie danych o stanie zdrowia. Organ emerytalny powinien zatem ograniczyć się do danych, które stanowią dowód okoliczności wpływających na wysokość świadczenia. Nie wynika również z przepisów prawa, aby zebranie danych o stanie zdrowia było niezbędne dla ustalenia wysokości emerytury. Zasady przetwarzania danych szczególnie chronionych, jakimi są informacje dotyczące stanu zdrowia, reguluje art. 27 ustawy. Zgodnie z ustępem drugim tego artykułu, przetwarzanie danych o stanie zdrowia jest dopuszczalne m.in., jeżeli przepis szczególny rangi ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą i stwarza pełne gwarancje ich ochrony.

Zbieranie danych o stanie zdrowia dla celów ponownego naliczenia wysokości emerytury koliduje więc z przepisami ustawy o ochronie danych osobowych. Nawet jeżeli informacje zawarte w legitymacjach zbieranych przez ZUS nie są wykorzystywane w jakimkolwiek celu, to samo ich zebranie i przechowywanie jest niezgodne z ustawą.

Rozwiązanie przedstawionego problemu powinno zatem zmierzać do tego, aby ZUS zaprzestał włączania do dokumentacji książeczek ubezpieczeniowych, a jedynie te dane w nich zawarte, których konieczność przetwarzania jest uzasadniona przepisami prawa i rzeczywistą potrzebą realizacji celu, jakim jest ponowne ustalenie wysokości emerytury.

Prezesa Zakładu Ubezpieczeń Społecznych (GI-DP-185/00 z dnia 21 listopada 2000 r.)

- ponownie w sprawie zatrzymywania w dokumentach legitymacji ubezpieczeniowych osób występujących o ponowne naliczenie wysokości emerytury i tym samym przetwarzania danych osobowych tam zawartych nieadekwatnych do celu przetwarzania danych, w szczególności danych o stanie zdrowia, w związku z pismem Zakładu Ubezpieczeń Społecznych (022-110/2000) w ww. sprawie.

Z przedstawionego stanowiska wynika, że zbieranie legitymacji od wnioskodawców wynika z regulacji §§ 20 oraz 21 rozporządzenia Rady Ministrów z dnia 7 lutego 1983 r. w sprawie postępowania o świadczenia emerytalno - rentowe i zasad wypłaty tych świadczeń (Dz. U. Nr 10 poz. 49 z późn. zm.), zwanego dalej rozporządzeniem, zgodnie z którą jest ona środkiem dowodowym stwierdzającym wysokość zarobku lub dochodu stanowiącego podstawę wymiaru emerytury lub renty. Przetwarzanie tych danych jest więc niewątpliwie niezbędne dla realizacji celu, jakim jest naliczenie wysokości świadczenia. Ponadto stwierdzono, że podstawę przetwarzania danych dotyczących okresów niezdolności do pracy stanowi ustawa z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz. U. Nr 162 poz. 1118 z późn. zm.). Wyrażono przy tym opinię, iż informacja taka nie stanowi danych osobowych, co jednak nie ma zasadniczego znaczenia w sprawie, gdyż w przypadku, gdy istnieje podstawa ustawowa do przetwarzania danych o stanie zdrowia, działanie takie nie narusza ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133 poz. 883 z późn. zm.), zwanej dalej ustawą. Zgodnie z art. 27 ust. 2 tej ustawy przetwarzanie danych o stanie zdrowia jest dopuszczalne m. in., gdy zezwalają na to przepisy rangi ustawowej.

Należy jednak zauważyć, że ZUS przetwarza również dane zawarte w książeczce ubezpieczeniowej, które wykraczają poza zakres, jaki jest niezbędny dla realizacji

przedmiotowego celu (informacje o leczeniu, wynikach badań, numerach statystycznych choroby) i tego faktu dotyczyło głównie wystąpienie Generalnego Inspektora. Nie można przyjąć za trafne stanowiska zaprezentowanego w piśmie Zakładu Ubezpieczeń Społecznych, że dane zawarte w legitymacji ubezpieczeniowej nie są w żaden sposób przetwarzane, gdyż w świetle definicji przetwarzania danych, określonej w art. 7 ustawy, przechowywanie danych również stanowi ich przetwarzanie. Przetwarzanie takich danych budzi wątpliwości co do zgodności takiego postępowania z ustawą.

Należy zaznaczyć, że są to dane o szczególnym charakterze i ustawa wprowadza specjalne unormowania odnoszące się do możliwości ich przetwarzania. Podstawy takiej nie może stanowić przepis rangi rozporządzenia (w tym wypadku przywołany § 28 rozporządzenia w sprawie postępowania o świadczenia emerytalno-rentowe i zasad wypłaty tych świadczeń, zgodnie z którym organ emerytalny ma prawo zatrzymywać książeczki ubezpieczeniowe). Przepis ten mógł stanowić podstawę do takiego przetwarzania przed wejściem w życie ustawy o ochronie danych osobowych, jednak obecnie zbieranie danych osobowych powinno odbywać się w zgodzie z regulacjami wprowadzonymi przez tę ustawę.

Stanowisko powyższe znajduje potwierdzenie w wyroku Trybunału Konstytucyjnego z dnia 19 maja 1998 r. OTK 1998/4/46, który uznał, iż informacja o stanie zdrowia (rodzaju schorzenia) w postaci numeru statystycznego choroby należy do sfery życia prywatnego jednostki. Z wyroku tego wynika ponadto, że regulowanie spraw dotyczących korzystania z konstytucyjnych praw i wolności obywatelskich m.in. w aspekcie ochrony danych osobowych, zastrzeżone jest do wyłącznej regulacji ustawowej.

Mając więc na względzie przepis art. 47 i 51 ust. 2 Konstytucji oraz z art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych, Generalny Inspektor Ochrony Danych Osobowych postulował uregulowanie przedmiotowych kwestii w drodze ustawy lub zmianę przepisów rozporządzenia tak, aby jego unormowania nie naruszały Ustawy Zasadniczej i ustawy o ochronie danych osobowych.

Prezesa Zakładu Ubezpieczeń Społecznych (GGI-024-3/00 z dnia 31 października 2000 r.)

- w sprawie przedstawienia istotnych, z punktu widzenia ochrony danych osobowych założeń projektowych w zakresie wniesienia uzupełnień do programu PŁATNIK, mających na celu jego dostosowanie do wymogów określonych w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133 poz. 883 z późn. zm.)

Z doniesień prasowych (Computerword, 16 października 2000 r.) wynika, że firma Prokom Software S.A. rozsyła wybranym jednostkom do testowania nową wersję programu PŁATNIK. Generalny Inspektor Ochrony Danych Osobowych wskazał na celowość umożliwienia mu ustosunkowania się do sposobu realizacji wymogów ustawy o ochronie danych osobowych oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. 1998 Nr 80, poz. 521).

Prezesa Najwyższej Izby Kontroli (GI – 3/00 z dnia 3 stycznia 2000 r.)

- w sprawie dostępu do danych o stanie zdrowia przez inspektorów NIK.

Wystąpienie do Prezesa NIK zainicjowane zostało zasygnalizowanym żądaniem sporządzenia i przekazania inspektorowi NIK listy pacjentów Instytutu Gruźlicy i Chorób Płuc w Warszawie, która to lista miała umożliwić „rozesłanie do pacjentów formularzy i zebranie pisemnych oświadczeń dotyczących przedmiotu kontroli.” Z uzyskanych informacji wynikało, że lista taka - pod groźbą postawienia zarzutu utrudniania kontroli - została inspektorowi NIK przekazana.

Żądania takie budzą wątpliwości z punktu widzenia zgodności z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.) .

Ustawa o ochronie danych osobowych wprowadza odrębne rygory w odniesieniu do przetwarzania danych szczególnie chronionych, do których należą m.in. dane o stanie zdrowia. Dane osobowe pacjentów (imię, nazwisko, adres pacjenta) w połączeniu z nazwą placówki medycznej, z której pochodzą, stają się danymi sensytywnymi, ponieważ wskazują na stan zdrowia osób, których informacja dotyczy. W szczególności odnosi się to do danych o pacjentach, uzyskanych w tak specjalistycznym zakładzie opieki zdrowotnej, jak Instytut Gruźlicy i Chorób Płuc.

Jako przesłankę dopuszczalności przetwarzania danych szczególnie chronionych (sensytywnych), art. 27 ust. 2 ustawy wymienia zezwolenie przepisu szczególnego innej ustawy na przetwarzanie takich danych bez zgody osoby, której one dotyczą. Oznacza to, że inna ustawa musi wyraźnie zezwalać na przetwarzanie danych o stanie zdrowia, czyli na udostępnianie danych określonym podmiotom bądź na zbieranie i wykorzystywanie danych przez określone podmioty. Nieuprawnione przetwarzanie danych sensytywnych zagrożone jest karą grzywny, ograniczenia wolności albo pozbawienia wolności do lat 3 (art. 49 ust. 2 ustawy o ochronie danych osobowych).

Ustawa z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 1995 r. Nr 13, poz. 59 z późn. zm.) nie upoważnia inspektorów NIK do przetwarzania danych sensytywnych, m.in. dotyczących stanu zdrowia. Nie upoważniają inspektorów NIK do przetwarzania danych sensytywnych również akty prawne regulujące ochronę zdrowia. Z tego względu brak jest ustawowych podstaw do przekazywania danych konkretnych pacjentów w trakcie kontroli prowadzonej przez inspektorów NIK.

W związku z powyższym GODO zwrócił się do Prezesa NIK o nakazanie usunięcia danych uzyskanych z Instytutu Gruźlicy i Chorób Płuc oraz o zwrócenie inspektorom NIK uwagi na zagrożenia przetwarzania danych szczególnie chronionych, wymienionych w art. 27 i 28 ustawy o ochronie danych osobowych.

W ww. sprawie do Prezesa Najwyższej Izby Kontroli ponownie zostało skierowane pismo (GI – 138/00 z dnia 3 lutego 2000 r.) o braku ustawowych podstaw do przetwarzania danych o stanie zdrowia w trakcie kontroli prowadzonych przez inspektorów NIK. GODO podkreślił, iż mając świadomość, że brak stosownych zapisów w ustawie o Najwyższej Izbie Kontroli uniemożliwia prowadzenie kontroli przez inspektorów NIK we wszystkich aspektach prowadzenia działalności kontrolnej zgodnie z art. 5 ust. 1 ustawy o NIK, prosi o rozważenie nowelizacji ustawy o Najwyższej Izbie Kontroli z uwzględnieniem wymogów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.), deklarując pomoc w dostosowywaniu przepisów ustawy o Najwyższej Izbie Kontroli do wymogów ustawy o ochronie danych osobowych.

Komendanta Głównego Policji (GI – 475/00 z dnia 24 maja 2000 r.)

- w sprawie nieuzasadnionych odmów udzielania informacji będących w dyspozycji organów Policji.

Generalny Inspektor Ochrony Danych Osobowych poinformował, że do Biura GODO wpływają liczne pisma dotyczące odmowy udzielania informacji będących w dyspozycji organów Policji, mimo, iż informacje takie mogą być udzielane na podstawie art. 29 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883, z późn. zm.), zwanej dalej ustawą. Udzielanie informacji w oparciu o powołany przepis może nastąpić w celach innych niż włączenie do zbioru. Oznacza to, iż udostępnienie danych nie może skutkować utworzeniem zbioru danych będącego zestawem danych osobowych o określonej strukturze i dostępności według określonego kryterium. Zgodnie z art. 29 ust. 2 ustawy, dane osobowe, z wyłączeniem danych sensytywnych (wymienionych w art. 27

ustawy), mogą być udostępnione w celu innym niż włączenie do zbioru, osobom lub podmiotom, które uzasadnią wiarygodną potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą. Ma to szczególne znaczenie w odniesieniu do organów Policji, które mają specyficzne rodzaje danych i dlatego powinny dołożyć staranności przy ocenie zasadności wniosku.

Rozstrzygnięcie w przedmiocie udostępnienia danych należy zawsze do administratora danych, który każdorazowo rozstrzyga o zasadności wniosku.

W związku z powyższym GODO zwrócił się o podjęcie - w ramach nadzoru - działań zmieniających dotychczasową praktykę stosowania ustawy o ochronie danych osobowych, szczególnie w aspekcie art. 29 tej ustawy.

Związku Banków Polskich (GI – 194/00 z dnia 3 marca 2000 r.)

- w sprawie nieprawidłowości w działaniach banków, dotyczących nieuwzględniania żądań klientów poprawiania ich danych o miejscu zamieszkania lub pobytu.

Generalny Inspektor Ochrony Danych Osobowych poinformował Prezesa Związku Banków Polskich iż – jak wynika z licznych skarg klientów - informują oni banki o zmianie swego miejsca zamieszkania lub pobytu. Wnoskują jednocześnie, by wszelka korespondencja była kierowana na nowy adres. Działanie takie ma prawne umocowanie nie tylko w przepisach prawa cywilnego (art. 729 K.c.) , ale również w przepisach ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.). Art. 32 ust. 1 pkt 6 ustawy, uprawnia każdego, którego dane są przetwarzane, do żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane. Z kolei na podstawie art. 35 ustawy, administrator danych zobowiązany jest bez zbędnej zwłoki, m. in. do uzupełnienia i uaktualnienia danych osobowych w razie wykazania przez osobę, której dane dotyczą, że są one niekompletne, czy nieaktualne. W razie niedopełnienia tego obowiązku Generalny Inspektor Ochrony Danych Osobowych może, na wniosek osoby, nakazać administratorowi danych, w drodze decyzji, jego dopełnienie.

Analiza konkretnych skarg wskazuje, że banki nie aktualizują znajdujących się w ich posiadaniu baz danych osobowych swoich klientów, co prowadzi do ujemnych następstw dla klientów banków oraz do naruszeń przepisów o ochronie danych osobowych. W wielu

przypadkach klienci banków kierują do Generalnego Inspektora Ochrony Danych Osobowych prośbę o interwencję.

W związku z powyższym GIODO zwrócił się do Prezesa Związku Banków Polskich o podjęcie działań zmierzających do przestrzegania przez banki przepisów o ochronie danych osobowych, ale także przepisów prawa bankowego, gwarantujących prawa klientów.

Związku Banków Polskich (GI-908/000 z dnia 22 września 2000 r.)

- w sprawie niewywiązywania się przez Związek Banków Polskich, przetwarzający dane osobowe klientów w Systemie Międzybankowej Informacji Gospodarczej - Bankowy Rejestr, z obowiązku informacyjnego nałożonego na administratorów danych osobowych przepisami art.24 i 25 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.).

Wystąpienie Generalnego Inspektora skierowane zostało do Związku Banków Polskich w związku z licznie napływającymi do Biura GIODO skargami dotyczącymi działalności Związku Banków Polskich oraz poszczególnych banków przetwarzających dane osobowe klientów w Systemie Międzybankowej Informacji Gospodarczej - Bankowy Rejestr.

Z analizy treści skarg wynikało, iż banki przekazujące dane osobowe niesolidnych dłużników do Rejestru Bankowego, jak również Związek Banków Polskich, który Rejestr prowadzi, nie wywiązują się z ciążącego na nich - na mocy art. 24 i 25 ustawy - obowiązku informacyjnego.

Banki w momencie zawierania umów o świadczenie usług bankowych nie informują swoich klientów o istniejącej możliwości przekazania dotyczących ich danych do Rejestru Bankowego. Uchybiają tym samym wymogom art. 24 ust. 1 ustawy, zgodnie z którym administrator danych w przypadku zbierania danych osobowych od osoby, której one dotyczą, obowiązany jest poinformować ją o:

- adresie swojej siedziby i pełnej nazwie,
- celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
- prawie wglądu do swoich danych oraz ich poprawiania,
- dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

Niezależnie od obowiązku informacyjnego spoczywającego na bankach, obowiązek taki - stosownie do przepisu art. 25 ust. 1 ustawy - ciąży również na Związku Banków Polskich, któremu przekazywane są dane osobowe niesolidnych klientów banków, celem umieszczenia ich w Rejestrze Bankowym. Realizacja tego obowiązku winna nastąpić bezpośrednio po utrwaleniu zebranych danych, zaś zakres informacji, jakich Związek obowiązany jest udzielić osobom, których dane przetwarza w Systemie Międzybankowej Informacji Gospodarczej, zbliżony jest do tego, o którym stanowi art. 24 ust. 1 ustawy. Obok informacji o adresie i pełnej nazwie administratora danych, celu zbierania danych, odbiorcach lub kategoriach ich odbiorców, prawie wglądu do swoich danych oraz ich poprawiania, Związek Banków Polskich winien informować osoby zainteresowane o zakresie zbieranych danych oraz źródle, z którego pochodzą. Generalnemu Inspektorowi Ochrony Danych Osobowych wielokrotnie sygnalizowano natomiast, iż Związek Banków Polskich nie wywiązuje się z obowiązku informacyjnego wobec osób, których dane przetwarza w Systemie. Wydaje się, iż przyczyny takiego stanu rzeczy upatrywać należy w niezgodnych z przepisami ustawy o ochronie danych osobowych postanowieniach Regulaminu Wymiany Informacji w Systemie Międzybankowej Informacji Gospodarczej - Bankowy Rejestr, zwanego dalej regulaminem. Z brzmienia pkt 5.1. rozdziału II regulaminu wynika, iż Związek Banków Polskich upoważnił banki przekazujące do Rejestru Bankowego dane o niesolidnych klientach, do wykonania ciążącego na nim obowiązku informacyjnego. Działanie takie w świetle ustawy uznać należy za niedopuszczalne. Administrator danych nie może bowiem scedować ciążącego na nim z mocy prawa obowiązku na inny podmiot.

Z treści skarg kierowanych do Biura Generalnego Inspektora Ochrony Danych Osobowych wynika ponadto, iż klienci banków nie są informowani o tym, jak długo dotyczące ich dane figurować będą w Rejestrze Bankowym, oraz w jakich przypadkach są one z Rejestru usuwane. Do częstych należą sytuacje, w których skarżący zwracają się do Generalnego Inspektora o nakazanie usunięcia ich danych z Rejestru Bankowego informując, iż mimo uregulowania zobowiązań finansowych wobec banku, dane ich nadal są w Rejestrze przetwarzane. Podkreślić należy, iż obowiązek informacyjny jest jednym z fundamentalnych instrumentów, który pozwala osobom uprawnionym na rzeczywiste sprawowanie kontroli w przedmiocie zgodności z prawem przetwarzania ich danych osobowych. Precyzyjne jego wypełnianie gwarantuje prawną ochronę interesów osób, których dane dotyczą. Nie wywiązywanie się przez administratorów danych z nałożonego na nich obowiązku prowadzić może do ujemnych następstw dla klientów banku oraz stanowi naruszenie przepisów ustawy o ochronie danych osobowych. W związku z powyższym konieczne jest wyczerpujące

informowanie ich zarówno o okolicznościach wymienionych w art. 24 ust. 1 i art. 25 ust. 1 ustawy, jak również o tych, wynikających z postanowień regulaminu, bezpośrednio odnoszących się do sytuacji dłużników banku, których dane przetwarzane są w Rejestrze.

Jednocześnie GODO zwrócił uwagę, iż stanowienie o sytuacji niesolidnych klientów banków w akcie prawnym mającym rangę wewnętrznie obowiązującego regulaminu, narusza normy konstytucyjne. Zgodnie z art. 87 Konstytucji Rzeczypospolitej Polskiej, źródłem obowiązującego w Polsce prawa są Konstytucja, ustawy, ratyfikowane umowy międzynarodowe oraz rozporządzenia. Aktami tego rodzaju są także, na obszarze działania organów, które je ustanowiły, akty prawa miejscowego. Tylko przepisy w nich zawarte mogą być źródłem powszechnie obowiązujących praw i obowiązków. W tej sytuacji Generalny Inspektor wskazał na konieczność uregulowania przedmiotowej kwestii w akcie normatywnym, którego unormowania - stosownie do art. 87 Konstytucji - będą miały charakter powszechny.

Związku Banków Polskich (GI – 531/00 z dnia 3 czerwca 2000 r.)

- w sprawie zasadności odmowy uwzględniania żądań zaprzestania przetwarzania danych osobowych przekazywanych do Związku Banków Polskich.

Wystąpienie skierowane zostało do Związku Banków Polskich w związku z sygnałami od klientów banków, wskazującymi na niejednolitą praktykę banków, mylnie informujących klientów o przysługujących im prawach, jak i w związku z pismami kierowanymi do GODO przez sam Związek Banków Polskich dotyczącymi odmowy uwzględniania żądań zaprzestania przetwarzania danych osobowych przekazywanych do Związku Banków Polskich.

GODO wyjaśnił, iż stosownie do art. 32 ust. 1 pkt 7 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.), każdej osobie, której dane są przetwarzane, przysługuje prawo wniesienia, w przypadkach wymienionych w art. 23 ust. 1 pkt 4 i 5, pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację. Powołany przepis wyraźnie ogranicza prawo zgłaszania żądania zaprzestania przetwarzania danych jedynie do sytuacji, gdy przetwarzanie danych osobowych jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego lub, gdy jest ono niezbędne do wypełnienia usprawiedliwionych celów administratora danych, o których mowa w art. 3 ust. 2 ustawy, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Związek Banków Polskich przetwarzając dane osobowe w Systemie Międzybankowej Informacji Gospodarczej przetwarza je na podstawie przesłanki wynikającej z art. 23 ust. 1 pkt 2 ustawy. Na przetwarzanie danych zezwala bowiem przepis art. 105 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. Nr 140, póź. 939 z późn. zm.). W związku z powyższym, jeżeli osoby, których dane są przetwarzane w Systemie Międzybankowej Informacji Gospodarczej, spełniają kryteria wynikające z załącznika nr 1 do Regulaminu Wymiany Informacji w Systemie Międzybankowej Informacji Gospodarczej, to nie przysługuje im uprawnienie złożenia żądania zaprzestania przetwarzania ich danych osobowych. W konsekwencji, składanie w powyższych okolicznościach żądania zaprzestania przetwarzania danych osobowych należy uznać za nieuprawnione i wobec tego nieskuteczne. Nie została bowiem spełniona podstawowa przesłanka materialno-prawna uprawniającą do formułowania takiego żądania. Analogicznie należy interpretować przepis art. 32 ust. 1 pkt 8 ustawy, dotyczący możliwości wniesienia sprzeciwu wobec przetwarzania danych w celach marketingowych i wobec przekazywania danych innemu administratorowi. Ma on zastosowanie wyłącznie wtedy, gdy dane są przetwarzane na podstawie art. 23 ust. 1 pkt 4 i 5 ustawy.

W celu zapewnienia zgodności przetwarzania danych osobowych przez banki z przepisami prawa oraz dla uniknięcia kierowania do GIODO nieuzasadnionych wniosków o wszczęcie postępowania administracyjnego, celowe byłoby - zdaniem Generalnego Inspektora - poinformowanie osób zgłaszających żądania i sprzeciwu, o których mowa w art. 32 ust. 1 pkt 7 i 8 ustawy, iż nie mogą być one uwzględnione ze względu na brak uprawnienia do ich składania.

GIODO poinformował jednocześnie, iż z kierowanych do niego pism wynika, że niektóre banki, mylnie interpretując przepis art. 32 ust. 1 pkt 7 i 8 ustawy, powiadamiają swoich klientów o przysługującym im uprawnieniu do złożenia żądania zaprzestania przetwarzania danych i sprzeciwie wobec przetwarzania danych przez Związek Banków Polskich.

W związku z powyższym GIODO zwrócił się o podjęcie działań mających na celu zapewnienie odstąpienia przez banki od praktyki błędnego informowania swoich klientów, iż w sytuacji przetwarzania ich danych osobowych w Systemie Międzybankowej Informacji Gospodarczej, przysługuje im uprawnienie złożenia żądania zaprzestania przetwarzania danych lub sprzeciwu. Jednocześnie wskazał na wymogi ustawy określone w art. 24 ust. 1 i art. 25 ust. 1, dotyczące obowiązku informacyjnego.

Inne wystąpienia do organów państwa

Rzecznika Praw Obywatelskich (GI – 474/00 z dnia 24 maja 2000 r.)

- w sprawie zbadania zgodności z prawem uchwały Rady Miejskiej w Tarnowie z dnia 27 grudnia 1999 r., dotyczącej obowiązku ujawniania informacji o stanie zdrowia i stopniu inwalidztwa kontrolerom w autobusach komunikacji miejskiej, oraz - w razie podzielenia wątpliwości - o podjęcie stosownych działań w ramach posiadanych kompetencji.

W dniu 13 marca 2000 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło pismo, w którym Miejski Rzecznik Konsumentów zwrócił się z pytaniem, czy żądanie okazania odcinka świadczenia emerytalno - rentowego podczas kontroli biletów nie jest przekroczeniem ustawy o ochronie danych osobowych. Podnosił ponadto, iż nie wydaje się być zasadnym, aby pracownikom firmy zajmującej się kontrolą biletów była potrzebna znajomość wysokości świadczenia emerytalno - rentowego osób kontrolowanych. Do pisma Miejski Rzecznik Konsumentów dołączył tekst uchwały Nr XVII/298/99 Rady Miejskiej w Tarnowie z dnia 27 grudnia 1999 r.

W odpowiedzi na pismo Generalny Inspektor uznał, iż podnoszona przez Miejskiego Rzecznika Konsumentów kwestia jest obojętna z punktu widzenia ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.), albowiem nie zachodzi tu przetwarzanie danych osobowych w zbiorze danych. Zgodnie z art. 7 ust. 1 cytowanej ustawy, przetwarzaniem danych osobowych są jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych. W opisywanej sytuacji kontrolerzy nie dokonują żadnej z wymienionych operacji. Dane uzyskane na podstawie odcinka emerytalno - rentowego są udostępniane na czas dokonania kontroli i nie podlegają dalszemu przetwarzaniu. Ponadto Generalny Inspektor nie uznał się za organ właściwy do badania zgodności postanowień przedmiotowej uchwały rady miejskiej z przepisami prawa.

Niemniej jednak w ocenie Generalnego Inspektora ujawnienie informacji dotyczących stanu zdrowia czy stopnia inwalidztwa przy dokonywaniu kontroli biletów autobusowych wydaje się za daleko posuniętą ingerencją w sferę prywatności emerytów i rencistów. W doktrynie na ogół przyjmuje się, że prywatność odnosi się m.in. do ochrony informacji dotyczących danej osoby i gwarancji pewnego stanu niezależności, w ramach której człowiek może decydować o zakresie i zasięgu udostępniania i komunikowania innym osobom informacji o swoim życiu. Istnienie prawa do prywatności w polskim porządku

prawnym znalazło potwierdzenie w orzecznictwie Sądu Najwyższego, który w orzeczeniu z dnia 8 kwietnia 1994 r. (III ARN 18/94) odniósł koncepcję ochrony dóbr osobistych (art. 23 i 24 Kodeksu cywilnego) do sfery życia prywatnego i sfery intymności.

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483), w art. 47 i art. 51, wyraźnie normuje prawo do prywatności, stanowiąc jednocześnie, iż jedyne jego ograniczenia mogą wynikać tylko z aktu o randze ustawy i nie mogą naruszać istoty wolności i praw. Zgodnie bowiem z art. 47 Konstytucji, każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz decydowania o swoim życiu osobistym, natomiast w myśl art. 51 ust. 1 nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.

Bliższa analiza sprawy zasygnalizowanej przez Miejskiego Rzecznika Konsumentów daje podstawę do zgłoszenia zastrzeżeń, zarówno co do strony formalnej aktu, jak i jego poszczególnych postanowień. W tej sytuacji wydaje się zasadne rozpatrzenie problemu nie na gruncie ustawy o ochronie danych osobowych, ale na gruncie przepisów Konstytucji i ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. Nr 13, poz. 74 z późn. zm.).

W związku z powyższym GODO przekazał sprawę w celu merytorycznego jej rozpoznania, z uprzejmą prośbą o jej rozpoznanie i podjęcie stosownych działań w ramach przysługujących kompetencji.

Urzędu Nadzoru Ubezpieczeń Zdrowotnych (GI –708/00 z dnia 19 lipca 2000 r.)

- w sprawie podjęcia przewidzianych prawem działań nadzorczych wobec Pomorskiej Regionalnej Kasy Chorych z siedzibą w Gdańsku, z powodu naruszenia obowiązków określonych w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.), zwanej dalej „ustawą”.

Generalny Inspektor Ochrony Danych Osobowych poinformował, że Pomorska Regionalna Kasa Chorych, realizując obowiązek, o którym mowa art. 40 ustawy, zgłosiła do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych dwa zbiory danych osobowych o nazwach:

- „Baza danych osobowych ubezpieczonych w PRKCh" (numer zgłoszenia R 000154/99),
- „Baza danych osobowych personelu wykonującego świadczenia medyczne na rzecz ubezpieczonych w PRKCh" (numer zgłoszenia R 000164/99).

Po rozpatrzeniu zgłoszeń stwierdzono, iż istnieje przesłanka odmowy rejestracji zbioru danych, o której mowa w art. 44 ust. 1 pkt 3 ustawy, bowiem urządzenia i systemy informatyczne służące do przetwarzania danych osobowych nie spełniają podstawowych warunków technicznych i organizacyjnych, o których mowa w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 80, poz. 521). W związku z tym w dniu 7 maja 1999 r. zwrócono się do Pomorskiej Regionalnej Kasy Chorych o złożenie pisemnych wyjaśnień w sprawie (znak pism DRZDO/R/174/99, DRZDO/R/176/99). Z powodu braku potwierdzenia odbioru, pisma te zostały ponownie wysłane w dniu 14 czerwca 1999 r. (znak pisma DRZDO/310/99).

Z uwagi na zbyt długi termin oczekiwania na odpowiedź, Generalny Inspektor Ochrony Danych Osobowych w dniu 26 czerwca 2000 r. po raz trzeci zwrócił się do PRKCh o przesłanie pisemnych wyjaśnień (znak pism DRZDO/5549/00, DRZDO/5550/00), wskazując, iż niezastosowanie się do przewidzianych prawem żądań Generalnego Inspektora Ochrony Danych Osobowych stanowi naruszenie art. 14 i 15 ustawy o ochronie danych osobowych.

Zawarte w zgłoszeniu informacje oraz brak jakichkolwiek wyjaśnień ze strony wnioskodawcy obliguje Generalnego Inspektora Ochrony Danych Osobowych, stosownie do treści art. 44 ust. 1 i 2 ustawy, do wydania decyzji o odmowie rejestracji przedmiotowych zbiorów danych i jednoczesnego nakazania wstrzymania przetwarzania danych osobowych w zbiorach lub ich usunięcia ze zbiorów. Nakaz ten, na podstawie art. 44 ust. 3 ustawy, podlega natychmiastowemu wykonaniu z mocy prawa. Wydanie tego typu decyzji w praktyce spowoduje konieczność zaprzestania realizacji przez Pomorską Regionalną Kasę Chorych zadań określonych w ustawie z dnia 6 lutego 1997 r. o powszechnym ubezpieczeniu zdrowotnym (Dz. U. Nr 28, poz. 153 z późn. zm.).

Pismo podobnej treści, informujące o zgłoszeniu do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych przez Pomorską Regionalną Kasę Chorych, dwóch zbiorów danych osobowych o nazwach:

- „Baza danych osobowych ubezpieczonych w PRKCh" (numer zgłoszenia R 000154/99),
- „Baza danych osobowych personelu wykonującego świadczenia medyczne na rzecz ubezpieczonych w PRKCh" (numer zgłoszenia R 000164/99),

nie spełniających warunków do zarejestrowania, z wnioskiem o podjęcie interwencji wobec Pomorskiej Regionalnej Kasy Chorych, skierowane zostało także do **Przewodniczącego Rady Krajowego Związku Kas Chorych oraz do Pełnomocnika Rządu ds. Wprowadzenia Powszechnego Ubezpieczenia Zdrowotnego.**

Pełnomocnika Rządu ds. Wprowadzenia Powszechnego Ubezpieczenia Zdrowotnego (GI-DIS-188/00 z dnia 4 lipca 2000 r.)

- w sprawie przekazywania przez Kujawsko - Pomorską Regionalną Kasę Chorych w Bydgoszczy świadczeniodawcom danych osobowych pacjentów, którzy zrezygnowali z ich usług, z prośbą o podjęcie działań mających na celu wyeliminowanie niezgodnych z przepisami o ochronie danych osobowych praktyk stosowanych przez ww. Kasę Chorych.

Zgodnie z art. 23 ust. 1 pkt 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.), przetwarzanie danych jest dopuszczalne wtedy, gdy zezwalają na to przepisy prawa. Sposób i zakres przetwarzania danych osób ubezpieczonych przez Kasy Chorych został określony w rozdziale 7a ustawy z dnia 6 lutego 1997 r. o powszechnym ubezpieczeniu zdrowotnym (Dz. U. Nr 28, poz. 153 z późn. zm.) oraz w rozporządzeniu Ministra Zdrowia i Opieki Społecznej z dnia 15 stycznia 1999 r. w sprawie ustalenia zakresu niezbędnych danych gromadzonych przez świadczeniodawców oraz w systemach informatycznych Kas Chorych, a także zakresu i procedury wymiany danych pomiędzy Kasami Chorych oraz Kasami Chorych a świadczeniodawcami, Urzędem Nadzoru Ubezpieczeń Zdrowotnych i Krajowym Związkiem Kas Chorych (Dz. U. Nr 7, poz. 66 z późn. zm.).

Przepis art. 141a ust. 1 pkt 5 ustawy o powszechnym ubezpieczeniu zdrowotnym ma zastosowanie wyłącznie do rozliczeń ze świadczeniodawcami za świadczenia wykonane na rzecz tych pacjentów, którzy złożyli deklarację o korzystaniu z usług danego ośrodka. Ponadto stosownie do art. 141a ust. 2 ustawy o powszechnym ubezpieczeniu zdrowotnym, który określa zakres przetwarzanych przez Kasy Chorych danych osób ubezpieczonych, a konkretnie jego pkt 8, zgodnie z którym dla realizacji zadań, o których mowa w art. 141a ust. 1 wskazanej ustawy, Kasy Chorych mają prawo przetwarzania danych dotyczących udzielonych ubezpieczonemu świadczeń zdrowotnych, których charakterystyka zawiera m.in. rodzaj udzielonego świadczenia oraz świadczeniodawcę wykonującego usługę.

W związku z powyższym, należy stwierdzić, że przekazywanie przez Kujawsko - Pomorską Regionalną Kasę Chorych świadczeniodawcom danych osób, którzy zrezygnowali z ich usług, jako nie znajdujące uzasadnienia w powołanym wyżej przepisie, pozostaje w

sprzeczności z art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych. Z punktu widzenia zgodności z ustawą o ochronie danych osobowych za wystarczające do prawidłowego rozliczania się ze świadczeniodawcami należy uznać informowanie danego ośrodka wyłącznie o liczbie pacjentów, którzy zrezygnowali z jego usług, bez przekazywania dotyczących ich danych osobowych.

**Związku Rewizyjnego Spółdzielni Mieszkaniowych Rzeczypospolitej Polskiej
(GI-DP-52/00 z dnia 26 stycznia 2000 r.)**

- w sprawie nieprawidłowości w działalności Spółdzielni Mieszkaniowej „BRÓDNO” w Warszawie, sygnalizowanych w skargach mieszkańców – członków Spółdzielni.

Generalny Inspektor Ochrony Danych Osobowych poinformował, iż wystąpienie skierowane zostało do ZRSM RP, w związku z napływającymi do Generalnego Inspektora Ochrony Danych Osobowych skargami mieszkańców — członków Spółdzielni Mieszkaniowej „BRÓDNO” w Warszawie, wskazującymi na nieprawidłowości w działalności tej Spółdzielni. Skargi te skłoniły Generalnego Inspektora Ochrony Danych Osobowych do wszczęcia postępowania administracyjnego w celu wyjaśnienia wszystkich okoliczności sprawy i usunięcia ewentualnych uchybień w procesie przetwarzania danych osobowych.

W toku postępowania ustalono, iż w dniu 26 listopada 1994 r. w Spółdzielni Mieszkaniowej „BRÓDNO” w Warszawie, zwanej dalej Spółdzielnią, odbyło się zebranie grupy członków Spółdzielni, którzy uznali się za Zebranie Przedstawicieli i podjęli uchwałę o zmianach w składzie Rady Nadzorczej. Dzień później nowo powołana Rada odwołała dotychczas działający Zarząd i powołała nowy, w innym składzie. Sąd Apelacyjny w Warszawie orzekł w prawomocnym wyroku z dnia 30 stycznia 1997 r. (sygn. akt I Acr 933/96), że uchwały tego gremium, obradującego 26 listopada 1994 r., jako zwołanego przez osoby nieuprawnione, nie są uchwałami organu Spółdzielni i z punktu widzenia prawa są to tzw. uchwały nie istniejące (acti non existi). Oznacza to, iż zarówno uchwała z dnia 26 listopada 1994 r., jak również podjęte po dniu 26 listopada 1994 r. czynności prawne w imieniu i na rzecz Spółdzielni przez powołane w wyżej wskazany sposób organy, nie wywarły skutków prawnych.

Jak wynika ze skarg kierowanych do Generalnego Inspektora Ochrony Danych Osobowych, nie posiadający prawnego umocowania Zarząd i Rada Nadzorcza do chwili obecnej działają na szkodę członków Spółdzielni, godząc w ich prawa. Najbardziej jaskrawym przykładem, z punktu widzenia ochrony danych osobowych, jest podejmowanie

przez te organy Spółdzielni uchwał o wykluczeniu poszczególnych mieszkańców z grona członków Spółdzielni. Niewątpliwie praktyka ta jest rażącym naruszeniem prawa.

Wobec powyższego Generalny Inspektor Ochrony Danych Osobowych, na podstawie art. 12 pkt 5 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.) zwrócił się o zbadanie przedstawionej sprawy i podjęcie działań zmierzających do zabezpieczenia praw członków wspomnianej Spółdzielni, także z punktu widzenia ochrony danych osobowych.

Część VI. PROPAGOWANIE IDEI OCHRONY DANYCH OSOBOWYCH

1. W ramach propagowania idei ochrony danych osobowych Generalny Inspektor jak też upoważnieni pracownicy Biura, prowadzili w 2000 r. szkolenia oraz wykłady w zakresie stosowania przepisów ustawy o ochronie danych osobowych w instytucjach państwowych i samorządowych, jednostkach wymiaru sprawiedliwości, szkołach wyższych oraz u innych podmiotów (załącznik nr 5).
2. W dniach 26 – 27 czerwca 2000 r. Generalny Inspektor zorganizował, wraz z Biurem Wymiany Informacji o Pomocy Technicznej Komisji Europejskiej – TAIEX, „Seminarium o ochronie danych osobowych”.

Tematyka spotkania koncentrowała się wokół ochrony danych osobowych w prawie pracy, sektorze ubezpieczeń oraz służbie zdrowia. W ramach spotkania poruszano głównie problem konfliktu interesów istniejącego między pracownikami a pracodawcami oraz wskazano na konieczność doprecyzowania przepisów prawa pracy pod kątem ochrony danych osobowych pracowników. Hans Peter Viethen z niemieckiego Ministerstwa Pracy zajął się problematyką monitorowania działań pracowników w miejscu pracy, wskazując na coraz to nowsze problemy, powstające wskutek rozwoju technologii informatycznych.

W ramach seminarium referaty wygłosili:

- Hans Pieter Viethen, Niemcy - Ministerstwo Pracy, pt. „Ochrona danych osobowych w prawie pracy”,
- Prof. Dr hab. Michał Seweryński, Uniwersytet Łódzki, pt. „Ochrona danych osobowych w prawie pracy – sytuacja w Polsce”,
- Graham Sutton, Wielka Brytania, pt. „Ochrona danych osobowych w sektorze ubezpieczeń”,
- Dr Małgorzata Gersdorf, Uniwersytet Warszawski, pt. „Ochrona danych osobowych w sektorze ubezpieczeń – sytuacja w Polsce”,
- Diana Alonso Blas, Urząd Ochrony Danych Osobowych w Hiszpanii, pt. „Ochrona danych osobowych w służbie zdrowia”,
- Ewa Kulesza, Generalny Inspektor Ochrony Danych Osobowych;

- Franciszek Gajek, Szpital Wojewódzki w Olsztynie, pt. „Ochrona danych osobowych w służbie zdrowia – sytuacja w Polsce”.

We współpracy z Polską Izbą Ubezpieczeń oraz Rzecznikiem Praw Obywatelskich, Generalny Inspektor Ochrony Danych Osobowych zorganizował, w dniu 4 grudnia 2000 r., seminarium, pt. „Przetwarzanie danych osobowych na potrzeby ubezpieczeń prywatnych”.

Głównym problemem poruszonym w ramach seminarium była kwestia pogodzenia interesów zakładów ubezpieczeń z prawem ubezpieczonych do ochrony ich prywatności, a także ze spoczywającym na władzy publicznej obowiązkiem ochrony konsumentów przed nieuczciwymi praktykami rynkowymi, stosowanymi w sektorze ubezpieczeniowym.

Arwid Mednis, przedstawiciel Polski w Komitecie Ekspertów Rady Europy ds. Ochrony Danych Osobowych, przedstawił i omówił w swoim referacie założenia projektu Rekomendacji Rady Europy o ochronie danych osobowych zbieranych i przetwarzanych dla celów ubezpieczeń. Waltraut Kotschy, Komisarz Ochrony Danych Osobowych w Austrii oraz Augustin Puente Escobar, Dyrektor Departamentu Prawnego hiszpańskiej Agencji Ochrony Danych Osobowych zapoznali uczestników seminarium z rozwiązaniami prawnymi, jak również praktyką, jaka ma miejsce w Austrii i Hiszpanii, w zakresie przetwarzania danych osobowych przez firmy ubezpieczeniowe.

W ramach seminarium referaty wygłosili:

Arwid Mednis, przedstawiciel Polski w Komitecie Ekspertów Rady Europy ds. Ochrony Danych Osobowych, pt. „Omówienie projektu Rekomendacji Rady Europy o ochronie danych osobowych zbieranych i przetwarzanych dla celów ubezpieczeń”,

Waltraut Kotschy, Komisarz Ochrony Danych Osobowych w Austrii, pt. „Austriackie przepisy prawne w zakresie umów ubezpieczeniowych: zakres danych zbieranych przez prywatne firmy ubezpieczeniowe oraz wykorzystanie danych genetycznych dla celów ubezpieczeń”,

Augustin Puente Escobar, Dyrektor Departamentu Prawnego hiszpańskiej Agencji Ochrony danych Osobowych, pt. *„Ochrona danych osobowych przetwarzanych dla celów ubezpieczeń prywatnych: rozwiązania prawne i praktyczne”*,

Dariusz Kupiecki, Przewodniczący Grupy Roboczej ds. Systemów Ochrony Danych Osobowych Polskiej Izby Ubezpieczeń, pt. *„Przetwarzanie danych osobowych w działalności ubezpieczeniowej – konflikt interesów czy wspólnota wartości”*,

Dr Ryszard Zelwiański, Biuro Rzecznika Praw Obywatelskich, pt. „Zagrożenia dla ochrony danych osobowych w prywatnych ubezpieczeniach na zdrowie i życie”,

Jarosław Trelka, Dyrektor Departamentu Rejestracji Zbiorów Danych Osobowych Biura GODO, pt. „Podstawy prawne i praktyka przetwarzania danych osobowych przez zakłady ubezpieczeniowe w Polsce. Omówienie doświadczeń Generalnego Inspektora Ochrony Danych Osobowych w tym zakresie oraz postulaty i zalecenia pod adresem instytucji ubezpieczeniowych”.

Do tradycji należą również stałe kontakty Generalnego Inspektora z takimi mediami, jak: ośrodki telewizji publicznej i komercyjnej, stacje radiowe, prasa codzienna i periodyczna o zasięgu lokalnym i ogólnopolskim, agencje informacyjne oraz portale internetowe.

W ramach przekazywania obywatelom informacji dotyczących ochrony danych osobowych za pośrednictwem mediów, poza codzienną z nimi współpracą, Generalny Inspektor Ochrony Danych Osobowych organizował również konferencje prasowe. W okresie sprawozdawczym odbyło się osiem konferencji z udziałem przedstawicieli stacji telewizyjnych i radiowych, dziennikarzy prasowych oraz agencji informacyjnych (załącznik nr 6).

Spotkania z dziennikarzami poświęcone były, m.in. działalności Kas Chorych, firm ubezpieczeniowych i firm marketingowych w kontekście obowiązywania ustawy o ochronie danych osobowych. Stałą pozycję podczas konferencji prasowych stanowiło przekazywanie dziennikarzom materiałów informacyjnych dotyczących działalności Biura GODO, zawierających bieżącą statystykę skarg, pism z prośbą o interpretację, danych dotyczących rejestracji zbiorów danych, przeprowadzonych kontroli i zawiadomień o popełnieniu przestępstw skierowanych do prokuratury przez Generalnego Inspektora Ochrony Danych Osobowych.

W 2000 roku, na łamach dziennika Rzeczpospolita, miesięczników Gazeta Samorządu i Administracji oraz Prawo i Życie regularnie ukazywały się wystąpienia Generalnego Inspektora Ochrony Danych Osobowych dotyczące interpretacji przepisów ustawy o ochronie danych osobowych (załącznik nr 7). Artykuły poświęcone problematyce ochrony prywatności oraz wywiady z Generalnym Inspektorem Ochrony Danych Osobowych publikowane były w dziennikach i periodykach o zasięgu ogólnopolskim i lokalnym: dzienniku Rzeczpospolita, Gazecie Wyborczej, Trybunie, Życiu, Gazecie Prawnej, Gazecie Prawo i Gospodarka, tygodniku Wprost i innych (załącznik nr 7).

W omawianym okresie Generalny Inspektor wielokrotnie gościł na antenie stacji telewizyjnych i radiowych. Brał udział w cyklicznie prowadzonych audycjach radiowych, poświęconych ochronie danych osobowych. Generalny Inspektor Ochrony Danych Osobowych udzielił szeregu wypowiedzi dla dziennikarzy programów informacyjnych (Telewizja Polska – Redakcja Panoramy, Wiadomości, Teleexpressu, Telewizyjnego Kuriera Warszawskiego, Telewizja Polsat, Polsat 2 – Infor, TVN, TV4, RTL7; Polskie Radio – Program I, II, III, IV, Radio ZET, RMF FM, Radio WAWA, Radio ESKA, Radio KOLOR, Polska Agencja Prasowa, Informacyjna Agencja Prasowa i inne) oraz występował w programach publicystycznych, których tematem była ochrona prywatności (Telewizja Polska - Monitor Wiadomości, Telewizja Polsat – Polityczne graffiti, Telewizja Polsat 2 – Infor Prawny, Infor Ubezpieczeniowy i inne).

W ramach przeprowadzonej w 2000 r. modyfikacji strony internetowej Biura GODO, została ona powiększona o szereg nowych działów tematycznych. W obecnym kształcie na stronie znajdują się m.in. akty prawne oraz wykaz literatury z zakresu ochrony danych osobowych; odpowiedzi na najczęściej pojawiające się pytania obywateli, kierowane do Generalnego Inspektora Ochrony Danych Osobowych; informacje dotyczące rejestracji zbiorów danych osobowych, a także aktualizowana co kwartał statystyka obejmująca działalność Biura. Obszerna część serwisu internetowego poświęcona została „polityce informacyjnej” GODO. W dziale „Materiały informacyjne” zamieszczone zostały m.in. sprawozdania z działalności Generalnego Inspektora z ubiegłych lat oraz informacje prasowe (artykuły), które ukazały się na łamach gazet i były poświęcone zagadnieniom ochrony danych osobowych. W ramach tego działu zamieszczone zostały również omówienia krajowych konferencji naukowych, jak również sprawozdania z wyjazdów zagranicznych Generalnego Inspektora Ochrony Danych Osobowych oraz pracowników Biura.

Składane w okresie sprawozdawczym, przez Generalnego Inspektora Ochrony Danych Osobowych, wizyty w urzędach ochrony danych osobowych innych państw, służyły wymianie doświadczeń oraz zapoznaniu się z przyjętą praktyką ochrony prywatności.

W dniach 15 – 20 kwietnia 2000 r., Generalny Inspektor Ochrony Danych Osobowych oraz pracownicy Biura uczestniczyli w szkoleniu organizowanym przez Biuro Federalnego Rzecznika ds. Ochrony Danych Osobowych w Bonn. Głównym tematem szkolenia była międzynarodowa ochrona danych osobowych w sektorze prywatnym, jak również w sektorze telekomunikacji (handel elektroniczny / Internet). W ramach wykładów poruszano problematykę prawa do informacyjnego samookreślenia człowieka.

W dniach 5 – 7 czerwca 2000 r., dr Ewa Kulesza była gościem greckiego Urzędu Ochrony Danych Osobowych. Celem wizyty było zapoznanie się z ustawodawstwem i praktyką Grecji w zakresie ochrony danych osobowych. Generalny Inspektor przedstawił również własne doświadczenia, w zakresie ochrony danych osobowych w Polsce.

Generalny Inspektor, w dniach 18 – 19 września 2000 r., przebywał w Państwowym Inspektoracie Ochrony Danych Osobowych na Litwie. Wizyta GIODO miała na celu nawiązanie współpracy z tym urzędem, a także zapoznanie pracowników litewskiego Inspektoratu z doświadczeniami w tworzeniu niezależnego organu ochrony danych osobowych.

Dr Ewa Kulesza oraz pracownicy Biura GIODO uczestniczyli w 22 międzynarodowej konferencji dotyczącej ochrony prywatności i ochrony danych osobowych, która odbyła się w Wenecji, w dniach 28 – 30 września 2000 r. Poruszana podczas konferencji problematyka dotyczyła głównie konieczności stworzenia efektywnej ochrony prywatności i danych osobowych w obliczu dynamicznego rozwoju nowoczesnych technologii.

W dniach 16 – 17 października 2000 r., Generalny Inspektor Ochrony Danych Osobowych gościł z wizytą w Agencji Ochrony Danych Osobowych w Hiszpanii. Generalny Inspektor miał okazję zapoznać się ze strukturą i funkcjonowaniem hiszpańskiego urzędu oraz charakterystyką rozpatrywanych przez tę instytucję spraw.

W okresie od 6 do 7 listopada 2000 r., Generalny Inspektor przebywał w szwedzkim Urzędzie Ochrony Danych Osobowych. Wizyta posłużyła wzajemnej wymianie doświadczeń i nawiązaniu współpracy między Urzędami.

Generalny Inspektor Ochrony Danych Osobowych oraz pracownicy Biura, uczestniczyli również w pracach międzynarodowych grup roboczych zajmujących się m.in. problematyką ochrony danych w sektorze telekomunikacji.

W dniach 22 – 23 maja 2000 r., na zaproszenie dr Ewy Kuleszy, Biuro Generalnego Inspektora Ochrony Danych Osobowych odwiedził Juan Manuel Fernández López, Dyrektor Urzędu Ochrony Danych Osobowych z Hiszpanii (Agencia de Protección de Datos). Wizyta służyła wymianie doświadczeń, jak również rozszerzeniu współpracy między Urzędami. W ramach spotkania Dyrektor hiszpańskiego Urzędu zapoznał się ze strukturą i funkcjonowaniem polskiego Biura oraz przyjętą w naszym kraju praktyką ochrony prywatności (załącznik nr 8).

WNIOSKI KOŃCOWE

Rok 2000 r. był drugim pełnym rokiem kalendarzowym funkcjonowania ustawy o ochronie danych osobowych i działalności Generalnego Inspektora Ochrony Danych Osobowych/

1. Podobnie, jak w roku 1999, w roku 2000 największą ilość spraw stanowiło rozpatrywanie wniosków rejestracyjnych, zgłoszonych w końcu 1999 roku w celu wykonania obowiązku rejestracyjnego nałożonego na administratorów danych osobowych art. 40 ustawy o ochronie danych osobowych.

Przeprowadzone postępowania wskazywały, że wnioski o zarejestrowanie zbiorów danych, zwłaszcza kierowane do Generalnego Inspektora w ostatnim wyznaczonym przez ustawę terminie, albo po upływie terminu, wypełnione były w sposób niestaranny, czasem jedynie w części. Natomiast ustawa wyraźnie wskazuje, co winno zawierać zgłoszenie zbioru danych do rejestracji, nakazując Generalnemu Inspektorowi wydanie decyzji o odmowie rejestracji zbioru w przypadku, gdy nie zostały spełnione wymogi formalne zgłoszenia.⁵²⁸ Ponieważ ustawa łączy daleko idące skutki dla administratora danych osobowych w przypadku odmowy zarejestrowania zbioru danych - decyzja o odmowie musi zawierać nakaz wstrzymania przetwarzania danych lub ich usunięcia – każde indywidualne zgłoszenie musiało zostać starannie przeanalizowane oraz połączone z koniecznością wyjaśnienia wszystkich wątpliwości powstałych na gruncie zgłoszenia, co w znacznym stopniu opóźniło proces rejestracji zgłoszonych zbiorów danych.

Z tego względu do końca okresu sprawozdawczego nie wszystkie zgłoszenia zostały rozpatrzone.

Doświadczenia uzyskane na podstawie prowadzonej przez 2000 r. rejestracji zbiorów danych wskazują na niedoskonałość ustawy o ochronie danych osobowych. W odczuciu Generalnego Inspektora ustawa wiąże zbyt daleko idące, negatywne skutki

⁵²⁸ Zgodnie z art. 44 ustawy, Generalny Inspektor wydaje decyzję o odmowie rejestracji zbioru danych, jeżeli zgłoszenie nie zawiera jednego z elementów wymienionych w art. 41 ust. 1, tj.: wniosku o wpisanie zbioru do rejestru, oznaczenia podmiotu prowadzącego zbiór i adresu jego siedziby lub miejsca zamieszkania, w tym numeru identyfikacyjnego rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany, oraz podstawę prawną upoważniającą do prowadzenia zbioru, zakresu i celu przetwarzania danych, sposobu zbierania i udostępniania danych, opisu środków organizacyjnych i technicznych zastosowanych w celu zabezpieczenia zbioru oraz informacji o sposobie wypełnienia wymagań technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

prawne ze zgłoszeniem zbioru w sposób nie odpowiadający wymogom formalnym, nakazuje bowiem wydanie decyzji odmawiającej rejestrację (wraz z nakazem usunięcia danych ze zbioru bądź wstrzymania przetwarzania danych), podczas gdy w niektórych wypadkach wystarczyłoby zarejestrowanie zbioru i wydanie decyzji nakazującej usunięcie uchybień. Przyszła nowelizacja ustawy o ochronie danych osobowych winna iść w kierunku złagodzenia przepisów dotyczących rejestracji zbiorów.

2. Kontrole przeprowadzane przez informatyków, zarówno w małych jednostkach organizacyjnych (np. dysponujących jednym stanowiskiem komputerowym, na którym przetwarzano dane osobowe), jak też dużych, często wielooddziałowych firmach działających na terenie całego kraju połączonych rozbudowanymi sieciami komputerowymi typu WAN i ośrodkami komputerowymi o dużej mocy obliczeniowej, dają asumpt do następujących uwag:

Pomimo, iż ustawa o ochronie danych osobowych i rozporządzenie w wymaganiach określających warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy służące do przetwarzania danych osobowych nie bierze pod uwagę wielkości podmiotów, to w rzeczywistości w niektórych małych jednostkach ich wielkość powoduje, iż stawianie im wymagań określonych w rozporządzeniu staje się bezprzedmiotowe. Całkowicie odmiennie do wymienionych wyżej wymagań, należy się jednak odnieść w przypadku dużych jednostek organizacyjnych, posługujących się złożonym systemem informatycznym, mieszczących się często w wielu różnych budynkach zlokalizowanych, np. na terenie całej Polski .

Z tego względu celowa byłaby nowelizacja przepisów wykonawczych do ustawy o ochronie danych osobowych, tj. rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 80, poz. 521), znacząco i jednoznacznie różnicująca warunki organizacyjne i techniczne w zależności od rodzajów danych przetwarzanych przez administratorów i wielkości podmiotu przetwarzającego dane.

Z przeprowadzonych kontroli wynika, że w dużych jednostkach organizacyjnych w celu wykonania zadań organizacyjno technicznych jakim powinny odpowiadać systemy informatyczne do przetwarzania danych wymienionych w rozporządzeniu powołano najczęściej odpowiednią komórkę organizacyjną. W trakcie kontroli można było

zauważyć, że do zagadnień związanych z ochroną danych, w tym także danych osobowych, podchodzi się poważnie i z dużą odpowiedzialnością.

Na uwagę zasługuje fakt, że administratorzy danych będący dużymi jednostkami organizacyjnymi, nie mieli na ogół kłopotów z realizacją podstawowych wymagań technicznych i organizacyjnych stawianych urządzeniom i systemom informatycznym przetwarzającym dane osobowe w zakresie bezpieczeństwa przetwarzania. Duże jednostki organizacyjne, zwłaszcza związane z sektorem finansowym dysponowały najczęściej odpowiednim dokumentem określającym tzw. politykę bezpieczeństwa, który zawierał elementy, o których mowa w § 2 rozporządzenia. Dokument ten składał się na ogół z części dotyczącej bezpieczeństwa fizycznego oraz z części dotyczącej bezpieczeństwa systemów informatycznych uwzględniając różne rodzaje ryzyka i zagrożeń na jakie ich systemy mogą być narażone. Na szczególną uwagę zasługują instytucje finansowe, które dokładają dużych starań dla zagwarantowania bezpieczeństwa fizycznego oraz bezpieczeństwa systemów informatycznych zarówno pod kątem niezawodności ich funkcjonowania jak i ochrony zawartych w nich informacji, co wynika z budowanej w tych instytucjach kultury ochrony zarówno aktywów materialnych jak i informacyjnych, stosowania wysokich standardów w zakresie bezpieczeństwa niektóre, także z obowiązujących przepisów, np. ustawy o ochronie informacji niejawnych. Ponadto w przypadku organizacji finansowych pewne standardy dotyczące bezpieczeństwa narzucane są przez ich przepisy wewnętrzne.

Ważne jest również to, że wymienione instytucje określając politykę bezpieczeństwa, odpowiednią wagę przykładają na ogół nie tylko do ochrony przetwarzanych tam danych przed zniszczeniem lub utratą, ale przede wszystkim do ochrony przed ich nie autoryzowanym przetwarzaniem oraz ujawnieniem wypełniając tym samym jeden z głównych warunków, jakim zgodnie z wymaganiami rozporządzenia powinny spełniać systemy informatyczne przetwarzające dane osobowe.

Nieco inną sytuację zaobserwowano w jednostkach organizacyjnych, zwłaszcza tych, które należą do organów władzy publicznej, oraz będących pod kontrolą państwa. W wielu takich jednostkach, działania mających na celu właściwe zabezpieczenie danych osobowych przetwarzanych w systemach informatycznych rozpoczęto dopiero po wejściu w życie ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2000 r. nr 12, poz. 136 z późn. zm.).

W dużych jednostkach organizacyjnych takich jak towarzystwa emerytalne, banki, telekomunikacja, itp. wyznaczony był administrator bezpieczeństwa informacji oraz

sporządzone były odpowiednie instrukcje, o których mowa w § 6 i § 11 rozporządzenia. Jednakże istotne zastrzeżenia inspektorów budziła często jakość merytoryczna sporządzonych instrukcji, w szczególności, gdy ich treść zawiera niemal wyłącznie sformułowania zawarte w § 6.2 rozporządzenia nie zawierające żadnych indywidualnych elementów odzwierciedlających stan rzeczywiście występujących w danej jednostce zagrożeń, czy też charakterystyki objawienia się potencjalnie możliwych, niebezpiecznych dla ochrony informacji zdarzeń, ponieważ takie elementy powinny być zawarte w indywidualnej instrukcji sporządzonej na potrzeby konkretnej jednostki.

Podobne zastrzeżenia odnotowano również w odniesieniu do instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji. Instrukcja taka powinna być przygotowana stosownie do skali problemów, jakie występują w zarządzaniu poszczególnych systemów informatycznych.

Oceniając przekrojowo jakość wymienionych wyżej instrukcji, należy stwierdzić, że w dużych jednostkach organizacyjnych, poza nielicznymi wyjątkami, były one na ogół dobre. Jednakże podkreślić należy, iż w wielu przypadkach instrukcje zostały znacznie zmodyfikowane w wyniku, a nawet w trakcie przeprowadzonych w 2000 r. inspekcji; wiele z kontrolowanych jednostek, w których odnotowano w czasie kontroli liczne uchybienia, przedstawione zalecenia potraktowało bardzo poważnie i poczyniły wiele wysiłku, aby sprostać postawionym wymogom.

Wiele zastrzeżeń zarówno w dużych jak i małych jednostkach organizacyjnych stawianych administratorom danych podczas kontroli odnosiło się do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych pomimo, że w nielicznych tylko przypadkach odnotowano całkowity jej brak. Zasadniczymi uchybieniami odnotowanymi w kontrolowanych jednostkach odnoszącymi się do sposobu prowadzenia ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych były: brak identyfikatora użytkownika (dla osób przetwarzających dane osobowe w systemach informatycznych), brak daty nadania odebrania uprawnień do przetwarzania danych oraz niekompletność i brak koordynacji przy jej prowadzeniu.

Ostatnie z wymienionych uchybień w zakresie prowadzenia ewidencji wynikało najczęściej z faktu, że w jednostce nie było wyznaczonej osoby, która odpowiedzialna była by za te czynności lub faktu rozłożenia tej odpowiedzialności na wiele osób, najczęściej administratorów poszczególnych systemów informatycznych. Skutkiem takich

działań było to, że każdy z administratorów ograniczał się do utworzenia jedynie listy aktualnych użytkowników swojego systemu w dowolnej wymyślonej przez siebie formie.

O ile generalnie można stwierdzić, iż niektóre większe jednostki podejmowały próby stworzenia dokumentu określającego politykę bezpieczeństwa, to w mniejszych jednostkach nie stwierdzono nawet takich prób. Nie mówiąc już o pełnowartościowym, zawierającym całościowe spojrzenie na sprawy związane z ochroną danych, dokumentem. Przyczyna tego zjawiska tkwi najczęściej w tym, że niektóre podmioty nie dostrzegają rzeczywistych potrzeb i korzyści z wdrożenia polityki bezpieczeństwa.

Charakterystycznym dla małych jednostek organizacyjnych było również to, iż pomimo posiadanej często wiedzy na temat wymagań, jakie nakłada na administratorów ustawa o ochronie danych osobowych, jednostki takie, nie posiadały na ogół instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, o której mówi § 11 rozporządzenia. W wielu przypadkach wynikało to z faktu, że w małych jednostkach organizacyjnych administracją systemów informatycznych zajmują się firmy zewnętrzne na podstawie umowy outsorsingu, które na ogół nie dostarczają swoim klientom żadnych dokumentacji zarządzania administrowanym systemem, a same jednostki korzystające z usług outsorsingowych, będące formalnie administratorem przetwarzanych danych osobowych, nie przyłożyły należytej uwagi do wymaganych przez ustawę warunków techniczno - organizacyjnych. Jak wynika z przeprowadzonych kontroli, tylko w nielicznych przypadkach sporządzono aneksy do zawartych umów outsorsingowych, w których dookreślono zakres przetwarzania danych osobowych i czynności jakie zobowiązany jest dopełnić zleceniobiorca w związku z wejściem w życie ustawy.

Bardzo niepokojącym faktem, który zaobserwowano podczas prowadzonych kontroli zarówno w dużych jak i małych jednostkach organizacyjnych jest to, że pomimo upływu 2 lat od wejścia w życie rozporządzenia nadal tylko w nielicznych przypadkach systemy służące do przetwarzania danych w pełni odpowiadają przyjętym tam wymogom.

Wiele z kontrolowanych w 2000 r. systemów informatycznych, nie spełniało warunków określonych w § 16 punkt 1, 2 i 3 rozporządzenia, odnoszących się odpowiednio do obowiązku: odnotowania daty pierwszego wprowadzenia danych, obowiązku odnotowania źródła pochodzenia danych, oraz obowiązku odnotowania identyfikatora użytkownika wprowadzającego dane. Ponadto nadal tylko nieliczne systemy dostosowane są do realizacji wymogów określonych w § 16 punkt 4 i 5 rozporządzenia.

Podobne zastrzeżenia odnoszą się do realizacji wymogów określonych w § 17 rozporządzenia, który mówi że „system informatyczny służący do przetwarzania danych osobowych powinien umożliwiać udostępnienie na piśmie, w powszechnie zrozumiałej formie, treści danych o każdej osobie, której dane są przetwarzane, wraz z informacjami, o których mowa w § 16.”

Natomiast pozytywnym akcentem, jaki można zaobserwować w działalności administratorów bezpieczeństwa informacji w dużych jednostkach organizacyjnych, jest podejmowanie działań zmierzających do dostosowania systemów informatycznych do pełnej realizacji wymagań określonych w § 16 i 17 rozporządzenia. Sposób ich realizacji jest różny. W niektórych jednostkach wymienia się stare systemy informatyczne na nowe, spełniające wymagania ustawy o ochronie danych osobowych, w innych natomiast do eksploatowanych obecnie systemów dobudowuje się specjalne moduły. Czas jaki rezerwują sobie jednak administratorzy danych na wykonanie wspomnianych czynności naprawczych jest w niektórych przypadkach zbyt długi (np. okres 2-3 lat).

3. W dalszym ciągu znaczącym problemem w praktyce – w szczególności organów administracji publicznej – była nadinterpretacja przepisów ustawy o ochronie danych osobowych, ograniczająca dostęp do danych z powołaniem się na ustawę o ochronie danych osobowych. Zakres pytań oraz skarg kierowanych do Generalnego Inspektora wskazuje, że w bardzo wielu wypadkach urzędnicy odmawiali udzielenia informacji, naruszając własne przepisy lub wykazując ich całkowitą nieznajomość (np. przepisów ustawy o aktach stanu cywilnego). Ponadto zgłaszane do Biura GODO przypadki dają podstawę do przypuszczeń, iż w dalszym ciągu w wielu sytuacjach ustawa o ochronie danych osobowych wykorzystywana była do świadomego ograniczania dostępu głównie do informacji o działalności podmiotów publicznych.

Na „zamknięcie” dostępu do informacji niewątpliwie miało wpływ również tworzone aktualnie ustawodawstwo, kładące nacisk na szczegółowe określenie podmiotów uprawnionych do uzyskania informacji. Ilustracją w tym względzie mogą być skargi na odmowę udzielenia informacji, np. komornikom wykonującym wyrok sądowy lub jednostkom organizacyjnym pomocy społecznej prowadzącym postępowanie w sprawie udzielenia świadczenia, przez Zakład Ubezpieczeń Społecznych. Przyczyną odmowy udzielenia informacji przez ZUS jest sposób sformułowania art. 50 ust. 3 ustawy o powszechnym ubezpieczeniu społecznym, zawierający enumeratywne wyliczenie

podmiotów uprawnionych do uzyskania informacji o osobach ubezpieczonych („Dane zgromadzone na koncie ubezpieczonego /.../ mogą być udostępnione sądom, prokuratorom, organom kontroli skarbowej oraz Urzędowi Nadzoru nad Funduszami Ubezpieczeniowymi, z uwzględnieniem przepisów dotyczących ochrony danych osobowych”). W rezultacie żaden podmiot nie wskazany wprost w powołanym przepisie, nie może uzyskać informacji, mimo, iż informacja ta jest niezbędna do wykonywania określonych prawem zadań.

Z tego względu wydaje się celowy postulat pod adresem Ustawodawcy tworzenia przepisów w sposób, który będzie dawał dostateczny dostęp podmiotom działającym w ramach i na podstawie przepisów prawa, do informacji i danych osobowych niezbędnych do wykonywania zadań.

4. W 2000 r. zwiększyła się ilość skarg na naruszenia prawa przez administratorów danych osobowych, kierowanych do Generalnego Inspektora, jednakże w świetle prowadzonych postępowań wyjaśniających stwierdzić można, iż jedynie około 25 do 30 % skarg jest zasadnych.

Nowym zjawiskiem, które pojawiło się w skargach kierowanych do Generalnego Inspektora jest żądanie przyznania przez Generalnego Inspektora wysokich odszkodowań za naruszenie – zdaniem skarżących - ich prawa do ochrony danych oraz potrzeb wynikających z braku środków finansowych, stanu rodzinnego czy bezrobocia. Zjawisko to nasiliło się zwłaszcza po wydaniu wyroku sądu cywilnego w Łodzi, przyznającego odszkodowanie za naruszenie przepisów ustawy o ochronie danych przez Petro Bank.

5. W roku 2000 odnotować należy postępujący wzrost świadomości prawnej obywateli zarówno w zakresie szeroko pojmowanej ochrony danych osobowych, jak i samego obowiązku zgłaszania prowadzonych zbiorów danych do rejestracji. Przyczyniła się do tego działalność edukacyjna Generalnego Inspektora Ochrony Danych Osobowych. Była ona realizowana w formie szkoleń oraz porad i wskazówek udzielanych przez pracowników Biura Generalnego Inspektora Ochrony Danych Osobowych. Także strona internetowa ([www. giodo.gov.pl](http://www.giodo.gov.pl)) zawierała informacje przydatne dla poznania i zrozumienia określonych aspektów ochrony danych osobowych (np. sposób prawidłowego wypełnienia zgłoszenia zbioru danych do rejestracji). Przyniosło to efekt w postaci, np. coraz lepszego sporządzania wniosków rejestracyjnych. Ponadto w związku z wieloma nieprawidłowościami jakie występowały w zgłoszeniach zbiorów danych do rejestracji Generalny Inspektor Ochrony Danych Osobowych zwracał się za

pośrednictwem prasy o ich usunięcie do dnia 15 listopada 2000 r. Informowano przy tym, że zarówno błędy, jak i braki we wnioskach zgłoszeniowych uniemożliwiają zarejestrowanie zbioru.

6. Podobnie, jak w latach poprzednich Generalny Inspektor Ochrony Danych Osobowych w niewielkim zakresie mógł liczyć na wsparcie swoich działań przez organy ścigania.

Na podstawie art. 19 ustawy o ochronie danych osobowych Generalny Inspektor jest zobowiązany do kierowania do organów ścigania zawiadomienia o popełnieniu przestępstwa w razie stwierdzenia, że działanie lub zaniechanie kierownika jednostki organizacyjnej, jej pracownika lub innej osoby będącej administratorem danych wyczerpuje znamiona przestępstwa określonego w ustawie. W związku z tym w okresie sprawozdawczym skierowanych zostało do organów ścigania 46 zawiadomień o naruszeniu ustawy o ochronie danych osobowych, z tego jedynie w dwóch przypadkach postępowania zakończyły się skierowaniem do sądu aktów oskarżenia, natomiast w zbyt wielu sprawach prokuratura odmówiła wszczęcia postępowania lub umorzyła postępowanie już wszczęte ze względu na „znikomą szkodliwość czynu”. Stawia to pod znakiem zapytania realność prawnokarnej ochrony prawa obywateli do ochrony danych osobowych.

Iluzoryczność ochrony prawnokarnej, wraz z uciążliwością dla skarżących uczestniczenia w długotrwałym postępowaniu przygotowawczym prowadzonym przez prokuraturę w wielu przypadkach sprawia, że osoby wnoszące uzasadnioną skargę na niezgodne z prawem działania administratorów danych osobowych, składają oświadczenia, iż nie są zainteresowane prowadzeniem postępowania w sprawie, w związku z czym postępowania są umarzane. W wielu przypadkach również podobne oświadczenia są składane, ponieważ skarżący w momencie składania skargi w ogóle nie rozważali możliwości czy potrzeby prowadzenia postępowania karnego, uznając, że sprawa powinna być załatwiona wyłącznie w postępowaniu administracyjnym.

W związku ze zdarzającymi się coraz częściej przypadkami składania oświadczeń o których mowa wyżej, w przyszłej nowelizacji ustawy, powinna być rozważona możliwość zmiany obowiązujących przepisów ustawy w części dotyczącej obowiązku Generalnego Inspektora zawiadamiania organów ścigania o popełnieniu przestępstwa.

Wydaje się, że celowym byłoby zrezygnowanie przez ustawodawcę z konieczności ścigania z urzędu wszystkich przestępstw określonych w ustawie o ochronie danych

osobowych i dopuszczenie – w niektórych przypadkach (np. w odniesieniu do art. 54) – ścigania przestępstw jedynie z oskarżenia prywatnego.

7. W ciągu trzech lat stosowania ustawy, nawet w przypadku skazania sprawców przestępstw określonych w ustawie o ochronie danych osobowych, w żadnym przypadku sąd nie wymierzył kary pozbawienia wolności. Należy podkreślić, iż wymierzania kary pozbawienia wolności nie wymaga Dyrektywa, na której wzorowana była polska ustawa o ochronie danych osobowych.

W ocenie Generalnego Inspektora Ochrony Danych Osobowych przewidziana w przepisach karnych ustawy o ochronie danych osobowych kara pozbawienia wolności, przy niektórych rodzajach przestępstw nawet do 3 lat (art. 49 ust. 2), jest sankcją nadmiernie surową.

Z tego też względu wydaje się celowe odejście od zagrożenia karą pozbawienia wolności w przyszłej nowelizacji ustawy o ochronie danych osobowych, z możliwością podwyższenia wysokości kary grzywny i ograniczenie sankcji jedynie do kary grzywny i ograniczenia wolności.

8. Ze względu na rozbieżności pomiędzy brzmieniem niektórych przepisów Dyrektywy 95/46/EC Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych a przepisami polskiej ustawy o ochronie danych osobowych, w 2000 r. przygotowana została nowelizacja polskiej ustawy, dostosowująca polskie przepisy do wymogów unijnych. W zakresie dostosowania definicji danych osobowych, brak pełnej zbieżności przepisów polskiej ustawy był przedmiotem zarzutów stawianych przez Komisję Europejską. Z tego względu nowelizacja była niezbędna.

Nowelizacja dotyczy dwóch głównych punktów: dostosowania definicji danych osobowych oraz wprowadzenia do polskiej ustawy przepisu, stanowiącego odpowiednik art. 15 Dyrektywy, zakazującego podejmowania decyzji indywidualnych wyłącznie na podstawie zautomatyzowanego przetwarzania danych.

Projekt nowelizacji przewiduje zastąpienie dotychczasowego art. 6 ustawy („W rozumieniu ustawy za dane osobowe uważa się każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby”) przepisem o następującym brzmieniu: „Art. 6.1. W rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby

fizycznej. 2. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. 3. Informacji nie uważa się za umożliwiającą określenie tożsamości, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań”, przy czym pierwsze dwa ustępy art. 6 są dosłownym przeniesieniem definicji zawartej w Dyrektywie 95/46/WE, natomiast proponowany ust. 3 jest odzwierciedleniem wskazówki interpretacyjnej z pkt. 15 preambuły do Dyrektywy, wskazującej, iż przetwarzanie danych podlega Dyrektywie (i dostosowanemu do niej ustawodawstwu) tylko wtedy, gdy następuje automatycznie lub gdy dane mają być ujęte w systemie ewidencyjnym skonstruowanym według kryteriów, mających na celu umożliwienie łatwego dostępu do danych.

Spełnieniem wymogów zawartych w art. 15 Dyrektywy, wymagającej gwarancji dla każdej osoby nie podlegania decyzji mającej dla niej skutki prawne lub poważnie wpływającej na jej sytuację, która oparta jest wyłącznie na zautomatyzowanym przetwarzaniu danych, jest propozycja zamieszczenia przepisu art. 26 a w brzmieniu: „1. Niedopuszczalne jest ostateczne rozstrzygnięcie indywidualnej sprawy osoby, której dane dotyczą, jeżeli jego treść jest wyłącznie wynikiem operacji na danych osobowych, prowadzonych w systemie informatycznym. 2. Przepisu ust. 1 nie stosuje się, jeżeli rozstrzygnięcie zostało podjęte podczas zawierania lub wykonywania umowy i uwzględnia wnioski osoby, której dane dotyczą”. Dodatkową gwarancją dla osoby, której dane dotyczą, jest prawo tej osoby do wniesienia do administratora żądania ponownego, indywidualnego rozpatrzenia sprawy rozstrzygniętej z naruszeniem art. 26a (art. 32 ust. 1 pkt. 9) oraz obowiązek administratora rozpatrzenia sprawy albo przekazania jej wraz z uzasadnieniem Generalnemu Inspektorowi, który wydaje stosowną decyzję (art. 32 ust. 3a).

Zaproponowana nowelizacja ustawy o ochronie danych łagodzi także m.in. pewne rygory wynikające z obowiązku informacyjnego nałożonego na administratora danych osobowych. Dyrektywa pkt 40 Preambuły wyraźnie podkreśla, iż „Jeśli podmiot danych wie o przetwarzaniu lub ujawnianiu jego danych, informowanie go o tym nie jest już konieczne.” Z tego względu w nowelizacji proponuje się, aby administrator danych zwolniony był z obowiązku informacyjnego określonego w art. 25 ustawy, gdy dane są przetwarzane przez administratora na podstawie przepisów prawa oraz gdy osoba, której dane dotyczą, posiada informacje wymienione w ust. 1 przepisu.

Nowelizacja zmienia nieco zasady przetwarzania danych szczególnie chronionych. Pierwsza ze zmian obejmuje przeniesienie dotychczasowego ust. 1 z art. 28 do art. 27, jako ust. 1a. W dotychczasowym brzmieniu art. 28 ust. 1 przetwarzanie danych „dotyczących skazań, orzeczeń o ukaraniu, mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym można prowadzić wyłącznie na podstawie ustawy „co ogranicza prawo osoby, której dane dotyczą, do dysponowania rozstrzygnięciami jej dotyczącymi. Z tego względu, a także z uwagi na to, iż Dyrektywa wymienia dane dotyczące przestępstw, osób skazanych lub środków bezpieczeństwa w części dotyczącej szczególnej kategorii danych, ale bez zastrzeżenia odrębnego, surowszego reżimu ich przetwarzania, w projekcie nowelizacji ustawy przewiduje się dołączenie danych, wskazanych w art. 28 ust. 1, do katalogu danych szczególnie chronionych wymienionych w art. 27 ust. 1, wskazując na możliwość stosowania przesłanek przetwarzania w takim zakresie, w jakim odnosi się to do innych danych podlegających szczególnej ochronie.

W nowelizacji ustawy tworzy się ponadto odrębna przesłankę przetwarzania danych szczególnie chronionych – przetwarzanie na potrzeby badań naukowych (art. 27 ust. 2 pkt 9). W dotychczasowym brzmieniu ustawy takiej przesłanki nie było, tymczasem przepisy Dyrektywy wyraźnie i wielokrotnie wskazują, iż „w ważnych kwestiach, uzasadnionych dobrem ogółu, Państwa Członkowskie powinny mieć prawo do odejścia od zakazu dotyczącego przetwarzania wrażliwych kategorii danych, jeżeli istnieją ku temu ważne powody uzasadnione dobrem publicznym, w takich dziedzinach, jak /.../ badania naukowe” (pkt. 34, por. też pkt 9 Preambuły do Dyrektywy). Z tego też względu w proponowanym pkt 9 przewiduje się przetwarzanie danych, jeśli „jest to niezbędne do prowadzenia badań naukowych, w tym przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego.” Przepis zawiera dodatkowe zabezpieczenie praw osób, których dane dotyczą w postaci warunku, iż „publikowanie wyników badań naukowych nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone.”

Podkreślić należy, iż szersza zakresowo nowelizacja, uwzględniająca doświadczenia nabyte w trakcie stosowania ustawy, jak też doświadczenia innych państw w zakresie ochrony danych, przygotowana zostanie w drugiej połowie 2001 r.

9. Doświadczenia z funkcjonowania Biura Generalnego Inspektora Ochrony Danych Osobowych stały się podstawą do nowelizacji załącznika do rozporządzenia Prezydenta Rzeczypospolitej Polskiej z dnia 29 maja 1998 r. w sprawie nadania statutu Biuru

Generalnego Inspektora Ochrony danych Osobowych.⁵²⁹ Nowelizacja, wprowadzona rozporządzeniem Prezydenta Rzeczypospolitej Polskiej z dnia 3 listopada 2000 r.⁵³⁰ dotyczyła zmian w strukturze organizacyjnej Biura GIODO wynikających z dotychczasowych doświadczeń z funkcjonowania Biura (w tym likwidacji Gabinetu GIODO oraz utworzenia Departamentu Skarg) oraz z konieczności dostosowania statutu do wymogów wprowadzonych m.in. ustawą o ochronie informacji niejawnych (utworzenie Pionu Ochrony).

⁵²⁹ Dz. U. Nr 73, poz. 464

⁵³⁰ Rozporządzenie z dnia 3 listopada 2000 r. zmieniające rozporządzenie w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych osobowych (Dz. U. Nr 98, poz. 1063).

Załączniki

Załącznik nr 1

**Centralne i naczelne organy administracji publicznej, które zgłosiły zbiory do rejestracji
Generalnemu Inspektorowi Ochrony Danych Osobowych.**

Lp.	Nazwa administratora	Nazwa zbioru	Numer zgłoszenia	Data wpływu zgłoszenia
1	Minister Finansów	Rejestr zaświadczeń	000009/2000	01.02.2000
2	Minister Finansów	Rejestr świadczeń zawodowych	000010/2000	01.02.2000
3	Minister Pracy i Polityki Społecznej	Docman	000946/2000	09.03.2000
4	Minister Gospodarki	Wniosek o nadanie odznaki honorowej „Zasłużony dla energetyki”	002576/2000	20.11.2000
5	Minister Gospodarki	Wniosek o nadanie stopnia górniczego	002577/2000	20.11.2000
6	Minister Gospodarki	Wniosek o nadanie odznaki honorowej „Zasłużony dla górnictwa RP”	002578/2000	20.11.2000
7	Narodowy Bank Polski (NBP)	Krezus-Informacja o zaciągniętym kredycie	002399/2000	03.11.2000
8	Narodowy Bank Polski (NBP)	Depoz	002400/2000	03.11.2000
9	Narodowy Bank Polski (NBP)	Inwpol- Lista osób, które nabyły akcje lub udziały w spółce z siedzibą za granicą	002401/2000	03.11.2000
10	Narodowy Bank Polski (NBP)	Dane licencyjne	002402/2000	03.11.2000
11	Narodowy Bank Polski (NBP)	Bankowa Informacja Statystyczna (BIS)	002403/2000	03.11.2000
12	Narodowy Bank Polski (NBP)	EWIB-wykaz banków krajowych (bez banków spółdzielczych i oddziałów banków zagranicznych w Polsce)	002404/2000	03.11.2000
13	Narodowy Bank Polski (NBP)	Zlecenia zagraniczne	002405/2000	03.11.2000
14	Narodowy Bank Polski (NBP)	Kontrola dostępu-Cotag	002406/2000	03.11.2000

15	Narodowy Bank Polski (NBP)	Polskie Inwestycje za granicą - lista osób, które nabyły akcje lub udziały w spółce z siedzibą za granicą	002407/2000	03.11.2000
16	Narodowy Bank Polski (NBP)	Baza kontaktowa-RWEF.XLS	002408/2000	03.11.2000
17	Narodowy Bank Polski (NBP)	„ADRESY”- pliki w word-exel-Lista osób uprawnionych do odbierania haseł do kluczowania zleceń na rynku bonów skarbowych (dane adresowe banku do korespondencji)	002409/2000	03.11.2000
18	Narodowy Bank Polski (NBP)	Mieszkania	002410/2000	03.11.2000
19	Narodowy Bank Polski (NBP)	Kasy walutowe	002411/2000	03.11.2000
20	Narodowy Bank Polski (NBP)	Krak	002412/2000	03.11.2000
21	Narodowy Bank Polski (NBP)	Synab Formularz D3 i B3 (dane archiwalne z lat 1991-1996)	002413/2000	03.11.2000
22	Narodowy Bank Polski (NBP)	Brudne (Excell)	002414/2000	03.11.2000
23	Narodowy Bank Polski (NBP)	Kompensa	002415/2000	03.11.2000
24	Narodowy Bank Polski (NBP)	Word - dane osób realizujących transporty	002416/2000	03.11.2000
25	Narodowy Bank Polski (NBP)	AN_SDK- Archiwum	002417/2000	03.11.2000
26	Narodowy Bank Polski (NBP)	Pożyczki	002418/2000	03.11.2000
27	Narodowy Bank Polski (NBP)	Mieszkania własnościowe	002419/2000	03.11.2000
28	Narodowy Bank Polski (NBP)	Rachunki w bankach za granicą - lista osób posiadających rachunki w bankach za granicą	002420/2000	03.11.2000
29	Narodowy Bank Polski (NBP)	Odsetki	002421/2000	03.11.2000
30	Narodowy Bank Polski (NBP)	System wymiany krajowych znaków pieniężnych - SWP	002422/2000	03.11.2000
31	Narodowy Bank Polski (NBP)	Kontrola dostępu w obiektach centrali	002423/2000	03.11.2000

		NBP		
32	Narodowy Bank Polski (NBP)	System ewidencji numizmatów	002424/2000	03.11.2000
33	Narodowy Bank Polski (NBP)	Ewidencja osób wyróżnionych odznaką „Zasłużony dla bankowości PRL” i „Zasłużony dla bankowości RP”	002425/2000	03.11.2000
34	Narodowy Bank Polski (NBP)	Adresy – dane adresowe prenumeratorów wydawnictw NBP ADRESY. ISF	002426/2000	03.11.2000
35	Narodowy Bank Polski (NBP)	GP/ ARTYKUŁY BIK 2000. NSF	002427/2000	03.11.2000
36	Narodowy Bank Polski (NBP)	GP/AUT.NSF- baza danych osobowych	002428/2000	03.11.2000
37	Narodowy Bank Polski (NBP)	Poczta (Ewidencja korespondencji nadsyłanej do prezesa NBP)	002429/2000	03.11.2000
38	Narodowy Bank Polski (NBP)	GP/WYDBIK 00.NSF- baza danych adresowych prenumeratorów „Banku i kredytu”	002430/2000	03.11.2000
39	Narodowy Bank Polski (NBP)	Skargi, wnioski i listy	002431/2000	03.11.2000
40	Narodowy Bank Polski (NBP)	Zarządy banków- plik tekstowy Word	002432/2000	03.11.2000
41	Narodowy Bank Polski (NBP)	Weksel	002433/2000	03.11.2000
42	Narodowy Bank Polski (NBP)	Adresarka	002434/2000	03.11.2000
43	Narodowy Bank Polski (NBP)	Kantory	002435/2000	03.11.2000
44	Narodowy Bank Polski (NBP)	Albumy	002436/2000	03.11.2000
45	Narodowy Bank Polski (NBP)	Ewidencja pożyczek (EPOZ)	002437/2000	03.11.2000
46	Narodowy Bank Polski (NBP)	IN_ZAG	002438/2000	03.11.2000
47	Najwyższa Izba Kontroli	Skargi i wnioski kierowane do Najwyższej Izby Kontroli	001739/2000	09.06.2000
48	Najwyższa Izba Kontroli	Kandydaci do pracy	002382/2000	31.10.2000

		w Najwyższej Izbie Kontroli		
49	Generalny Konserwator Zabytków	Rejestr skarg i wniosków	001341/2000	14.04.2000
50	Generalny Konserwator Zabytków	Rejestr umów o dzieło i zlecenie	001342/2000	14.04.2000
51	Generalny Konserwator Zabytków	Wykaz spraw dotyczących wywozu dóbr kultury za granicą	001343/2000	14.04.2000
52	Agencja Rynku Rolnego	Wykaz producentów, od których dokonano skupu zbóż z dopłatami ARR	002339/2000	25.10.2000
53	Agencja Rynku Rolnego	Wykaz przedsiębiorców skupujących zboże z dopłatami ARR	002340/2000	25.10.2000
54	Agencja Restrukturyzacji i Modernizacji Rolnictwa	Karty inwestycyjne	002093/2000	28.08.2000
55	Państwowy Urząd Nadzoru Ubezpieczeń	Skargi	001049/2000	22.03.2000

Załącznik nr 2**Zbiory danych osobowych zgłoszone do rejestracji przez administrację publiczną
szczebla wojewódzkiego w 2000 r.**

Lp.	Nazwa administratora	Nazwa zbioru	Numer zgłoszenia	Data wpływu zgłoszenia
1.	Wojewoda Śląski	Lista biegłych Wojewody Śląskiego z zakresu ochrony środowiska.	000223/00	17.01.2000
2.	Wojewoda Śląski	Rejestr osób, którym zostały zasądzone renty lub odszkodowania.	001504/00	12.05.2000
3.	Wojewoda Śląski	Rejestr lekarzy uprawnionych do przeprowadzania badań kierowców.	001505/00	12.05.2000
4.	Wojewoda Śląski	Rejestr przedstawicieli Wojewody w Radach Społecznych Samodzielnych Publicznych Zakładów Opieki Zdrowotnej.	001506/00	12.05.2000
5.	Wojewoda Śląski	Rejestr odwołań od decyzji administracyjnych z zakresu zatrudnienia i przeciwdziałania bezrobociu.	001507/00	12.05.2000
6.	Wojewoda Śląski	Rejestr osób ubiegających się o pomoc społeczną.	001508/00	12.05.2000
7.	Wojewoda Śląski	Wojewódzka ewidencja pojazdów.	002094/00	28.08.2000
8.	Wojewoda Podkarpacki	Żołnierze rezerwy reklamowani na wniosek i z urzędu.	000383/00	03.02.2000
9.	Wojewoda Opolski	Ewidencja egzaminatorów kandydatów na kierowców.	000454/00	03.01.2000
10.	Wojewoda Opolski	Wnioski lekarzy ubiegających się o uprawnienia do przeprowadzenia badań	000455/00	03.01.2000

		lekarskich kierowców.		
11.	Wojewoda Opolski	Wnioski osób starających się o rejestrację zakładów opieki zdrowotnej.	000456/00	03.01.2000
12.	Wojewoda Opolski	Wnioski o wydanie zezwolenia na prowadzenie domu pomocy społecznej.	000457/00	03.01.2000
13.	Wojewoda Opolski	Rejestr spraw Wojewódzkiego Zespołu ds. Orzekania o Stopniu Niepełnosprawności.	000458/00	03.01.2000
14.	Wojewoda Opolski	Rejestr osób, którym przysługują świadczenia z tytułu okresowego nie podwyższania płac w sferze budżetowej w zasięgu terytorialnym województwa opolskiego.	002119/00	05.09.2000
15.	Wojewoda Opolski	Rejestr zbioru pojazdów w zasięgu terytorialnym województwa opolskiego.	002120/00	05.09.2000
16.	Wojewoda Opolski	Orzeczenia wydane w postępowaniu odwoławczym z zakresu ustawy o zatrudnieniu i przeciwdziałaniu bezrobociu.	002767/00	22.12.2000
17.	Wojewoda Małopolski	Pracownicy zlikwidowanych przedsiębiorstw państwowych, których dokumentację nie archiwalną przechowuje Archiwum Zakładowe Małopolskiego Urzędu Wojewódzkiego w Krakowie.	001074/00	27.03.2000
18.	Wojewoda Małopolski	Pracownicy zlikwidowanych przedsiębiorstw państwowych, których dokumentację nie archiwalną przechowuje Archiwum Zakładowe	001075/00	27.03.2000

		Placówka Zamiejscowa w Nowym Sączu Małopolskiego Urzędu Wojewódzkiego.		
19.	Wojewoda Małopolski	Pracownicy zlikwidowanych przedsiębiorstw państwowych, których dokumentację nie archiwalną przechowuje Archiwum Zakładowe Placówka Zamiejscowa w Tarnowie Małopolskiego Urzędu Wojewódzkiego w Krakowie.	001076/00	27.03.2000
20.	Wojewoda Małopolski	Pracownicy sprywatyzowanych przedsiębiorstw państwowych, których organem założycielskim był Wojewoda Krakowski oraz Wojewoda Małopolski.	001077/00	27.03.2000
21.	Wojewoda Małopolski	Akta rejestracyjne personelu medycznego Prezydium Wojewódzkiego Rady Narodowej w Krakowie i Urzędów Wojewódzkich w Krakowie z lat 1973-1975 i 1990-1993.	001510/00	15.05.2000
22.	Wojewoda Świętokrzyski	Ewidencja powiadomień o mianowaniu bądź odwołania osób sprawujących funkcje organów osób prawnych Kościoła Katolickiego oraz innych kościołów lub związków wyznaniowych o uregulowanej sytuacji prawnej.	001906/00	27.07.2000
23.	Wojewoda Świętokrzyski	Drużyna Marzeń - DT	002113/00	01.09.2000
24.	Wojewoda Świętokrzyski	Rejestr zbiorów pojazdów w zasięgu terytorialnym	002114/00	01.09.2000

		województwa świętokrzyskie-go.		
25.	Wojewoda Świętokrzyski	Wykaz rolników poszkodowanych w wyniku klęsk żywiołowych na terenie województwa świętokrzyskie-go.	002184/00	14.09.2000
26.	Wojewoda Świętokrzyski	Psychologowie uprawnieni do badań kierujących pojazdami oraz kandydatów na instruktorów i egzaminatorów.	002752/00	19.12.2000
27.	Wojewoda Dolnośląski	Ewidencja pilotów i przewoźników turystycznych województwa dolnośląskiego i egzaminów państwowych na uprawnienia pilota wycieczek i przewoźnika turystycznego oraz jednostek organizacyjnych i osób fizycznych upoważnionych przez Wojewodę Dolnośląskiego do prowadzenia szkoleń dla kandydatów na pilotów wycieczek i przewodników turystycznych.	001988/00	09.08.2000
28.	Wojewoda Dolnośląski	System informatyczny ewidencji pojazdów „REJESTR”.	002074/00	23.08.2000
29.	Wojewoda Podlaski	Rejestr zbioru pojazdów w zasięgu terytorialnym województwa podlaskiego.	002018/00	16.08.2000
30.	Wojewoda Zachodniopomorski	Wojewódzka ewidencja pojazdów.	002188/00	18.09.2000
31.	Wojewoda Warmińsko-Mazurski	Wojewódzka ewidencja pojazdów w zasięgu terytorialnym województwa warmińsko-	002199/00	19.09.2000

		mazurskiego.		
32.	Wojewoda Kujawsko-Pomorski	Zbiór danych dotyczących kredytów suszowych.	002324/00	19.10.2000
33.	Wojewoda Mazowiecki	Wojewódzka ewidencja pojazdów województwa mazowieckiego.	002357/00	26.10.2000
34.	Wojewoda Lubelski	Wojewódzka ewidencja pojazdów.	002467/00	10.11.2000
35.	Marszałek Województwa Podlaskiego	Susza 2000	002799/00	29.12.2000
36.	Wojewódzki Inspektor Sanitarno-Epidemiologiczny w Gorzowie Wielkopolskim	Rejestr zgonów	000138/00	17.01.2000
37.	Wojewódzki Inspektor Sanitarno-Epidemiologiczny w Gorzowie Wielkopolskim	Rejestr osób zaszczepionych przeciw chorobom zakaźnym.	000163/00	17.01.2000
38.	Wojewódzki Inspektor Sanitarno-Epidemiologiczny w Gorzowie Wielkopolskim	Rejestr nosicieli HIV i chorych na AIDS.	000164/00	17.01.2000
39.	Wojewódzki Inspektor Sanitarno-Epidemiologiczny w Gorzowie Wielkopolskim	Wywiady epidemiologiczne.	000166/00	17.01.2000
40.	Wojewódzki Inspektor Sanitarno-Epidemiologiczny w Gorzowie Wielkopolskim	Rejestr osób chorych, zakażonych i nosicieli chorób zakaźnych wraz z dokumentacją.	000166/00	17.01.2000
41.	Wojewódzki Inspektor Sanitarno-Epidemiologiczny w Gorzowie Wielkopolskim	Lista osób egzaminowanych z podstawowych zasad higieny wraz z protokołami.	00016700	17.01.2000
42.	Wojewódzki Inspektor Sanitarno-Epidemiologiczny w Gorzowie Wielkopolskim	Dokumentacja chorób zawodowych.	000168/00	17.01.2000
43.	Wojewódzki Inspektor Sanitarno-	Oferty pracy.	000169/00	17.01.2000

	Epidemiologiczny w Gorzowie Wielkopolskim			
44.	Wojewódzki Inspektor Sanitarno-Epidemiologiczny w Gorzowie Wielkopolskim	Rejestr badań laboratoryjnych z dokumentacją.	000170/00	17.01.2000
45.	Wojewódzki Inspektor Inspekcji Handlowej w Lublinie.	Repertorium spraw skierowanych do prokuratury i policji.	000389/00	19.01.2000
46.	Wojewódzki Inspektor Inspekcji Handlowej w Lublinie	Repertorium spraw skierowanych do kolegium ds. wykroczeń.	000392/00	18.01.2000
47.	Wojewódzki Inspektor Inspekcji Handlowej w Lublinie	Repertorium nałożonych mandatów karnych.	000401/00	18.01.2000
48.	Wojewódzki Inspektor Inspekcji Handlowej w Lublinie	Rejestr skarg i wniosków dotyczących działalności przedsiębiorców.	000409/00	18.01.2000
49.	Wojewódzki Inspektorat Ochrony Roślin we Wrocławiu	Rejestr posiadaczy sprzętu do stosowania środków ochrony roślin.	000674/00	14.02.2000
50.	Lubuski Wojewódzki Inspektorat Ochrony Roślin	Rejestr osób eksportujących i reeksportujących, którym wydano świadectwo fitosanitarne.	000694/00	14.02.2000
51.	Lubuski Wojewódzki Inspektorat Ochrony Roślin	Rejestr osób, które złożyły skargi i wnioski.	000695/00	14.02.2000
52.	Lubuski Wojewódzki Inspektorat Ochrony Roślin	Rejestr osób, od których pobrano próby roślin, produktów roślinnych, przedmiotów i gleby do ekspertyzy laboratoryjnej.	000700/00	14.02.2000
53.	Lubuski Wojewódzki Inspektorat Ochrony Roślin	Rejestr osób, u których stwierdzono występowanie organizmów szkodliwych.	000702/00	14.02.2000
54.	Lubuski Wojewódzki Inspektorat Ochrony Roślin	Rejestr osób, którym nałożono karę grzywny w drodze mandatu i do których skierowano	000703/00	14.02.2000

		wniosek o ukaranie do kolegium ds. wykroczeń.		
55.	Lubuski Wojewódzki Inspektorat Ochrony Roślin	Rejestr osób posiadających sprzęt do stosowania środków ochrony.	000704/00	14.02.2000
56.	Wojewódzki Inspektorat Ochrony Roślin w Białymstoku	Zbiór wydanych decyzji w sprawie zwalczania organizmów szkodliwych i tytułów egzekucyjnych.	000884/00	03.03.2000
57.	Wojewódzki Inspektorat Ochrony Roślin w Białymstoku	Zbiór wydanych świadcstw zdrowotności.	000885/00	03.03.00
58.	Wojewódzki Inspektorat Ochrony Roślin w Białymstoku.	Zbiór kart rejestracyjnych występowania organizmów szkodliwych.	000886/00	03.03.2000
59.	Wojewódzki Inspektorat Ochrony Roślin w Białymstoku	Rejestr posiadaczy sprzętu do wykonywania zabiegów ochrony roślin.	000887/00	03.03.2000
60.	Wojewódzki Inspektorat Nadzoru Budowlanego w Szczecinie	Książka korespondencyj- na.	000942/00	09.03.2000
61.	Wojewódzki Inspektor Nadzoru Budowlanego w Lublinie	Rejestr spraw WINB.	001758/00	14.06.2000
62.	Wojewódzki Urząd Pracy w Szczecinie	Baza osób korzystających z usług Biura Terenowego Funduszu Gwarantowanych Świadczeń Pracowniczych w Szczecinie i Biura Terenowego Funduszu Gwarantowanych Świadczeń Pracowniczych w Koszalinie.	000693/00	16.02.2000
63.	Wojewódzki Urząd Pracy w Katowicach	Decyzje administracyjne, postanowienia, skargi i	002249/00	27.09.2000

		wnioski.		
64.	Wojewódzki Urząd Pracy w Katowicach	Pośrednictwo pracy.	002369/00	27.10.2000

Załącznik nr 3

Liczba zwolnień od rejestracji w zależności od podstawy wyłączenia

Podstawa wyłączenia		Liczba zwolnień
art. 43 ust. 1 pkt 1		0
art. 43 ust. 1 pkt 2		220
art. 43 ust. 1 pkt 3		0
art. 43 ust. 1 pkt 4	Osoby zatrudnione	235
	Osoby zrzeszone	92
	Osoby uczące się	157
	łącznie	484
art. 43 ust. 1 pkt 5		46
art. 43 ust. 1 pkt 6		5
art. 43 ust. 1 pkt 7		0
art. 43 ust. 1 pkt 8		13
art. 43 ust. 1 pkt 9		81
art. 43 ust. 1 pkt 10		0
art. 43 ust. 1 pkt 11		4
Ogółem:		853

Załącznik nr 4

Zbiory danych osobowych, które nie zostały zgłoszone do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych przez naczelne i centralne organy administracji publicznej

1. Zbiór danych osobowych osób powoływanych przez Prezesa Rady Ministrów na podstawie odrębnych przepisów (np. członków Rady Konsultacyjnej przy Prezesie Urzędu Regulacji Energetyki, członków Rady Statystyki, Przewodniczącego Komitetu Kinematografii, itp.).
2. Zbiory danych osobowych powstające w związku z realizacją uprawnień Ministra Kultury do powoływania i odwoływania:
 - Członków Krajowej Rady Bibliotecznej
 - Wskazania części członków Rady do Spraw muzeów
3. Zbiory danych osobowych powstające w związku z realizacją kompetencji Ministra Rolnictwa w sprawie ustalenia składu i zakresu czynności Komitetu do spraw wyścigów konnych.
4. Zbiory danych osobowych powstające w związku z realizacją kompetencji Ministra Spraw Wewnętrznych i Administracji do:
 - Wydawania decyzji w sprawach przydziału i opróżniania lokali mieszkalnych i tymczasowych kwater wydają będący dysponentami lokali w stosunku do: Komendanta Głównego Policji oraz zastępców Komendanta Głównego Policji.
 - Rozpatrywania spraw związanych z zaginięciem policjanta oraz stwierdzenia związku tego zaginięcia ze służbą
 - Wyrażania zgody na pokrycie kosztów pogrzebu policjanta zmarłego wskutek choroby pozostającej w związku ze służbą
 - Wyrażania zgody kierownikom polskich przedstawicielstw dyplomatycznych i urzędów konsularnych na wydawanie wiz repatriacyjnych

- Wyrażania zgody kierownikom polskich przedstawicielstw dyplomatycznych i konsularnych na wydawanie wiz pobytowych, np. dla osób, które mają być wydalone, niebezpieczne
- Wydawania wiz pobytowych cudzoziemcom, w stosunku do których wydano postanowienie o wszczęciu postępowania o nadanie statusu uchodźcy
- Wydawania dokumentu podróży lub decyzji o odmowie jego wydania, jeżeli przemawia za tym ważny interes cudzoziemca
- Wydawania decyzji w sprawach o nadanie lub pozbawienie statusu uchodźcy
- Wydawania cudzoziemcowi, który uzyskał status uchodźcy, dokumentu podróży przewidzianego w Konwencji Genewskiej oraz wydawania i przedłużania zezwolenia na zamieszkanie na czas oznaczony
- Wydawania w porozumieniu z Ministrem Spraw Zagranicznych decyzji w sprawach udzielania i pozbawiania azylu
- Powoływania spośród oficerów Państwowej Straży Pożarnej Komendanta wojewódzkiego Państwowej Straży Pożarnej
- Nadawania na wniosek Komendanta Głównego Państwowej Straży Pożarnej pierwszego stopnia aspiranckiego i stopni oficerskich

5. Zbiory danych prowadzone w związku z realizacją kompetencji Ministra Pracy do:

- Powoływania i odwoływania członków Komisji do Spraw Układów Zbiorowych Pracy.
- Powoływania i odwoływania Krajowej Rady Konsultacyjnej do Spraw osób Niepełnosprawnych.
- Powoływania i odwoływania członków Naczelnej Rady Zatrudnienia.
- Powoływania i odwoływania członków Rady Pomocy Społecznej.

6. Zbiory danych osobowych powstające w związku z realizacją kompetencji Ministra Edukacji do utworzenia Krajowej Rady Oświatowej i Rady do spraw Szkolnictwa Artystycznego.

7. Zbiory danych osobowych prowadzone przez Ministra Zdrowia w związku z realizacją kompetencji do:

- Powoływania i odwoływania Przewodniczącego Centralnej Komisji do Walki z Chorobami Wenerycznymi.
- Powoływania i odwoływania Przewodniczącego i członków Krajowej Rady Transplantacyjnej.
- Powoływania i odwoływania Przewodniczącego i członków Krajowej Rady do Spraw Krwiodawstwa i Krwiolecznictwa.
- Powoływania i odwoływania członków okręgowych komisji oraz Odwoławczej Komisji Kontroli Zawodowej.
- Przyznawania prawa wykonywania zawodu i używania tytułu felczera.

8. Zbiory danych osobowych przetwarzanych przez Ministra Spraw Zagranicznych powstające w związku z realizacją kompetencji Ministra do:

- Do przedstawiania 8 kandydatów do Rady do Spraw Uchodźców.
- Wydawania decyzji w sprawie udzielenia i pozbawienia azylu.
- Zwalniania (w porozumieniu z Ministrem Spraw Wewnętrznych i Administracji) z obowiązku uzyskania wizy przez szefów i członków personelu misji dyplomatycznych, kierowników urzędów konsularnych i członków personelu konsularnego państw obcych oraz innych osób zrównanych z nimi na podstawie ustaw, umów lub powszechnie ustalonych zwyczajów międzynarodowych, pod warunkiem wzajemności i posiadania przez te osoby odpowiednich dokumentów (tzw. legitymacji).
- Wydawania legitymacji szefom i członkom personelu misji dyplomatycznych, kierownikom urzędów konsularnych i członkom personelu konsularnego państw obcych oraz innym osobom zrównanym z nimi na podstawie ustaw, umów lub powszechnie ustalonych zwyczajów międzynarodowych, pod warunkiem wzajemności i posiadania przez te osoby odpowiednich dokumentów.
- Wydawania wiz szefom i członkom personelu misji dyplomatycznych.
- Wydawania wiz kierownikom urzędów konsularnych i członkom personelu konsularnego państw obcych.
- Wydawania i wznawiania ważności paszportów dyplomatycznych i paszportów służbowych.

9. Zbiory danych osobowych przetwarzanych przez Ministra Finansów:

- Powstające w związku z realizacją kompetencji Ministra do:
 - a. ogłaszania wykazu osób, którym umorzono znaczące kwoty zaległości podatkowych,
 - b. ogłaszania wykazu osób wpisanych na listę doradców podatkowych,
 - c. publikowania wykazu osób posiadających uprawnienia do wykonywania zawodu brokera,
 - d. publikowania wykazu aktuariuszy ubezpieczeniowych
- Zbiory danych osobowych związane z prowadzeniem rejestru osób ukaranych przez Główną Komisję Orzekającą w sprawach o naruszenie dyscypliny finansów publicznych.
- Zbiory danych osobowych powstające w związku ze sprawowaniem przez Ministra Finansów nadzoru nad izbami skarbowymi i urzędami skarbowymi.

10. Zbiory danych osobowych związane z prowadzeniem przez izby skarbowe i urzędy skarbowe następujących rejestrów:

- a. rejestr podatników (NIP),
- b. rejestr podatników podatku od osób fizycznych,
- c. rejestr podatników podatku od nieruchomości,
- d. rejestr podatników podatku rolnego,
- e. rejestr podatników podatku leśnego,
- f. rejestr podatników podatku od środków transportowych,
- g. rejestr podatników podatku od spadków i darowizn,
- h. rejestr podatników podatku od posiadania psów,
- i. rejestr podatników podatku od gier

11. Zbiory danych osobowych przetwarzanych przez **Ministra Sprawiedliwości – Prokuratora Generalnego**:

- Zbiory danych dotyczące osób posiadających uprawnienia do wykonywania zawodu prokuratora.

- Zbiory danych dotyczące osób posiadających uprawnienia do wykonywania zawodu sędziego.
- Zbiory danych dotyczące osób posiadających uprawnienia do wykonywania zawodu adwokata.
- Zbiory danych osobowych aplikantów adwokackich.
- Zbiory danych dotyczące osób posiadających uprawnienia radcowskie.
- Zbiory danych osobowych aplikantów radcowskich.
- Zbiory danych osobowych powstające w związku z załatwianiem skarg, wniosków w trybie administracyjnym.
- Zbiory danych osobowych powstające w związku z rejestracją korespondencji wpływającej do urzędu.
- Zbiory danych osobowych dotyczące aplikantów sądowych i aplikantów prokuratorskich.
- Zbiory danych dotyczące referendarzy sądowych

Załącznik nr 5

Szkolenia, wykłady w zakresie ustawy o ochronie danych osobowych przeprowadzone przez Generalnego Inspektora Ochrony Danych Osobowych oraz pracowników Biura GIODO

1. Krajowa Szkoła Administracji Publicznej – Generalny Inspektor Ochrony Danych Osobowych - Warszawa, 19 stycznia 2000 r.
2. Krajowa Szkoła Administracji Publicznej – Dyrektor Departamentu Prawnego GIODO - Warszawa, 8 marca 2000 r.
3. Ministerstwo Sprawiedliwości - Generalny Inspektor Ochrony Danych Osobowych; Dyrektor Departamentu Inspekcji, Dyrektor Departamentu Rejestracji Zbiorów Danych Osobowych GIODO - Jastrzębia Góra, 15 marca 2000 r.
4. Ministerstwo Sprawiedliwości – Dyrektor Departamentu Prawnego GIODO; Dyrektor Departamentu Rejestracji Zbiorów Danych Osobowych GIODO - Zakopane, 29 marca 2000 r.
5. Kancelaria Prezesa Rady Ministrów - Departament Legislacji - Generalny Inspektor Ochrony Danych Osobowych – Warszawa, 25 maja 2000 r.
6. Prokuratura Rejonowa – Dyrektor Departamentu Rejestracji Zbiorów Danych Osobowych GIODO - Popowo, 30 maja 2000 r.
7. Instytut Spraw Publicznych – Generalny Inspektor Ochrony Danych Osobowych - Warszawa, 28 czerwca 2000 r.
8. Prokuratura Rejonowa - Dyrektor Departamentu Inspekcji GIODO - Brok, 11 października 2000 r.
9. Najwyższa Izba Kontroli - Dyrektor Departamentu Inspekcji GIODO – Warszawa, 7 listopada 2000 r.
10. Poradnia psychologiczno-pedagogiczna - Dyrektor Departamentu Inspekcji GIODO - Mińsk Mazowiecki, 14 listopada 2000 r.
11. III Ogólnopolskie Forum Prawniczo-Medyczne - Dyrektor Departamentu Informatyki GIODO – Warszawa, 7 - 8 grudnia 2000 r.

Załącznik nr 6

Konferencje prasowe Generalnego Inspektora Ochrony Danych Osobowych

1. W dniu 6 stycznia 2000 r., pt. Kasy chorych żądają zbyt wielu danych osobowych,
2. Podsumowanie działalności Generalnego Inspektora Ochrony Danych Osobowych w 1999 r.
3. W dniu 25 stycznia 2000 r., pt. Bezprawne przekazywanie danych osobowych klientów PZU holenderskiej firmie „Holimpex”.
4. W dniu 20 kwietnia 2000 r., pt. Dostęp do informacji a ochrona danych osobowych.
5. W dniu 9 maja 2000 r., pt. Ochrona danych medycznych i ich przetwarzanie.
6. W dniu 23 maja 2000 r., pt. Ochrona danych osobowych w Hiszpanii i w Polsce – wymiana doświadczeń.
7. W dniu 27 lipca 2000 r., pt. Czy zostaną wydane akty prawne legalizujące nieprawne działania kas chorych?
8. W dniu 10 października 2000 r., pt. Zbyt szeroki zakres danych osobowych żądanych przy zameldowaniu i wymeldowaniu; Międzynarodowa konferencja w Wenecji „Jeden świat, jedna ochrona prywatności”; Rejestracja zbiorów danych osobowych.
9. W dniu 4 grudnia 2000 r. – na temat: „Przetwarzanie danych osobowych na potrzeby ubezpieczeń prywatnych” z udziałem, Prezesa Polskiej Izby Ubezpieczeń Jerzego Wysockiego zorganizowane przy okazji seminarium „Przetwarzanie danych osobowych na potrzeby ubezpieczeń prywatnych”

Załącznik nr 7

Artykuły prasowe dotyczące problematyki ochrony danych osobowych

Gazeta Samorządu i Administracji, GODO odpowiada:

- „Konsekwencje dla spóźnialskich”, 17.01-30.01.2000 r.
- „Rejestr pojazdów”, 31.01-13.02.2000 r.
- „Dane dla prokuratora”, 14.02-27.02.2000 r.
- „Wynagrodzenia w samorządzie”, 28.02-12.03.2000 r.
- „Dzienniki lekcyjne”, 13.03-26.03.2000 r.
- „Odwołania rozpatruje SKO”, 27.03-09.04.2000 r.
- „Kasa chorych i dane pacjentów”, 10.04-07.05.2000 r.
- „Podstawy przetwarzania danych; Informacje administratora”, 08.05-04.06.2000 r.
- „Kontrola w MOPS-ie; Bez zgody podopiecznego”, 5.06-2.07.2000 r.
- „Jakie dane ZOZ może uzyskać od gminy”, 03.07-30.07.2000 r.
- „Dane zwycięzcy przetargu”, 25.09-22.10.2000 r.

Rzeczpospolita, GODO sygnalizuje:

- „Podmioty publiczne nie są zobowiązane do podejmowania działań na ustne żądanie funkcjonariuszy urzędów celnych. Pismo z żądaniem określonych informacji musi powoływać się zarówno na określoną podstawę prawną, jak i na prowadzenie konkretnej sprawy”. (18 stycznia 2000 r.)
- „Odmowa udzielenia informacji przez jednostki organizacyjne ZUS podmiotom działającym na podstawie ustawodawstwa z zakresu pomocy społecznej nie znajduje uzasadnienia w przepisach ustawy o ochronie danych osobowych”. (21 stycznia 2000 r.)
- „Kasy chorych mogą żądać od administratorów (np. świadczeniodawców) udostępniania danych osobowych tylko wtedy, gdy posiadają stosowną podstawę prawną”. (1 luty 2000 r.)
- „Jeśli przy wykonywaniu czynności służbowych funkcjonariusz UOP występuje z żądaniem lub prośbą o pomoc do instytucji państwowych, jednostek gospodarczych oraz organizacji społecznych powinien to uczynić na piśmie. Wymagają tego przepisy prawa”. (8 luty 2000 r.)

- „Ustawa o ochronie danych osobowych wyraźnie odróżnia dane zwykłe od sensytywnych (wrażliwych). Przetwarzanie tych drugich jest generalnie zabronione i możliwe tylko w ściśle określonych w ustawie sytuacjach”. (14 lutego 2000 r.)
- „Ustawa o ochronie danych uprawnia każdego, którego dane są przetwarzane, do żądania od administratora danych uzupełnienia, uaktualnienia, sprostowania danych osobowych, a także czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane”. (24 marca 2000 r.)
- „Udostępnianie danych o właścicielach lokali przez zarządy nieruchomości innym właścicielom w tej samej wspólnotie mieszkaniowej jest możliwe w sytuacjach przewidzianych przez przepisy kodeksu cywilnego oraz ustawy o własności lokali”. (26 kwietnia 2000 r.)
- „Dane o stanie zdrowia należą do kategorii szczególnie chronionych. Ustawa o ochronie danych osobowych pozwala na ujawnianie ich tylko w ściśle określonych sytuacjach”. (4 maja 2000 r.)
- „Ustawa o ochronie danych osobowych gwarantuje każdej osobie, której dane są przetwarzane, prawo wniesienia (w przypadkach wymienionych w art. 23 ust. 1 pkt 4 i 5) pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację. Jednakże, jeżeli podstawą przetwarzania danych jest, np. przepis prawa to skorzystanie z tego uprawnienia nie jest możliwe”. (12 czerwca 2000 r.)
- „Urzędy skarbowe przeprowadzające kontrolę zakładów pracy chronionej nie mogą żądać dostępu do akt osobowych pracowników, gdyż nie znajduje to uzasadnienia w przepisach innych ustaw. Należy więc uznać, że ich działanie jest niezgodne z ustawą o ochronie danych osobowych, w szczególności z art. 27”. (15 czerwca 2000 r.)
- „Zbiorem danych jest zestaw danych osobowych uporządkowany w sposób pozwalający na bezpośredni dostęp do poszukiwanej informacji. Dostępność danych według określonego kryterium, np. alfabetycznego, jest cechą pozwalającą na odnalezienie informacji o danej osobie bez potrzeby przeglądania całego zestawu”. (20 lipca 2000 r.)
- „Zbieranie przez komitety wyborcze podpisów obywateli, wraz z ich danymi osobowymi, na listach popierających zgłoszenie kandydata w wyborach prezydenckich, nie narusza ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.), ponieważ odbywa się w ramach i na podstawie obowiązujących przepisów prawa”. (28 lipca 2000 r.)

- „Ustawa o ochronie danych osobowych nakłada na administratora danych obowiązek zgłoszenia prowadzonego zbioru danych do rejestracji Generalnemu Inspektorowi (zwolnienia zostały wymienione enumeratywnie w ustawie), a następnie aktualizowane zgłoszenia w terminie 30 dni od daty dokonania w zbiorze zmiany informacji znajdujących się we wniosku rejestracyjnym”. (31 lipca 2000 r.)
- „Żądanie przez ZUS danych osobowych osób trzecich, w celu ustalenia podstawy wymiaru emerytury osoby zatrudnionej przez pewien czas za granicą, narusza przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych”. (14-15 sierpnia 2000 r.)
- „Żądanie przez kontrolerów komunikacji miejskiej, okazania odcinka świadczenia emerytalno-rentowego, podczas kontroli biletów, nie stanowi naruszenia przepisów ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych, jednak może godzić w dobra osobiste emerytów i rencistów”. (16 sierpnia 2000 r.)
- „Udostępnianie danych osobowych z aktów stanu cywilnego nie narusza ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych, jeżeli odbywa się w ramach i na podstawie obowiązujących przepisów prawa”. (1 września 2000 r.)
- „Przechowywanie przez domy maklerskie formularzy, umów i innych dokumentów, które zawierają dane osobowe klientów, jest zgodne z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, jeżeli odbywa się w ramach i na podstawie stosownych przepisów prawa”. (29 września 2000 r.)
- „Zbieranie przez szkoły danych osobowych ucznia i jego rodziców nie narusza ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych, jeżeli odbywa się w ramach i na podstawie stosownych przepisów prawa”. (6 listopada 2000 r.)

Prawo i Życie

1. Opinie:

- „Przetwarzanie danych osobowych”

2. Pytania i odpowiedzi: „[Odpowiada dr Ewa Kulesza, generalny inspektor ochrony danych osobowych](#)”:

- „Czy firma kurierska jest administratorem danych; Pozyskiwanie danych osobowych przez kasy chorych; Odmowa udzielenia informacji a postępowanie egzekucyjne; Czy GIODO jest organem odwoławczym?”, maj 2000 r.

- „Informacja o numerach telefonicznych; Komornik i dłużnik; Dokumentacja lekarska a ubezpieczenia pracownicze, Jak dostarczać pisma urzędowe?; Do wiadomości stron”, lipiec 2000 r.
- „Prawo do informacji: Dostęp do dokumentów, Nadinterpretacja ustawy, Dostęp dziennikarzy do informacji”, październik 2000 r.

Wywiady Generalnego Inspektora Ochrony Danych Osobowych:

- „Dane pacjenta wartością chronioną”, Służba Zdrowia, 3 - 10 stycznia 2000 r.
- „Konieczne kompleksowe zmiany”, Gazeta Prawna Nr 6, 20 - 23 stycznia 2000 r.
- „Jakie zmiany są konieczne. Bez nowelizacji ustawy o ochronie danych osobowych grozi nam dalsza zabawa w kotka i myszkę”, Gazeta Prawna Nr 28, 6 - 9 kwietnia 2000 r.
- „Obywatel musi mieć dostęp do informacji ”, Rzeczpospolita, 25 kwietnia 2000 r.
- "Tajne/poufne", Wprost, 23 kwietnia 2000 r.
- „Jak chronione są ewidencje i rejestry? ”, Gazeta Samorządu i Administracji Nr 10/11, 8 maja - 4 czerwca 2000 r.
- „Prawo do prywatności. Moje nazwisko jest na furtce”, Prawo i Życie Nr 3, czerwiec 2000 r.
- „Ochrona (nie)konieczna. Obywatel musi mieć dostęp do informacji”, Wprost, 26 czerwca 2000 r.
- "Dla dobra publicznego", Gazeta Prawna, 7-9 lipca 2000 r.
- „Prywatność pod szczególną ochroną”, Trybuna Nr 180, 3 sierpnia 2000 r.
- „Płace - Ochrona danych i wynagrodzenia”, Wynagrodzenia Nr 21, 11 października 2000 r.

Załącznik nr 8

Zagraniczne szkolenia i udział w konferencjach generalnego inspektora oraz pracowników biura GODO

1. Szkolenie dla pracowników Biura Generalnego Inspektora Ochrony Danych Osobowych w Biurze Federalnego Rzecznika ds. Ochrony Danych Osobowych, Bonn (Niemcy), 15 - 20 kwietnia 2000 r (udział Generalnego Inspektora oraz pracowników Departamentu Prawnego, Departamentu Inspekcji i Departamentu Informatyki).
2. 27 spotkanie Międzynarodowej Grupy Roboczej ds. Ochrony Danych Osobowych w sektorze telekomunikacji, Kreta (Grecja), 4 - 5 maja 2000 r (udział dyrektora Departamentu Informatyki).
3. Wizyta Generalnego Inspektora Ochrony Danych Osobowych w greckim Urzędzie Ochrony Danych Osobowych, Ateny (Grecja), 5 - 7 czerwca 2000 r.
4. 13 konferencja zorganizowana przez Privacy Laws and Business, Cambridge (Wielka Brytania), 3 - 5 lipca 2000 r. (udział pracowników Departamentu Prawnego).
5. Konferencja nt. „Oprogramowanie P3P (Platform for Privacy Preferences)”, Kilonia (Niemcy), 27 – 30 sierpnia 2000 r. (udział Generalnego Inspektora).
6. 28 spotkanie Międzynarodowej Grupy Roboczej ds. Ochrony Danych Osobowych w sektorze telekomunikacji, Berlin (Niemcy), 13 - 14 września 2000 r. (udział Generalnego Inspektora i Dyrektora Departamentu Informatyki).
7. Wizyta Generalnego Inspektora Ochrony Danych Osobowych w Państwowym Inspektoracie Ochrony Danych Osobowych na Litwie, Wilno (Litwa), 18 - 19 września 2000 r.
8. Udział Generalnego Inspektora Ochrony Danych Osobowych w 22 międzynarodowej konferencji dotyczącej ochrony prywatności i danych osobowych - „Jeden świat, jedna ochrona prywatności”, „Na drodze ku elektronicznemu obywatelstwu”, Wenecja (Włochy), 28 – 30 września 2000 r. (udział Generalnego Inspektora oraz pracowników z Departamentów: Inspekcji, Prawnego i Rejestracji Zbiorów Danych Osobowych).
9. Wizyta w Agencji Ochrony Danych Osobowych w Hiszpanii (Agencia de Protection de Datos), Madryt (Hiszpania), 16 - 17 października 2000 r. (udział Generalnego Inspektora oraz pracowników Departamentu Inspekcji, Prawnego i Rejestracji Zbiorów Danych Osobowych).

10. 7 Szwajcarska Konferencja Rzeczników Ochrony Danych Osobowych, Bazylea (Szwajcaria), 24 – 25 października 2000 r. (udział Generalnego Inspektora).
11. 5 Sympozjum - Ochrona Danych Osobowych i Bezpieczeństwo Informacyjne, Zurich (Szwajcaria), 26 – 28 października 2000 r. (udział Generalnego Inspektora).
12. Wizyta w Data Inspection Board, Sztokholm (Szwecja), 6 – 7 listopada 2000 r. (udział Generalnego Inspektora oraz Dyrektora Departamentu Prawnego – wizyta finansowana ze środków Rady Europy).
13. Wizyty gości zagranicznych w Biurze GIODO, przybyłych na zaproszenie Generalnego Inspektora Ochrony Danych Osobowych:
14. Wizyta Dyrektora Urzędu Ochrony Danych Osobowych z Hiszpanii (Agencia de Protección de Datos), Juana Manuela Fernandez Lopeza, Warszawa, 22 – 23 maja 2000 r.