

GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

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

ZA OKRES

01.01.1999 r. – 31.12.1999 r.

Warszawa, lipiec 2000 r.

<u>WSTĘP</u>	8
--------------------	---

<u>CZEŚĆ I. ZAKRES SPRAW ROZPATRYWANYCH PRZEZ</u> <u>GENERALNEGO INSPEKTORA OCHRONY</u> <u>DANYCH OSOBOWYCH</u>	11
---	----

<u>A. Zagadnienia ogólne</u>	11
------------------------------------	----

<u>I. Definicja danych osobowych</u>	12
<u>II. Przetwarzanie danych osobowych w zbiorach</u>	15
<u>III. Przekazywanie danych osobowych za granicę</u>	16
<u>IV. Wyłączenia spod zastosowania ustawy</u>	17

<u>B. Sprawy z zakresu administracji samorządowej</u>	17
---	----

<u>I. Definicja administratora danych</u>	17
<u>II. Udostępnianie danych osobowych podmiotom uprawnionym do ich przetwarzania na mocy przepisów prawa</u>	20
<u>III. Udostępnianie danych osobowych na potrzeby badań naukowych</u>	25
<u>IV. Poszczególne rodzaje spraw z zakresu administracji samorządowej dotyczących przetwarzania danych</u>	25
<u>IV.1 Ewidencja i rejestracja pojazdów, wydawanie uprawnień do kierowania pojazdami</u>	25
<u>IV.2 Przetwarzanie danych osobowych w ramach postępowania administracyjnego</u>	27
<u>IV.3 Przetwarzanie danych osobowych w placówkach oświatowo-wychowawczych</u>	28
<u>IV.4 Sprawy lokalowe</u>	30
<u>IV.5 Przetwarzanie danych osobowych przez Straż Miejską</u>	30
<u>IV.6 Ujawnianie informacji o radnych i o pracownikach samorządowych</u>	32
<u>IV.7 Ujawnienie danych osób biorących udział w komisyjnym otwarciu mieszkania</u>	34
<u>IV.8 Oprawa ksiąg urzędu stanu cywilnego</u>	35
<u>IV.9 Przetwarzanie danych w ewidencjach</u>	35
<u>IV.10 Sprawy z zakresu pomocy społecznej</u>	38
<u>1) Zagadnienie podstaw przetwarzania danych osobowych, w tym zgody osoby ubiegającej się o świadczenie przez jednostki pomocy społecznej</u>	39

2) Zagadnienie zakresu danych gromadzonych przez jednostki organizacyjne pomocy społecznej	41
3) Udostępnianie danych uzyskanych w toku przygotowywania decyzji w sprawie przyznania świadczenia	42
4) Zagadnienie wykorzystywania danych zebranych w toku działań jednostek organizacyjnych pomocy społecznej na potrzeby badań	44
5) Skargi i pytania dotyczące podstaw i źródeł uzyskiwania informacji o danych niezbędnych do udzielenia świadczenia z pomocy społecznej	44
6) Sprawy dotyczące dopełnienia obowiązku rejestracji przez ośrodki pomocy społecznej	46
 <u>C. Przetwarzanie danych osobowych przez funkcjonariuszy służb publicznych</u>	48
<u>I. Podstawy prawne przetwarzania danych osobowych</u>	48
I.1 Udostępnianie danych osobowych funkcjonariuszom Policji, UOP, funkcjonariuszom innych służb publicznych	48
1) Legalność udostępniania	48
2) Forma wystąpienia funkcjonariuszy o udostępnienie im danych osobowych przetwarzanych przez inne podmioty	51
3) Zakres udostępnianych funkcjonariuszom danych	57
I.2 Udostępnianie danych osobowych przez Policję, UOP, Urząd Celny, Straż Graniczną i Służbę Więzienną innym podmiotom	58
<u>II. Obowiązki administratorów danych</u>	63
<u>III. Inne zagadnienia</u>	65
 <u>D. Sady, prokuratura i kolegia do spraw wykroczeń</u>	66
<u>I. Zagadnienia wstępne</u>	66
<u>II. Przetwarzanie danych osobowych przez sądy, prokuraturę i kolegia ds. wykroczeń</u>	66
II.1 Zakres i podstawy przetwarzania danych osobowych przez sądy	66
II.2 Przetwarzanie danych osobowych przez prokuraturę	75
II.3 Forma wystąpienia sądów i prokuratury o udostępnienie danych przetwarzanych przez inne jednostki	78
<u>III. Przetwarzanie danych osobowych przez kolegia do spraw wykroczeń</u>	79
 <u>E. Przetwarzanie danych osobowych w zakresie ochrony zdrowia</u>	80

<u>I. Zagadnienia wstępne</u>	80
<u>II. Przetwarzanie danych osobowych przez Kasy Chorych</u>	81
<u>II.1 Udostępnianie danych medycznych i kontrola świadczeniodawców</u>	81
<u>II.2 Przetwarzanie danych osobowych przez zakłady ubezpieczeniowe</u>	84
<u>II.3 Zagadnienie udostępniania danych inspektorom NIK</u>	85
<u>II.4 Inne zagadnienia</u>	86
<u>III. Udostępnianie danych osobowych zakładom pracy przez zakłady opieki</u> <u> zdrowotnej</u>	87
<u>IV. Obowiązki administratora danych</u>	88
<u>IV.1 Obowiązek informacyjny</u>	88
<u>IV.2 Obowiązek rejestracji</u>	89
<u>F. Stosunki pracy</u>	89
<u>I. Zakres danych przetwarzanych na potrzeby zatrudnienia</u>	90
<u>II. Obowiązki administratora danych, w tym dopełnianie obowiązku informacyjnego</u> <u> przez pracodawców</u>	94
<u>III. Udostępnianie danych osobowych pracowników</u>	96
<u>IV. Obowiązek zgłoszenia zbiorów danych do zarejestrowania</u>	107
<u>V. Powierzenie przez pracodawcę przetwarzania danych o pracownikach innemu</u> <u> podmiotowi</u>	108
<u>VI. Przetwarzanie danych osobowych kandydatów do pracy, osób poszukujących</u> <u> pracy</u>	109
<u>VII. Zabezpieczanie dokumentacji personalnej – danych pracowników</u>	110
<u>G. Ubezpieczenia prywatne</u>	111
<u>H. Przetwarzanie danych osobowych w sektorze telekomunikacyjnym</u> ...	115
<u>I. Zagadnienia wstępne</u>	115
<u>II. Podstawy prawne i zakres przetwarzania danych osobowych przez operatorów</u> <u> sieci telekomunikacyjnej użytku publicznego</u>	115
<u>III. Inne zagadnienia</u>	125

I. Przetwarzanie danych osobowych przez banki, Związek Banków Polskich i instytucje współpracujące z bankami..... 127

I. Podstawy prawne przetwarzania danych osobowych 127

I.1 Definicja administratora danych osobowych..... 128

I.2 Legalność przetwarzania..... 129

I.3 Zmiana celu przetwarzania danych osobowych..... 132

I.4 Udostępnianie danych osobowych innym podmiotom..... 134

I.5 Biuro Informacji Kredytowej..... 136

1) Podstawy prawne funkcjonowania 136

2) Obowiązki wynikające z przetwarzania danych 137

II. Obowiązki banków 139

II.1 Obowiązek usunięcia danych zbędnych do realizacji celu, dla którego zostały zebrane 139

II.2 Obowiązek odpowiedniego zabezpieczenia danych..... 139

II.3 Obowiązek informacyjny 143

II.4 Obowiązek rejestracji zbiorów danych..... 146

J. Działalność marketingowa..... 147

I. Zagadnienia wstępne 147

II. Podstawy prawne przetwarzania danych osobowych..... 148

III. Obowiązki administratora danych..... 151

III.1 Obowiązek informacyjny 151

III.2 Obowiązek rejestracji..... 156

III.3 Obowiązek zabezpieczenia danych..... 159

IV. Inne zagadnienia 160

K. Pozostałe zagadnienia 163

CZEŚĆ II. REJESTRACJA ZBIORÓW DANYCH OSOBOWYCH..... 166

I. Ilościowe przedstawienie dynamiki procesu rejestracyjnego 167

II. Jakościowe i ilościowe omówienie pozostałej korespondencji kierowanej do

Departamentu Rejestracji Zbiorów Danych Osobowych..... 171

III. Zawiadomienia o zwolnieniach i zgłoszeniach przez nieuprawnione podmioty . 171

<u>III.1 Zwolnienia z obowiązku zgłoszenia zbioru danych osobowych do rejestracji</u>	171
<u>1) Zbiory danych osobowych przetwarzanych przez właściwe organy dla potrzeb postępowania sądowego (art. 43 ust. 1 pkt 2)</u>	173
<u>a) zbiory danych przetwarzanych przez komisje rozwiązywania problemów alkoholowych</u>	173
<u>b) zbiory danych osobowych przetwarzanych w związku z umieszczeniem dziecka w rodzinie zastępczej</u>	173
<u>c) zbiory danych osobowych będące rejestrem testamentów</u>	173
<u>d) zbiory danych osobowych dotyczące spraw karno – skarbowych</u>	174
<u>e) zbiory danych osobowych dotyczące mandatów karnych nakładanych przez strażników gminnych</u>	174
<u>2) Zbiory danych osobowych dotyczących osób zatrudnionych, zrzeszonych lub uczących się (art. 43 ust. 4)</u>	175
<u>a) zbiory danych osobowych dotyczących osób zatrudnionych</u>	175
<u>b) zbiory danych osobowych dotyczących osób uczących się</u>	175
<u>c) zbiory danych osobowych dotyczące osób zrzeszonych</u>	176
<u>3) Zbiory danych osobowych dotyczące osób korzystających z usług medycznych, obsługi notarialnej, adwokackiej lub radcy prawnego</u>	177
<u>a) zbiory danych osobowych prowadzone przez zakłady opieki zdrowotnej</u>	177
<u>b) zbiory danych osobowych poradni psychologiczno-pedagogicznych</u>	177
<u>c) zbiory danych osobowych aptek</u>	177
<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</u>	177
<u>5) Zbiory danych osobowych przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub sprawozdawczości finansowej (art. 43 ust. 1 pkt 8), (np.: zgłoszenia nr R 009087/99, nr R 007688/99, nr R 005191/99)</u>	178
<u>6) Zbiory danych osobowych powszechnie dostępnych (art. 43 ust. 1 pkt 9)</u>	178
<u>a) zbiory kar pieniężnych</u>	178
<u>b) zbiory danych osobowych dotyczących osób reprezentujących podmioty prowadzące działalność gospodarczą</u>	178
<u>7) Zbiory danych osobowych przetwarzanych w zakresie drobnych bieżących spraw życia codziennego</u>	179
<u>III.2 Zgłoszenia zbiorów danych osobowych do rejestracji dokonane przez podmioty nieuprawnione</u>	179
<u>IV. Postępowania wyjaśniające</u>	181
<u>IV.1 Postępowania wyjaśniające zakończone rejestracją zbioru danych osobowych</u>	181

IV.2 Postępowania wyjaśniające zakończone wydaniem decyzji odmawiającej rejestracji.....	184
<u>V. Zaświadczenia</u>	194
<u>VI. Wnioski</u>	194
<u>CZEŚĆ III. ZAWIADOMIENIA DO PROKURATURY</u>	197
<u>CZEŚĆ IV. PROPAGOWANIE IDEI OCHRONY DANYCH</u> <u>OSOBOWYCH</u>	202
<u>WNIOSKI KOŃCOWE</u>	206
<u>ZAŁĄCZNIKI</u>	218
<u>Załącznik nr 1</u>	218
<u>Załącznik nr 2</u>	219
<u>Załącznik nr 3</u>	221
<u>Załącznik nr 4</u>	222
<u>Załącznik nr 5</u>	227
<u>Załącznik nr 6</u>	231
<u>Załącznik nr 7</u>	237
<u>Załącznik nr 8</u>	239

WSTĘP

Sprawozdanie Generalnego Inspektora Ochrony Danych Osobowych¹ obejmuje okres od 1 stycznia do 31 grudnia 1999 r.; jest to drugie sprawozdanie z działalności. W związku z powyższym okres sprawozdawczy objęty drugim sprawozdaniem częściowo pokrywa się z okresem sprawozdawczym pierwszego sprawozdania Generalnego Inspektora, które obejmowało okres od 23 kwietnia 1998 r., tj. od daty wyboru Generalnego Inspektora przez Sejm, do 30 kwietnia 1999 r. Jednakże z uwagi na fakt, iż pierwsze sprawozdanie poświęcone było głównie sprawom organizacyjnym Biura GODO, w części informacyjnej dotyczącej działalności merytorycznej omówienie tej działalności nie stanowi powtórzenia w sprawozdaniu za 1999 r.

Począwszy od 1999 r., sprawozdania Generalnego Inspektora obejmować będą pełne lata kalendarzowe.

Liczba spraw, jakie wpłynęły do Biura Generalnego Inspektora Ochrony Danych Osobowych w okresie sprawozdawczym wyniosła 72.617, w tym 1902 zapytania prawne dotyczące interpretacji ustawy o ochronie danych osobowych, 479 skarg i 262 wnioski o zaopiniowanie projektów aktów prawnych, a także 69.974 wnioski o rejestrację zbiorów danych osobowych.

Generalny Inspektor wszczął 57 postępowań, wydał 77 decyzji administracyjnych oraz 571 zaświadczeń rejestracyjnych. W 1999 r. przeprowadzonych zostało 71 kontroli, a także skierowano 18 zawiadomień do prokuratury z wnioskiem o wszczęcie postępowania w związku z naruszeniem ustawy o ochronie danych osobowych. W związku ze stwierdzeniem nieprawidłowości w działaniu organów szczebla centralnego lub podmiotów podporządkowanych tym organom oraz sformułowania zastrzeżeń, co do obowiązujących aktów prawnych, Generalny Inspektor skierował 40 wystąpień do organów centralnych.

W Biurze Generalnego Inspektora przyjęto 245 interesantów oraz przeprowadzono ok. 6520 rozmów telefonicznych udzielając wyjaśnień i porad prawnych.

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.), rozporządzenia Prezydenta Rzeczypospolitej Polskiej z dnia 29 maja 1998 r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. Nr 73, poz. 464), 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.).

Pracownicy Biura odpowiadali na liczne telefony od osób fizycznych oraz osób dzwoniących w imieniu osób prawnych i instytucji. Dziennie otrzymywali oni od kilkunastu do około 100 telefonów. Pytania obejmowały w szczególności kwestie związane z dopełnieniem obowiązku rejestracji (czy w ogóle ciąży on na zainteresowanym podmiocie, w jaki sposób należy go dopełnić, jak wypełnić wniosek zgłoszeniowy), a także rozlicznych problemów technicznych, związanych ze stosowaniem ustawy, na przykład ustanowienia administratora bezpieczeństwa informacji, sposobem zabezpieczenia zbiorów danych. Po upływie terminu rejestracji, pytania dotyczyły głównie wykonywania obowiązku informacyjnego.

W 1999 r. w szerokim zakresie rozpoczęte zostały działania inspekcyjne. W celu ustalenia zgodności przetwarzania danych osobowych z przepisami ustawy o ochronie danych osobowych, inspektorzy Biura Generalnego Inspektora Ochrony Danych Osobowych przeprowadzili 64 inspekcje oraz dokonali 6 czynności kontrolnych.

Problematyka kontroli dotyczyła: podstawy prawnej przetwarzania danych, źródeł pozyskiwania danych, zakresu, celu i rodzaju przetwarzania danych, sposobu dopełnienia obowiązków administratora danych wynikających z art. 24 i 25 ustawy o ochronie danych osobowych, sposobu zbierania i udostępniania danych, sposobu załatwienia sprzeciwów wynikających z art. 32 ust. 1 pkt 8 ustawy, zabezpieczania zbiorów danych osobowych oraz sposobu wypełnienia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W celu sprawdzenia wykonania decyzji administracyjnych przeprowadzono 4 kontrole, z których 3 zostały dokonane celem ustalenia realizacji zaleceń zawartych we wnioskach pokontrolnych, pozostałe inspekcje dotyczyły zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Z ogólnej liczby 63 dokonanych inspekcji, 18 przeprowadzono w spółkach marketingowych, 10 w towarzystwach emerytalnych i towarzystwach ubezpieczeniowych, 9 w spółkach telefonii komórkowej, 7 w bankach, 4 w organach administracji publicznej oraz 15 w innych podmiotach (np. wydawnictwo, spółdzielnia, szpital, Kasa Chorych, spółki telewizyjne).

W związku z inspekcjami Generalny Inspektor Ochrony Danych Osobowych wydał 17 decyzji nakazujących przywrócenie stanu zgodnego z prawem, skierował 4 zawiadomienia o popełnieniu przestępstwa oraz 1 wniosek o wszczęcie postępowania dyscyplinarnego.

W 1999 r. przeważająca liczba spraw, jakie wpłynęły do Biura Generalnego Inspektora związana była z wykonaniem obowiązku rejestracyjnego. Szczegółowe informacje

dotyczące wykonania obowiązku rejestracyjnego przez podmioty zobowiązane na podstawie art. 40 ustawy o ochronie danych osobowych przedstawione zostały w części II Sprawozdania.

Część I. ZAKRES SPRAW ROZPATRYWANYCH PRZEZ GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH

A. Zagadnienia ogólne

Zgodnie z art. 7 Konstytucji, organy władzy publicznej mogą działać tylko na podstawie prawa. Zakres działania i kompetencje tych organów powinny być określone w powszechnie obowiązujących przepisach prawa (ustawach, ratyfikowanych umowach międzynarodowych, rozporządzeniach i aktach prawa miejscowego na obszarze działania organów, które je ustanowiły).²

W czasie prac sejmowych nad ustawą podkreślano, że zagrożenie dla ochrony danych osobowych stanowi nie tylko zbyt duża swoboda w gromadzeniu i pozyskiwaniu danych osobowych przez firmy prywatne, niebezpieczeństwa dostrzegano również w działaniach organów administracji. Zwracano wówczas uwagę zwłaszcza na możliwość zbywania przez podmioty administracji publicznej (np. gminy) danych osobowych uzyskiwanych, np. na podstawie obowiązku ustawowego.³ Wydaje się, że mimo pewnych słabości, które ujawniły się w pierwszym okresie funkcjonowania ustawy w praktyce, ustawa o ochronie danych osobowych skutecznie zapobiegła tego typu sytuacjom.

Nie sposób wyobrazić sobie działania jakiegokolwiek urzędu czy organu administracji, który nie przetwarzałby danych osobowych. Bez ograniczenia autonomii informacyjnej jednostki nie byłoby możliwe funkcjonowanie aparatu państwowego. Choć niejednokrotnie jednostka nie ma żadnego wpływu na to, czy i jakie dane jej dotyczące są przetwarzane przez organy administracji, może jednak czuwać nad tym, aby dane zbierane przez organ władzy publicznej były merytorycznie poprawne i adekwatne w stosunku do celu, dla którego zostały zebrane. Obowiązek informacyjny i skorelowane z nim uprawnienia określone w art. 32 są właśnie instrumentem pozwalającym osobom uprawnionym na rzeczywiste sprawowanie kontroli nad zgodnym z prawem przetwarzaniem dotyczących ich danych osobowych. Bez prawnego umocowania tego obowiązku trudno byłoby wyobrazić sobie skuteczne działanie ustawy o ochronie danych osobowych. Z praktyki Generalnego Inspektora Ochrony Danych Osobowych wynika, że znacznie większe zagrożenie ochrony

² Por. art. 87 Konstytucji RP z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483); w państwie prawa kompetencje organów państwowych powinny być określone ustawowo, choć w praktyce liczne są wyjątki od tej zasady na rzecz określania niektórych kompetencji w rozporządzeniach wydawanych na podstawie i w celu wykonania ustawy.

³ Zwraća na to uwagę zwłaszcza poseł Irena Lipowicz.

prawa do prywatności, aniżeli przetwarzanie danych przez organy państwa niesie ze sobą działalność, np. prywatnych firm marketingowych.⁴ Stąd nie wydaje się trafnym rozwiązaniem nałożenie jednakowych obowiązków (w tym w zakresie informowania osób, których dotyczą dane) na organy administracji państwowej i firmy prywatne, które prowadzą bardziej agresywną i trudną do kontrolowania działalność.

Do Generalnego Inspektora napływały sygnały o trudnościach finansowych gmin zobowiązanych do wypełnienia obowiązku informacyjnego.⁵ W obecnym stanie prawnym, administratorzy danych będący organami samorządu terytorialnego nie są zwolnieni z obowiązku informacyjnego, choć ze względów praktycznych, *de lege ferenda* zwolnienie takie uznać należałoby za wskazane.⁶

I. Definicja danych osobowych

Wejście w życie nowej w polskim porządku prawnym ustawy o ochronie danych osobowych zrodziło wiele pytań co do rozumienia niektórych pojęć oraz prawidłowej ich interpretacji. Na gruncie ustawy o ochronie danych osobowych zasadnicze znaczenie ma definicja danych osobowych. Zgodnie z art. 6 ustawy, za dane osobowe uważa się każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby.⁷

Ta klarowna wydawałoby się definicja sprawia jednak w praktyce trudności, o czym świadczą pytania kierowane do Biura Generalnego Inspektora Danych Osobowych.

Wątpliwości budziła, np. kwestia, czy dane dotyczące sposobu obliczania ilości ryczałtowego zużycia wody na jednego mieszkańca w poszczególnych budynkach są danymi osobowymi. Generalny Inspektor odpowiadając poinformował, że parametry techniczne określające poziom zużycia wody i związany z tym sposób obliczania opłat nie mogą stanowić danych osobowych w rozumieniu ustawy. Nie dotyczą bowiem konkretnych osób i nie jest możliwe ustalenie na ich podstawie tożsamości określonej osoby.⁸ Przetwarzaniem danych jest już jednak udzielanie informacji o osobach, które nie uiściły opłat za pobraną wodę.⁹ Do danych osobowych nie można zaliczyć także informacji o tym, czy i na jakiej

4 Wniosek ten jest trafny wyłącznie w odniesieniu do państwa, w którym funkcjonują demokratyczne struktury władzy państwowej.

5 Por. np. GI-DP-1552/99; prośby dotyczyły na przykład wskazania źródeł finansowania wynikających z tego przedsięwzięcia kosztów.

6 Por. GI-DP-580/99.

7 O problemach związanych z definicją danych osobowych również w cz. III Sprawozdania - na tle uwag odnoszących się do kontroli podmiotów przetwarzających dane osobowe.

8 GI-DP-875/99

9 GI-DP-909/99

podstawie zbierane są czynsze, oraz który z urzędów wydał decyzję w sprawie wymiaru podatku i jaka była podstawa prawna tej decyzji.¹⁰

Pewne informacje można zakwalifikować jako dane osobowe tylko w określonym kontekście sytuacyjnym lub w zestawieniu z innymi danymi. Niejednokrotnie nawet imię i nazwisko nie umożliwia określenia tożsamości konkretnej osoby. Dane osobowe nie muszą mieć charakteru ściśle osobowego, tzn. nie muszą odnosić się bezpośrednio do osoby. Jeżeli w pewnych okolicznościach, np. informacje o marce samochodu pozwalają zidentyfikować jego właściciela, to stanowią one dane osobowe.¹¹

W praktyce powstał również problem, czy *numer ewidencyjny PESEL* jest daną osobową.

Numer ewidencyjny PESEL występując samodzielnie, w świetle definicji danych zawartej w ustawie o ochronie danych osobowych, nie jest informacją umożliwiającą identyfikację określonej osoby, mimo, że zawiera dane o urodzeniu tej osoby, jej numer porządkowy i liczbę kontrolną. Gdyby jednak numer ten występował wraz z imieniem i nazwiskiem, wówczas, przy spełnieniu również innych wymogów, znalazłoby zastosowanie przepisy ustawy o ochronie danych osobowych. Z tych powodów, odpowiadając na pytanie, czy pozostaje w zgodzie z ustawą wykorzystywanie numeru PESEL do znakowania przedmiotów (np. rowerów, telewizorów), Generalny Inspektor uznał, że umieszczanie wyłącznie numeru ewidencyjnego na tych przedmiotach nie podlega rygorom ustawy.¹²

Także z powołaniem się na ustawę o ochronie danych osobowych organy gminy odmawiały udzielania informacji dotyczącej gospodarki finansowej. W odpowiedzi na pismo, w którym poproszono o opinię, jaki jest stosunek art. 61 ustawy o samorządzie terytorialnym do przepisów ustawy o ochronie danych osobowych Generalny Inspektor wskazał, że *ani uchwała budżetowa, ani sprawozdanie z jej wykonania nie zawierają danych osobowych*. Zatem ustawa o ochronie danych osobowych w omawianej sytuacji nie znajduje zastosowania i nie ma potrzeby rozważania wzajemnego stosunku tych przepisów.¹³ Na podstawie art. 61 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. 1996 r. Nr 13, poz. 74 z późn. zm.) wójt, burmistrz lub prezydent niezwłocznie ogłasza uchwałę budżetową i sprawozdanie z jej wykonania. Zarząd natomiast, jest zobowiązany do poinformowania mieszkańców gminy

10 GI-DP-679/99

11 GI-DP-634/99

12 Por. GI-DP-848/99; w sprawie tej podkreślono, że ustawa o ochronie danych osobowych nie znajduje zastosowania także dlatego, że nie zachodzi przetwarzanie w zbiorze. Trzeba również podkreślić, że zazwyczaj takie znakowanie przedmiotów będzie stosowane za zgodą osoby uprawnionej, której dotyczą dane.

13 Por. GI-DP-68/99.

o założeniach projektu, kierunkach polityki społecznej i gospodarczej oraz wykorzystywaniu środków budżetowych.

W pytaniach kierowanych do Generalnego Inspektora pojawiały się wątpliwości, czy *ochroną objęte są dane osób zmarłych*. Ustawa o ochronie danych osobowych posługuje się pojęciem osoby fizycznej nie określając go jednak. Zgodnie z art. 8 k.c. każdy człowiek od chwili urodzenia posiada zdolność prawną, czyli zdolność do bycia podmiotem praw i obowiązków. Zdolność ta wygasa w chwili śmierci, gdyż, co jest oczywiste na gruncie obowiązującego prawa, zmarły nie może być podmiotem żadnych praw ani obowiązków.¹⁴ Wynikają stąd ważne konsekwencje także dla konstrukcji ochrony danych osobowych, bowiem art. 2 ust. 1 ustawy o ochronie danych osobowych, określa prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane. W związku z tym na pytanie czy można, w świetle ustawy o ochronie danych osobowych publikować informacje o osobach, które zmarły, Generalny Inspektor odpowiadał, że ustawa ta znajduje zastosowanie wyłącznie do ochrony danych osób żyjących. Słuszność tego stanowiska potwierdza również sama konstrukcja ustawy. Bowiem przewidziano w niej szereg rozwiązań i instytucji, które z natury rzeczy mogą przysługiwać wyłącznie osobom żyjącym (np. prawo wglądu do danych, ich poprawiania czy prawo wniesienia sprzeciwu).¹⁵

Często poruszonym problemem jest kwestia *prawnej ochrony danych osób prowadzących działalność gospodarczą*. Niejednokrotnie informacje o osobie prawnej są tożsame z danymi określonej osoby fizycznej. Zgodnie z art. 2 ust. 1 ustawa o ochronie danych osobowych określa prawa osób fizycznych, których dane są lub mogą być przetwarzane w zbiorach danych. Również z brzmienia art. 6 ustawy wynika, że dane osobowe to dane, które dotyczą osoby fizycznej.

Podjęcie działalności gospodarczej przez osoby fizyczne i jednostki organizacyjne nie posiadające osobowości prawnej, wymaga zgłoszenia do ewidencji działalności gospodarczej. Ewidencja ta, zgodnie z art. 16 ust. 2 ustawy z dnia 23 grudnia 1988 r. o działalności gospodarczej (Dz. U. Nr 41, poz. 324 z późn. zm.) jest jawna, co służy ułatwieniom obrotu gospodarczego i zapewnieniu jego bezpieczeństwa, a także oznacza, że każdy może uzyskać wgląd w ewidencję. W ewidencji znajdują się takie informacje, jak imię i nazwisko osoby (nazwa) prowadzącej działalność gospodarczą i jej adres (siedziba). Wiele skarg dotyczyło udostępniania przez organy administracji samorządowej danych osób

14 Por. art. 8 ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. Nr 16, poz. 93 z późn. zm.).

15 Por. GI-DP-97/99; kwestia ta pojawia się szczególnie często przy realizacji ustawowych zadań urzędów stanu cywilnego.

prowadzących działalność gospodarczą osobom trzecim. Ewidencja działalności gospodarczej zawiera dane o przedsiębiorcach, a nie o osobach fizycznych.¹⁶ Nawet jeśli działalność gospodarcza podejmowana jest przez osobę fizyczną, to w obrocie gospodarczym osoba ta występuje jako przedsiębiorca, zgadzając się tym samym na utratę ochrony, jaką daje ustawa o ochronie danych osobowych osobom fizycznym w zakresie, w jakim dotyczy to jej działalności gospodarczej.¹⁷ Uwagi te odnoszą się nie tylko do danych zawartych w ewidencji działalności gospodarczej, ale także w rejestrach zezwoleń na sprzedaż alkoholu, rejestrach działalności polegającej na usuwaniu, wykorzystywaniu i unieszkodliwianiu odpadów komunalnych i innych, o ile zawierają wyłącznie dane dotyczące podmiotów prowadzących działalność gospodarczą.¹⁸

Do Generalnego Inspektora Ochrony Danych Osobowych wpłynęła skarga w sprawie udostępnienia przez urząd gminy informacji o zastrzeżeniu przez osobę uprawnioną jej danych osobowych. W odpowiedzi stwierdzono, że ustawa weszła w życie dnia 30 kwietnia 1998 r. i nie znajduje zastosowania do zdarzeń, które nastąpiły przed tą datą.¹⁹ W sprawie tej Generalny Inspektor podkreślił również, że przekazanie przez urząd gminy żądanych informacji nie dotyczyło danych osobowych, zatem nie podlegało ocenie legalności z punktu widzenia ustawy o ochronie danych osobowych.

II. Przetwarzanie danych osobowych w zbiorach

Możliwość zastosowania ustawy o ochronie danych osobowych zależy nie tylko od stwierdzenia, że określone informacje są danymi osobowymi, ale także od tego, czy zostały spełnione inne jeszcze warunki. Zgodnie z art. 2 ust. 1 ustawa o ochronie danych osobowych określa prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych. Zbiorem, zgodnie z art. 7 pkt 1 ustawy, jest każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony, czy też podzielony funkcjonalnie. Zbiór akt postępowania administracyjnego zawierając dane stron, ich adresy i inne informacje, spełnia te kryteria i wobec tego jest zbiorem danych w rozumieniu ustawy. Na organie

16 Por. GI-DP-596/99, GI-DP-668/99, GI-DP-1091/99, GI-DP-1289/99.

17 GI-DP-1540/99, GI-DP-1596/99

18 GI-DP-1091/99, GI-DP-1194/99, GI-DP-1289/99

19 GI-DP-616/99; fakt, że określone zdarzenie nastąpiło przed wejściem w życie ustawy nie oznacza, że ustawa w ogóle nie znajduje zastosowania do danych osobowych zebranych przed jej wejściem w życie. Nie podlega ocenie pod kątem zgodności z ustawą o ochronie danych osobowych przesłanka, na podstawie której dane są przetwarzane, a ponadto administrator zwolniony jest z niektórych obowiązków (np. informacyjnego).

administracji (gminie) ciążą zatem takie same obowiązki, jak na innych administratorach danych, w szczególności zaś obowiązek właściwego zabezpieczenia danych.²⁰

Przedmiotem odpowiedzi Generalnego Inspektora Ochrony Danych Osobowych była zgodność z ustawą o ochronie danych osobowych uchwały rady gminy, na podstawie której emeryci i renciści II i III grupy inwalidzkiej mają prawo do bezpłatnych przejazdów autobusami linii miejskich, jednakże pod warunkiem okazania dowodu osobistego i ostatniego odcinka emerytury lub renty. Bezpłatne przejazdy przysługiwały także innym osobom, na podstawie legitymacji wydanej przez Zakład Komunikacji Miejskiej, po okazaniu decyzji emerytalnej lub rentowej, dowodu osobistego i ostatniego odcinka emerytury lub renty. Również i w tej sprawie podkreślono, że ustawa o ochronie danych osobowych chroni prawa osób fizycznych, których dane są lub mogą być przetwarzane w zbiorze. Ponieważ udostępnienie żądanych dokumentów nie jest przetwarzaniem danych osobowych w zbiorze, ustawa w omawianej sytuacji nie znajduje zastosowania.²¹

III. Przekazywanie danych osobowych za granicę

Ustawodawca polski wzorem innych krajów wprowadził pewne 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. Niezależnie jednak od poziomu ochrony jaką zapewnia inne państwo, dane osobowe można przysyłać 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.²²

²⁰ Por. GI-DP-1233/99.

²¹ Por. GI-DP-145/99; zauważyć należy ponadto, że w tej sprawie nie mamy w ogóle do czynienia z przetwarzaniem danych przez administratora.

²² GI-DP-807/99

IV. Wyłączenia spod zastosowania ustawy

Należy także zwrócić uwagę na postanowienia art. 2 ust. 3 ustawy o ochronie danych osobowych, zgodnie z którym w odniesieniu do zbiorów danych przetwarzanych doraźnie, wyłącznie ze względów technicznych, szkoleniowych lub w związku z dydaktyką w szkołach wyższych, mają zastosowanie jedynie przepisy art. 36 i nast. ustawy o ochronie danych osobowych. W świetle przepisu art. 2 ust. 3 dane wykorzystane przez samorządowe instytucje kultury w celu zorganizowania konkursu i wyłonienia laureatów, niezwłocznie po wykorzystaniu powinny zostać usunięte lub zanonimizowane, tj. zredagowane tak, aby uniemożliwić określenie tożsamości osoby, której dane dotyczą.²³

B. Sprawy z zakresu administracji samorządowej

I. Definicja administratora danych

Art. 7 pkt 4 ustawy o ochronie danych osobowych definiuje administratora danych jako organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3 ust. 1 i 2, decydujące o celach i środkach przetwarzania danych osobowych. Kwestia ta w praktyce budzi wiele wątpliwości, o czym świadczy liczba kierowanych do Generalnego Inspektora pytań. Jest oczywiste, że dyspozycja tego przepisu jest na tyle pojemna, by odnosiła się także do organów administracji publicznej, w tym organów samorządu terytorialnego.

Z racji wykonywania przez gminy ustawowych zadań, w ich jednostkach organizacyjnych prowadzone są różnego rodzaju zbiory, z których wymienić można, np. rejestr kierowców, rejestr pojazdów, ewidencję gruntów, ewidencję urzędów stanu cywilnego, rejestr pozwoleń i decyzji budowlanych, ewidencję ludności, ewidencję przedpoborowych, ewidencję podatków i windykacji i inne. Zbiory te prowadzone są na podstawie różnych aktów prawnych i służą realizacji odmiennych celów. Ponieważ inna jest ich specyfika, zbiory te wymagają różnych procedur dostępu i konieczne jest stosowanie w odniesieniu do nich innych zabezpieczeń. Ponadto, zbiory znajdujące się w posiadaniu gminy są niejednokrotnie wykorzystywane przez poszczególne jej jednostki organizacyjne (np. urzędy stanu cywilnego, Straż Miejską, ośrodki pomocy społecznej).

W świetle wagi, jaką przywiązuje ustawodawca do pojęcia administratora danych, niezwykle istotne jest ustalenie, komu ten status przysługuje. Nie zawsze jest to zadanie

²³ Por. GI-DP-1069/99.

proste ponieważ, jak zaznaczono wyżej, o tym, czy mamy do czynienia z administratorem danych przesądza m.in. fakt, że jest on uprawniony do decydowania o celach i środkach przetwarzania danych. To, czy o celach przetwarzania danych decyduje gmina, czy jej jednostka organizacyjna, w konkretnym przypadku może nastroczać kłopoty. Podobnie, jeżeli o celach decyduje organ nadzorujący, a o środkach przetwarzania danych jednostka, w której posiadaniu zbiór się znajduje.

Wśród kierowanych do Generalnego Inspektora Ochrony Danych Osobowych pism, w tej grupie spraw najczęściej pojawiało się pytanie o to, *kto pełni funkcję administratora danych w zakresie prowadzonej przez gminy ewidencji ludności*. Generalny Inspektor wskazywał, że zgodnie z art. 46 ust. 1 ustawy z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych (Dz. U. Nr 32, poz. 174 z późn. zm.) ewidencję prowadzą organy gminy. Administratorem danych w zakresie ewidencji ludności jest wójt, burmistrz lub prezydent miasta. Minister Spraw Wewnętrznych i Administracji sprawuje zwierzchni nadzór nad wykonywaniem obowiązków określonych w ustawie, a wojewodowie sprawują nadzór nad działalnością organów gmin w zakresie realizacji obowiązków określonych w ustawie. Zdaniem Generalnego Inspektora sprawowanie tego nadzoru nie oznacza, że podmioty wykonujące go mogą być uznane za administratora danych.²⁴ Istotne jest natomiast, że obowiązek prowadzenia ewidencji ludności został na gminę nałożony przez przepisy o charakterze bezwzględnie obowiązującym.²⁵ Ponadto, w ślad za tym wnioskiem podkreślono, że samodzielne jednostki organizacyjne podległe bezpośrednio gminie i przetwarzające dane osobowe na podstawie innych, niż określających kompetencje gminy przepisów ustawowych, są odrębnymi administratorami danych w rozumieniu ustawy o ochronie danych osobowych.

Status administratora danych w przypadku prowadzenia zbiorów przez podmioty publiczne uzyskiwany jest *ex lege* z chwilą spełnienia ustawowo określonych przesłanek. W konsekwencji administrator danych nie może skutecznie przekazać swoich obowiązków jako administratora danych, w drodze aktu władczego innemu podległemu jednostkom organizacyjnym, których kompetencje, jako im przynależne z mocy ustawy, nie pozwalają na bycie administratorem danych (jednostki te nie posiadają kompetencji władczych w przedmiocie swojej działalności). Jeżeli gmina przetwarza dane osobowe w zakresie swojej działalności oraz decyduje o celach i środkach przetwarzania przedmiotowych danych, wówczas jest ich administratorem z mocy ustawy. Administrator danych nie może przekazać zadań przynależnych wyłącznie jemu, a nałożone na gminę, jako administratora danych

24 Por. GI-DP-446/99.

osobowych, obowiązki wynikające z ustawy nie mogą być przekazane w drodze upoważnienia innym jednostkom organizacyjnym lub osobom fizycznym.²⁶ Administrator danych to nie funkcja, ale raczej status związany z przetwarzaniem danych osobowych. Nie jest więc również prawnie skuteczne upoważnienie pracownika do pełnienia obowiązków administratora danych. Pracownik może być wyznaczony jedynie na administratora bezpieczeństwa informacji, zgodnie z § 3 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).²⁷ Administrator może także, w świetle art. 31 ustawy o ochronie danych osobowych, powierzyć przetwarzanie danych innemu podmiotowi w drodze umowy pisemnej. Jednak powierzenie to nie powoduje zmiany statusu administratora danych, ani wyłączenia jego odpowiedzialności za niezgodne z prawem przetwarzanie danych osobowych.²⁸

Na mocy art. 4 i 5 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. Nr 91, poz. 578 z późn. zm.) powiat może przekazywać zadania własne (na wniosek zainteresowanej gminy), oraz zawierać porozumienia w sprawie powierzenia prowadzenia zadań publicznych z jednostkami lokalnego samorządu terytorialnego, a także z województwem, na którego obszarze znajduje się terytorium powiatu. Jeżeli zatem, w drodze takiego porozumienia dojdzie do przekazania gminie zadań powiatu (np. związanych z rejestracją pojazdów i wydawaniem uprawnień do kierowania pojazdami) gminy stają się *ex lege* administratorem danych w rozumieniu art. 7 ust. 4 ustawy o ochronie danych osobowych, ponieważ to właśnie one decydują o celach i środkach przetwarzania danych zawartych w tych zbiorach.²⁹

Na pytanie, w jaki sposób na status administratora danych wpływa nadanie numeru NIP oraz numeru REGON, i czy w związku z tym administratorem danych jest starostwo powiatowe, starosta czy powiat, Generalny Inspektor odpowiedział, że brak numeru NIP oznacza tylko, że powiat nie podlega obowiązkowi ewidencyjnemu na podstawie ustawy z dnia 13 października 1995 r. o zasadach ewidencji i identyfikacji podatników i płatników (Dz. U. 142, poz. 702 z późn. zm.). Zwrócono także uwagę, że zgodnie z art. 2 ustawy o samorządzie powiatowym, powiat wykonuje określone ustawami zadania publiczne w

25 Por. GI-DP-473/99, GI-DP-500/99, GI-DP-1202/99.

26 Por. GI-DP-1351/99.

27 Por. GI-DP-580/99.

28 Por. GI-DP-594/99.

29 Por. GI-DP-987/99, por. także sprawę GI-DP-940/99.

imieniu własnym i na własną odpowiedzialność oraz ma osobowość prawną. Jest więc administratorem danych przetwarzanych w zakresie swoich kompetencji.³⁰

Generalny Inspektor odpowiadał również, że w odniesieniu do zbiorów aktów stanu cywilnego administratorem danych jest urząd stanu cywilnego. W odniesieniu do zbiorów danych osób korzystających z usług ośrodka pomocy społecznej, administratorem jest ten ośrodek. Biblioteka natomiast jest administratorem zbioru danych czytelników.³¹

Inna natomiast jest sytuacja Straży Miejskiej. Wykonuje ona swoje zadania na podstawie ustawy z dnia 29 sierpnia 1997 r. o Strażach Gminnych (Dz. U. Nr 123, poz. 779) i stosownie do przepisu art. 6 tej ustawy jest jednostką organizacyjną gminy. W szczególnie uzasadnionych przypadkach, rada gminy może postanowić o umiejscowieniu komendy Straży w strukturze urzędu gminy. Zdaniem Generalnego Inspektora, gdy Straż Miejska stanowi odrębną jednostkę organizacyjną, funkcję administratora danych pełni komenda Straży Miejskiej, jeżeli natomiast komenda umiejscowiona jest w strukturze urzędu, za administratora należy uznać gminę.³²

Generalny Inspektor uznał także, że jednostki komunalne będące, np. zakładami budżetowymi, wykonujące w imieniu gminy zadania, które służą zaspokojeniu potrzeb społeczności lokalnej są administratorami danych w rozumieniu ustawy.³³ Dotyczy to również szkół, przedszkoli oraz innych jednostek organizacyjnych resortu oświaty. Nie posiadają jednak statusu administratora zakłady obsługujące te jednostki.³⁴

II. Udostępnianie danych osobowych podmiotom uprawnionym do ich przetwarzania na mocy przepisów prawa

Do Generalnego Inspektora zwrócił się urząd miasta z prośbą o wyjaśnienie, czy w świetle art. 28 ust. 1 ustawy o ochronie danych osobowych uzasadnione jest występowanie do Centralnego Rejestru Skazanych z *pytaniem o karalność* kandydatów na ławników i członków kolegium ds. wykroczeń.

Art. 132 ustawy z dnia 20 czerwca 1985 r. Prawo o ustroju sądów powszechnych (Dz. U. 1994 r. Nr 7 poz. 25) stanowi, że ławnikiem może być osoba, która korzysta z pełni

30 Por. GI-DP-1110/99.

31 Por. GI-DP-1076/99.

32 Por. GI-DP-871/99; powyższy problem pojawił się w kontekście ustalenia, czy zbiór danych przetwarzanych przez Straż Miejską podlega zgłoszeniu do rejestracji Generalnemu Inspektorowi.

33 GI-DP-859/99, GI-DP-1248/99, GI-DP-1439/99

34 GI-DP-1218/99

praw cywilnych i obywatelskich. Natomiast zgodnie z art. 7 § 1 ustawy z dnia 20 maja 1971 r. o ustroju kolegiów ds. wykroczeń (Dz. U. Nr 12, poz. 118) na członka kolegium wybiera się osoby, które korzystają z pełni praw publicznych. Powstał zatem problem ustalenia, czy sformułowania „korzystanie z pełni praw cywilnych i obywatelskich” oraz „korzystanie z pełni praw publicznych” są tożsame z określeniem „osoba nie karana”. Korzystanie z pełni praw publicznych nie jest jednoznaczne z niekaralnością, ponieważ nie każde skazanie kończy się orzeczeniem środka karnego w postaci pozbawienia praw publicznych. Zdaniem Generalnego Inspektora przepisy te nie stanowią podstawy prawnej żądania przez urząd miasta informacji dotyczących karalności kandydatów na ławników i członków kolegiów ds. wykroczeń z Centralnego Rejestru Skazanych.³⁵

Na wniosek jednej z partii politycznych przedmiotem zainteresowania Generalnego Inspektora Ochrony Danych Osobowych była działalność Wydziału Finansowego Urzędu Miasta.³⁶ Zarzuty dotyczyły zbyt szerokiego, zdaniem wnoszącego skargę, *zakresu informacji żądanych od podatników* składających wniosek o zaniechanie poboru podatku od spadku i darowizny oraz przechowywania tych danych mimo, że stały się już zbędne do zrealizowania celu, dla którego zostały zebrane. Ustawa z dnia 29 sierpnia 1997 r. Ordynacja podatkowa (Dz. U. Nr 137, poz. 926 z późn. zm.) przewiduje przyznawanie ulg takich, jak np.: rozłożenie zapłaty podatku na raty czy zaniechanie poboru podatku. Taka możliwość istnieje również w odniesieniu do podatków w całości stanowiących dochody gmin, a realizowanych za pośrednictwem urzędów skarbowych.³⁷ Zgodnie z art. 122 i 187 § 1 ustawy Ordynacja podatkowa, organ podatkowy zobowiązany jest do przeprowadzenia postępowania wyjaśniającego w każdej sprawie. Wnioskodawca w takim postępowaniu powinien wykazać, że pobranie podatku zagraża egzystencji jego i jego rodziny. Orzecznictwo Naczelnego Sądu Administracyjnego wskazuje, że ustawodawca upoważnił organy podatkowe do orzekania o zaniechaniu poboru w ramach tzw. uznania administracyjnego, pozostawiając tym organom ocenę, czy w konkretnej sprawie okoliczności uzasadniają zaniechanie poboru i w jakiej wysokości.³⁸ Decyzja o zaniechaniu poboru podatku jest przy tym odstępstwem od zasady powszechności podatku i ma charakter wyjątkowy, musi być zatem starannie

35 GI-DP-530/99; informacja uzyskana z Centralnego Rejestru Skazanych obejmuje dane o tym, za jakie przestępstwo określona osoba została skazana, nie wskazuje natomiast, czy osoba ta korzysta z praw cywilnych i obywatelskich czy publicznych.

36 Por. GI-DP-672/99.

37 Por. art. 17 ust. 1 ustawy z dnia 26 listopada 1998 r. o dochodach samorządu terytorialnego w latach 1999-2000 (Dz. U. Nr 150, poz. 983).

38 Por. orzeczenie NSA w Krakowie z dnia 21 grudnia 1995 r., sygn. akt S.A./Kr 1884/95.

udokumentowana i uzasadniona w oparciu o konkretne ustalenia faktyczne.³⁹ Uwzględniając, że dochody z tytułu podatku od spadków i darowizn stanowią dochód gminy, właśnie gmina zobowiązana jest do ustalenia kryteriów stosowania ulg. Gmina posiada zatem uprawnienia do określania, np. wzoru oświadczenia (i zakresu zawartych w nim danych o sytuacji majątkowej podatnika), które staje się załącznikiem do wniosku o zaniechanie poboru podatku oraz dokumentem, na podstawie którego można ustalić sytuację majątkową wnioskodawcy, a wnioskodawca powołujący się na swoją szczególnie trudną sytuację materialną winien wskazać okoliczności potwierdzające ten fakt. W odniesieniu do zarzutu, że dane są przechowywane mimo, że nie istnieje już taka potrzeba, Generalny Inspektor wskazał na art. 70 § 1 ordynacji podatkowej, który stanowi, że zobowiązania podatkowe przedawniają się z upływem 5 lat. Z jego treści wynika, że przez okres 5 lat akta spraw podatkowych muszą być przechowywane przez organy podatkowe. Generalny Inspektor w omawianej sprawie nie dopatrywał się naruszenia ustawy o ochronie danych osobowych.

W ramach tej grupy spraw wyróżnić należy problematykę udostępniania danych osobowych administrowanych przez jednostki samorządu terytorialnego podmiotom uprawnionym do tego na mocy odrębnych przepisów. Pytania kierowane do Generalnego Inspektora Ochrony Danych Osobowych dotyczyły m.in. konieczności stosowania wniosku, o którym stanowi art. 29 przez sądy, prokuraturę, Policję i inne służby.⁴⁰

Zdaniem Generalnego Inspektora Ochrony Danych Osobowych organy administracji publicznej zobowiązane są do udzielenia żądanych danych funkcjonariuszom Policji, UOP, Straży Granicznej, Urzędu Celnego, Służby Celnej, a także sądom, prokuraturze i innym podmiotom uprawnionym do tego z mocy prawa. W tych przypadkach art. 29 ustawy o ochronie danych osobowych nie znajduje zastosowania, a organy te nie muszą występować o udostępnienie danych na wniosek, o którym mowa w art. 29. Zasady i tryb udzielania tym organom pomocy przez instytucje i organy administracji określają przepisy wykonawcze do ustaw regulujących działanie tych organów.

Zagadnienie udostępniania danych osobowych osobom trzecim szczególnie wyraźnie występuje w związku z działalnością urzędów stanu cywilnego. Ustawa o ochronie danych osobowych w art. 5 stanowi, że 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

39 Por. orzeczenie NSA w Szczecinie z dnia 5 grudnia 1995 r., sygn. S.A./Sz. 1101/95.

40 Z racji jednak obszerności i wagi tego problemu, omówiony on został szerzej na stronie 71 niniejszego Sprawozdania.

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 z późn. zm.). Krąg podmiotów uprawnionych do otrzymania skróconego odpisu aktu stanu cywilnego określony został w art. 83 ust. 1 i ust. 2 tej ustawy. Do Generalnego Inspektora zwracały się osoby, którym odmówiono wydania odpisów aktu stanu cywilnego, przy czym urzędy stanu cywilnego powoływały się na przepisy o ochronie danych osobowych.⁴¹ Odpisy aktów stanu cywilnego i zaświadczenia o dokonywanych w księgach stanu cywilnego wpisach lub o ich braku mogą być wydawane na wniosek sądu lub innego organu państwowego, a także osoby, której stan cywilny został w akcie stwierdzony, jej wstępnego, zstępnego, rodzeństwa, małżonka lub przedstawiciela ustawowego, jak również na wniosek osób, które wykażą w tym interes prawny. Wykazanie istnienia jednej z tych okoliczności powoduje, że urząd stanu cywilnego jest obowiązany udzielić żądanych informacji.⁴²

Art. 29 ustawy o ochronie danych osobowych stanowi, że dane osobowe udostępnia się na pisemny umotywowany wniosek, chyba że przepis szczególny stanowi inaczej. Z uwagi na to, że przepisy ustawy Prawo o aktach stanu cywilnego, regulując wyczerpująco kwestię dostępu do akt stanu cywilnego, stanowią *lex specialis* wobec przepisów ustawy o ochronie danych osobowych, nie stosuje się wniosku, o którym mowa w art. 29 ustawy o ochronie danych osobowych.⁴³

Art. 26 ust. 1 pkt 2 nakłada na administratora danych obowiązek zapewnienia, aby dane osobowe zbierane były dla oznaczonych, zgodnych z prawem celów i nie były poddawane przetwarzaniu niezgodnemu z tymi celami.

Do Biura Generalnego Inspektora wpłynęła skarga w sprawie wykorzystania informacji uzyskanych drogą służbową do celów prywatnych.⁴⁴ Ustalono, że funkcjonariusz Straży Miejskiej wystąpił do urzędu miejskiego o udostępnienie danych dotyczących miejsca zamieszkania osoby wnoszącej skargę, opatrując wniosek pieczęcią. Udostępniona informacja została przez funkcjonariusza wykorzystana, jako dowód w postępowaniu sądowym, którego był stroną. Zważywszy, że wystąpienie o udostępnienie danych w formie zastrzeżonej jedynie dla czynności służbowych, w celach niezwiązanych z ich wykonywaniem jest przekroczeniem przez funkcjonariusza uprawnień, Generalny Inspektor zwrócił się do komendanta Straży Miejskiej z żądaniem wszczęcia postępowania dyscyplinarnego przeciwko

41 GI-DP-265/99

42 Należy podkreślić, że takie działanie jest przejawem nadinterpretacji ustawy.

43 GI-DP-311/99

44 GI-DIS-392/99

funkcjonariuszowi. Jak wynika z udzielonej Generalnemu Inspektorowi odpowiedzi, w stosunku do osoby, która dopuściła się przekroczenia uprawnień, wyciągnięte zostały konsekwencje służbowe.

Problem stosowania wniosku określonego w art. 29 ustawy o ochronie danych osobowych przewija się nie tylko wśród spraw dotyczących problematyki przetwarzania danych osobowych przez organy samorządu terytorialnego. Generalny Inspektor podkreślał wielokrotnie, że art. 29 znajduje zastosowanie wyłącznie w sytuacji, gdy udostępnienie danych następuje w celu innym, niż włączenie do zbioru.⁴⁵ Włączenie to może przybrać różne formy; mogą to być działania polegające zarówno na włączeniu do zbioru jak i na jego utworzeniu.⁴⁶

Do Generalnego Inspektora, zwrócił się sołtys, któremu urząd gminy odmówił udostępnienia zestawu danych osobowych mieszkańców sołectwa, pomimo, że wystąpił on o udostępnienie tych danych na wniosku określonym w art. 29 ustawy o ochronie danych osobowych.⁴⁷ W odpowiedzi stwierdzono, że art. 29 nie znajduje zastosowania w przypadku, gdy udostępniany zestaw danych prowadzony jest w formie zbioru w rozumieniu ustawy o ochronie danych osobowych. W takiej sytuacji konieczne jest spełnienie którejkolwiek z przesłanek określonych w art. 23 ust. 1 ustawy o ochronie danych osobowych.

Udostępnienie danych osobom fizycznym i podmiotom, które nie są uprawnione do ich otrzymania na mocy przepisów prawa jest możliwe, gdy podmioty te w sposób wiarygodny uzasadnią potrzebę posiadania tych danych. Udostępnienie danych nie może przy tym naruszać praw i wolności osób, których te dane dotyczą. Do administratora danych należy ocena wniosku i podjęcie decyzji, czy udostępnienie danych będzie zgodne z ustawą o ochronie danych osobowych.⁴⁸ Organ przetwarzający dane decyduje o zasadności wniosku przy uwzględnieniu art. 30 ustawy o ochronie danych osobowych.⁴⁹

Generalny Inspektor podkreślał także, że spełnienie obowiązku informacyjnego wobec osoby, której dane dotyczą nie stanowi udostępnienia danych osobie trzeciej.⁵⁰

Generalny Inspektor Ochrony Danych Osobowych odpowiadał także, że udzielenie informacji adresowej nie wymaga informowania osoby, której dane dotyczą o fakcie udostępnienia danych.⁵¹

45 Por. GI-DP-1381/99.

46 Por. GI-DP-166/99.

47 GI-DP-1008/99

48 Por. GI-DP-1009/99, por. także GI-DP-166/99, GI-DP-1024/99.

49 Por. GI-DP-874/99.

50 Por. GI-DP-580/99.

III. Udostępnianie danych osobowych na potrzeby badań naukowych

Do Generalnego Inspektora Ochrony Danych Osobowych wpłynęło pismo dotyczące zgodności z prawem przeprowadzenia ogólnokrajowego badania „Sytuacja społeczno-zawodowa bezrobotnych kobiet oraz bariery i stymulatory ich aktywizacji zawodowej”.⁵² Badanie polegało na przeprowadzeniu wywiadu z losowo wybranymi bezrobotnymi kobietami. Wymagało to wykorzystania imiennych kartotek tych kobiet, oraz informacji o ich adresach. Generalny Inspektor zwrócił uwagę, że zgodnie z ustawą o ochronie danych osobowych, dane te mogą być pozyskiwane bezpośrednio od osób, których dane dotyczą, bądź od osób trzecich. Ustawa dopuszcza przetwarzanie danych osobowych w celu innym niż ten, dla którego zostały zebrane, jeżeli nie narusza to praw i wolności osoby, której dane dotyczą i jeśli następuje to w celu badań naukowych, w szczególności badań socjologicznych. Konieczne jednak jest rozróżnienie sytuacji, gdy badania prowadzone są jednorazowo, bądź mają charakter badań powtarzalnych. Zbiór danych przetwarzanych w ramach badania jednorazowego (jak w tym przypadku) traktować można, jako sporządzony doraźnie, wyłącznie dla celów technicznych, pod warunkiem, że po wykorzystaniu, dane ze zbioru zostaną niezwłocznie usunięte bądź poddane anonimizacji (art. 2 ust. 3 ustawy o ochronie danych osobowych). W odniesieniu do takiego typu zbiorów mają zastosowanie wyłącznie przepisy rozdziału 5 ustawy, których celem jest ochrona danych przed udostępnieniem osobom nieupoważnionym.

IV. Poszczególne rodzaje spraw z zakresu administracji samorządowej dotyczących przetwarzania danych

IV.1 Ewidencja i rejestracja pojazdów, wydawanie uprawnień do kierowania pojazdami

Wśród tej grupy spraw szczególnie dużo pytań dotyczyło kwestii prowadzenia ewidencji pojazdów. Z dniem 30 czerwca 1999 r. upłynął ustawowy termin prowadzenia przez wojewodów, wojewódzkich ewidencji pojazdów. Jednocześnie ustawa z dnia 20 czerwca 1997 r. Prawo o ruchu drogowym (Dz. U. Nr 98, poz. 602 z późn. zm.) nałożyła na Ministra Spraw Wewnętrznych i Administracji obowiązek utworzenia Centralnej Ewidencji Pojazdów i Kierowców. Ewidencja taka nie powstała jednak do chwili obecnej, pomimo upływu przeznaczonego na jej utworzenie terminu. W związku z tym, do Generalnego Inspektora zwracały się starostwa z pytaniami, czy dopuszczalne jest przekazywanie danych z

⁵¹ Por. GI-DP-754/99.

zakresu rejestracji pojazdów na żądanie urzędu wojewódzkiego na zasadach sprzed dnia 1 lipca 1999 r. Generalny Inspektor stwierdził, że art. 15 pkt 4 ustawy z dnia 5 czerwca 1998 r. o administracji rządowej w województwie (Dz. U. Nr 91, poz. 577) nie stanowi właściwej podstawy, która upoważniałaby starostę do udostępniania wojewodzie żądanych danych. Jest to sytuacja wymagająca wydania odpowiednich przepisów.⁵³ Należy jednak zauważyć, że spór dotyczy nie tyle ochrony danych osobowych, ile kompetencji określonych organów administracji publicznej, tymczasem uprawnienia Generalnego Inspektora Ochrony Danych Osobowych nie sięgają tak daleko, by mógł on rozstrzygać tego rodzaju kwestie kompetencyjne.

Częste były pytania o obowiązek uzyskiwania zgody na przetwarzanie danych osobowych osoby składającej wniosek o zarejestrowanie pojazdu, lub o wydanie uprawnień do kierowania pojazdem. Przetwarzanie danych osobowych jest dopuszczalne w razie spełnienia przynajmniej jednej z przesłanek określonych w art. 23 ust. 1 ustawy o ochronie danych osobowych. Jako przesłanki legalności przetwarzania danych art. 23 wymienia m. in. zgodę osoby, której dotyczą dane. Uzyskanie zgody nie jest jednak jedynym warunkiem dopuszczalności przetwarzania danych osobowych, jak to często bywa mylnie postrzegane. Przetwarzanie danych osobowych jest dopuszczalne również wtedy, gdy tak stanowią przepisy prawa. W odniesieniu do organów administracji właśnie ta przesłanka ma najistotniejsze znaczenie.

W myśl art. 73 ust. 1 ustawy z dnia 20 czerwca 1997 r. Prawo o ruchu drogowym (Dz. U. Nr 98, poz. 602 z późn. zm.), rejestracji pojazdu dokonuje starosta na wniosek właściciela. Ustawa określa także rodzaje dokumentów niezbędnych do zarejestrowania pojazdu. Rejestracji pojazdu zgodnie z art. 72 ustawy dokonuje się na podstawie dowodu własności pojazdu, karty pojazdu (jeżeli była wydana), wyciągu ze świadectwa homologacji albo odpisu decyzji zwalniającej pojazd z homologacji lub zaświadczenia o pozytywnym wyniku badania technicznego pojazdu (o ile są wymagane), dowodu rejestracyjnego (jeżeli pojazd był zarejestrowany), dowodu odprawy celnej przywózowej (jeśli pojazd został sprowadzony z zagranicy i jest rejestrowany po raz pierwszy). Ponieważ przetwarzanie danych osobowych właścicieli pojazdów znajduje podstawę prawną w przepisach wspomnianej wyżej ustawy, uzyskiwanie zgody na przetwarzanie danych jest zbędne.⁵⁴

52 GI-DP-517/99, GI-DP-532/99

53 Por. GI-DP-628/99, GI-DP- 635/99, GI-DP-665/99

54 GI-DP-1650/99

Podobne uwagi należy poczynić w stosunku do przetwarzania danych tzw. wrażliwych. Ustawa o ochronie danych osobowych w art. 27 ust. 2 enumeratywnie wymienia przypadki, kiedy przetwarzanie danych wrażliwych jest dopuszczalne. W myśl punktu 2 art. 27 ust. 2 ustawy o ochronie danych osobowych, przetwarzanie takich danych jest możliwe, gdy przepis szczególny innej ustawy zezwala na przetwarzanie danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony. W związku z tym, przetwarzanie danych osobowych zawartych w orzeczeniu lekarskim o braku przeciwwskazań zdrowotnych do kierowania pojazdami, stanowiącym podstawę do uzyskania prawa jazdy zgodnie z art. 90 ustawy Prawo o ruchu drogowym, nie wymaga uzyskania zgody osoby, której dane dotyczą.⁵⁵

IV.2 Przetwarzanie danych osobowych w ramach postępowania administracyjnego

Często budziła wątpliwości kwestia ochrony danych osobowych w ramach toczącego się postępowania administracyjnego. Problem ten wiąże się ściśle z zasadą informowania stron, zasadą czynnego udziału strony w postępowaniu administracyjnym i przepisami dotyczącymi udostępniania akt postępowania. Pytano m.in., czy stanowi naruszenie ustawy o ochronie danych osobowych udostępnianie listy osób podpisujących skargę przeciwko sprzedaży napojów alkoholowych,⁵⁶ udostępnienie pełnomocnikowi strony listy z nazwiskami osób sprzeciwiających się budowie spopieliarni zwłok,⁵⁷ przesyłanie decyzji stronom postępowania.⁵⁸

W odpowiedzi podkreślano, że w myśl art. 9 k.p.a. organy administracji publicznej są obowiązane do należytego i wyczerpującego informowania stron o okolicznościach faktycznych i prawnych, które mogą mieć wpływ na ustalenie ich praw i obowiązków będących przedmiotem postępowania administracyjnego. Jednocześnie na podstawie art. 10 § 1 k.p.a. organy te obowiązane są zapewnić stronom czynny udział w każdym stadium postępowania, a przed wydaniem decyzji umożliwić im wypowiedzenie się, co do zebranych dowodów i materiałów oraz zgłoszonych żądań. Niezbędnym składnikiem decyzji jest m.in. oznaczenie strony lub stron,⁵⁹ a decyzję, w myśl art. 109 § 1 k.p.a. doręcza się stronom na piśmie. Procedura udostępniania stronom postępowania administracyjnego akt sprawy została uregulowana w art. 73 k.p.a. Organ administracji jest zobowiązany umożliwić stronie przeglądanie akt sprawy oraz sporządzanie z nich notatek i odpisów. Przepis ten rozwija

55 GI-DP-1651/99

56 GI-DP-399/99

57 GI-DP-453/99

58 GI-DP-501/99, GI-DP-193/99; niejednokrotnie w skargach pisze się o udostępnieniu danych osobom „tylko pośrednio zainteresowanym rozstrzygnięciem”.

zatem zasadę czynnego udziału strony wynikającą z art. 10 k.p.a. Generalny Inspektor przypomniał także orzeczenie Naczelnego Sądu Administracyjnego (wyrok z dnia 8 kwietnia 1998 r. sygnatura I S.A./Gd 1657/97), zgodnie z którym 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.⁶⁰

W opisywanych wyżej sprawach przetwarzanie polegające na udostępnianiu danych zawartych w decyzjach oraz aktach postępowania, pozostaje w zgodzie z przepisami ustawy o ochronie danych osobowych, ponieważ odbywa się na podstawie przepisu prawa (tj. art. 23 ust. 1 pkt 2 ustawy). Jednocześnie zwrócono uwagę, że z przepisów kodeksu postępowania administracyjnego nie wynika konieczność zamieszczania w decyzji imion i nazwisk oraz adresów osób otrzymujących decyzję do wiadomości.⁶¹

Do Generalnego Inspektora skierowano skargę na niezgodne z prawem przekazanie danych osobowych wraz z aktami dwóch innych spraw do załatwienia innemu organowi wg kompetencji. O fakcie tym poinformowano jednym pismem wszystkie strony udostępniając w ten sposób ich dane osobowe. Generalny Inspektor wszczął czynności wyjaśniające, na podstawie których ustalono, że udostępnienie tych danych było skutkiem pomyłki, za którą osoby, których dotyczyły dane zostały przeproszone.⁶²

Art. 107 § 1 kodeksu postępowania administracyjnego określa niezbędne składniki, które musi zawierać każda decyzja administracyjna. W decyzji musi znaleźć się m.in. oznaczenie strony lub stron. Stronami postępowania administracyjnego nie mogą być bliżej nieokreślone podmioty (np. wszyscy mieszkańcy danej wsi), lecz osoby ściśle wskazane z imienia i nazwiska. Tym samym, skoro określenie stron jest wymagane przez przepisy prawa, zamieszczanie na decyzjach wydawanych przez urząd gminy danych osobowych strony lub, jak to ma miejsce w przypadku decyzji o zabudowie, stron jest zgodne z prawem.⁶³

IV.3 Przetwarzanie danych osobowych w placówkach oświatowo-wychowawczych

Generalny Inspektor podejmował także sprawy dotyczące ochrony danych osobowych w szkołach. Do Biura GIODO napływały pisma, w których pytano, czy zgodne z ustawą o ochronie danych osobowych jest umieszczanie w dziennikach lekcyjnych danych osobowych rodziców. Podstawę prawną dla przetwarzania takich danych stanowi § 4

59 Zob. przypis nr 33.

60 GI-DP-453/99

61 GI-DP-193/99, GI-DP-405/99, GI-DP-313/99, GI-DP-453/99

62 Por. GI-DIS-25/99.

63 GI-DP-1309/99

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). Przepis ten stanowi, że szkoły prowadzą księgi uczniów i szczegółowo określa, jakie dane wpisuje się w takich księgach. Umieszczanie w dziennikach lekcyjnych imienia, nazwiska oraz daty, miejsca urodzenia i adresu zamieszkania ucznia, imion i nazwisk rodziców lub opiekunów prawnych i adresów ich zamieszkania nie narusza przepisów ustawy o ochronie danych osobowych.⁶⁴

W związku ze skargą dotyczącą udostępnienia danych osobowych dzieci uczęszczających do przedszkola pracownikowi urzędu miasta i gminy, Generalny Inspektor Ochrony Danych Osobowych zwrócił się do dyrektora tego przedszkola o złożenie niezbędnych wyjaśnień.⁶⁵ Zgodnie z art. 90 ust. 1 ustawy z dnia 7 września 1991 r. o systemie oświaty (Dz. U. 1996 r. Nr 67, poz. 329 z późn. zm.) niepubliczne przedszkola uzyskują dotacje z budżetu gminy. Natomiast § 7 ust. 2 rozporządzenia Ministra Edukacji Narodowej z dnia 23 października 1992 r. w sprawie szczegółowych zasad ustalania wysokości i udzielania dotacji niepublicznym szkołom oraz placówkom oświatowo-wychowawczym i resocjalizacyjnym (Dz. U. Nr 81, poz. 419) stanowi, że organowi dotującemu przysługuje prawo kontroli wykorzystywania dotacji. Z uzyskanych od burmistrza miasta i gminy wyjaśnień wynikało, że dane osobowe dzieci uczęszczających do przedszkola zostały pozyskane przez upoważnionego pracownika urzędu miasta i gminy, w celu stwierdzenia zgodności ze stanem faktycznym okoliczności związanych z udzielaniem dotacji przeznaczonych dla tej placówki. Kwestia udostępniania danych osobowych dzieci uczęszczających do przedszkola podejmowana była przez Generalnego Inspektora Ochrony Danych Osobowych również na gruncie odmiennego stanu faktycznego. Sprawa dotyczyła nieudostępnienia zarządowi miasta dokładnych adresów rodziców dzieci uczęszczających do przedszkola, a także nieudostępnienia osobie kontrolującej działalność przedszkola informacji o stanie zdrowia dzieci zawartych w orzeczeniach Poradni Psychologiczno-Pedagogicznej.⁶⁶ Generalny Inspektor zauważył, że ustawa o ochronie danych osobowych ustanawia zakaz przetwarzania danych tzw. wrażliwych, do których zalicza się m.in. dane o stanie zdrowia. Udostępnienie takich danych jest możliwe w wyjątkowych przypadkach, które wyczerpująco wymienia art. 27 ust. 2 ustawy o ochronie danych osobowych. Zgodnie z art. 27 ust. 2 pkt 2

64 GI-DP-1550/99

65 Por. GI-DP-402/99.

66 GI-DP-418/99

przetwarzanie takich danych jest możliwe m.in., jeżeli przepis szczególny innej ustawy zezwala na przetwarzanie danych bez zgody osoby, której dane dotyczą i stwarza pełne gwarancje ich ochrony. Podstawą żądania zarządu miasta i wydziału oświaty urzędu miejskiego nie może być art. 18 a ustawy z dnia 8 marca 1990 r. o samorządzie gminnym, który stanowi, że rada gminy kontroluje działalność zarządu i gminnych jednostek organizacyjnych i w tym celu powołuje komisję rewizyjną. Prawo kontroli przedszkola, jako gminnej jednostki organizacyjnej przysługuje działającej w imieniu rady komisji rewizyjnej, a nie wydziałowi oświaty urzędu miasta. Wydział ten, jako wewnętrzny organ urzędu miejskiego podlegający zarządowi może kontrolować jednostki gminy jedynie na podstawie art. 33 ust. 5 ustawy samorządowej. Przepis ten jednakże upoważnia wyłącznie do wykonywania zwierzchnictwa służbowego, w żadnym wypadku kontrola dokonywana na tej podstawie nie może polegać na przejmowaniu kompetencji kierowników gminnych jednostek organizacyjnych, w tym dyrektora przedszkola. Zdaniem Generalnego Inspektora nie ma żadnych normatywnych podstaw do udostępniania danych osobowych konkretnych osób zarządowi miasta.

IV.4 Sprawy lokalowe

Art. 5 ust. 3 ustawy z dnia 2 lipca 1994 r. o najmie lokali i dodatkach mieszkaniowych (Dz. U. Nr 120, poz. 787 z późn. zm.) nakłada na gminy obowiązek zapewnienia społecznej kontroli zasad gospodarowania zasobem mieszkaniowym. Gminy realizują ten postulat podając do publicznej wiadomości dane osób, z którymi w pierwszej kolejności mają zostać zawarte umowy najmu.⁶⁷ Zdaniem Generalnego Inspektora Ochrony Danych Osobowych nieuzasadnione jest ograniczanie pojęcia „społeczna kontrola” wyłącznie do kontroli sprawowanej przez organizacje społeczne, stowarzyszenia i inne podobne podmioty. Sformułowanie to oznacza kontrolę sprawowaną przez wszystkie podmioty, w szczególności przez mieszkańców gminy tworzących z mocy prawa samorządową wspólnotę gminną. Im właśnie przede wszystkim przysługuje prawo kontroli działalności władz gminnych.⁶⁸

IV.5 Przetwarzanie danych osobowych przez Straż Miejską

⁶⁷ Na przykład wywieszając w urzędach gmin listy z danymi osobowymi osób, z którymi mają zostać zawarte umowy.

⁶⁸ GI-DP-33/99, GI-DP-91/99, GI-DP-189/99, GI-DP-343/99

W związku z artykułami prasowymi oraz napływającymi skargami Generalny Inspektor badał legalność przetwarzania danych przez Straż Miejską.⁶⁹ Sprawy dotyczyły niezarejestrowania zbioru danych posiadanych przez Straż i przetwarzania danych osobowych bez odpowiedniej podstawy prawnej.

Zadania Straży Miejskiej określa ustawa z dnia 29 sierpnia 1997 r. o Strażach Gminnych (Dz. U. Nr 123, poz. 779). W myśl art. 10 ust. 1 ustawy, Straż wykonuje zadania w zakresie ochrony porządku publicznego wynikające z ustaw i aktów prawa miejscowego. Wykonując zadania, o których mowa w art. 10 ustawy, strażnik ma prawo m.in.: legitymowania osób w celu ustalenia ich tożsamości, ujęcia osób stwarzających w sposób oczywisty bezpośrednie zagrożenie dla życia i zdrowia ludzkiego, a także dla mienia i niezwłocznego doprowadzenia tych osób do najbliższej jednostki Policji. Straż ma prawo nakładania grzywien w postępowaniu mandatowym za wykroczenia w trybie przewidzianym przepisami o postępowaniu w sprawach o wykroczenia, dokonywania czynności sprawdzających, kierowania wniosków o ukaranie do kolegium do spraw wykroczeń i oskarżania przed takim kolegium, oraz wnoszenia środków odwoławczych w trybie przewidzianym przepisami o postępowaniu w sprawach o wykroczenia (art. 12 ust. 1 ustawy). Także rozporządzenie Rady Ministrów z dnia 16 czerwca 1998 r. w sprawie zakresu i sposobu wykonywania przez strażników gminnych niektórych czynności (Dz. U. Nr 84, poz. 536) w § 5 stanowi, że strażnik jest zobowiązany do udokumentowania w notatniku służbowym danych dotyczących osoby legitymowanej, rodzaju dokumentu lub oświadczenia, które stanowiły podstawę do ustalenia tożsamości. Art. 28 ust. 1 ustawy o ochronie danych osobowych stanowi, że 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. W ocenie Generalnego Inspektora Straż Miejska przetwarzała kwestionowane dane zgodnie z dyspozycją art. 28 ust. 1 ustawy o ochronie danych osobowych.

Generalny Inspektor odpowiadał na pytanie, czy zgodnie z ustawą o ochronie danych osobowych Straż Miejska, będąca wydziałem urzędu miejskiego, może posiadać dostęp do danych osobowych zawartych w zbiorach danych innych wydziałów tego urzędu.⁷⁰ W odpowiedzi stwierdzono, że udostępnianie w celu weryfikacji jest formą przetwarzania danych. O udostępnieniu danych można jednak mówić dopiero, gdy dostęp do danych uzyskuje odrębny wobec administratora danych podmiot. W sytuacji, gdy Straż Miejska nie

69 por. sprawy GI-DP-349/99, GI-DP-882/99 oraz GI-DP-905/99.

jest odrębnym od administratora danych podmiotem lecz „wydziałem urzędu miejskiego”, mamy do czynienia z przetwarzaniem danych przez tego samego administratora danych.

IV.6 Ujawnianie informacji o radnych i o pracownikach samorządowych

Do Generalnego Inspektora zwracano się z pytaniami dotyczącymi prawa odmowy udzielenia dziennikarzom informacji o wysokości wynagrodzenia za pracę członków zarządu gminy. Zdaniem pytających, dane te należą do sfery prywatności człowieka, a ich przetwarzania (udostępniania) nie można uzasadnić realizowaniem zadań dla dobra publicznego. Generalny Inspektor przypomniał orzeczenie Naczelnego Sądu Administracyjnego, w którym stwierdzono, że dane płacowe burmistrza, sekretarza i skarbnika gminy nie stanowią tajemnicy państwowej, służbowej i nie leżą w sferze życia prywatnego.⁷¹ Informacje o wynagrodzeniu tych osób związane są z ich działalnością publiczną i muszą być jawne dla społeczności lokalnej.⁷² Zdaniem Generalnego Inspektora nie można odmówić takich informacji powołując się na ustawę o ochronie danych osobowych.⁷³

Kwestia udostępnienia informacji o radnych rady miasta wnioskującym o to mieszkańcom, wiąże się ściśle z konstytucyjnym prawem do informacji o działalności organów władzy publicznej. Ponadto, zgodnie z art. 23 ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. 1996 r. Nr 13, poz. 74 z późn. zm.), radny jest zobowiązany do utrzymywania stałej więzi z mieszkańcami i przyjmowania postulatów od wyborców. Jest oczywiste, że lista radnych jest dostępna dla wszystkich wyborców. Jedynie kwestią techniczną jest, w jaki sposób radni, których nazwiska są znane wyborcom, wywiązują się z obowiązku utrzymywania stałego kontaktu z nimi. Z punktu widzenia ustawy o ochronie danych osobowych brak jest przeszkód do udostępnienia danych osobowych radnych, którzy powinni zrobić to w taki sposób, aby wywiązać się z obowiązków nałożonych na nich przez ustawę.⁷⁴

Wątpliwości dotyczyły także zgodności z prawem umieszczania w Kalendarzu Samorządowym danych personalnych marszałków i wicemarszałków sejmików

70 GI-DP-515/99

71 Orzeczenie NSA sygn. akt I S.A. 1254/92 z 8 lutego 1993 r.

72 GI-DP-910/99

73 GI-DP-1644/99

74 GI-DP-468/99

wojewódzkich i sejmiku krajowego, przewodniczących rad gmin i rad powiatowych oraz wójtów, a także osób kierujących organizacjami samorządowymi.⁷⁵ W odpowiedzi Generalny Inspektor Ochrony Danych Osobowych poinformował, że skoro art. 61 Konstytucji ustanawia zasadę jawności życia publicznego, dając obywatelowi prawo do uzyskiwania informacji dotyczących działalności organów władzy publicznej oraz osób pełniących funkcje publiczne, to stanowi on zarazem przesłankę dopuszczalności przetwarzania danych osobowych, o której mowa jest w art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych. Generalny Inspektor dodał także, że dane tych osób są powszechnie dostępne, co stanowi także przesłankę umożliwiającą ich przetwarzanie. Umieszczanie zatem takich informacji o osobach pełniących funkcje publiczne nie stoi w sprzeczności z ustawą o ochronie danych osobowych.

Z podobnym pytaniem spotkał się Generalny Inspektor w jednym z pism, w którym pytano, czy nie narusza ustawy udostępnienie posłowi danych osobowych osób zajmujących kierownicze stanowiska w urzędzie miasta oraz wszystkich osób reprezentujących gminę w spółkach prawa handlowego. Generalny Inspektor Ochrony Danych Osobowych podkreślił, że dopuszczalność udostępnienia takich danych wynika w tej sytuacji nie tylko z zasady jawności życia publicznego. Podstawę udzielenia takich informacji stanowi także przepis szczególny. Zgodnie z art. 19 ust. 1 ustawy z dnia 9 maja 1966 r. o wykonywaniu mandatu posła i senatora (Dz. U. Nr 73, poz. 350 z późn. zm.), poseł ma prawo do uzyskiwania informacji i materiałów oraz wglądu w materiały dotyczące działalności organów samorządu terytorialnego oraz spółek komunalnych. Skoro zatem przepis szczególny zezwala na określone przetwarzanie danych osobowych to udzielenie żądanych informacji nie narusza ustawy o ochronie danych osobowych.

Znaczna liczba pytań i skarg dotyczyła udostępniania organom kontrolującym (np. komisji rewizyjnej) danych o wynagrodzeniach pracowników samorządowych, korzystania przez nich ze zwolnień lekarskich, oraz innych informacji znajdujących się w aktach osobowych.⁷⁶ Art. 16 ust. 1 ustawy z dnia 5 czerwca 1999 r. o samorządzie powiatowym (Dz. U. Nr 91, poz. 578) stanowi, że rada powiatu może kontrolować działalność zarządu oraz powiatowych jednostek organizacyjnych i w tym celu powołuje się komisję rewizyjną. Jednakże przepis ten upoważnia radę powiatu do kontroli jedynie w zakresie kompetencji nadanych jej przez przepisy prawa. Zdaniem Generalnego Inspektora niezależność zarządu

⁷⁵ GI-DP-407/99

⁷⁶ GI-DP-295/99, GI-DP-271/99, GI-DP-319/99, GI-DP-323/99, GI-DP-333/99, GI-DP-439/99, GI-DP-499/99, GI-DP-504/99, GI-DP-531/99, GI-DP-731/99, GI-DP-735/99, GI-DP-781/99

przejawia się m.in. poprzez prowadzenie własnej polityki kadrowej i płacowej. Potwierdzają ją także przepisy prawa pracy - pracodawcą jest bowiem nie rada powiatu, lecz urząd powiatowy ze starostą, jako jego kierownikiem. W ocenie Generalnego Inspektora przekazanie takich informacji komisji rewizyjnej stanowiłoby udostępnienie danych osobom nieuprawnionym do ich otrzymania, zwłaszcza że w tej sytuacji mogłoby dojść do ujawnienia danych tzw. wrażliwych. Uprawnienia kontrolne rady powiatu dotyczyć mogą jedynie osób wybieranych bezpośrednio przez radę. Zgodnie z art. 2 ustawy z dnia 22 marca 1990 r. o pracownikach samorządowych (Dz. U. Nr 21, poz. 124 z późn. zm.) oraz art. 27 ustawy o samorządzie powiatowym, starosta, wicestarosta i członkowie zarządu są zatrudniani na podstawie wyboru, jeżeli statut powiatu tak stanowi. W tym zakresie rada może żądać informacji, o które wystąpiła do zarządu. Z uwagi na to, że określone dane osób pełniących funkcje publiczne (np. wysokość wynagrodzenia starosty) są jawne, istnieje obowiązek ich udostępnienia nie tylko radzie powiatu, ale też każdemu mieszkańcowi wspólnoty samorządowej.⁷⁷

IV.7 Ujawnienie danych osób biorących udział w komisyjnym otwarciu mieszkania

Komitet Helsiński w Polsce zwrócił się do Generalnego Inspektora Ochrony Danych Osobowych z prośbą o zbadanie sprawy nieujawnienia danych osób biorących udział w komisyjnym otwarciu mieszkania. Do burmistrza wystąpiła osoba, której mieszkanie zostało w ten sposób otwarte z prośbą o udostępnienie danych osobowych osób, które brały udział w tej czynności. Odmowa udzielenia takich informacji została uzasadniona potrzebą ochrony danych osobowych. Generalny Inspektor Ochrony Danych Osobowych zwrócił uwagę, że zgodnie z ustawą o ochronie danych osobowych każdy zainteresowany może mieć wgląd do danych o innych osobach, które znajdują się w zbiorach instytucji publicznych. Wyjątkiem od tej zasady mogą być informacje objęte tajemnicą (państwową lub służbową). Podkreślono, że zgodnie z przepisami ustawy o samorządzie gminnym o ustroju gminy stanowi jej statut. Statut może regulować kwestie związane z powoływaniem wszelkiego rodzaju komisji o charakterze zarówno doraźnym jaki i stałym. W statucie gminy nie można jednak powoływać innych organów, niż przewidziane w ustawie o samorządzie gminnym i określać ich zadań i uprawnień kosztem kompetencji organów ustawodawczych (wyrok NSA III S.A. 1179/95 Wokanda 1996/29). Zdaniem Generalnego Inspektora jawność osób biorących udział w powoływanych komisjach wynika z ogólnej zasady jawności życia publicznego (art. 61

⁷⁷ Por. GI-DP-187/99.

Konstytucji RP) i nie może doznawać ograniczeń w drodze indywidualnych decyzji podejmowanych, np. przez burmistrza. Ograniczenie jawności życia publicznego, jako zasady, może wynikać jedynie z przepisów prawa, a każdą odmowę udostępnienia żądanych informacji (nie tylko danych osobowych) organ administracji publicznej powinien uzasadnić konkretnym przepisem prawa.⁷⁸

IV.8 Oprawa ksiąg urzędu stanu cywilnego

Wątpliwości budziła kwestia, czy oprawa ksiąg urzędu stanu cywilnego przez zakład introligatorski nie narusza ustawy o ochronie danych osobowych.⁷⁹ W odpowiedzi stwierdzono, że w rozumieniu ustawy o ochronie danych osobowych przetwarzaniem danych jest wykonywanie jakichkolwiek operacji na danych osobowych takich, jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie. Nie jest jednak przetwarzaniem danych osobowych dokonywanie czynności czysto technicznych, takich jak, np. poddanie oprawie zbioru danych lub jego części.

IV.9 Przetwarzanie danych w ewidencjach

Generalny Inspektor otrzymał pismo z pytaniem, czy ustawa o ochronie danych osobowych daje podstawę dla odmowy udzielenia przez wydział geodezji urzędu gminy informacji o gruntach i budynkach zawartych w operacie ewidencyjnym.⁸⁰ W odpowiedzi Generalny Inspektor poinformował, że zgodnie z uregulowaniami ustawy z dnia 17 maja 1989 r. Prawo geodezyjne i kartograficzne (Dz. U. Nr 30, poz. 163 z późn. zm.), a w szczególności art. 24 tej ustawy, dane zawarte w operacie stanowią zbiór danych w rozumieniu ustawy o ochronie danych osobowych. Zgodnie z treścią art. 24 ustawy Prawo geodezyjne i kartograficzne, tylko informacje o gruntach i budynkach zawarte w operacie ewidencyjnym są jawne. Ani ustawa Prawo geodezyjne i kartograficzne, ani przepisy wykonawcze do niej, nie dają podstaw do przyjęcia, że również inne informacje zawarte w operacie są jawne. W konsekwencji podmiot, który chce uzyskać dane inne, niż odnoszące się do gruntów i budynków, a będące danymi osobowymi w rozumieniu art. 6 ustawy o ochronie danych osobowych w celu innym, niż włączenie do zbioru musi legitymować się jedną z przesłanek określonych w art. 29 ustawy o ochronie danych osobowych.

⁷⁸ Por. GI-DP-938/99.

⁷⁹ Por. GI-DP-193/99; w sprawie tej Generalny Inspektor uznał również, że wykaz numerów telefonicznych dotyczących określonych osób zatrudnionych w instytucjach państwowych lub samorządowych należy uznać za dane powszechnie dostępne.

Do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło pismo, w którym pytano, czy w przypadku udostępniania danych zawartych w ewidencji gruntów osobie, której dane dotyczą należy stosować wniosek wymieniony w art. 29 ustawy o ochronie danych osobowych.⁸¹ Generalny Inspektor stwierdził, że w przypadku, gdy wypis z ewidencji gruntów zawiera jedynie dane osoby, która wystąpiła z wnioskiem, nie następuje udostępnienie danych osobowych osobom trzecim. Zatem stosowanie wniosku z art. 29 ustawy o ochronie danych osobowych jest zbędne.

Szczególnie wiele pytań dotyczyło dopuszczalności udostępniania danych podmiotów gospodarczych z ewidencji działalności gospodarczej. Generalny Inspektor podkreślał wielokrotnie, że ewidencja zawiera nie tyle dane osób fizycznych, ile dane przedsiębiorców i wobec tego ustawa o ochronie danych osobowych nie znajduje zastosowania. Jednocześnie wskazywano, że zgodnie z art. 16 ust. 2 ustawy z dnia 23 grudnia 1988 r. o działalności gospodarczej, ewidencja ta jest jawna. Wgląd do rejestru może mieć każdy i to bez uzasadniania swego żądania. Można dokonywać odpisów i notatek z rejestru, a jedynym ograniczeniem może być określenie szczegółowych zasad dostępu do rejestru w postaci wskazania miejsca i czasu, w jakim można żądać wglądu w jego treść.⁸²

Generalnemu Inspektorowi Ochrony Danych Osobowych została przekazana przez samorządowe kolegium odwoławcze sprawa odwołania od decyzji wójta odmawiającej umożliwienia wglądu do danych osobowych zawartych w ewidencji działalności gospodarczej.⁸³ Wnioskodawca żądał udostępnienia danych z prowadzonej przez wójta ewidencji dla celów wszczętego postępowania sądowego. Uzasadniając odmowę stwierdzono, że udostępnienie innych informacji aniżeli potwierdzenie, że dana firma prowadzi określony rodzaj działalności, stanowiłoby naruszenie dóbr osobistych osoby, której dane figurują w ewidencji. Odwołanie od decyzji (sic!) zostało wniesione do samorządowego kolegium odwoławczego, które uznało się za niewłaściwe i przekazało sprawę do rozstrzygnięcia Generalnemu Inspektorowi Ochrony Danych Osobowych. Generalny Inspektor uznał, że ustawa o ochronie danych osobowych nie znajduje zastosowania do danych zawartych w ewidencji działalności gospodarczej, a powoływanie się na fakt niespełnienia przesłanek określonych w art. 29 ustawy o ochronie danych osobowych oraz żądanie wniosku przewidzianego w tym przepisie nie ma podstawy prawnej. Gmina powinna udzielić

80 GI-DP-216/99

81 GI-DP-1178/99

82 Por. np. GI-DP-57/99, por. także GI-DP-1039/99.

83 GI-DP-1675/99, por. także GI-DP-1401/99.

żądanych informacji znajdujących się w ewidencji. Generalny Inspektor zwrócił także uwagę, że zgodnie z art. 219 k.p.a. odmowa wydania zaświadczenia następuje w drodze postanowienia, na które służy zażalenie.⁸⁴ Organem wyższej instancji, do którego kierowane są środki zaskarżenia od decyzji i postanowień organów gminy wydawanych w ramach realizacji jej zadań, jest Samorządowe Kolegium Odwoławcze, chyba że przepis szczególnie stanowi inaczej. Z przepisów prawa nie wynika, że Generalny Inspektor Ochrony Danych Osobowych jest obowiązany lub uprawniony do rozpatrywania zażaleń na wydane w toku instancji postanowienia w sprawie odmowy udostępnienia danych osobowych. Do zadań Generalnego Inspektora, określonych w art. 12 ustawy o ochronie danych osobowych, należy m.in. kontrola zgodności przetwarzania danych z przepisami o ochronie danych osobowych, wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych, prowadzenie rejestru zbiorów danych, itd. Również treść art. 18 ust. 1 pkt 2 ustawy o ochronie danych osobowych wskazuje, że Generalny Inspektor posiada kompetencje do wydania decyzji w przedmiocie udostępnienia danych osobowych wyłącznie w odniesieniu do konkretnej sytuacji, po przeprowadzeniu postępowania administracyjnego, w razie stwierdzenia naruszenia przepisów o ochronie danych osobowych. Zgodnie bowiem z treścią tego przepisu, w razie stwierdzenia niezgodnego z prawem przetwarzania danych osobowych, Generalny Inspektor Ochrony Danych Osobowych z urzędu lub na wniosek osoby zainteresowanej nakazuje administratorowi danych, w drodze decyzji administracyjnej, przywrócenie stanu zgodnego z prawem, a w szczególności uzupełnienie, uaktualnienie, sprostowanie, udostępnienie lub nieudostępnienie danych osobowych. Generalny Inspektor nie jest jednak organem odwoławczym w sprawie dotyczącej odmowy udostępnienia danych osobowych w sytuacji, gdy administratorem danych jest podmiot, którego decyzje lub postanowienia zaskarżane są w trybie instancyjnym.⁸⁵ Dopiero, gdy administratorem danych, który odmówił udostępnienia danych, jest podmiot nie będący organem administracji publicznej, Generalny Inspektor Ochrony Danych Osobowych z urzędu lub na wniosek osoby zainteresowanej, wydaje decyzję w przedmiocie udostępnienia danych osobowych.

Generalny Inspektor zajmował się problemem, czy gmina może wyrazić zgodę na udostępnienie danych osobowych swoich mieszkańców z *wojewódzkiej bazy danych ewidencji PESEL*, wraz z adresami, na wniosek Centrum Zdrowia Publicznego w celu wdrożenia i uruchomienia systemu Rejestru Usług Medycznych, nie naruszając przy tym

84 Por. także GI-DP-593/99, GI-DP-874/99.

ustawy o ochronie danych osobowych.⁸⁶ Obowiązek prowadzenia przez określone podmioty rejestrów usług medycznych wynika z treści rozdziału 3a ustawy z dnia 30 sierpnia 1991 r. o zakładach opieki zdrowotnej (Dz. U. Nr 91, poz. 408 z późn. zm.). Art. 32e pkt 9 tej ustawy przewiduje delegację dla Ministra Zdrowia i Opieki Społecznej do wydania, w porozumieniu z odpowiednimi ministrami, rozporządzenia określającego m.in. szczegółowe zasady i tryb rejestracji usług medycznych, sposób przekazywania danych do poszczególnych rejestrów oraz sposób wymiany informacji między podmiotami prowadzącymi rejestr, z uwzględnieniem spraw związanych z bezpieczeństwem państwa, wykaz usług medycznych podlegających rejestrowaniu i ich kody rejestrowe, wzór wykazu osób objętych rejestrem, podmiotów udzielających usługi medyczne oraz zakres danych objętych wykazami. Z uwagi na to, że odpowiedni akt nie został wydany, zdaniem Generalnego Inspektora należy odwołać się do treści pozostałych przepisów prawa dotyczących prowadzenia rejestrów usług medycznych. Art. 32f ustawy o zakładach opieki zdrowotnej precyzuje, jakim podmiotom udostępniane są dane i informacje zawarte w rejestrach usług medycznych. Z treści tego przepisu wynika, że dane i informacje do rejestrów usług medycznych przekazywane są przez podmioty udzielające usługi medyczne. Takie sformułowanie wskazuje, że rejestr usług medycznych tworzy się w oparciu o informacje pochodzące od tych podmiotów, a nie na podstawie ewidencji PESEL.

IV.10 Sprawy z zakresu pomocy społecznej

Problemy, które powstawały na gruncie przetwarzania danych osobowych na potrzeby pomocy społecznej dotyczyły sześciu grup zagadnień: podstaw przetwarzania danych osobowych, w tym zgody osoby ubiegającej się o świadczenie przez jednostki pomocy społecznej, zakresu danych przetwarzanych przez podmioty pomocy społecznej, udostępniania danych uzyskanych w toku przygotowywania decyzji w sprawie przyznania świadczenia, wykorzystywania danych zebranych w toku działań jednostek organizacyjnych pomocy społecznej na potrzeby badań, podstaw i źródeł uzyskiwania informacji o danych niezbędnych do udzielenia świadczenia z pomocy społecznej oraz istnienia lub nieistnienia obowiązku rejestracyjnego zbiorów danych przetwarzanych na potrzeby pomocy społecznej.

Do Generalnego Inspektora napłynęły również skargi ze strony ośrodków pomocy społecznej na odmowy udzielania informacji przez jednostki organizacyjne ZUS, z powołaniem się na zakaz wynikający z ustawy o ochronie danych osobowych, w przypadkach

85 Zob. także GI-DP-1578/99.

86 GI-DP-1363/99

zwracania się o udzielenie informacji niezbędnych do udzielenia świadczeń z pomocy społecznej. W każdym przypadku Generalny Inspektor informował wskazane inspektoraty ZUS o braku podstaw do odmowy udzielenia informacji pracownikom pomocy społecznej, prowadzącym określone postępowanie administracyjne w celu przyznania świadczenia, oraz zasygnalizował istniejące problemy Prezesowi ZUS.⁸⁷

1) Zagadnienie podstaw przetwarzania danych osobowych, w tym zgody osoby ubiegającej się o świadczenie przez jednostki pomocy społecznej

Generalną podstawą przetwarzania danych na potrzeby udzielania świadczeń z pomocy społecznej jest ustawa z dnia 29 listopada 1990 r. o pomocy społecznej (Dz. U. z 1998 r. Nr 64, poz. 414 z późn. zm.), która – ze względu na szeroki zakres przesłanek udzielania pomocy, do których należą m.in. niepełnosprawność, długotrwała choroba, alkoholizm, narkomania, czy trudności w przystosowaniu do życia po opuszczeniu zakładu karnego - upoważnia do gromadzenia i wykorzystywania danych, także szczególnie chronionych, jak stan zdrowia czy fakt karalności.

Istnienie podstawy ustawowej do przetwarzania danych jest wystarczającą przesłanką do gromadzenia i wykorzystywania tych danych, w związku z czym nie ma potrzeby spełnienia jakiegokolwiek innej przesłanki, w postaci, np. zgody osoby, której dane dotyczą. Należy przy tym zaznaczyć, że zgodnie z art. 6 ust. 1a ustawy o pomocy społecznej brak współdziałania osoby lub rodziny z pracownikiem socjalnym, przejawiający się odmową udzielenia informacji niezbędnych do udzielenia świadczenia, może stanowić podstawę do odmowy przyznania lub wstrzymania świadczeń. W sytuacji żądania udzielenia zgody na przetwarzanie danych przez osobę korzystającą ze świadczeń pomocy społecznej żądanie takie rodzi często podejrzenie, że dane te będą wykorzystywane w inny jeszcze sposób, anizeli tylko do udzielenia świadczenia (np. w celu przekazania firmie prywatnej), chociaż w praktyce nigdy o takim działaniu Generalny Inspektor nie został poinformowany.

Tymczasem znaczna część problemów sygnalizowanych Generalnemu Inspektorowi, wynikająca z braku znajomości ustawy o ochronie danych osobowych, dotyczyła sytuacji żądania zgody od osoby ubiegającej się o świadczenie oraz formy oświadczenia o wyrażeniu zgody na przetwarzanie danych. W wielu skargach przewijało się przekonanie, że dane

⁸⁷ Pismo GI/1148/99 z dnia 17 listopada 1999 r.

osobowe uzyskane przez ośrodek pomocy społecznej zostaną wykorzystane nie tylko do przyznania świadczenia.

Przykładem może być skarga osoby korzystającej ze świadczeń pomocy społecznej, która w sposób kategoryczny zaprotestowała przeciwko podpisaniu zgody na przetwarzanie jej danych osobowych, mimo, iż w oświadczeniu, które miała podpisać wyraźnie zostało wskazane, że dane te będą stanowić podstawę do wydania decyzji (udzielenia pomocy) przez ośrodek. Skarżąca wyraziła ponadto pogląd, iż „dane osobowe biednych osób zostaną zapewne sprzedane firmom sprzedającym „talizmany, które odmieniają los”, że „wiele naiwnych, nieszczęśliwych osób za grosze otrzymane z ośrodka kupi nie jedzenie dla dzieci, lecz talizman”.⁸⁸ W odpowiedzi na skargę, wyjaśniono skarżącej, że podstawą zbierania danych osób ubiegających się o przyznanie świadczeń z funduszy pomocy społecznej jest ustawa o pomocy społecznej, o czym, jak też o obowiązku podania danych wymaganych przez przepisy, powinna zostać poinformowana przez pracownika socjalnego w momencie udzielania informacji. W sprawie tej wysłane zostało również pismo do ośrodka pomocy społecznej ze wskazaniem konieczności dopełniania obowiązku informacyjnego, zgodnie z art. 24 ustawy o ochronie danych osobowych, w momencie zbierania danych osoby ubiegającej się o otrzymanie pomocy oraz o zbędności żądania od klientów pomocy społecznej wyrażania zgody na przetwarzanie danych, wykorzystywanych na potrzeby udzielania świadczenia.

Podobne w istocie zapytania były kierowane do Generalnego Inspektora od pracowników ośrodków pomocy społecznej. W jednej ze spraw kierownik ośrodka pomocy społecznej zapytał o podstawę przetwarzania danych oraz o zgodne z prawem postępowanie w przypadku odmowy udzielenia zgody na przetwarzanie jej danych przez osobę ubiegającą się o świadczenia z pomocy społecznej.⁸⁹

Ośrodki pomocy społecznej zwracały się również z pytaniami o konieczność uzyskania zgody klienta pomocy społecznej na udzielanie informacji innym organom i podmiotom.⁹⁰ Na pytania te udzielana była odpowiedź, iż udzielanie informacji zawierających dane osobowe podmiotom uprawnionym na podstawie przepisów prawa, zwalnia z obowiązku uzyskiwania zgody tych osób.

Do Generalnego Inspektora zwrócono się z pytaniem, czy należy uzyskiwać zgodę na przetwarzanie danych osobowych członków rodziny zastępczej. Zgodnie z § 14

⁸⁸ GI-DIS-378/99

⁸⁹ GI-DP-1508/99, podobnie w sprawach: GI-DP-739/99, GI-DP-822/99, GI-DP-1403/99.

⁹⁰ GI-DP-822/99

rozporządzenia Rady Ministrów z dnia 8 lipca 1999 r. w sprawie rodzin zastępczych (Dz. U. Nr 63, poz. 713) rodzinie zastępczej przysługuje pomoc pieniężna na każde umieszczone w niej dziecko. Z uwagi na to, że wysokość tej pomocy uzależniona jest od sytuacji dochodowej rodziny, zdaniem Generalnego Inspektora, przepis ten stanowi wystarczającą podstawę dla starosty do żądania informacji o dochodach rodziny, a wyrażenie zgody na przetwarzanie danych osobowych nie jest konieczne.⁹¹

2) Zagadnienie zakresu danych gromadzonych przez jednostki organizacyjne pomocy społecznej

Pytania dotyczyły szerokiej gamy zagadnień: od pojęcia danych osobowych, po zasadność żądania przez ośrodki pomocy społecznej określonych informacji niezbędnych w toku postępowania administracyjnego, w celu przyznania świadczenia.

Wobec ogólnikowości definicji danych osobowych zawartej w art. 6 ustawy o ochronie danych osobowych, pytania dotyczyły samego pojęcia danych osobowych oraz stwierdzenia, czy dane gromadzone przez ośrodki pomocy społecznej są danymi osobowymi.⁹² W świetle postanowień ustawy o pomocy społecznej, niewątpliwie dane przetwarzane przez ośrodki pomocy społecznej są danymi osobowymi, a ośrodki upoważnione są do przetwarzania zarówno danych „zwykłych”, jak i danych szczególnie chronionych przez ustawę (dane o stanie zdrowia, o nałogach, o karalności).

Pytania obywateli dotyczyły, np. zgodności z prawem żądania i zbierania przez organy pomocy społecznej informacji o dochodach osoby ubiegającej się o świadczenie.⁹³ Pytania dotyczące podstaw żądania udokumentowania dochodów (w postaci, np. zaświadczeń o wysokości dochodów w rodzinie) kierowane były również od organów samorządowych w związku z podejmowanymi przez te organy działaniami socjalnymi na rzecz mieszkańców gmin.⁹⁴ W odpowiedzi udzielane było wyjaśnienie, iż żądanie ujawnienia takich informacji uzasadnione jest obowiązkami gminy w zakresie zaspokajania potrzeb mieszkańców, w tym potrzeb socjalnych. Jednym z kryteriów udzielania świadczeń z pomocy społecznej jest kryterium dochodowe, uzasadnione jest zatem żądanie zaświadczenia (lub oświadczenia) o wysokości dochodów w celu zweryfikowania spełnienia kryterium przyznania świadczenia.⁹⁵

91 GI-DP-1186/99

92 GI-DP-822/99

93 GI-DP-512/99

94 GI-DP-553/99

95 GI-DP-553/99

Skarżący wnosili również o usunięcie z dokumentacji sporządzanej przez pracowników socjalnych w toku prowadzonego wywiadu środowiskowego zapisów, które według nich nietrafnie opisują ich sytuację osobistą, czy rodzinną oraz, na tej podstawie, spowodowanie przez Generalnego Inspektora uchylecia decyzji.⁹⁶ W odpowiedzi skarżącemu, pouczając o przysługującym każdemu obywatelowi prawie żądania uzupełnienia i sprostowania danych, wskazano jednocześnie na możliwość wykorzystania drogi administracyjnej, w postaci złożenia odwołania od decyzji do organu II instancji, który jest uprawniony do oceny materiału dowodowego, na którym oparł się organ I instancji wydając decyzję.

3) Udostępnianie danych uzyskanych w toku przygotowywania decyzji w sprawie przyznania świadczenia

Powtarzające się najczęściej pytania zadawane przez organy pomocy społecznej dotyczyły możliwości udostępniania danych uzyskanych w toku przygotowywania decyzji w sprawie udzielenia świadczenia sądom, prokuraturze, Policji i innym organom domagającym się udostępnienia tych danych na podstawie przepisu prawa.⁹⁷ W odpowiedzi na tak sformułowane pytania informowano, że ustawa o ochronie danych osobowych nie uchyliła obowiązywania innych aktów normatywnych, w tym upoważniających w szczególności organy ścigania i wymiaru sprawiedliwości do uzyskiwania wiadomości niezbędnych w toku prowadzonych spraw.⁹⁸

Przy okazji pytań wyjaśniany był problem stosowania art. 29 ustawy o ochronie danych osobowych w przypadku udzielania informacji podmiotom uprawnionym do ich uzyskiwania na podstawie przepisów prawa.

Ponieważ art. 29 dotyczy udostępniania danych „w celu innym, niż włączenie do zbioru”, a wszystkie organy państwa, działając w ramach i na podstawie przepisów prawa tworzą zbiory prowadzonych spraw, sam przepis i formularz udostępniania danych w nim określony, nie znajduje zastosowania, jakkolwiek niewątpliwie organy państwa zwracając się

⁹⁶ GI-DIS-90/99

⁹⁷ GI-DP-1237/99, GI-DP-1211/99

⁹⁸ Zaznaczyć należy, iż trudności m.in. organów wymiaru sprawiedliwości w uzyskaniu od ośrodków pomocy społecznej informacji niezbędnych do prowadzenia postępowań związane są m.in. z treścią art. 36 ust. 2 ustawy o pomocy społecznej, zgodnie z którym „/.../ W szczególności nie należy podawać do wiadomości nazwisk osób korzystających z pomocy społecznej oraz rodzaju i zakresu przyznanego świadczenia”. Tak sformułowany przepis jest interpretowany, jako wykluczający udzielanie informacji nawet podmiotom upoważnionym na podstawie przepisu prawa.

o udzielenie informacji muszą przestrzegać formy pisemnej, z podaniem podstawy prawnej żądania informacji oraz sprawy, do której posiadanie informacji jest niezbędne.⁹⁹

Podobnie, w skardze na miejski ośrodek pomocy społecznej w sprawie udostępnienia danych osobowych osoby korzystającej z pomocy tego ośrodka zakładowi robót publicznych. Z uwagi na to, że zakład robót publicznych współdziałał z ośrodkiem pomocy społecznej w realizacji pomocy osobom korzystającym ze świadczeń pomocy społecznej poprzez organizowanie miejsc pracy, celowe było przekazanie danych osoby bezrobotnej.¹⁰⁰

Odmienne stanowisko zajął Generalny Inspektor w odniesieniu do sprawy udzielania informacji radnym bądź komisji rewizyjnej rady gminy co do przyznawania świadczeń z pomocy społecznej konkretnym osobom. W odpowiedzi na pytanie w sprawie¹⁰¹ zostało stwierdzone, że brak jest podstaw prawnych do udzielania tego typu informacji radnym bądź organom gminy. Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 1996 r. Nr 13, poz. 74 z późn. zm.) stanowi, iż rada gminy kontroluje działalność zarządu oraz gminnych jednostek organizacyjnych powołując w tym celu komisję rewizyjną, której jednakże uprawnienia kontrolne obejmują jedynie sprawy wprost zastrzeżone do jej kompetencji, np. wykonanie uchwał. Do bezpośredniej ingerencji w działalność urzędu gminy niezbędny byłby szczególny przepis prawa, którego jednak brak. Z tego względu żądanie informacji o wysokości zasiłków lub dodatków socjalnych wypłacanych konkretnym osobom nie znajduje podstaw prawnych.¹⁰²

Skarga na miejski ośrodek pomocy społecznej w sprawie udziału psychologów w sporządzaniu przez pracowników pomocy społecznej wywiadu środowiskowego. Skarżący zarzucał, że w trakcie sporządzania wywiadu środowiskowego pracownik socjalny przebywał w towarzystwie psychologa. Zgodnie z przepisami § 3 rozporządzenia Ministra Pracy i Polityki Społecznej z dnia 24 lipca 1997 r. w sprawie sposobu przeprowadzania wywiadu środowiskowego (rodzinnego), wzoru kwestionariusza wywiadu 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.), wywiad przeprowadza pracownik socjalny posługujący się legitymacją pracownika socjalnego wydaną przez pracodawcę. Skoro wywiad przeprowadzono w obecności osoby do tego nie uprawnionej ujawniając dane osobowe skarżącego, naruszona została ustawa o ochronie

⁹⁹ GI-DP-739/99; inne stanowisko zostało zajęte w sprawie GI-DP-14/99.

¹⁰⁰ GI-DIS-175/99

¹⁰¹ Podobnie w sprawie GI-DP-53/99.

¹⁰² Podobnie w sprawie GI-DP-275/99, GI-DP-296/99, GI-DP-361/99.

danych osobowych, która w art. 26 ust. 1 pkt 1 stanowi, że dane winny być przetwarzane zgodnie z prawem. W tej sytuacji przeprowadzono postępowanie i wydano decyzję nakazującą ośrodkowi usunięcie uchybień w procesie przetwarzania danych poprzez przeprowadzanie wywiadów środowiskowych zgodnie z przepisami prawa, w szczególności bez udziału osób trzecich.¹⁰³

4) Zagadnienie wykorzystywania danych zebranych w toku działań jednostek organizacyjnych pomocy społecznej na potrzeby badań

Do Biura GIODO kierowane były również prośby o udzielenie zgody lub wyrażenie opinii nt. możliwości wykorzystywania danych zawartych w wywiadach środowiskowych na potrzeby prowadzenia badań naukowych lub pisanie pracy naukowej.¹⁰⁴ W odpowiedzi na przedstawioną prośbę zwrócona została uwaga na to, iż Generalny Inspektor nie udziela zgody na udostępnienie określonych danych osobowych natomiast podejmowanie rozstrzygnięć w tym zakresie leży w gestii samego administratora danych (w tym przypadku w gestii ośrodka pomocy społecznej). Z uwagi jednak na zawartą w samej ustawie o pomocy społecznej szczególną klauzulę, dotyczącą niepodawania danych zebranych na potrzeby wydania decyzji o udzieleniu pomocy, ewentualne udostępnienie danych do badań mogłoby nastąpić po uprzednim zanonimizowaniu kwestionariuszy wywiadu środowiskowego.

5) Skargi i pytania dotyczące podstaw i źródeł uzyskiwania informacji o danych niezbędnych do udzielenia świadczenia z pomocy społecznej

W kilku przypadkach obywatele zgłaszali pytania i skargi dotyczące ujawniania ich danych przez, np. podmioty zatrudniające na żądanie ośrodków pomocy społecznej, kwestionując w ogóle możliwość udostępniania danych, np. o wysokości zarobków przez pracodawcę organowi pomocy społecznej czy pracownikowi socjalnemu. Przy rozpatrywaniu skarg i pytań uwzględniona została treść art. 42 ustawy o pomocy społecznej, zgodnie z którym sądy, organy państwowe i inne jednostki organizacyjne są obowiązane, nie później jednak niż w terminie 7 dni, udostępnić lub udzielić pracownikowi socjalnemu odpowiednich informacji, które mają znaczenie dla rozstrzygnięcia o przyznaniu lub odmowie przyznania świadczeń oraz ich rozmiarów, a ponadto treść art. 51, zgodnie z którym organy administracji rządowej i samorządowej są obowiązane do udzielania pracownikowi socjalnemu pomocy w

¹⁰³ Sprawa nie jest zakończona, ponieważ obie strony, zarówno skarżący, jak i ośrodek pomocy społecznej, wniosły o ponowne rozpatrzenie sprawy; zob. również GI-DIS-308/99, GI-DEC/58/99/DIS-308/99/ DP-26/99

¹⁰⁴ Sprawy: GI-DP-497/99, GI-DP- 463/99.

zakresie wykonywania tych czynności. W toku załatwiania spraw Generalny Inspektor zwracał również uwagę na to, iż jednostki organizacyjne udzielające informacji ośrodkom pomocy społecznej nie mogą uzależniać udzielania informacji od zgody udzielanej przez osoby, których dane dotyczyły, ponieważ udzielanie informacji odbywa się na podstawie przepisów prawa, a ośrodek pomocy społecznej jest uprawniony do uzyskiwania wszelkich informacji niezbędnych do prowadzenia postępowania.

Przykładem jest sprawa, w której obywatel zarzucił Ministerstwu Sprawiedliwości ujawnienie danych o dochodach bez jego zgody.¹⁰⁵ W wyniku wyjaśnienia sprawy okazało się, iż ujawnienie danych nastąpiło na wniosek centrum pomocy społecznej i, po raz drugi, temuż centrum za zgodą samego zainteresowanego.

Ośrodki pomocy społecznej (centra pomocy rodzinie) w pismach kierowanych do Generalnego Inspektora sygnalizowały z kolei trudności w uzyskaniu informacji niezbędnych do zweryfikowania danych w toku postępowania o przyznanie świadczeń z pomocy społecznej. Jak wskazywano w pismach, do zadań organów pomocy społecznej należy sprawowanie nadzoru nad domami pomocy społecznej, w tym również ustalanie odpłatności za pobyt mieszkańców w tych placówkach. Podstawą ustalania odpłatności jest udokumentowany dochód mieszkańców, z których większość otrzymuje świadczenia wypłacane przez organy emerytalno-rentowe. Z uwagi na przeprowadzane waloryzacje świadczeń, a także z uwagi na fakt, iż uzyskanie informacji od samych zainteresowanych nie zawsze jest możliwe (zagubienie decyzji, niechęć do udostępniania decyzji), najprostszą i najkorzystniejszą dla podopiecznych domów pomocy społecznej drogą ustalania stanu faktycznego jest korzystanie z informacji w ZUS. Tymczasem ZUS odmawia udzielania informacji, powołując się na ustawę o ochronie danych osobowych.¹⁰⁶ W związku z zasygnalizowaną sytuacją, pismem z dnia 17 listopada 1999 r. Generalny Inspektor zwrócił się do Prezesa Zakładu Ubezpieczeń Społecznych z prośbą o podjęcie w ramach nadzoru, działań zmieniających obecną praktykę.¹⁰⁷ W piśmie sygnalizacyjnym zwrócona została uwaga na treść art. 42 ustawy o pomocy społecznej, przepisu stanowiącego wystarczającą przesłankę do przetwarzania danych osobowych w rozumieniu przepisów art. 23 ust. 1 pkt 2 i art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych i to w odniesieniu do danych zwykłych, jak również tzw. danych wrażliwych, np. o stanie zdrowia, do których przetwarzania jednostki pomocy społecznej są upoważnione. Brak zatem podstaw prawnych

¹⁰⁵ GI-DIS-370/99

¹⁰⁶ GI-DP-1290/99, podobny problem w sprawie GI-DP-1415/99.

¹⁰⁷ GI/1148/99

do odmowy udzielania informacji przez jednostki ZUS jednostkom pomocy społecznej na gruncie przepisów o ochronie danych osobowych.

O podjętych działaniach poinformowane zostały również ośrodki sygnalizujące nieprawidłowości.

Pytania organów pomocy społecznej dotyczyły również możliwości korzystania z informacji gromadzonych przez placówki samorządowe, np. izbę wytrzeźwień.¹⁰⁸ Z uwagi na treść art. 42 i 51 ustawy o pomocy społecznej Generalny Inspektor stwierdził, iż nie ma podstaw do odmowy udzielania informacji ośrodkom pomocy społecznej przez jednostki samorządowe.

6) Sprawy dotyczące dopełnienia obowiązku rejestracji przez ośrodki pomocy społecznej

Na gruncie ustawy o ochronie danych osobowych powstawały wątpliwości co do konieczności dopełnienia obowiązku rejestracyjnego przez ośrodki pomocy społecznej oraz domy pomocy społecznej i inne placówki udzielające świadczeń na podstawie ustawy o pomocy społecznej.

Pisma kierowane do Generalnego Inspektora zawierały pytania co do konieczności dopełnienia obowiązku rejestracji oraz wskazania podmiotu, na którym ciąży obowiązek zgłoszenia zbioru do zarejestrowania.¹⁰⁹

W odpowiedzi udzielone zostało wyjaśnienie, iż brak jest podstaw prawnych do zwolnienia z obowiązku rejestracji zbiorów tworzonych na potrzeby udzielania świadczeń z pomocy społecznej. Art. 43 ust. 1 ustawy o ochronie danych osobowych zawierający katalog zbiorów zwolnionych z obowiązku rejestracji, nie zawiera bowiem tej kategorii zbiorów. Obowiązek dokonania zgłoszenia zbioru do zarejestrowania spoczywa na kierowniku jednostki organizacyjnej (ośrodka pomocy społecznej, centrum pomocy rodzinie czy domu pomocy społecznej) przy czym, jeśli zbiory dotyczące klientów pomocy społecznej prowadzone są przez jednostki podległe organizacyjnie jednostce pomocy (np. zbiory prowadzone przez ośrodki będące jednostkami organizacyjnymi miejskiego ośrodka), to zbiór do zarejestrowania winien zgłosić kierownik ośrodka.

¹⁰⁸ GI-DP-1086/99

¹⁰⁹ Np. sprawy GI-DP-335/99, GI-DP-705/99, GI-DP-739/99, GI-DP- 838/99, GI-DP-1089/99.

Obowiązek zgłoszenia zbioru do zarejestrowania dotyczy również zbiorów prowadzonych w domach pomocy społecznej.¹¹⁰

110 GI-DP-565/99

C. Przetwarzanie danych osobowych przez funkcjonariuszy służb publicznych

I. Podstawy prawne przetwarzania danych osobowych

Przedmiotem wielu pism obywateli do Generalnego Inspektora Ochrony Danych Osobowych jest zagadnienie przetwarzania danych przez Policję, UOP, Służbę Celną, Straż Graniczną.

Zgodnie z art. 7 Konstytucji organy władzy publicznej mogą działać tylko na podstawie prawa. Przepisy prawa muszą więc określać zakres działań, zadania i tryb postępowania konkretnych organów. Kompetencje wyżej wymienionych służb uregulowane zostały m.in. w ustawie z dnia 6 kwietnia 1990 r. o Policji (Dz. U. Nr 30, poz. 179 z późn. zm.), ustawie z dnia 6 kwietnia 1990 r. o Urzędzie Ochrony Państwa (Dz. U. 1999 r. Nr 51, poz. 526 z późn. zm.), ustawie z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. Nr 78, poz. 462 z późn. zm.) a także ustawie z dnia 24 lipca 1999 r. o Służbie Celnej (Dz. U. Nr 72, poz. 802 z późn. zm.) i ustawie z dnia 26 kwietnia 1996 r. o Służbie Więziennej (Dz. U. Nr 61, poz. 283 z późn. zm.) oraz w przepisach wykonawczych do tych ustaw.

I.1 Udostępnianie danych osobowych funkcjonariuszom Policji, UOP, funkcjonariuszom innych służb publicznych

1) Legalność udostępniania

Ustawa o ochronie danych osobowych w art. 23 ust. 1 określa przesłanki legalności przetwarzania danych. Zgodnie z art. 23 ust. 1 pkt 2 przetwarzanie danych jest dopuszczalne, jeżeli zezwala na to przepis prawa.

Wiele pytań kierowanych do Generalnego Inspektora Ochrony Danych Osobowych dotyczyło podstawy prawnej udostępniania Policji, funkcjonariuszom UOP, Straży Granicznej i Służby Celnej danych osobowych przetwarzanych przez inne organy.

Generalny Inspektor odpowiadając na pytania zwracał uwagę, że zgodnie z art. 15 ustawy o Policji, policjanci wykonując określone w tej ustawie zadania, mają prawo m.in. żądania niezbędnej pomocy od instytucji państwowych, organów administracji rządowej i samorządu terytorialnego oraz jednostek gospodarczych prowadzących działalność w zakresie

użyteczności publicznej.¹¹¹ Organy te, jednostki i instytucje mają obowiązek, w granicach swojego działania, udzielenia pomocy, w ramach obowiązujących przepisów prawa.

Policja ma także prawo zwracania się o niezbędną pomoc do innych jednostek gospodarczych i organizacji społecznych, jak również zwracania się w nagłych wypadkach do każdej osoby o udzielenie doraźnej pomocy, w ramach obowiązujących przepisów prawa.

W związku z wizytą Ojca Świętego Jana Pawła II w Polsce, Policja podejmowała działania zmierzające do zapewnienia Papieżowi bezpieczeństwa. Do Generalnego Inspektora kierowano pytania, czy w świetle ustawy o ochronie danych osobowych dopuszczalne jest żądanie policjantów udostępnienia im danych osobowych pracowników jednostek organizacyjnych (zakładów pracy) usytuowanych w pobliżu trasy przejazdu Papieża. W odpowiedzi podkreślano, że udostępnienie takich danych jest Policji niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego.¹¹² Zgodnie bowiem z art. 1 ust. 2 pkt 1 i 2 ustawy o Policji, do podstawowych zadań Policji należy ochrona bezpieczeństwa i porządku publicznego, w tym zapewnienie spokoju w miejscach publicznych. Zakres uprawnień organów Policji uregulowany jest w art. 15 ust. 1 pkt 7 ustawy o Policji. Udostępnienie takich danych funkcjonariuszom było zatem w pełni zasadne.

Do Generalnego Inspektora napłynęły zapytania dotyczące uprawnień Policji do monitorowania miejsc publicznych (ulic, banków, hoteli itp.) za pomocą kamer.¹¹³ Generalny Inspektor odpowiadając zwrócił uwagę na fakt, że zastosowanie ustawy o ochronie danych osobowych zależeć będzie od ustalenia, czy w danej sytuacji dane osobowe (tj. wizerunki osób utrwalone na filmie) przetwarzane są w zbiorze danych osobowych w rozumieniu art. 7 pkt 2 ustawy o ochronie danych osobowych. Ustawa ta (zgodnie z art. 2 ust. 1) chroni bowiem prawa osób fizycznych, których dane są lub mogą być przetwarzane w zbiorach danych. Ustawa znajdzie zatem zastosowanie o tyle, o ile będzie można mówić o przetwarzaniu danych osobowych w zbiorze w rozumieniu art. 7 pkt 1 ustawy o ochronie danych osobowych.

Zapewnienie porządku i bezpieczeństwa publicznego jest ustawowym zadaniem Policji, toteż monitorowanie miejsc publicznych, szkół, placów, banków itp. znajduje podstawę prawną w art. 14 ust. 1 ustawy o Policji. Generalny Inspektor podkreślał jednak, że obraz z kontrolowanego miejsca powinien docierać wyłącznie do właściwej jednostki Policji,

¹¹¹ Por. np. GI-DP-272/99, GI-DP-442/99, GI-DP-479/99, GI-DP-1102/99.

¹¹² por. GI-DP- 260/99, GI-DP-272/99, GI-DP-476/99.

¹¹³ por. np. GI-DP-425/99.

wątpliwe natomiast wydaje się transmitowanie obrazu przez, np. lokalną telewizję kablową (ponieważ nie służy to, np. ochronie porządku w szkole).¹¹⁴

Generalny Inspektor Ochrony Danych Osobowych otrzymał skargę dotyczącą bezprawnego, zdaniem wnoszącego skargę, udostępnienia przez kierownika urzędu stanu cywilnego danych osobowych tej osoby komendantowi Policji.¹¹⁵ W odpowiedzi zwrócono uwagę, że zgodnie z art. 25 ustawy z dnia 29 września 1986 r. Prawo o aktach stanu cywilnego (Dz. U. Nr 36, poz. 180 z późn. zm.) księgi stanu cywilnego, za zezwoleniem kierownika urzędu stanu cywilnego, można udostępnić upoważnionym przedstawicielom organów państwowych. Z treści art. 25 ustawy prawo o aktach stanu cywilnego wynika więc, że kierownik urzędu stanu cywilnego jest uprawniony do udostępniania Policji żądanych danych osobowych.

Skargi dotyczyły także udostępniania Policji oryginałów list płac w celu dokonania ekspertyzy przez biegłego grafologa¹¹⁶ oraz udostępnienia Policji numeru ewidencyjnego PESEL przez Ministra Spraw Wewnętrznych i Administracji.¹¹⁷ W odpowiedzi na pierwszą ze skarg wskazano, że przekazanie Policji listy płac nie stanowi naruszenia ustawy o ochronie danych osobowych. Jak wynika z pisemnych wyjaśnień udzielonych Generalnemu Inspektorowi Ochrony Danych Osobowych udostępnienie miało miejsce jedynie w związku z toczącym się postępowaniem sądowym, na żądanie uprawnionego organu. Również w drugim przypadku Policja wykonywała swoje prawem określone zadania i miała prawo do otrzymania żądanych informacji.

Pytania dotyczące legalności udostępniania danych pojawiały się nie tylko w odniesieniu do Policji, ale dotyczyły także działań funkcjonariuszy UOP, Wojskowych Służb Informacyjnych i innych jednostek.¹¹⁸ Na podstawie art. 7 ust. 1 pkt 5 ustawy o Urzędzie Ochrony Państwa, funkcjonariusze UOP mogą żądać niezbędnej pomocy od instytucji państwowych, organów administracji rządowej i samorządu terytorialnego oraz jednostek gospodarczych prowadzących działalność w zakresie użyteczności publicznej; wymienione organy, instytucje i jednostki obowiązane są, w ramach swojego działania, do udzielenia tej pomocy w granicach obowiązujących przepisów prawa. Generalny Inspektor uważa, że

¹¹⁴ GI-DP-365/99

¹¹⁵ GI-DIS-295/99

¹¹⁶ GI-DIS-275/99

¹¹⁷ GI-DIS-181/99

¹¹⁸ Por. np. GI-DP-83/99.

przepis ten stanowi wystarczającą podstawę do udostępniania danych osobowych funkcjonariuszom Urzędu Ochrony Państwa.¹¹⁹

Uprawnienia Straży Granicznej określa art. 11 ust. 1 pkt 9 ustawy o Straży Granicznej. Straż może żądać udzielenia niezbędnej pomocy od instytucji państwowych, organów administracji rządowej i samorządu terytorialnego, oraz jednostek gospodarczych prowadzących działalność w zakresie użyteczności publicznej; wymienione instytucje, organy i jednostki obowiązane są, w ramach swoich działań, do udzielenia tej pomocy, w granicach wyznaczonych prawem. Straż Graniczna może również zwracać się o niezbędną pomoc do innych jednostek gospodarczych i organizacji społecznych, a w nagłych wypadkach do każdej osoby o udzielenie doraźnej pomocy, w ramach obowiązujących przepisów prawa. Przedmiotem zainteresowania Straży Granicznej są najczęściej fotokopie dowodów osobistych wraz z fotografiami, wykazy mieszkańców budynków wskazanych przez Straż Graniczną, wykazy cudzoziemców zameldowanych na terenie gminy, a także inne dane osób wskazanych przez Straż Graniczną. Udzielanie pomocy, zdaniem Generalnego Inspektora, obejmuje także udostępnianie żądanych danych osobowych.¹²⁰

Także ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (Dz. U. Nr 89, poz. 555, zm. Dz. U. 1999 r. Nr 83, poz. 931) przyznaje pewne znaczne uprawnienia organom prowadzącym postępowanie karne, stanowiąc prawną podstawę udostępniania danych osobowych tym organom. Art. 15 kodeksu postępowania karnego przewiduje, że wszystkie instytucje państwowe, samorządowe i społeczne są obowiązane w zakresie swego działania do udzielania pomocy organom prowadzącym postępowanie karne (Policji i innym organom).

2) Forma wystąpienia funkcjonariuszy o udostępnienie im danych osobowych przetwarzanych przez inne podmioty

Liczna grupa pytań kierowanych do Generalnego Inspektora Ochrony Danych Osobowych dotyczyła formy, w jakiej funkcjonariusze powinni zwracać się o udostępnienie danych osobowych przetwarzanych przez innych administratorów danych. W przypadku Policji, UOP, Straży Granicznej i Służby Celnej, ze względu na specyfikę zadań i metod pracy tych służb, problem nabiera szczególnej wagi.

Ustawa o ochronie danych osobowych w art. 29 ust. 1 przewiduje, że w przypadku udostępnienia danych w celu innym, niż włączenie do zbioru, administrator udostępnia

¹¹⁹ Por. np. GI-DP-1400/99, GI-DP-1168/99.

posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa. W ust. 3 art. 29 ustawodawca postanowił także, że dane osobowe 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 wniosku określa rozporządzenie Ministra Spraw Wewnętrznych 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.). Wiele pytań prawnych do Generalnego Inspektora dotyczy kwestii, czy Policja, UOP, Służba Celna i Straż Graniczna (a także inne jednostki) mają obowiązek występowania z żądaniem udostępnienia danych osobowych właśnie na wniosek, o którym mówi art. 29 ustawy o ochronie danych osobowych.¹²¹ Często są przypadki niestosowania przez funkcjonariuszy tych służb wniosku w jakiegokolwiek formie pisemnej. W praktyce powoduje to wiele konfliktów, nieporozumień oraz nie sprzyja efektywnemu prowadzeniu działań przez odpowiednie organy. Administratorzy danych (o których mowa w art. 3 ust. 1 ustawy o ochronie danych osobowych) odmawiając udostępnienia danych narażają się na zarzut utrudniania postępowania.

Generalny Inspektor Ochrony Danych Osobowych uważa, że przepis art. 29 znajduje zastosowanie wyłącznie wtedy, gdy podmiot mający uzasadnioną potrzebę otrzymania danych osobowych nie zamierza ich przetwarzać w zbiorze. Policja i inne wspomniane wyżej organy, czy to prowadząc postępowanie karne, czy dokonując innych czynności są administratorami zbiorów danych osobowych, a udostępnienie danych następuje właśnie w celu włączenia do zbioru.¹²² Z tego powodu odpowiadając na pytania dotyczące tej kwestii, podkreślano, że służby te nie są obowiązane do występowania z żądaniem udostępnienia danych na wspomnianym wniosku. Organy te obowiązane są zatem tylko do wykazania istnienia jednej z przesłanek legalności przetwarzania danych określonych w art. 23, art. 27

¹²⁰ Por. sprawa GI-DP-1102/99.

¹²¹ Niemal 30% pytań kierowanych do Generalnego Inspektora Ochrony Danych Osobowych odnoszących się do działalności Policji, UOP i innych służb dotyczy konieczności stosowania wniosku określonego w art. 29 ustawy o ochronie danych osobowych; por. m.in.: GI-DP-289/99/336, GI-DP-237/99/352, GI-DP-479/99/490, GI-DP-491/99/525, GI-DP-1122/99/1569, GI-DP-1142/99/1340, GI-DP-1168/99/1643.

¹²² Zob. np. sprawę GI-DP-489/99/514; godna uwagi jest m.in. konstatacja, że akta postępowania przygotowawczego stanowią zbiór danych osobowych w rozumieniu art. 7 pkt 1 ustawy o ochronie danych osobowych; por. także GI-DP-1589/99.

lub 28 ustawy o ochronie danych osobowych¹²³. Najczęściej jest to przesłanka o której mowa w art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych.¹²⁴ Organy powołują się bowiem na przepisy regulujące ich zakres działania, kompetencje i właściwość. Należy jednak podkreślić, że najczęściej konflikty te są przejawem niezrozumienia przepisów prawa. Przepisy niezbyt jasno określają niektóre powinności administratorów zbiorów danych osobowych, a świadomość grożącej tym administratorom odpowiedzialności karnej nie ułatwia podjęcia decyzji o udostępnieniu żądanych przez funkcjonariuszy danych osobowych.

Problem wniosku, o którym mówi art. 29 nie jest wszakże jedyną kwestią budzącą zaniepokojenie Generalnego Inspektora w odniesieniu do formy żądania udostępnienia danych osobowych przez funkcjonariuszy. Często pojawia się bowiem pytanie, jakie minimalne wymogi muszą zostać spełnione, aby można było udostępnić dane osobowe podmiotom uprawnionym do tego na mocy prawa. Odpowiadając na te pytania Generalny Inspektor zwraca uwagę na przepisy szczególne, regulujące tryb współpracy służb mundurowych z organami administracji i innymi podmiotami oraz sposób uzyskiwania pomocy od tych organów i instytucji.¹²⁵

Sposób udzielania pomocy Policji reguluje wydane na podstawie art. 15 ust. 8 ustawy o Policji 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 § 4 ust. 1 z żądaniem lub prośbą o udzielenie pomocy występuje na piśmie właściwy komendant lub upoważniony przez niego policjant. Wystąpienie powinno zawierać określenie podstawy prawnej, rodzaju i zakresu pomocy, uzasadnienie faktyczne oraz upoważnienie dla policjanta. Wystąpienie nie jest wymagane, jeżeli policjanci wykonują czynności służbowe:

- 1) na pisemne polecenie sądu, prokuratora, organów administracji państwowej lub samorządu terytorialnego,
- 2) w celu ratowania życia lub zdrowia ludzkiego, a także mienia,
- 3) związane z prowadzeniem pościgu za sprawcą przestępstwa.

¹²³ GI-DP-489/99/514, GI-DP-495/99/526

¹²⁴ Zgodnie z art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych przetwarzanie danych jest dopuszczalne, jeżeli zezwala na to przepis prawa.

¹²⁵ Por. np. GI-DP-177/99, GI-DP-498/99, GI-DP- 1168/99

W powyższych przypadkach do żądania lub zwracania się z prośbą o udzielenie pomocy upoważniony jest każdy policjant. Powinien on jednak ustnie poinformować osobę, do której się zwraca o zaistnieniu wyżej wymienionej sytuacji, oraz o podstawie prawnej, rodzaju i zakresie pomocy.

Sposób występowania o uzyskanie pomocy przez funkcjonariuszy UOP określa rozporządzenie Rady Ministrów z dnia 30 lipca 1990 r. w sprawie określenia trybu korzystania przez funkcjonariuszy Urzędu Ochrony Państwa z niezbędnej pomocy instytucji państwowych, jednostek gospodarczych, organizacji społecznych i obywateli (Dz. U. Nr 56, poz. 326). Zgodnie z rozporządzeniem do wystąpienia z żądaniem lub prośbą o udzielenie pomocy występują uprawnieni kierownicy jednostek organizacyjnych Urzędu Ochrony Państwa wykonujący czynności operacyjno-rozpoznawcze i dochodzeniowo-śledcze. Wystąpienie powinno być sporządzone na piśmie. Jedynie w nagłych wypadkach możliwe jest zwrócenie się do każdego obywatela o udzielenie doraźnej pomocy. Funkcjonariusz wówczas obowiązany jest okazać legitymację służbową lub znak identyfikacyjny, oraz poinformować w jakiej jednostce pełni służbę. W takim wypadku należy jednak określić zakres i rodzaj pomocy.

Z sygnałów otrzymywanych przez Generalnego Inspektora wynika jednoznacznie, że funkcjonariusze UOP zwracając się do urzędów administracji nie stosują pisemnego wniosku, żądając udostępnienia danych osobowych okazują jedynie legitymację służbową.¹²⁶ W związku z prośbami organów administracji o przedstawienie w tej sprawie swojego poglądu, Generalny Inspektor podkreślał, że nie jest to kwestia sporna wymagająca zajęcia przezeń stanowiska. Przepisy prawa jasno precyzują sposób działania funkcjonariuszy Urzędu Ochrony Państwa, a funkcjonariusze ci żądając udzielenia określonych informacji zobowiązani są stosować tryb określony w tych przepisach.¹²⁷ Jest oczywiste, że podejmując działania dbają oni o to, aby nie pozostawiać śladów swojej pracy w postaci, np. pisemnych wniosków. Trzeba jednak podkreślić, że czynności takie nie mogą stać w sprzeczności z prawem.

Warto zaznaczyć, że przepisy regulujące sposób uzyskiwania przez funkcjonariuszy informacji od organów administracji publicznej, znacznie komplikują, a niejednokrotnie wręcz uniemożliwiają odpowiednim służbom wykonywanie ich ustawowych zadań. Do Generalnego Inspektora zwracali się administratorzy danych z pytaniami, czy jest

126 GI-DP-83/99

dopuszczalne umożliwienie Policji, funkcjonariuszom Urzędu Ochrony Państwa, Straży Granicznej i Urzędu Celnego dostępu do danych osobowych w drodze teletransmisji danych.¹²⁸ Funkcjonariusze występowali najczęściej do administratorów o udostępnienie danych gromadzonych w systemie ewidencji PESEL i wojewódzkich bazach adresowych¹²⁹ oraz danych o osobach posiadających uprawnienia do kierowania pojazdami.¹³⁰ Niejednokrotnie pytający zastrzegali, że komunikacja odbywałaby się pomiędzy wyznaczonymi pracownikami z zastosowaniem haseł i innych środków bezpieczeństwa. W odpowiedzi na pismo Podsekretarza Stanu w Ministerstwie Spraw Wewnętrznych i Administracji Generalny Inspektor podkreślał, że organy władzy publicznej mogą działać tylko na podstawie prawa. Przepisy prawa muszą określać kompetencje, zadania i tryb postępowania konkretnych organów. Generalny Inspektor podkreślał, że zgodnie z wspomnianym wyżej rozporządzeniem niezbędne jest występowanie przez Policję z wnioskiem sporządzonym w formie pisemnej. Wniosek powinien zawierać uzasadnienie, podstawę prawną oraz numer sprawy w celu wskazania, że uzyskane dane zostały włączone do zbioru spraw. Powinien również zawierać zakres i przeznaczenie danych.¹³¹

Zasady współdziałania organów celnych z organami administracji publicznej określają przepisy rozporządzenia Rady Ministrów z dnia 14 czerwca 1999 r. w sprawie zasad współdziałania organów celnych z organami administracji publicznej oraz innymi państwowymi i samorządowymi jednostkami organizacyjnymi, a także zakresu ich świadczeń na rzecz organów celnych (Dz. U. Nr 53, poz. 551). Rozporządzenie nakłada na organy administracji publicznej i inne wymienione w nim podmioty publiczne (państwowe i samorządowe jednostki organizacyjne) zwane w rozporządzeniu „jednostkami współdziałającymi” obowiązek współdziałania w granicach swoich kompetencji ustawowych, m.in. poprzez niezwłoczne przekazywanie informacji o osobach, w stosunku do których organy celne podjęły działania, w tym przez udostępnianie odpisów lub wypisów z prowadzonych rejestrów, a także kopii dokumentów dotyczących takich spraw. Zgodnie jednak z § 2 pkt 2 powołanego rozporządzenia, działania jednostek współdziałających podejmowane są na pisemny wniosek organu celnego, a jedynie w razie zaistnienia okoliczności wymagających natychmiastowego działania, funkcjonariusz celny może zażądać podjęcia czynności bez zachowania formy pisemnej lub formy porozumienia (§ 4 pkt 1),

127 GI-DP-1400/99

128 GI-DP-427/99, GI-DP-939/99

129 GI-DP-435/99

130 GI-DP-498/99

131 zob. GI-DP-435/99.

wówczas musi jednak niezwłocznie potwierdzić żądanie w formie pisemnej, określając w szczególności zakres czynności jednostki współdziałającej, oraz uzasadniając konieczność podjęcia natychmiastowego działania.

Zaniepokojenie Generalnego Inspektora wzbudziła sprawa ukarania sekretarza miasta i gminy przez Urząd Celny, za utrudnianie kontroli celnej poprzez odmowę dostępu do bazy danych o właścicielach samochodów sprowadzonych z zagranicy, tj. o przestępstwo z art. 86 ustawy karnej skarbowej z dnia 26 października 1971 r. (Dz. U. 1984 r. Nr 22, poz. 103 z późn. zm.).¹³² Sekretarz miasta i gminy, obawiając się odpowiedzialności karnej przewidzianej w ustawie o ochronie danych osobowych nie zgodził się na udostępnienie żądanych danych bez złożenia przez pracowników Urzędu Celnego pisemnego wniosku. W związku z tym, w październiku 1999 roku Generalny Inspektor zwrócił się do Prezesa Głównego Urzędu Cei o wszczęcie postępowania mającego na celu wyjaśnienie tego rodzaju przypadków łamania prawa przez funkcjonariuszy urzędów celnych oraz o podjęcie działań, których celem byłoby uniknięcie podobnych naruszeń w przyszłości.

W wystąpieniu podniesiono, że żądanie udostępnienia danych bez pisemnego potwierdzenia zasadności posiadania danych rodzi podejrzenie, że funkcjonariusze urzędów celnych nadużywają swoich uprawnień i bez uzasadnionej potrzeby, lub w innych celach aniżeli prowadzenie postępowania, domagają się wglądu w dokumentację prowadzoną przez podmioty publiczne. Zgodnie z przepisami przywołanego wyżej rozporządzenia podmioty publiczne nie są zobowiązane do podejmowania działań na ustne żądanie funkcjonariuszy urzędów celnych. Wykładnia literalna przepisów §§ 2 i 4 rozporządzenia regulującego zasady współdziałania organów celnych z organami administracji publicznej prowadzi do wniosku, że żądanie udostępnienia danych musi wiązać się z określoną, prowadzoną przez organy celne sprawą, a zatem pismo uzasadniające potrzebę posiadania określonych informacji musi powoływać się zarówno na określoną podstawę prawną, jak i na fakt prowadzenia konkretnej sprawy. Działania funkcjonariuszy celnych naruszają więc przepisy bezpośrednio do nich adresowane. Praktyka powyższa, zdaniem Generalnego Inspektora Ochrony Danych Osobowych, stanowi również naruszenie ustawy o ochronie danych osobowych. Wprawdzie ustawa nie określa szczegółowego wzoru wniosku, z jakim powinny się zwracać organy państwa o udostępnienie danych osobowych, jeżeli dane takie mają zostać włączone do zbioru, jednakże odsyła do kodeksu postępowania administracyjnego, z którego wynika

132 GI-DP-1232/99

zasada pisemności. Każde zatem wystąpienie organu państwowego musi odbywać się w formie pisemnej, chyba że przepis prawa stanowi inaczej.

W odpowiedzi na wystąpienie, do Biura Generalnego Inspektora Ochrony Danych Osobowych w dniu 29 grudnia 1999 r. wpłynęło pismo od Prezesa Głównego Urzędu Cel.¹³³ Wynika z niego, że praktyka wskazuje na częste przypadki odmowy udostępnienia danych pomimo, że wnioski w tych sprawach spełniały wymogi formalne¹³⁴ oraz zawierały właściwą podstawę prawną i uzasadnienie prowadzenia danego postępowania. Ponadto Prezes GUC podkreślił, że nie są mu znane jakiekolwiek skargi na niewłaściwe postępowanie funkcjonariuszy celnych w zakresie uzyskiwania danych osobowych.

3) Zakres udostępnianych funkcjonariuszom danych

Zgodnie z art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych zakres udostępnianych danych osobowych powinien być adekwatny w stosunku do celu przetwarzania tych danych.

W odpowiedziach na pytania prawne Generalny Inspektor wielokrotnie wskazywał na to, że dane osobowe można udostępnić funkcjonariuszom tylko w takim zakresie, jaki wynika z powołanych przez te organy przepisów. Należy pamiętać, że zakres danych udostępnianych określonym podmiotom może podlegać szczególnej regulacji zawartej w przepisach odrębnych aktów prawnych.¹³⁵ Musi z tych przepisów wyraźnie wynikać uprawnienie do przetwarzania danych osobowych w określonym zakresie (np. czy chodzi o udostępnienie danych konkretnej osoby, czy o udostępnienie całego zbioru)¹³⁶ lub uprawnienie dla organu występującego o udostępnienie danych do określania zakresu żądanej pomocy.¹³⁷ Generalny Inspektor otrzymywał również sygnały dotyczące zbyt szerokiego zakresu danych przetwarzanych przez Policję w protokołach przesłuchań świadka.¹³⁸

Wśród skarg dotyczących zbyt szerokiego zakresu zbieranych danych na szczególną uwagę zasługuje sprawa dotycząca niezgodnego z prawem przetwarzania danych osobowych kandydatów na funkcjonariuszy Inspekcji Celnej w ramach badania poligraficznego. W toku kontroli stwierdzono, że kandydaci na funkcjonariuszy poddawani są badaniom poligraficznym w celu określenia ich przydatności do pracy na danym stanowisku w Inspekcji

133 DP-I-055-2-408/99/2204/2280/2380, pismo z dnia 24 grudnia 1999 r.

134 Z pisma tego wynika, że funkcjonariusze występujący o udostępnienie danych osobowych stosują wniosek, o którym jest mowa w art. 29 ustawy o ochronie danych osobowych.

135 GI-DP-146/99

136 GI-DP-260/99, GI-DP-1102/99

137 GI-DP-272/99

138 GI-DP-1613/99

Celnej. Badanie to przeprowadzone jest dobrowolnie, a warunkiem wstępnej rozmowy ze specjalistą przeprowadzającym badanie jest uprzednia zgoda kandydata. W trakcie rozmowy badanemu wyjaśniane są zasady działania poligrafu, informuje się również o sposobie przechowywania danych, a także o tym, że badanie może zostać w każdej chwili przerwane. W opinii Generalnego Inspektora ustawa o ochronie danych osobowych porządkując przepływ informacji nakłada jednocześnie szereg ograniczeń służących zachowaniu koniecznej równowagi pomiędzy interesem zarówno osoby przetwarzającej dane osobowe jak i tej, której dane są przetwarzane.

Fundamentalne dla ochrony danych osobowych są dwie zasady: celowości i adekwatności. Zasadę adekwatności należy rozumieć jako obowiązek zachowania równowagi pomiędzy zakresem żądanych informacji, czyli dobrem osoby, której dane dotyczą, a interesem administratora danych. Dopiero jeżeli zostanie zachowana równowaga pomiędzy tymi dobrami będzie można mówić o słusznym interesie administratora danych. Faktem jest, że specyfika ustawowych zadań Inspekcji Celnej wymaga od jej pracowników nienagannej opinii. Ocena przydatności kandydata nie może jednak odbywać się w sposób niezgodny z przepisami prawa. Generalny Inspektor Celny dysponuje jako pracodawca wystarczającymi środkami, które umożliwiają przeprowadzenie prawidłowej selekcji kandydatów. Temu celowi służą przede wszystkim środki przewidziane w ustawie z dnia 24 lipca 1999 r. o Służbie Celnej (Dz. U. Nr 72, poz. 802 z późn. zm.). Wśród nich wystarczy wymienić możliwość zasięgnięcia informacji o karalności, przeprowadzenia przez specjalistę rozmowy kwalifikacyjnej, a ponadto w odniesieniu do funkcjonariuszy możliwość przeprowadzenia w uzasadnionych wypadkach badań psychofizycznych.¹³⁹ Zdaniem Generalnego Inspektora Ochrony Danych Osobowych, zakres informacji zdecydowanie wykracza poza ramy prawem przewidziane. Należy jednocześnie podkreślić, że zgoda osoby, której dane dotyczą nie zawsze jest wystarczającą przesłanką legalności przetwarzania danych. Zgodnie bowiem z art. 28 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. W związku z tym Generalny Inspektor postanowił wszcząć w tej sprawie postępowanie.¹⁴⁰

1.2 Udostępnianie danych osobowych przez Policję, UOP, Urząd Celny, Straż Graniczną i Służbę Więzienną innym podmiotom

¹³⁹ Por. art. 2 i 39 cyt. ustawy o Służbie Celnej.

¹⁴⁰ GI-DIS-30/00/DP-7/00

Generalny Inspektor Ochrony Danych Osobowych podejmował również działania w sprawach dotyczących udostępniania danych osobowych przez organy państwa innym podmiotom.

Zgodnie z art. 7 pkt 2 ustawy o ochronie danych osobowych przetwarzaniem są jakiegokolwiek operacje dokonywane na danych osobowych, a pośród innych wymienionych przykładowo przez ustawodawcę postaci przetwarzania danych osobowych, znajduje się także udostępnianie. Ażeby jednak można było udostępniać dane osobowe innym podmiotom, konieczne jest istnienie jednej z przesłanek określonych w ustawie o ochronie danych osobowych. W odniesieniu do organów państwa przesłanką legalności przetwarzania danych osobowych są odpowiednie uregulowania prawne. W zależności od rodzaju przetwarzanych danych powinny to być przepisy ustawowe lub też przepisy zawarte w aktach prawnych niższej rangi. Administrator danych (w tym wypadku organ przetwarzający dane osobowe) ma również obowiązek zapewnienia, aby dane były zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami.

Do Generalnego Inspektora zwrócił się Naczelnik Wydziału Ruchu Drogowego Biura Koordynacji Służby Prewencyjnej Komendy Głównej Policji z pytaniem, czy dopuszczalne w świetle ustawy o ochronie danych osobowych, jest przekazanie danych osobowych za granicę przez Policję, w sytuacji, gdy zagraniczna firma ubezpieczeniowa zwraca się o udostępnienie adresu, daty urodzenia, numeru PESEL.¹⁴¹ Sprawa dotyczyła przypadku, gdy obywatel Polski został posądzony o spowodowanie kolizji na terenie Polski, w której poszkodowany został obywatel innego państwa - Republiki Czeskiej. Z dokumentów Policji wynikało, że sprawcą zdarzenia był obywatel Czech. W odpowiedzi Generalny Inspektor przypomniał, że możliwość przekazywania danych osobowych z granicę przewiduje art. 47 ustawy o ochronie danych osobowych. Przepis ten wymaga jednak, aby kraj do którego dane mają być przekazane zapewniał danym osobowym ochronę co najmniej równą ochronie przewidzianej w Polsce. Generalny Inspektor uznał jednak, że zastrzeżenie to nie ma zastosowania, gdy przesłanie danych osobowych wynika z obowiązku nałożonego na administratora danych przepisami prawa. Bez względu zatem na poziom ochrony ustanowionej przepisami innego kraju należy dane przekazać, jeżeli przepis polskiego prawa tak stanowi. Takim przepisem jest art. 8a ustawy z dnia 28 lipca 1990 r. o działalności ubezpieczeniowej (Dz. U. 1996 r. Nr 11, poz. 62 z późn. zm.). Nakłada on na organy m.in. Policji obowiązek przekazywania zakładom ubezpieczeń informacji niezbędnych do ustalenia

141 GI-DP-251/99

okoliczności wypadków i okoliczności służących do określenia wysokości odszkodowania. Istotne jest także to, że przepis art. 8a nie odróżnia zakładów krajowych od zagranicznych. Zdaniem Generalnego Inspektora żądanie czeskiego zakładu ubezpieczeń znajduje podstawę w powołanym przepisie ustawy o działalności ubezpieczeniowej.

W sprawie dotyczącej udostępnienia osobom niepowołanym danych osobowych zawartych w notatkach urzędowych przez jednego z komendantów Policji podkreślono, że skoro zainteresowany złożył już zawiadomienie do prokuratury, podejmowanie czynności wyjaśniających przez Generalnego Inspektora byłoby niecelowe.¹⁴²

Generalny Inspektor podjął również postępowanie w związku ze skargą na funkcjonariusza Policji w sprawie udostępnienia danych osobowych osobom nieuprawnionym.¹⁴³ W toku postępowania, stwierdzono, że policjant postępował zgodnie z przepisami prawa. W związku ze złożonym wnioskiem rodziny o wszczęcie poszukiwań, zgodnie z ustawą o Policji podjęte zostały czynności w tej sprawie. Informacje zostały przekazane rodzinie zgodnie z prawem, Generalny Inspektor nie dopatrzył się zatem naruszenia ustawy o ochronie danych osobowych.

Do Generalnego Inspektora Ochrony Danych Osobowych kierowano pytania dotyczące dopuszczalności ujawniania przez Policję danych osobowych nieżyjących dawców zastawek serca do przeszczepów pracownikom Banku Zastawek Serca Kardiochirurgii Instytutu Pediatrii Centrum Zdrowia Dziecka. W odpowiedzi stwierdzono, że ustawa nie reguluje kwestii przetwarzania danych osób zmarłych. Konkluzja taka, choć nie wyrażona wprost, wynika z samej konstrukcji ustawy o ochronie danych osobowych. Ustawa przewiduje bowiem szereg rozwiązań, które mogą dotyczyć tylko osób żyjących (np. prawo wglądu do danych i ich poprawiania, obowiązek informowania osób, których dane dotyczą).¹⁴⁴

Ustawa o ochronie danych osobowych określa prawa osób fizycznych, których dane są lub mogą być przetwarzane w zbiorach danych (art. 2 ust. 1 ustawy).

Generalny Inspektor Ochrony Danych Osobowych otrzymał skargę, w związku z opublikowaniem w prasie artykułu polemicznego zawierającego dane osobowe autora krytykowanego artykułu. W związku z tym, że zamieszczenie w artykule prasowym personaliów wnoszącego skargę nie stanowiło przetwarzania danych osobowych w zbiorze

¹⁴² GI-DIS-185/99

¹⁴³ Zob. DEC/GI/DIS20/99.

¹⁴⁴ GI-DP-224/99; ponadto art. 6 ustawy o ochronie danych osobowych definiuje dane osobowe, jako każdą informację dotyczącą osoby fizycznej, a za osobę fizyczną nie można uznać osoby zmarłej.

danych, Generalny Inspektor nie dopatrył się naruszenia przepisów ustawy o ochronie danych osobowych; dla dochodzenia takich roszczeń właściwa jest droga sądowa.¹⁴⁵

Przepisem, który stanowi podstawę prawną udostępniania danych osobowych przetwarzanych przez organy administracji osobom trzecim jest art. 29 ustawy o ochronie danych osobowych. Przepis ten jest swoistą furtką dla podmiotów, które wiarygodnie uzasadnią potrzebę posiadania danych, a nie mogą wykazać się istnieniem innej przesłanki określonej w ustawie o ochronie danych osobowych.

Do Generalnego Inspektora Ochrony Danych Osobowych wpłynęło pismo od poszkodowanego w związku z zorganizowanymi w styczniu 1999 r. blokadami dróg, który żądał od Policji udostępnienia nazwisk organizatorów oraz rolników biorących udział w blokadach.¹⁴⁶ Poszkodowany zamierzał wystąpić na drogę sądową przeciwko tym osobom. Niektóre jednostki Policji powołując się na ustawę o ochronie danych osobowych odmawiały udostępnienia takich informacji. Osoba wnioskująca o udostępnienie danych uzyskała jednak potrzebne informacje od komendanta miejskiego. Wspomnianemu komendantowi, postawiono jednak zarzut popełnienia przestępstwa określonego w art. 51 ust. 1 ustawy o ochronie danych osobowych. Generalny Inspektor uznał, że z § 2 art. 29 ustawy o ochronie danych osobowych wynika, iż udostępnienie danych w celu innym niż włączenie do zbioru może nastąpić również w sytuacji, gdy osoby nie są wprawdzie uprawnione wprost przepisami prawa do posiadania danych, jednakże w sposób wiarygodny uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą. Zgodnie z przepisami ustawy o ochronie danych osobowych, dane udostępnia się na pisemny umotywowany wniosek, który powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie. Administratorem danych w takich przypadkach jest Policja, z mocy prawa uprawniona do przetwarzania danych osobowych. Wprawdzie art. 29 nie nakłada obowiązku udostępnienia danych przez Policję, daje jednak uprawnienie do takiego udostępnienia. Odmowa zatem udostępnienia danych, uzasadniona brakiem oparcia w przepisach ustawy o ochronie danych osobowych stanowi, zdaniem Generalnego Inspektora, nadinterpretację. Generalny Inspektor zwrócił się także z pismem do Ministra Spraw Wewnętrznych i Administracji z prośbą o przekazanie powyższych uwag podwładnym funkcjonariuszom oraz o stosowną pomoc.¹⁴⁷ Stosownej treści pismo wysłane zostało również do prokuratora

¹⁴⁵ GI-DP-1631/99; w artykule krytykowane były pewne osoby, funkcjonariusze Policji.

¹⁴⁶ GI-DP-406/99

¹⁴⁷ Zob. pismo z dnia 2 lipca 1999 r., znak: GI/687/99.

prowadzącego postępowanie w sprawie popełnienia przestępstwa przez komendanta miejskiego Policji.

Podobny problem został Generalnemu Inspektorowi zasygnalizowany przez osoby poszkodowane w wypadkach komunikacyjnych. Osoby te zwracają się do Policji o udostępnienie danych sprawców kolizji lub wypadków drogowych. Policja odmawia jednak podawania takich informacji powołując się na ustawę o ochronie danych osobowych.¹⁴⁸

Od osadzonego w zakładzie karnym wpłynęło pismo z prośbą o interwencję. W sprawie tej miało dojść do udostępnienia akt osobopoznawczych osadzonego i karty widzeń osobie niepowołanej. Po uzyskaniu wyjaśnień od dyrektora zakładu karnego, osoby, której rzekomo udostępniono akta, oraz kierownika działu ochrony zakładu karnego, Generalny Inspektor, wobec braku dowodów świadczących o udostępnieniu przedmiotowych danych osobowych uznał skargę za bezzasadną.¹⁴⁹

Ustawa z dnia 9 stycznia 1997 r. Kodeks celny (Dz. U. Nr 23, poz. 117 z późn. zm.) w art. 257 określa zasady prowadzenia listy agentów celnych. Lista ta zawierająca m.in. dane osobowe osób fizycznych prowadzona jest przez Prezesa Głównego Urzędu Ceł. Art. 258 kodeksu celnego określa natomiast tryb wydawania koncesji na prowadzenie agencji celnej. Koncesję wydaje i cofa Prezes Głównego Urzędu Ceł. Do Generalnego Inspektora zwróciło się Ogólnopolskie Zrzeszenie Agencji Celných ze skargą na odmowę udostępnienia przez Prezesa Głównego Urzędu Ceł wykazu podmiotów gospodarczych, które posiadają koncesję na prowadzenie działalności w formie agencji celnej. Dane te nie zostały Zrzeszeniu udostępnione, co umotywowano koniecznością przestrzegania ustawy o ochronie danych osobowych. Podkreślono również, że przepisy prawa celnego nie przewidują publikacji listy, bądź udostępniania jej w jakiegokolwiek formie. Ponadto uzasadniano, że zgodnie z § 16 ust. 3 rozporządzenia Ministra Finansów z dnia 10 grudnia 1997 r. w sprawie agencji celnych i agentów celnych (Dz. U. Nr 154, poz. 1008) wpis na listę agentów celnych dokonywany jest w drodze decyzji administracyjnej, a wpisana osoba fizyczna otrzymuje kopię decyzji, którą może w razie wątpliwości okazać. Generalny Inspektor zgodził się z argumentacją Prezesa GUC, podkreślając równocześnie, że ustawa o ochronie danych osobowych określa prawa wyłącznie osób fizycznych, a nie podmiotów gospodarczych.¹⁵⁰

148 GI-DP-1568/99

149 GI-DIS-297/99

150 GI-DP-197/99

II. Obowiązki administratorów danych

Ustawa o ochronie danych osobowych nakłada na administratorów danych liczne obowiązki. Wśród najważniejszych wymienić należy obowiązek dołożenia staranności, aby zakres zbieranych danych był zgodny z celem zbierania danych (art. 26 ust. 1 pkt 2), obowiązek właściwego zabezpieczenia danych osobowych (art. 36 i nast.), obowiązek informacyjny wobec osoby, której dotyczą dane i inne.

Do Generalnego Inspektora zgłaszano wątpliwości, czy pracodawca przekazując dane osobowe pracowników Policji obowiązany jest powiadomić ich o tym fakcie. W odpowiedzi stwierdzono, że w myśl art. 34 ustawy o ochronie danych osobowych w sprawach informowania osoby, której dane dotyczą stosuje się przepisy art. 30. Zgodnie zatem z art. 30 administrator odmawia poinformowania osoby, której dane są zbierane o ich udostępnieniu, jeżeli spowodowałoby to zagrożenie m.in. dla życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego. W omawianej sprawie okoliczności stanu faktycznego¹⁵¹ uzasadniały, w opinii Generalnego Inspektora, zaniechanie przez pracodawcę poinformowania pracowników o fakcie udostępnienia ich danych organom Policji.

Przedmiotem innego pisma było pytanie o to, czy organy celne mają obowiązek informowania osób, których dane dotyczą o fakcie przetwarzania ich danych osobowych. Generalny Inspektor odpowiedział, że art. 24 ust. 1 ustawy o ochronie danych osobowych nakłada na administratorów danych obowiązek informacji, obowiązek ten nie istnieje jednak, jeżeli ustawa zezwala na przetwarzanie danych bez ujawnienia faktycznego celu ich zbierania. W związku z tym organy celne mają obowiązek informowania osób, których dane przetwarzają w związku z wykonywaniem swoich ustawowych zadań. Ponadto podkreślono, że administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą.¹⁵²

W piśmie z dnia 17 marca 1999 r. Główny Urząd Ceł wyraził wątpliwości dotyczące ochrony danych osobowych w związku z kierowaniem do zagranicznych administracji celnych wniosków o pomoc lub realizacją takich wniosków otrzymywanych od zagranicznych administracji celnych.¹⁵³

Jak wyjaśniono, umowy dwustronne o współpracy i pomocy wzajemnej w sprawach celnych (o charakterze państwowym lub rządowym), realizowane są przez administracje celne

¹⁵¹ Działania Policji miały na celu zapewnienie bezpieczeństwa Papieżowi Janowi Pawłowi II, w czasie jego wizyty w Polsce w 1999 r.

¹⁵² GI-DP-383/99

¹⁵³ GI-DP-233/99

państw-stron w sprawach, w których toczy się postępowanie celne, karne skarbowe lub wyjaśniające. W ramach tych postępowań administracje celne przekazują sobie nawzajem m.in. decyzje wymiarowe, postanowienia o wszczęciu lub umorzeniu postępowania lub na skutek prośby o dokonanie konkretnych ustaleń, zebrania informacji i wyjaśnień mogących pomóc w prowadzeniu postępowania. W odpowiedzi Generalny Inspektor wskazał, że przepisów ustawy o ochronie danych osobowych nie stosuje się, jeżeli umowa międzynarodowa, której stroną jest Rzeczpospolita Polska, stanowi inaczej.¹⁵⁴

Wiele kontrowersji dotyczyło ujawnianie danych osobowych zawartych w protokole przesłuchania świadka osobie podejrzanej o popełnienie przestępstwa. Odpowiadając Generalny Inspektor stwierdził, że żądanie przez Policję podania danych, które mają znaleźć się w protokole przesłuchania, znajduje uzasadnienie w przepisach prawa. Stosownie do art. 191 ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (Dz. U. Nr 89, poz. 555 z późn. zm.) przesłuchanie świadka rozpoczyna się od zapytania o imię, nazwisko, wiek, zatrudnienie, miejsce zamieszkania, karalność za fałszywe zeznanie oraz stosunek do stron. Z chwilą złożenia zawiadomienia o przestępstwie także pokrzywdzony zaczyna podlegać normom regulującym postępowanie karne. Kodeks postępowania karnego przewiduje m.in., że akta sprawy (w tym również dane osoby pokrzywdzonego) będą udostępniane osobie podejrzanej. Jednocześnie kodeks postępowania karnego zawiera przepisy pozwalające świadkowi na nie ujawnianie jego tożsamości lub konkretnych danych osobowych (np. art. 191 § 3, art. 184 k.p.k.).¹⁵⁵

Zgodnie z art. 26 ust. 1 pkt 3 administrator powinien zapewnić, aby zbierane dane były merytorycznie poprawne.¹⁵⁶ Obowiązek ten dotyczy również organów prowadzących postępowanie karne. W postępowaniu karnym obowiązek ten występuje w nieco zmodyfikowanej formie. W toku postępowania przygotowawczego organ prowadzący zbiera wszelkie dowody mogące przyczynić się do wyjaśnienia istotnych okoliczności sprawy. Stosownie do art. 2 § 2 k.p.k. podstawę wszelkich rozstrzygnięć powinny stanowić prawdziwe ustalenia faktyczne. Oceny jednakże poszczególnych dowodów może dokonywać organ procesowy. Przyjęcie stanowiska, że jakakolwiek nieprawdziwa informacja o charakterze osobowym, dotycząca podejrzanego zawarta w aktach postępowania przygotowawczego stanowi naruszenie ustawy o ochronie danych osobowych, prowadziłoby

¹⁵⁴ Zob. art. 4 cyt. ustawy.

¹⁵⁵ GI-DP-1613/99

¹⁵⁶ Jest to jeden z najważniejszych przepisów ustawy ustanawiający tzw. zasadę merytorycznej poprawności danych osobowych przetwarzanych w zbiorach.

do sytuacji, że funkcje stron procesowych musiałyby przejąć Generalny Inspektor Ochrony Danych Osobowych. Prowadziłoby to, w opinii Generalnego Inspektora, do przejęcia przez organ niesądowy funkcji wymiaru sprawiedliwości.¹⁵⁷

III. Inne zagadnienia

Wśród grupy spraw, które napłynęły do Generalnego Inspektora Ochrony Danych Osobowych na uwagę zasługuje m.in. indywidualna skarga osoby warunkowo zwolnionej z zakładu karnego. Przedmiotem tej skargi było naruszanie przez administrację zakładu tajemnicy korespondencji poprzez wprowadzenie cenzury listów otrzymywanych i wysyłanych przez osadzonych. Podstawowym prawem każdego obywatela gwarantowanym w przepisach ustawy zasadniczej jest wolność i tajemnica komunikowania się. Prawo to zgodnie z art. 49 może ulec ograniczeniu w przypadkach określonych w ustawie i w sposób w niej określony. Generalny Inspektor zwrócił uwagę, że stosownie do art. 105 § 4 kodeksu karnego wykonawczego, dyrektor zakładu karnego ma prawo podejmowania decyzji dotyczących zatrzymania lub cenzurowania korespondencji, jeżeli wymagają tego względy bezpieczeństwa zakładu, informując o tym sędziego penitencjarnego oraz skazanego. Generalny Inspektor uznał, że jest niewłaściwy do rozstrzygania kwestii zaginięcia oraz cenzury korespondencji w zakładach karnych.¹⁵⁸

W odpowiedzi na indywidualną skargę odnoszącą się do niezasadnego, zdaniem wnoszącego skargę, skierowania na badania psychiatryczne, Generalny Inspektor uznał, że rozpatrzenie tej kwestii nie leży w jego kompetencji. Jednocześnie poinformowano o sposobie uregulowania tego zagadnienia przez przepisy kodeksu postępowania karnego. Osoba ta ponownie zwróciła się o rozpatrzenie skargi, Generalny Inspektor podtrzymał jednak swoje poprzednie stanowisko.¹⁵⁹

W związku z pismem, które wpłynęło do Biura Generalnego Inspektora Ochrony Danych Osobowych, dotyczącym opinii wydanej przez komendanta komisariatu Policji, Generalny Inspektor stwierdził, że nie jest organem właściwym do oceny zasadności wydanej opinii, ponadto ewentualne sporządzenie nieprawdziwej opinii nie stanowi naruszenia ustawy o ochronie danych osobowych.¹⁶⁰

¹⁵⁷ GI-DP-755/99

¹⁵⁸ GI-DIS-182/99; warto przy okazji tej sprawy zauważyć, że nie zachodzi tu sytuacja przetwarzania danych osobowych w zbiorze, co jest warunkiem powołania się na ustawę o ochronie danych osobowych przez osoby fizyczne.

¹⁵⁹ GI-DIS-221/99

¹⁶⁰ GI-DP-242/99, w sprawie tej Generalny Inspektor wyraził również zdanie, że przepisy ustawy nie mają zastosowania do sytuacji, które miały miejsce przed tą datą.

D. Sądy, prokuratura i kolegia do spraw wykroczeń

I. Zagadnienia wstępne

W 1999 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło wiele skarg i zapytań prawnych, dotyczących przetwarzania danych osobowych przez organy sądowe, prokuratury i kolegia do spraw wykroczeń. Zgodnie z art. 7 Konstytucji organy władzy publicznej mogą działać tylko na podstawie prawa. Przepisy prawa muszą więc określać zakres działań, zadania i tryb postępowania konkretnych organów. Przesłanki legalności przetwarzania danych określa 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.), zgodnie z którym przetwarzanie danych jest dopuszczalne, jeżeli zezwala na to przepis prawa.

Kompetencje sądów, prokuratury oraz kolegiów d/s wykroczeń uregulowane zostały w kodeksach określających przepisy proceduralne i materialne poszczególnych dziedzin prawa, 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. regulaminie wewnętrznym 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.), ustawie z dnia 6 kwietnia 1990 r. o Policji (Dz. U. Nr 30, poz. 179 z późn. zm.).

II. Przetwarzanie danych osobowych przez sądy, prokuraturę i kolegia ds. wykroczeń

II.1 Zakres i podstawy przetwarzania danych osobowych przez sądy

W 1999 r. Generalny Inspektor Ochrony Danych Osobowych otrzymał wiele skarg dotyczących legalności wykorzystywania w toczącym się procesie karnym danych osobowych stron i uczestników postępowania oraz zapytań o ich zakres. Zapytujący - najczęściej osoby pokrzywdzone w sprawie i świadkowie - wyrażali obawę, iż udostępnienie własnych danych osobowych, zawartych w aktach sądowych - zagraża ich żywotnym interesom i tym samym narusza ustawę o ochronie danych osobowych.

Szczególnie wiele skarg kierowali do Generalnego Inspektora przesłuchiwani w charakterze świadka. Przedmiotem większości z nich było bezprawne, zdaniem skarżących, ujawnienie danych osobowych w trakcie przesłuchania na rozprawie sądowej. W odpowiedzi na powyższe wątpliwości Generalny Inspektor zwrócił uwagę skarżących na przepisy

kodeksu postępowania karnego, zgodnie z którymi sędzia prowadzący postępowanie sądowe jest upoważniony do uzyskania w ramach przesłuchania, takich danych świadka jak: imię, nazwisko, wiek, zajęcie, miejsce zamieszkania, karalność za fałszywe zeznanie lub oskarżenie oraz stosunek do stron (art. 191 § 1). Zgodnie z art. 355 kodeksu postępowania karnego rozprawa główna odbywa się jawnie. Ograniczenia jawności określa ustawa. Jedynie w przypadku, gdy zachodzi uzasadniona obawa niebezpieczeństwa dla życia świadka, jego zdrowia, wolności albo mienia w znacznych rozmiarach, albo osoby dla niego najbliższej, sąd może wydać postanowienie o zachowaniu w tajemnicy danych osobowych świadka (art. 184 § 1 kodeksu postępowania karnego). Dane dotyczące miejsca zamieszkania świadka sąd zastrzega wówczas wyłącznie do swojej wiadomości, zaś doręczenia pism procesowych dokonuje się na adres instytucji, w której świadek jest zatrudniony, lub na inny wskazany przez niego adres (art. 191 § 3 kodeksu postępowania karnego).¹⁶¹ Organy postępowania kształtują swe przekonania na podstawie wszystkich przeprowadzonych dowodów, ocenianych swobodnie z uwzględnieniem zasad prawidłowego rozumowania oraz wskazań wiedzy i doświadczenia życiowego (art. 7 kodeksu postępowania karnego). Przewodniczący składu sędziowskiego kieruje rozprawą i czuwa nad jej prawidłowym przebiegiem, bacząc, aby zostały wyjaśnione wszystkie istotne okoliczności sprawy, a w miarę możliwości także okoliczności sprzyjające popełnieniu przestępstwa. Swobodna ocena dowodów odnosi się do wyboru określonych środków dowodowych i do sposobu ich przeprowadzenia. Mają być one oceniane rzetelnie i w związku z całym materiałem dowodowym. Powyższe przepisy w ocenie Generalnego Inspektora, zgodnie z art. 23 ust. 1 ustawy o ochronie danych osobowych, stanowią wystarczającą przesłankę zasadności i legalności przetwarzania danych osobowych świadków przez sądy. Jednocześnie Generalny Inspektor nie uznał się właściwym do dokonania oceny prawidłowości dopuszczenia bądź niedopuszczenia wniosków dowodowych oraz do oceny prawidłowości rozstrzygnięcia merytorycznego i treści uzasadnienia wyroku lub postanowienia (o co wnioskowali skarżący), kwestie te pozostawiając do wyłącznej kompetencji sądu.¹⁶²

Ponadto Generalny Inspektor otrzymał zapytania, odnoszące się do zgodności z ustawą o ochronie danych osobowych procedury ujawniania danych stron we wniosku o zwolnienie z kosztów sądowych. Odpowiadając Generalny Inspektor poinformował, że zgodnie z art. 113 § 1 kodeksu postępowania cywilnego zwolnienia z kosztów sądowych domagać się może osoba fizyczna, która złoży oświadczenie, że nie jest w stanie ponieść ich

¹⁶¹ Por. GI-DIS-33/99/229, GI-DIS-45/99/196/197, GI-DIS-281/99/751.

ciężaru bez uszczerbku dla utrzymania koniecznego dla siebie i rodziny. Oświadczenie powinno obejmować dokładne dane o stanie rodzinnym, majątku i dochodach. Od sądu zależy uznanie tego oświadczenia za dostateczne do zwolnienia od kosztów sądowych. Niezbędne jest więc przedstawienie sądowi takich danych, które umożliwią mu ocenę, czy strona jest w stanie ponieść koszty sądowe.¹⁶³ Powyższe żądanie wypełnia przesłankę określoną w art. 23 ust 1 pkt. 2 ustawy o ochronie danych osobowych i tym samym nie stoi z nią w sprzeczności.

Szczególnie duża liczba pism kierowanych do Generalnego Inspektora dotyczyła zasadności udostępniania przez sądy akt spraw - zawierających niejednokrotnie dane wrażliwe - stronom w postępowaniu procesowym, uczestnikom postępowania w postępowaniu nieprocesowym oraz ich pełnomocnikom. Ustawa o ochronie danych osobowych w art. 27 ust 1 definiuje zakaz przetwarzania danych wrażliwych, 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. Jednocześnie ust. 2 art. 27 ustawy, dopuszcza przetwarzanie przedmiotowych danych, w przypadku wystąpienia którejkolwiek z wymienionych w nim przesłanek, 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. Zgodnie z art. 9 kodeksu postępowania cywilnego rozpoznanie spraw odbywa się jawnie, chyba że przepis szczególny stanowi inaczej. Strony i uczestnicy postępowania mają prawo przeglądać akta sprawy i otrzymywać odpisy lub wyciągi z tych akt. „(...) strony i uczestnicy postępowania mają zawsze prawo do przeglądania akt sprawy oraz do otrzymywania wyciągów z tych akt. Nawet zatem wówczas, gdy rozpatrywanie sprawy następuje na posiedzeniu niejawnym, akta sprawy są zawsze jawne – dostępne dla uczestników postępowania, to znaczy że mogą oni przeglądać je w sekretariacie sądu i otrzymywać wyciągi z tych akt. Poza stronami i uczestnikami postępowania inne podmioty nie mają wglądu do akt sprawy”.¹⁶⁴

Indywidualne skargi dotyczyły naruszenia przez sądy ustawy o ochronie danych osobowych, poprzez udostępnienie danych innym podmiotom, niż strony i uczestnicy postępowania (np. Kasie Rolniczego Ubezpieczenia Społecznego), danych osobowych

162Por. GI-DIS-71/99/228, GI-DIS-170/99/524, GI-DIS-176/99/544, GI-DIS-356/99/1072.

163 GI-DP-162/99/57

164 T. Ereciński, J. Gudowski, M. Jędrzejewska: Komentarz do kodeksu postępowania cywilnego, Wydawnictwo Prawnicze, Warszawa 1997 r. s. 51; por. GI-DIS-33/99/229, GI-DIS-36/99/194, GI-DIS-172/99/501, GI-DP-432/99/486.

zawartych w księdze wieczystej. Generalny Inspektor Ochrony Danych Osobowych poinformował skarżących, że zgodnie z brzmieniem art. 2 ustawy z dnia 6 lipca 1982 r. o księgach wieczystych i hipotece (Dz. U. Nr 19, poz. 147 z późn. zm.) księgi wieczyste są jawne, w związku z czym nie istnieje możliwość prawnie wiążącego zastrzeżenia o nieudostępnieniu danych zawartych w księgach wieczystych. Oznacza to, że dostęp do zawartych w księdze wieczystej informacji posiada każdy zainteresowany.¹⁶⁵

W okresie sprawozdawczym do Generalnego Inspektora wpływały również pisma od sądów, w których zwracano się o zajęcie stanowiska, czy w świetle uregulowań ustawy o ochronie danych osobowych, dopuszczalna jest praktyka udostępniania całości akt sprawy karnej zakładom ubezpieczeń społecznych po uprawomocnieniu się orzeczenia sądowego, jak i przed nadaniem mu prawomocności w związku z toczącym się postępowaniem odszkodowawczym. Generalny Inspektor odpowiadając zwrócił uwagę, iż w postępowaniu karnym, zgodnie z treścią art. 156 § 1 kodeksu postępowania karnego, akta postępowania sądowego udostępnia się stronom, obrońcom, pełnomocnikom, przedstawicielom ustawowym, a za zgodą prezesa także innym osobom. Prawo zapoznania się treścią akt sprawy karnej przysługuje nie tylko bezpośrednim uczestnikom postępowania i ich pełnomocnikom. Niekiedy bowiem przepis szczególny nakłada na sądy obowiązek ujawnienia informacji o przebiegu i rozstrzygnięciu końcowego procesu innym podmiotom. I tak, art. 8a ustawy o działalności ubezpieczeniowej (Dz. U. z 1996 r. Nr 11 poz. 62 z późn. zm.) zobowiązuje sądy, organy prokuratury, Policję oraz inne organy i instytucje ustalające okoliczności wypadków i zdarzeń do udzielania informacji oraz udostępniania materiałów niezbędnych do ustalania okoliczności tych wypadków i zdarzeń oraz do określenia wysokości odszkodowania lub świadczenia na wniosek zakładu ubezpieczeń lub Ubezpieczeniowego Funduszu Gwarancyjnego. W świetle powyższego przepisu udostępnianie akt sprawy karnej w zakresie adekwatnym do potrzeb prowadzonego przez zakład ubezpieczeń postępowania odszkodowawczego, wypełnia przesłanki określone w art. 23 i art. 27 ustawy o ochronie danych osobowych.¹⁶⁶

Osobna problematyka spraw dotyczyła podstaw prawnych udostępniania przez sąd akt spraw na żądanie innego sądu. W ocenie skarżących udostępnienie w trakcie toczącej się sprawy cywilnej o alimenty, akt sprawy karnej, gdzie znajdują się informacje dotyczące skazania, lub skazania, które w myśl przepisów prawa uległo już zatarciu, stanowi czyn bezprawny. Generalny Inspektor po wnikliwym rozpatrzeniu sprawy i zasięgnięciu informacji

¹⁶⁵ GI-DIS-120/99/331/467

u wiceprezesa Sądu Okręgowego nie dopatrył się naruszenia przepisów ustawy o ochronie danych osobowych i jednocześnie zwrócił uwagę na orzecznictwo Sądu Najwyższego (OSN 1974, Nr 12, poz. 203), zgodnie z którym akta innej sprawy stanowią źródło wiadomości dla stron i sądu; dowody przeprowadzone w innej sprawie mogą być wykorzystane jako materiał pomocniczy przy ocenie wiarygodności i mocy dowodów przeprowadzonych bezpośrednio przed sądem. Objęta dyspozycją art. 233 kodeksu postępowania cywilnego zasada swobodnej oceny dowodów oznacza, iż niezbędnym w trakcie toczącego się postępowania jest dokonanie ustaleń faktycznych zgodnych z rzeczywistym stanem rzeczy. Dlatego też sąd w trakcie toczącego się postępowania ma prawo dopuścić, zgodnie z art. 232 kodeksu postępowania cywilnego, każdy dowód, który uzna za konieczny w celu wyjaśnienia wszystkich okoliczności sprawy.¹⁶⁷

Odrębna grupa spraw dotyczyła zasadności udostępnienia sądom danych osobowych przez inne organy. Przedmiotem skarg była m.in. kwestia udostępnienia przez Zakład Ubezpieczeń Społecznych danych osobowych osób w związku z toczącym się postępowaniem karnym lub cywilnym. Generalny Inspektor nie dopatrył się w tym zakresie uchybień. Zgodnie bowiem z art. 15 § 2 kodeksu postępowania karnego wszystkie instytucje państwowe i społeczne są zobowiązane, w zakresie swego działania, do udzielania pomocy organom prowadzącym postępowanie karne. Oznacza to, iż np. sądy, prokuratura czy Policja, jako organy prowadzące postępowanie karne posiadają upoważnienie ustawowe do żądania udzielenia informacji o osobach, jeżeli posiadanie informacji jest niezbędne dla potrzeb prowadzonego postępowania. Zgodnie z art. 248 § 1 kodeksu postępowania cywilnego każdy jest obowiązany 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. Przewodniczący sądu może, w myśl art. 208 kodeksu postępowania cywilnego, zażądać na rozprawę od państwowej jednostki organizacyjnej lub jednostki samorządu terytorialnego znajdujących się u nich dowodów, jeżeli strona sama dowodów otrzymać nie może. A zatem, Zakład Ubezpieczeń Społecznych jako państwowa jednostka organizacyjna, udostępniając bez zgody skarżących ich dane osobowe sądom lub prokuratorom, działa zgodnie z przepisami prawa. Natomiast, udostępnianie przez ZUS danych wrażliwych innym jednostkom lub osobom bez

166 GI-DP-15/99/192, GI-DP-683/99/715

167 GI-DIS-69/99/352, GI-DIS-176/99/544

zgody wnoszących skargę, jest dopuszczalne tylko na zasadach wyszczególnionych w art. 27 ust. 2 ustawy o ochronie danych osobowych.¹⁶⁸

Innym problemem, który pojawił się w napływających do Biura zapytaniach, była kwestia 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. Stosowanie bowiem dotychczasowego wzoru druku „Potwierdzenia odbioru” nie znajduje 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 w druku „Potwierdzenie odbioru” informacji o rodzaju przesyłanego pisma nie jest niezbędne do doręczenia przesyłki. Według Generalnego Inspektora umieszczanie danych o rodzaju pisma niewątpliwie narusza prywatność osoby, do której kierowana jest przesyłka, a w przypadku przesyłania pism zawierających informacje o wyniku postępowania stanowić będzie naruszenie ustawy o ochronie danych osobowych. W związku z powyższym Generalny Inspektor Ochrony Danych Osobowych w piśmie z dnia 1 czerwca 1999 r., zwrócił się do Ministra Sprawiedliwości z prośbą o spowodowanie zmiany opisanej praktyki, poprzez wycofanie z użytku druku „Potwierdzenia odbioru”, wprowadzonego pismem Ministerstwa Sprawiedliwości z dnia 21 lipca 1997 r.¹⁶⁹ i zastąpienie go drukiem, w treści którego nie będzie zawarta informacja o rodzaju przesyłanego pisma. Na skutek tej interwencji Ministerstwo Sprawiedliwości uznało za niedopuszczalne zamieszczanie na kopertach adresowanych do obywateli jakichkolwiek innych, poza sygnaturą akt sprawy, oznaczeń wysyłanej korespondencji i poleciło prezesom wszystkich sądów zmianę dotychczasowej praktyki oznaczania korespondencji.¹⁷⁰ 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).

¹⁶⁸ GI-DIS-84/99/242, GI-DP-237/99/352

¹⁶⁹ Sygn. L.Dz.O.I.0133/82/96.

¹⁷⁰ GI-DIS-226/99/617, GI/558/99, GI-DIS-241/99/631, O.I.0133/18/99

Odrębnym zagadnieniem rozpatrywanym przez Generalnego Inspektora Ochrony Danych Osobowych w omawianym roku sprawozdawczym była kwestia przetwarzania danych dotyczących m.in. skazań i orzeczeń wydanych w postępowaniu sądowym. Wejście w życie ustawy o ochronie danych osobowych uregulowało przedmiotową kwestię w art. 28, zgodnie z którym przetwarzanie danych dotyczących skazań, orzeczeń o ukaraniu, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym można prowadzić wyłącznie na podstawie ustawy. Do Generalnego Inspektora wpłynęły skargi dotyczące przetwarzania danych osobowych skarżącego w postaci udostępniania przez sądy innym podmiotom, informacji o skazaniu, które z mocy prawa uległo już zatarciu.

Generalny Inspektor na podstawie art. 61 § 1 kodeksu postępowania administracyjnego wszczął postępowanie administracyjne, w wyniku którego ustalono, iż na żądanie przedstawiciela administracji rządowej Prezes Sądu Rejonowego udostępnił z archiwum sądu, informacje o treści zapadłego w sprawie orzeczenia, tj. o fakcie wydania wyroku, na podstawie którego skarżącemu warunkowo umorzono postępowanie karne wyznaczając okres próby na jeden rok. Skarżący, w korespondencji skierowanej do Prezesa Sądu Rejonowego, zawarł swój sprzeciw co do przetwarzania informacji na temat jego karalności z pominięciem Centralnego Rejestru Skazanych, wskazując na fakt, iż jego skazanie uległo zatarciu z mocy prawa. W odpowiedzi na powyższe, Prezes sądu wskazał przepisy ustawy o ochronie danych osobowych i kodeksu postępowania karnego uprawniające do udostępniania organowi państwowemu informacji o przebiegu postępowania karnego, a nawet udostępniania akt sprawy innym podmiotom. Generalny Inspektor po przeanalizowaniu przedmiotowej sprawy nie podzielił powyższego stanowiska, uznając, iż zarówno Prezes Sądu Rejonowego, jak i podmiot zwracający się o udostępnienie przedmiotowych danych nie mieli upoważnienia ustawowego do przetwarzania danych osobowych dotyczących treści orzeczenia wydanego w postępowaniu sądowym. Pismem z dnia 30 października 1998 r. Generalny Inspektor Ochrony Danych Osobowych złożył zawiadomienie o popełnieniu przestępstwa przez wyżej wymienione podmioty.¹⁷¹

Następnie, w drugim postępowaniu administracyjnym ustalono, iż na żądanie Izby Notarialnej Sąd Rejonowy udostępnił dane osobowe skarżącego w postaci odpisu wyroku o skazaniu, które z mocy prawa uległo już zatarciu. Działanie powyższe miało bezpośredni wpływ na negatywne zaopiniowanie kandydatury skarżącego na stanowisko notariusza. Zgodnie z ustawą z dnia 14 lutego 1991 r. Prawo o notariacie (Dz. U. Nr 22, poz. 91)

171 GI-366/98

notariuszem może być ten, kto jest nieskazitelnego charakteru (art. 11). W ocenie Generalnego Inspektora pojęcie „nieskazitelnego charakteru” nie jest pojęciem równoznacznym z określeniem „nie karany”, zaś art. 11 Prawa o notariacie nie stanowi upoważnienia ustawowego dla Izby Notarialnej do żądania informacji o karalności zarówno od wnioskodawcy, jak również do kierowania zapytania o karalność do organu innego, niż Centralny Rejestr Skazanych. Zdaniem Generalnego Inspektora nie istnieje również podstawa prawna do udostępnienia przez sąd informacji o zatartym skazaniu. Obaj sędziowie udostępniając dane o karalności powoływali się na uprawnienie do udzielenia informacji wynikające z treści art. 156 § 1 kodeksu postępowania karnego. Podkreślenia wymaga jednak okoliczność, iż przepis ten dotyczy wyłącznie czynności procesowych i nie może być podstawą do ujawniania danych po zakończeniu procesu karnego.

Z konstytucyjnej zasady niezawisłości sędziowskiej wynika, że sędziowie w sprawowaniu swojego urzędu są niezawisli i podlegają tylko Konstytucji oraz ustawom. Oznacza to, iż zobowiązani są również do przestrzegania zasad wynikających z ustawy o ochronie danych osobowych. Zgodnie z cytowanym już artykułem 28 ustawy, przetwarzanie danych o skazaniu może odbywać się wyłącznie na podstawie aktu prawnego o randze ustawy. W polskim systemie prawnym nie istnieje przepis, który upoważniałby jakikolwiek podmiot do udzielania informacji o skazaniu, które uległo zatarciu. Przepisy art. 106 i nast. kodeksu karnego szczegółowo regulują zasadę zatarcia skazania i skutki, jakie te normy wywołują. Intencją wprowadzenia przepisów dotyczących zatarcia skazania było to, aby umożliwić powrót do normalnego życia osobie, która wprawdzie popełniła przestępstwo, ale odbyła karę i przez określony w ustawie czas przestrzegała porządku prawnego. Fakt odbycia kary uznać należy za zadośćuczynienie społeczeństwu z powodu naruszenia ogólnie przyjętych zasad postępowania. Nie można karać osoby przez całe życie i w każdej sytuacji wypominać kiedyś popełniony błąd. Ustawodawca wprowadzając różny czas, jakiego upływ jest niezbędny do zatarcia skazania, uwzględnił rodzaj czynu i jego stopień społecznej szkodliwości. Jednocześnie uznał, iż nie istnieją odrębne kategorie sprawców lub czynów, których popełnienie wyłączałoby możliwość zastosowania instytucji zatarcia skazania. Oznacza to, iż każdy ma prawo oczekiwać, iż po upływie określonego czasu będzie uznawany za nie karanego. Zgodnie ze stanowiskiem doktryny uznanie skazania za niebyłe przywraca skazanemu status nie karanego, dlatego może on twierdzić wobec władz i urzędów, że nie był skazany.¹⁷² Zatem w ocenie Generalnego Inspektora, działanie sędziów polegające na

¹⁷² K. Buchała, A. Zoll: Komentarz do kodeksu karnego, Zakamycze 1998 r.

udostępnianiu informacji o skazaniach, które z mocy prawa uległy zatarciu zasługuje na szczególnie negatywną opinię. W stosunku do osób wykonujących zawód sędziego norma działania zgodnego z prawem jest nie tylko standardem, ale ma szczególne znaczenie dla ich oceny, jako osób sprawujących wymiar sprawiedliwości w Rzeczypospolitej Polskiej. Uwzględniając autorytet i prestiż, jakim się cieszą sędziowie, należy stwierdzić, iż w stosunku do nich oczekiwania działania zgodnego z prawem są największe. Zatem szczególnie krytycznie i nagannie należy ocenić działania sędziów polegające na udostępnieniu informacji o skazaniach, które z mocy prawa uległy zatarciu, jako działania sprzeczne z prawem. Takie postępowanie w ocenie Generalnego Inspektora Ochrony Danych Osobowych daje podstawy do wszczęcia postępowania dyscyplinarnego, co zasygnalizowano w wystąpieniu Generalnego Inspektora do Ministra Sprawiedliwości z dnia 23 lipca 1999 roku.¹⁷³

Mając powyższe na uwadze, Generalny Inspektor Ochrony Danych Osobowych wydał decyzję nakazującą usunięcie danych osobowych dotyczących karalności skarżącego z jego akt osobowych znajdujących się w Izbie Notarialnej.¹⁷⁴

Do Generalnego Inspektora wpłynęła ponadto skarga, dotycząca udostępniania danych osobowych prasie przez Sąd Lustracyjny.

Skarżącemu wyjaśniono, iż zgodnie z art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych, przetwarzanie danych jest dopuszczalne wtedy, gdy zezwalają na to przepisy prawa. Podstawą prawną przetwarzania danych przez dziennikarza jest ustawa z dnia 26 stycznia 1984 r. Prawo prasowe (Dz. U. Nr 5, poz. 24). W myśl art. 12 ust. 1 pkt 2 ustawy Prawo prasowe, dziennikarz jest obowiązany chronić dobra osobiste, a ponadto interesy działających w dobrej wierze informatorów i innych osób, które okazują mu zaufanie. Na podstawie art. 14 ust. 6 cytowanej ustawy nie wolno bez zgody zainteresowanej osoby publikować informacji oraz danych dotyczących prywatnej sfery życia, chyba że wiąże się to bezpośrednio z działalnością publiczną danej osoby. Natomiast w myśl art. 3 ust. 1 ustawy z dnia 11 kwietnia 1997 r. o ujawnieniu pracy lub służby w organach bezpieczeństwa państwa lub współpracy z nimi w latach 1944-1990 osób pełniących funkcje publiczne (Dz. U. Nr 70, poz. 443 z późn. zm.), adwokat jest traktowany jako osoba pełniąca funkcję publiczną. Jednocześnie Generalny Inspektor zauważył, iż informacja podana w prasie o wykonywanym przez skarżącego zawodzie adwokata jest informacją możliwą do ustalenia w sposób ogólnie dostępny.¹⁷⁵

¹⁷³ GI/766/99

¹⁷⁴ DEC 43/GI-DIS-70/99/720,721

¹⁷⁵ GI-DIS-254/99/710,939, GI-DP-1299/99, sprawa jest w toku.

II.2 Przetwarzanie danych osobowych przez prokuraturę

W roku 1999 do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło wiele skarg i zapytań w przedmiocie przetwarzania przez prokuraturę danych osobowych. Przedmiotem skarg był brak podstaw i zbyt duży, zdaniem skarżących, zakres zbieranych danych, przetwarzanie danych osobowych nieprawdziwych oraz niewłaściwe zabezpieczenie dokumentów zawierających dane osobowe.

Przedmiotem prowadzonych postępowań było również nieprzestrzeganie zasad ochrony danych osobowych przez prokuraturę.

Znaczna liczba skarg dotyczyła m.in. ujawnienia na wysypisku śmieci dokumentów zawierających dane osobowe uczestników postępowania karnego prowadzonego przez Prokuraturę Okręgową. Na obecnym etapie postępowania ustalono, że w przedmiotowej sprawie prowadzone jest śledztwo przez Prokuraturę Okręgową,¹⁷⁶ które swym zakresem obejmuje również przestępstwa określone w ustawie o ochronie danych osobowych.¹⁷⁷

W omawianym okresie sprawozdawczym do Generalnego Inspektora wpłynęła skarga na przetwarzanie danych osobowych zawartych w aktach Prokuratury Rejonowej, poprzez udostępnienie ich bez zgody skarżącego redakcji lokalnej gazety. W ramach przeprowadzonych czynności kontrolnych Generalny Inspektor zwrócił się do Prokuratury oraz do wskazanego w skardze komisariatu Policji z żądaniem złożenia pisemnych wyjaśnień w sprawie. W świetle zebranych materiałów dowodowych nie potwierdziły się zarzuty, że w/w organy udostępniły redakcji „Gazety na Pomorzu” dane osobowe zawarte w aktach skarżącego. Jednocześnie Generalny Inspektor poinformował skarżącego, iż ustawa o ochronie danych osobowych ma zastosowanie do przetwarzania danych osobowych w zbiorach (art. 2 ust. 2). Zbiorem ustawa określa każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie. Oznacza to, iż tam, gdzie nie istnieje pewna struktura i określony dostęp do danych osobowych nie można mówić o zbiorze danych, co jednocześnie wyklucza stosowanie przepisów ustawy o ochronie danych osobowych. Publikacje w prasie, które nie przyjmują formy zbioru, nie są przetwarzaniem w zbiorze i tym samym nie podlegają ochronie wynikającej z przepisów ustawy. W związku z poczynionymi ustaleniami, Generalny Inspektor uznał, iż właściwą płaszczyzną dochodzenia podniesionych w skardze roszczeń jest ewentualnie droga procesu cywilnego, zaś w zakresie

¹⁷⁶ Sygn. akt. V Ds. 21/99

¹⁷⁷ GI-DIS-451/99, GI-DIS-453/99, GI-DIS-454/99, GI-DIS-455/99, GI-DIS-463/99

reakcji publicznoprawnej na ewentualne naruszenie dóbr osobistych zastosowanie mogą znaleźć przepisy rozdziału XXVII kodeksu karnego i prawa prasowego.¹⁷⁸

Jedno z pytań stawianych w kierowanych do Generalnego Inspektora pismach, dotyczyło kwestii legalności wykorzystania w akcie oskarżenia danych osobowych o skazaniu, które z mocy prawa uległo zatarciu. Art. 26 ust. 1 pkt. 3 ustawy o ochronie danych osobowych ustanawia zasadę merytorycznej poprawności danych osobowych przetwarzanych w zbiorach. Zbiorem danych osobowych są akta postępowania karnego, toczącego się przed organami Policji, czy też prokuratury. Organ prowadzący postępowanie karne powinien zadbać o to, aby dane zawarte w aktach były zgodne z rzeczywistym stanem rzeczy, aby były prawdziwe. W postępowaniu karnym obowiązuje jednak szereg istotnych zasad proceduralnych, które modyfikują wskazany wyżej obowiązek administratora. W toku postępowania przygotowawczego organ prowadzący zbiera wszystkie dowody mogące przyczynić się do wyjaśnienia istotnych okoliczności sprawy. Stosownie do art. 2 § 2 kodeksu postępowania karnego *„podstawę wszelkich rozstrzygnięć powinny stanowić prawdziwe ustalenia faktyczne”*, jednakże oceny poszczególnych dowodów może dokonywać każdy organ procesowy, w tym także prokurator. Prokurator przedstawia w toku postępowania wszelkie dowody świadczące, jego zdaniem, o winie oskarżonego, ale ostateczne przypisanie oskarżonemu winy następuje dopiero w prawomocnym wyroku sądowym. Sąd dokonuje swoich ustaleń niezależnie od ustaleń postępowania przygotowawczego. Zasada ta dotyczy także dowodu uprzedniej karalności, którym według utrwalonej judykatury może być wyłącznie zaświadczenie z Centralnego Rejestru Skazanych. *„Przyjmując za okoliczność obciążającą oskarżonego jego poprzednią karalność, sąd powinien się upewnić, czy skazanie wykazane informacją Centralnego Rejestru Skazanych, nie uległo zatarciu z mocy prawa”*.¹⁷⁹ Zdaniem Generalnego Inspektora, fakt umieszczenia w aktach postępowania karnego informacji o karalności stanowi przejaw swobodnej oceny dowodów dokonywanej przez prokuratora – informacja ta podlega jednak ostatecznie ocenie sądu.¹⁸⁰

Liczna grupa spraw dotyczyła podstaw prawnych przesłuchiwania osób w charakterze świadków i umieszczania ich danych osobowych w dokumentacji postępowania przygotowawczego. Zakres kompetencji Generalnego Inspektora Ochrony Danych Osobowych określony został w art. 12 i 14 ustawy o ochronie danych osobowych. Z treści art. 18 ust. 1 cytowanej ustawy wynika, iż Generalny Inspektor, w razie stwierdzenia naruszenia

178 GI-DIS-32/99/383

179 Wyrok Sądu Apelacyjnego w Krakowie z dnia 30 stycznia 1992 r. Nr II Akr 197/91, KZS 1992/2/13.

180 GI-DP-755/99/879

przepisów ustawy, z urzędu lub na wniosek osoby zainteresowanej nakazuje administratorowi danych, w drodze decyzji administracyjnej, przywrócenie stanu zgodnego z prawem. Jednocześnie ust. 3 tego przepisu stanowi, iż w przypadku, gdy przepisy innych ustaw regulują odrębnie wykonywanie czynności, o których mowa w ust. 1, stosuje się przepisy tych ustaw. Zasady i zakres gromadzenia materiału dowodowego niezbędnego do dokonania oceny okoliczności zdarzenia oraz podjęcia decyzji w sprawie, uregulowane są szczegółowo w przepisach kodeksu postępowania karnego, kodeksu postępowania cywilnego, w ustawie o Prokuraturze, a także w ustawie o Policji. W związku z powyższym Generalny Inspektor uznał się za niewłaściwy do oceny zasadności i legalności przeprowadzenia postępowania przygotowawczego, jak również do oceny zasadności i legalności, wydanego w tym zakresie postanowienia, uznając w tym przedmiocie wyłączną właściwość prokuratury i sądu.¹⁸¹

Do Generalnego Inspektora kierowano również skargi, w których skarżący domagali się sprostowania postanowienia wydanego przez prokuratora, jednakże Generalny Inspektor i w tym przypadku uznał się za organ niewłaściwy do jakiegokolwiek ingerencji w treść wydanych przez prokuraturę postanowień i nie znalazł podstaw do stwierdzenia naruszenia ustawy o ochronie danych osobowych. Stanowisko powyższe podzielił Naczelny Sąd Administracyjny w postanowieniu wydanym w dniu 9 listopada 1999 r.¹⁸² Zgodnie z art. 2 ust. 2 ustawę stosuje się do przetwarzania danych osobowych w systemach informatycznych oraz w kartotekach, skorowidzach, księgach, wykazach, i innych zbiorach ewidencyjnych. Przepisów ustawy nie stosuje się w przypadkach, gdy przepisy innych ustaw regulują odrębnie wykonywanie czynności, usuwanie uchybień, dokonywanie sprostowań itp. (art. 18 ust. 3 cyt. ustawy). Wszelkich sprostowań w postępowaniu karnym, w tym także w postępowaniu przygotowawczym, dokonuje organ, który popełnił omyłkę. Sprostowanie następuje w drodze postanowienia, na które służy zażalenie do wyższej instancji.¹⁸³

Do Generalnego Inspektora Ochrony Danych Osobowych wpłynęły również żądania wydania decyzji w przedmiocie usunięcia informacji o karalności zawartych w protokole przesłuchania podejrzanego. Rozpatrując przedmiotowe skargi Generalny Inspektor stwierdził, iż nie może wydać decyzji nakazującej usunięcie danych osobowych, w sytuacji gdy przetwarzanie danych osobowych wynika z treści art. 18 ust. 3 ustawy o ochronie danych osobowych, który stanowi, że w przypadku, gdy przepisy innych ustaw regulują przetwarzanie danych, stosuje się przepisy tych ustaw. Uznając, iż przepisy procedury karnej

181 GI-DIS-22/99/714, GI-DIS-135/99/425, GI-DP-963/99/1389, GI-DP-709/99/891

182 Sygn. akt. II SAB 153/99.

183 Art. 105 § 1-4 kodeksu postępowania karnego; por. GI-DIS-129/99/608/839.

szczegółowo regulują zasady przetwarzania danych osobowych (m.in. gromadzenia, udostępniania, usuwania, prostowania), Generalny Inspektor uznał, że nie jest uprawniony do ingerowania w tryb postępowania karnego.¹⁸⁴

II.3 Forma wystąpienia sądów i prokuratury o udostępnienie danych przetwarzanych przez inne jednostki

W licznych pismach i skargach Generalny Inspektor Ochrony Danych Osobowych spotykał się z problemem formy, w jakiej należy występować o udostępnienie danych. Ustawa o ochronie danych osobowych w art. 29 ust. 1 stanowi, że w przypadku udostępniania danych osobowych w celach innych niż włączenie do zbioru, administrator danych udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na podstawie przepisów prawa. Z kolei ust. 3 art. 29 stanowi, iż dane osobowe 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 wniosku określa rozporządzenie 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.). Pytania w korespondencji kierowanej do Biura dotyczyły najczęściej zagadnienia, czy sądy i prokuratury mają obowiązek występować z żądaniem udostępnienia danych osobowych na wymienionym w ustawie wniosku. Generalny Inspektor uznał, że odpowiedzi należy szukać w interpretacji ust. 1 art. 29 ustawy. Przepis ten bowiem znajduje zastosowanie wyłącznie w przypadkach udostępnienia danych osobowych w celach innych niż włączenie do zbioru. Akta spraw prowadzonych przez sądy i prokuratury stanowią zbiór danych osobowych, w konsekwencji czego wspomniany przepis nie znajduje wobec nich zastosowania. Z tego powodu Generalny Inspektor w odpowiedzi na pytania, podkreślił, iż organy takie jak sądy i prokuratura nie mają obowiązku zwracania się o udostępnienie danych osobowych na potrzeby prowadzonych postępowań na wspomnianym wniosku. Organy te są zobowiązane tylko do wykazania istnienia jednej z przesłanek, określonych w art. 23 i 27 ustawy o ochronie danych osobowych.¹⁸⁵

184 DEC-GI-DIS-77/99/7

185 GI-DP-495/99/526, GI-DP-683/99/715

III. Przetwarzanie danych osobowych przez kolegia do spraw wykroczeń

Do Biura Generalnego Inspektora w omawianym okresie sprawozdawczym napływały najczęściej zapytania odnoszące się do kwestii rejestracji zbiorów danych osobowych prowadzonych przez właściwe organy dla potrzeb postępowania przed kolegium ds. wykroczeń. W odpowiedzi na powyższe Generalny Inspektor uznał, iż zbiory danych osobowych prowadzone przez różne organy dla potrzeb postępowania przed kolegium ds. wykroczeń nie podlegają obowiązkowi rejestracji w Biurze Generalnego Inspektora Ochrony Danych Osobowych. Uzasadniając swoje stanowisko Generalny Inspektor stwierdził, że art. 43 ust. 1 ustawy o ochronie danych osobowych, zwalnia z obowiązku rejestracji zbiory prowadzone dla potrzeb postępowania sądowego. Postępowanie sądowe stanowią przepisy proceduralne stosowane przez organy wymiaru sprawiedliwości, którymi stosownie do art. 175 Konstytucji RP są: Sąd Najwyższy, sądy powszechne, sądy administracyjne i sądy wojskowe. Postępowanie prowadzone przez inne organy nie jest postępowaniem sądowym *sensu stricto*. Jednakże kolegia orzekają o winie osoby obwinionej, a więc *de facto* sprawują wymiar sprawiedliwości poprzez wydanie orzeczeń w przedmiocie popełnienia przez obwinionego wykroczenia. Postępowanie unormowane przez przepisy ustawy z dnia 20 maja 1971 r. Kodeks postępowania w sprawach o wykroczenia (Dz. U. Nr 12, poz. 116 z późn. zm.) jest postępowaniem *quasi* sądowym, zaś zbiory danych prowadzone przez kolegia oraz inne organy dla potrzeb kolegiów są prowadzone dla potrzeb postępowania sądowego w rozumieniu art. 43 ust 1 pkt 2 ustawy o ochronie danych osobowych.¹⁸⁶

Inne wątpliwości dotyczyły legalności udostępniania danych osobowych kandydatów na członków kolegiów ds. wykroczeń i kwestii rejestracji takiego zbioru. Generalny Inspektor wyjaśnił, iż ustawa o ochronie danych osobowych określa zasady postępowania przy przetwarzaniu danych osobowych oraz prawa osób fizycznych w zbiorach. Przetwarzanie danych jest dopuszczalne jedynie w sytuacjach określonych w art. 23 przedmiotowej ustawy, m in. w przypadku, gdy zezwalają na to przepisy prawa. Z przepisów regulujących tryb zgłaszania oraz sposób wyboru kandydatów na ławników i członków kolegiów do spraw wykroczeń, w szczególności z ustawy z dnia 20 czerwca 1985 r. o ustroju sądów powszechnych (Dz. U. 1994 r. Nr 7, poz. 25 z późn. zm.), ustawy z dnia 20 maja 1971 r. o ustroju kolegiów do spraw wykroczeń (Dz. U. Nr 12, poz. 118 z późn. zm.) nie wynika, aby dane kandydatów były powszechnie dostępne. Informacje o kandydatach, zgłaszanych przez uprawnione organizacje i osoby, zbierają gminy i one przygotowują wybory. Dane

186 GI-DP-955/99/995, GI-DP-932/99/965

kandydatów przedkładane są radzie gminy, która dokonuje wyboru kierując się wskazaniem powyższych ustaw. Generalny Inspektor zauważył, że w przeciwieństwie, np. do wyborów do Sejmu czy organów samorządu terytorialnego, gdzie listy kandydatów są jawne, wybory na członków kolegiów nie są powszechne i obywatele nie mają prawa głosu w przedmiotowej sprawie. Odnośnie rejestracji zbioru danych osobowych kandydatów na członków kolegiów, ustawa o ochronie danych osobowych wprowadza wymóg zgłoszenia zbiorów do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, z wyjątkiem przypadków wymienionych w art. 43 ust. 1. Zgodnie z art. 43 ust. 1 pkt 2 z obowiązku rejestracji danych zwolnieni są administratorzy danych przetwarzanych przez właściwe organy dla potrzeb postępowania sądowego. W ocenie Generalnego Inspektora, zbiór kandydatów na stanowisko członka kolegium spełnia wymogi określone w tym przepisie, w związku z czym nie podlega obowiązkowi rejestracji.¹⁸⁷

E. Przetwarzanie danych osobowych w zakresie ochrony zdrowia

I. Zagadnienia wstępne

W 1999 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęły liczne skargi i zapytania prawne dotyczące ochrony danych osobowych w służbie zdrowia. Wiele spraw związanych było z reformą służby zdrowia i funkcjonowaniem Kas Chorych. Na podstawie ustawy o ochronie danych osobowych dane dotyczące stanu zdrowia, zgodnie z art. 27, uznawane są za wrażliwe i przepis ten zabrania ich przetwarzania. Ustęp 2 tego artykułu przewiduje jednak możliwość przetwarzania danych o stanie zdrowia, m.in. gdy:

- a. osoba, której dane dotyczą, wyrazi na to zgodę na piśmie, chyba, że chodzi o usunięcie dotyczących jej danych (art. 27 ust. 2 pkt 1),
- b. przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą i stwarza pełne gwarancje ich ochrony (art. 27 ust. 2 pkt 2),
- c. gdy przetwarzanie jest prowadzone 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 7).

Wiele pytań dotyczyło zakresu udostępnianych danych oraz sposobów ich przekazywania między świadczeniodawcami a Kasami Chorych.

187 GI-DP-932/99/965

II. Przetwarzanie danych osobowych przez Kasy Chorych

II.1 Udostępnianie danych medycznych i kontrola świadczeniodawców

Zagadnienia te regulowane są przez przepisy ustawy z dnia 6 lutego 1997 r. o powszechnym ubezpieczeniu zdrowotnym (Dz. U. Nr 28, poz. 153 z późn. zm.) oraz 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 nad Ubezpieczeniami Zdrowotnymi i Krajowym Związkiem Kas Chorych (Dz. U. Nr 7, poz. 66).

W związku z przeprowadzaną reformą służby zdrowia najwięcej problemów budziło funkcjonowanie Kas Chorych. Pytania dotyczyły głównie *przekazywania danych* między Kasami Chorych, oraz *zakresu informacji* przekazywanych do Kas Chorych. Problemem było przetwarzanie numeru PESEL i możliwość przekazywania między Kasami Chorych danych zawierających między innymi numer PESEL. Generalny Inspektor poinformował, że stosownie do art. 141a ust. 2 pkt 2 o powszechnym ubezpieczeniu zdrowotnym dla realizacji zadań, o których mowa w ust. 1 tego przepisu, Kasy Chorych mają prawo do przetwarzania numeru PESEL. Zakres danych przekazywanych między Kasami Chorych nie może być jednak szerszy, niż określony w rozporządzeniu opisanym wyżej, gdyż sposób jednoznaczny określa ono jakie dane dotyczące świadczeń wykonywanych na rzecz ubezpieczonych świadczeniodawcy przekazują Kasom Chorych, z którymi mają zawarte umowy (§ 3 ust. 1), a także jakie dane przekazują na wniosek Kasy Chorych (§ 3 ust. 2).¹⁸⁸

Problemem była także kwestia *dopuszczalności weryfikowania* przez Kasę Chorych numerów PESEL w terenowym banku danych i *obowiązek informacyjny* Kas Chorych. Generalny Inspektor poinformował, że Kasa Chorych powinna wykazać podstawę prawną żądania przekazania jej numerów PESEL przez terenowy bank danych. Analiza przepisów ustawy o powszechnym ubezpieczeniu zdrowotnym, oraz 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. – w zakresie terenowych banków danych) nie pozwala na stwierdzenie, że na mocy tych przepisów Kasy Chorych mogą zbierać dane osoby, której dane dotyczą, bez jej zgody, w

188 GI-DP-954/99

związku z czym Kasy Chorych nie są zwolnione z obowiązku informacyjnego określonego w art. 24 ustawy o ochronie danych osobowych.¹⁸⁹

Ważnym problemem poruszonym przez świadczeniodawców była kwestia dopuszczalność *kserowania przez Kasy Chorych dokumentacji medycznej* w związku z kontrolą świadczenia usług medycznych. Generalny Inspektor poinformował, że świadczeniodawcy zobowiązani są do przekazywania Kasom Chorych wyłącznie informacji wymienionych enumeratywnie w § 3 i 4 rozporządzenia z dnia 15 stycznia 1999 r. cytowanego wyżej. Podkreślono także, że określenie w przepisie art. 141a ustawy o powszechnym ubezpieczeniu zdrowotnym zakresu danych, do przetwarzania których upoważnione są Kasy Chorych, nie powinno być traktowane jako upoważnienie do kserowania dokumentacji medycznej. Zaznaczono także, że zgodnie z art. 61 ust. 3 tej ustawy, podmiot kontrolowany zobowiązany jest do przedłożenia niezbędnych dokumentów, udzielania informacji i pomocy podczas kontroli. A zatem w przypadku przeprowadzenia lub zlecenia kontroli bieżącej realizacji umowy o udzielenie świadczeń przez Kasy Chorych podmiot kontrolowany zobowiązany jest jedynie do przedłożenia niezbędnych dokumentów.¹⁹⁰

Szereg pism kierowanych do Generalnego Inspektora dotyczyło próśb o informacje na temat zasad udostępniania dokumentacji medycznej,¹⁹¹ zakresu danych, jakie świadczeniodawcy mogą udostępnić w trakcie kontroli prowadzonej przez Kasy Chorych,¹⁹² i jakie ogólnie dane mogą być udostępniane Kasom Chorych.¹⁹³ Pytania powyższe wynikały z nieznamomości art. 141a ustawy o powszechnym ubezpieczeniu zdrowotnym, oraz rozporządzenia z 15 stycznia 1999 r., wspomnianego wyżej. Przepisy bowiem regulują tę sprawę bardzo szczegółowo i brak jest potrzeby jakiegokolwiek dodatkowej wykładni.

Ponieważ wspomniane wcześniej rozporządzenie Ministra Zdrowia i Opieki Społecznej z 15 stycznia 1999 r. nie zobowiązuje świadczeniodawców do udostępniania Kasom Chorych imienia i nazwiska, daty urodzenia oraz adresu świadczeniobiorcy, Kasy Chorych nie są uprawnione do otrzymania tych kategorii danych.¹⁹⁴ Odrębnym zagadnieniem jest *problem chorych, nosicieli wirusa HIV i chorujących na AIDS*. Dane dotyczące tej grupy ludzi powinny być szczególnie chronione i niepokój budzi nadmierna, zdaniem niektórych,

189 GI-DP-778/99

190 GI-DP-1382/99

191 GI-DP-1252/99

192 GI-DP-869/99

193 GI-DP-571/99, GI-DP- 509/99, GI-DP-524/99, GI-DP-390/99

194 GI-DP-1536/99

wnikliwość Kas Chorych w procedurach rozliczeniowych.¹⁹⁵ Pełna dyskrekcja, w przypadku leczenia tych chorób jest niezbędna i Kasy Chorób winny zrozumieć złożoność problemu.

Z zagadnieniem kontroli przeprowadzanej przez Kasy Chorych wiąże się wystąpienie do Ministra Zdrowia i Opieki Społecznej. Pismem z dnia 27 sierpnia 1999 r.¹⁹⁶ Generalny Inspektor wystąpił w sprawie trudności interpretacyjnych art. 61 ust. 2 ustawy z dnia 6 lutego 1997 r. o powszechnym ubezpieczeniu zdrowotnym (Dz. U. Nr 28, poz. 153 z późn. zm.). Przepis ten stanowi, że kontrole dokumentacji medycznej i jakości udzielanych świadczeń zdrowotnych mogą być przeprowadzane tylko przez upoważnionych przez Kasę Chorych lekarzy, pielęgniarki, położne lub przedstawicieli innych zawodów medycznych, o ile zakres kontroli ich dotyczy. Do czynności kontrolnych prowadzonych przez Kasy Chorych mogą być zatem dopuszczeni przedstawiciele innych zawodów medycznych, których nie obowiązuje tajemnica ani lekarska, ani pielęgniarki lub położnej. Generalny Inspektor oczekuje na odpowiedź.

Generalny Inspektor zajął się także poprawnością oświadczenia zawartego w skierowaniu na leczenie uzdrowiskowe wynikającego 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, albowiem 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”.¹⁹⁷ Pismem z dnia 21 czerwca 1999 r.¹⁹⁸ Generalny Inspektor wystąpił do Ministra Zdrowia i Opieki Społecznej w sprawie tego kwestionariusza w części dotyczącej wyrażenia zgody na przetwarzanie danych osobowych. Niepokój budzi zwłaszcza to, że dane o stanie zdrowia mogą być ujawnione także osobom, w stosunku do których nie obowiązują przepisy o tajemnicy lekarskiej, jak pielęgniarki czy położne. 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. Generalny Inspektor wnosił o rozważenie możliwości

195 Pismo Przewodniczącego Komisji Praw Człowieka i Praworządności Senatu Rzeczypospolitej Polskiej z dnia 24 listopada 1999 r., BPS/PCP/IV/0130/1120/99.

196 GI/879/99

197 GI-DP-116/99

198 GI/644/99

nowelizacji rozporządzenia Ministra Zdrowia i Opieki Społecznej z dnia 30 grudnia 1998 r., o którym mowa wyżej. Rozporządzenie do tej pory nie zostało zmienione.

Niektóre Kasy Chorych żądały od świadczeniodawców imiennych list zatrudnionych u nich lekarzy. Generalny Inspektor po analizie przepisów uznał, że żaden z przepisów prawa, na które powołuje się Kasa Chorych (ustawa o zakładach opieki zdrowotnej i ustawa o powszechnym ubezpieczeniu zdrowotnym oraz akty wykonawcze do tych ustaw), nie upoważnia jej do żądania listy zatrudnionych pracowników, a zatem udostępnienie takiego zbioru bez podstawy prawnej stanowiłoby naruszenie ustawy o ochronie danych osobowych.¹⁹⁹ W związku z tego typu niepokojącymi sygnałami Generalny Inspektor Ochrony Danych Osobowych skierował wystąpienie do Pełnomocnika Rządu ds. Wprowadzenia Powszechnego Ubezpieczenia Zdrowotnego z prośbą o podjęcie działań zmierzających do zapewnienia przestrzegania przez Kasy Chorych przepisów o ochronie danych osobowych, a w szczególności do ograniczenia wysuwanych przez nie żądań udostępnienia danych wyłącznie do sytuacji, gdy jest to zgodne z przepisami prawa. Podkreślono, że Kasy Chorych bez podstawy prawnej żądały od świadczeniodawców kopii umów o pracę z zatrudnionymi przez nich pracownikami pod rygorem odrzucenia ofert. Żądania te były niezgodne z prawem, jako pozbawione podstawy prawnej opisanej tak w art. 23 ust. 1, 27 ust. 2 czy 28 ustawy o ochronie danych osobowych. Generalny Inspektor oczekuje na odpowiedź.²⁰⁰

II.2 Przetwarzanie danych osobowych przez zakłady ubezpieczeniowe

Na styku z przepisami ubezpieczeniowymi powstawały problemy udostępnienia dokumentacji lekarskiej przez jednostki służby zdrowia zakładom ubezpieczeń w celu likwidacji szkody.²⁰¹ Podstawą prawną udostępniania danych stanowi art. 18 ust. 3 pkt 6 ustawy z dnia 30 sierpnia 1991 r. o zakładach opieki zdrowotnej (Dz. U. Nr 91, poz. 408 z późn zm.), zgodnie z którym zakład opieki zdrowotnej udostępnia dokumentację organom rentowym, zakładom ubezpieczeniowym oraz zespołom do spraw orzekania o stopniu niepełnosprawności, w związku z prowadzonym przez nie postępowaniem. Ustawowa podstawa przetwarzania danych zgodna jest zatem z art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych, który dopuszcza przetwarzanie danych wrażliwych, jeżeli przepis

199 GI-DP-954/99

200 Pismo Generalnego Inspektora do Pełnomocnika Rządu ds. Wprowadzenia Powszechnego Ubezpieczenia Zdrowotnego z dnia 29 listopada 1999 r.; GI/1186/99.

201 GI-DP-646/99

szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą i stwarza pełne gwarancje ich ochrony.

Także w sprawie towarzystw ubezpieczeń na życie przepisy te stanowią podstawę udostępnienia danych medycznych. Należy jednak pamiętać o innych uregulowaniach tego zagadnienia w ustawie z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego (Dz. U. Nr 111, poz. 535 z późn. zm.).²⁰² Zasad wynikających z ustawy o ochronie danych osobowych nie narusza także udostępnianie wykazu pacjentów podmiotowi świadczącemu usługi medyczne, który w części zleca wykonanie tych usług innemu podmiotowi świadczącemu usługi medyczne.²⁰³ Zgodnie z art. 18 ust. 3 pkt 2 ustawy o zakładach opieki zdrowotnej zakład udostępnia dokumentację 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.

W związku z licznymi skargami na towarzystwa ubezpieczeniowe, które prowadzą ubezpieczenia na życie, Generalny Inspektor zwrócił się pismem z dnia 5 marca 1999 r.²⁰⁴ do Prezesa Urzędu Ochrony Konkurencji i Konsumentów o zbadanie, czy uzależnienie zawarcia umowy przez osobę składającą wniosek o ubezpieczenie, od złożenia oświadczenia w którym wyrażona jest zgoda na przekazywanie towarzystwu ubezpieczeniowemu przez każdego lekarza, zakład opieki zdrowotnej, oraz każdą inną osobę, która dysponuje danymi na temat stanu zdrowia tej osoby nie stanowi praktyki monopolistycznej. Szczególne zaniepokojenie wzbudził fragment oświadczenia, który mówił o zgodzie na udostępnianie danych o stanie zdrowia także od innych osób, nie będących lekarzami, pielęgniarkami czy położnymi, dysponujących takimi danymi. Problemem jest to, że prawie identyczne deklaracje znajdują się w ofercie większości towarzystw ubezpieczeniowych prowadzących ubezpieczenia na życie. Sprawa jest w toku.

II.3 Zagadnienie udostępniania danych inspektorom NIK

Z zagadnieniem dostępu do danych medycznych wiąże się także sprawa dostępu inspektorów Najwyższej Izby Kontroli do danych o pacjentach Instytutu Gruźlicy i Chorób Płuc. Zgodnie z art. 27 ust. 2 ustawy o ochronie danych osobowych przesłanką dopuszczalności przetwarzania takich danych wrażliwych jest, oprócz pisemnej zgody pacjenta, przepis innej ustawy zezwalający na takie działania. Zdaniem Generalnego

202 GI-DP-293/99

203 GI-DP-274/99

204 GI/231/99

Inspektora ogólny przepis ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 1995 r. Nr 13, poz. 59 z późn. zm.) nie może być podstawą żądania udostępnienia danych o pacjentach.²⁰⁵

II.4 Inne zagadnienia

Emocje wzbudzało umieszczanie w lokalnej gazecie danych oraz wizerunku noworodka. Zgodnie z art. 2 ust. 1 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. Skoro publikowanie w lokalnej gazecie danych oraz wizerunku noworodka nie jest przetwarzaniem w zbiorze danych nie mamy do czynienia z naruszeniem przepisów ustawy.²⁰⁶

Sprawa umieszczania w Księżeczce Usług Medycznych numeru statystycznego choroby była przedmiotem analizy Generalnego Inspektora. Numer ten umieszczany jest w Księżeczce Usług Medycznych na podstawie przepisów odnoszących się do przetwarzania i ochrony danych, zawartych w ustawie o powszechnym ubezpieczeniu zdrowotnym, a więc zgodne jest to z art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych jako, że przepisy innej ustawy zezwalają na przetwarzanie takich danych.²⁰⁷ Warto dodać, że zgodnie z art. 18 ust. 3 pkt 7 ustawy o zakładach opieki zdrowotnej zakład udostępnia dokumentację rejestrom usług medycznych w zakresie niezbędnym do prowadzenia rejestrów.

W toku prowadzone są sprawy dotyczące przekazania prywatnej przychodni danych osobowych pacjentów zarejestrowanych w zlikwidowanej przychodni prowadzonej przez zakład opieki zdrowotnej.²⁰⁸

Pismem z dnia 5 stycznia 1999 r.²⁰⁹ Generalny Inspektor zwrócił się o podjęcie przez Ministra Zdrowia i Opieki Społecznej, w ramach nadzoru nad jednostkami służby zdrowia, działań zmierzających do zmiany praktyki istniejącej w jednostkach służby zdrowia, a polegającej na wykładaniu w przychodniach list pacjentów zawierających ich dane osobowe (imię, nazwisko, adres, PESEL), co nie jest zgodne z ustawą o ochronie danych osobowych. Tą drogą mogą być bowiem przekazywane dane osobowe innym pacjentom bez faktycznej zgody osoby, której one dotyczą i bez ustawowej podstawy prawnej.

205 GI-DP-1652/99

206 GI-DIS-423/99

207 GI-DIS-53/99

208 GI-DIS-460/99, GI-DIS-314/99

209 GI/6/99

Pismem z dnia 2 czerwca 1999 r.²¹⁰ Generalny Inspektor wystąpił do Ministra Zdrowia i Opieki Społecznej w sprawie niespójności przepisów regulujących opiekę zdrowotną obywateli z prośbą o podjęcie inicjatywy ustawodawczej w celu usunięcia niespójności przepisów prawa. Zwrócono szczególną uwagę na sprzeczności w ustawach z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego (Dz. U. Nr 111, poz. 535 z późn. zm.), z dnia 5 grudnia 1996 r. o zawodzie lekarza (Dz. U. z 1997 r. Nr 28, poz. 152 z późn. zm.), czy wreszcie z dnia 30 sierpnia 1991 r. o zakładach opieki zdrowotnej (Dz. U. Nr 91, poz. 408 z późn. zm.), dotyczące udostępniania danych osobowych o pacjentach. Każda z tych ustaw zawiera swoje własne uregulowania dotyczące tajemnicy lekarskiej i przesłanek jej uchylenia. Każda w inny sposób opisuje krąg osób lub instytucji, którym wolno udostępnić dane, co powoduje trudności interpretacyjne w ich stosowaniu co do możliwości i zakresu informacji udzielanych o pacjentach. W odpowiedzi z dnia 2 lipca 1999 r.²¹¹ Minister Zdrowia i Opieki Społecznej stwierdził, że jego zdaniem, brak jest podstaw do podjęcia działań legislacyjnych w tym zakresie, albowiem przedstawione sprzeczności nie występują. Sprawa jest otwarta.

III. Udostępnianie danych osobowych zakładom pracy przez zakłady opieki zdrowotnej

W związku z tym, że zakłady pracy wносиły o ujawnienie im przez zakłady opieki zdrowotnej zestawień nazwisk z rodzajem przeprowadzonych badań pracowników, ZOZ-y zwracały się wielokrotnie do Generalnego Inspektora o wyrażenie opinii w przedmiotowej sprawie.

Ustawa Kodeks pracy daje zakładom pracy prawo zlecania ZOZ-om przeprowadzenie wstępnych i kresowych badań lekarskich pracowników. Na tej samej podstawie prawnej, pracodawca nie może dopuścić do pracy pracownika bez aktualnego orzeczenia lekarskiego stwierdzającego brak przeciwwskazań do pracy na określonym stanowisku. Natomiast w myśl przepisu art. 229 § 7 kodeksu pracy, pracodawca jest zobowiązany 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

210 GI/562/99

profilaktyczne kończy się orzeczeniem lekarskim stwierdzającym brak przeciwwskazań do pracy na określonym stanowisku. Stosownie do § 3 ust. 4 orzeczenia lekarskie są wydawane w formie zaświadczeń, których wzory, w zależności od rozpoznania, określają załączniki 1 i 2 powyższego rozporządzenia. Zaświadczenie takie powinno zawierać: pieczęć zakładu opieki zdrowotnej, takie dane pracownika jak imię, nazwisko, datę i miejsce 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 ujawnienia zakładowi zestawień nazwisk z rodzajem przeprowadzonych badań. Badania profilaktyczne przeprowadza się na podstawie skierowania wydanego przez pracodawcę, które zgodnie z § 4 ust. 2 pkt 1, powinno zawierać określone rodzaje badania profilaktycznego, jakie ma być wykonane. Dysponując cennikiem i określeniem rodzaju badania jakie powinno być przeprowadzone u danego pracownika, zakłady pracy są w stanie określić wysokość przewidywalnych, z tego tytułu, kosztów. Uzasadnione zatem wydaje się być wydawanie przez ZOZ zaświadczeń o ilości przeprowadzonych badań u określonej liczby pracowników, bez zestawienia z nazwiskami. W opinii Generalnego Inspektora zaświadczenie przedstawiane zakładom pracy przez ZOZ-y mogłoby zawierać informacje o tym, ile danego rodzaju badań przeprowadzono w danym okresie u określonej liczby osób oraz określać koszt jednostkowego badania.²¹²

IV. Obowiązki administratora danych

IV.1 Obowiązek informacyjny

Wiele problemów dotyczyło niedopełnienia przez zakłady opieki zdrowotnej obowiązku informacyjnego, o którym mowa w art. 25 ustawy o ochronie danych osobowych. Zgodnie z art. 24 i 25 ustawy, na administratorze danych spoczywa obowiązek poinformowania osób, których dane dotyczą, o okolicznościach w tych przepisach określonych w momencie zbierania danych, jeśli zbiera je od osób, których dane dotyczą (art. 24) lub niezwłocznie po ich utrwaleniu, jeśli zbiera je nie od tych osób (art. 25). W myśl art. 25 w przypadku zbierania danych nie od osoby, której dane dotyczą, administrator danych jest zobowiązany poinformować tę osobę bezpośrednio po utrwaleniu zebranych danych o: 1) adresie siedziby i pełnej nazwie, 2) celu i zakresie zbierania danych, a w szczególności o

211 Pismo Podsekretarza Stanu w Ministerstwie Zdrowia i Opieki Społecznej; PR-023-MT-MŁ-1432/99.
212 GI-DP-415/99/836

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. Obowiązek taki dotyczy wszystkich administratorów danych, także jednostki służby zdrowia,²¹³ które winny informować osoby, których dane dotyczą, o posiadaniu tych danych w swoich zbiorach i o tym, że są administratorami ich danych. Dotyczy to przypadków, gdy zbiory powstały po wejściu w życie ustawy o ochronie danych osobowych, czyli po dniu 30 kwietnia 1998 r. Sprawa jest w toku.

Do Biura Generalnego Inspektora wpływały również zapytania przedstawicieli firm medycznych, dotyczące zasadności zwolnienia od obowiązku informacji, w przypadku, gdy posiadane przez nie dane osobowe lekarzy są przetwarzane w celu kontroli pracy przedstawicieli medycznych i sprawdzania prawdziwości raportów przedstawianych przez tych przedstawicieli.²¹⁴ W udzielanych odpowiedziach wyjaśniono, że przetwarzanie danych w celu analizy działania firmy wykracza poza zakres pojęcia działalności statystycznej, naukowej i historycznej określonego w art. 32 ust. 4 ustawy. W związku z tym administrator danych przetwarzający dane jest zobowiązany do wypełnienia obowiązku informacyjnego w art. 24 ustawy o ochronie danych osobowych.

IV.2 Obowiązek rejestracji

Zupełnie odrębnym zagadnieniem było pytanie o obowiązek rejestracji zbiorów danych osobowych zakładów opieki zdrowotnej.²¹⁵ Zgodnie z art. 43 ust. 1 pkt 5 ustawy z obowiązku rejestracji zbioru danych osobowych zwolnieni są administratorzy danych dotyczących osób korzystających z ich usług medycznych, a zatem zakłady opieki zdrowotnej są zwolnione z obowiązku rejestracyjnego wynikającego z art. 40 ustawy, co wszakże nie zwalnia ich z obowiązku stosowania pozostałych przepisów ustawy. Zasada ta dotyczy danych wszystkich podmiotów świadczących usługi medyczne.

F. Stosunki pracy

Po wejściu w życie ustawy o ochronie danych osobowych powstało szereg problemów związanych przetwarzaniem danych osobowych na potrzeby zatrudnienia.

Zagadnienia rozstrzygane w Biurze Generalnego Inspektora można podzielić na 7 grup. Sprawy dotyczyły: zakresu danych przetwarzanych na potrzeby zatrudnienia, w tym

213 GI-DIS-314/99

214 GI-DP-1040/99/1065

215 GI-DP-1428/99

określenia danych, do przetwarzania których pracodawcy nie są upoważnieni z uwagi na brak ustawowych podstaw gromadzenia danych, obowiązków pracodawcy, w tym dopełniania obowiązku informacyjnego, udostępniania danych o pracownikach, w szczególności udostępniania informacji o dochodach osób zatrudnionych, wykonywania obowiązku rejestracyjnego zbiorów danych osobowych dotyczących osób zatrudnionych, powierzenia przez pracodawcę przetwarzania danych pracowników innemu podmiotowi, przetwarzania danych kandydatów do pracy i osób poszukujących pracy, czy problemów związanych z zabezpieczaniem dokumentacji personalnej.

I. Zakres danych przetwarzanych na potrzeby zatrudnienia

Sygnalizowane Generalnemu Inspektorowi w skargach sprawy dotyczą zakresu danych i informacji o pracownikach, żądanych przez pracodawcę.

W odpowiedzi na pytania o zakres ankiety osobowej pracownika i zasadność żądania niektórych informacji w ankiecie osobowej pracownika oraz żądania niektórych dokumentów²¹⁶ udzielana była odpowiedź, iż podstawą przetwarzania danych osobowych pracownika jest kodeks pracy i wydane na jego podstawie rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracowników (Dz. U. Nr 62, poz. 286 z późn. zm.). Rozporządzenie szczegółowo wylicza dane, których pracodawca może żądać, w tym m.in. także dane o stanie rodzinnym pracownika. Przepisy szczególne mogą stanowić podstawę gromadzenia innych jeszcze danych dotyczących pracownika, np. danych o stanie majątkowym.²¹⁷ Pozostałe informacje o pracowniku – jeśli brak jest podstawy prawnej ich żądania – mogą być przetwarzane jedynie za zgodą pracownika (np. dane o przynależności związkowej).

W wyniku skargi Związku Zawodowego Pracowników GUC na niezgodne z ustawą o ochronie danych osobowych przetwarzanie danych przez Główny Urząd Cel, Generalny Inspektor Ochrony Danych Osobowych wszczął w tej sprawie postępowanie.²¹⁸ W toku kontroli ustalono, że Prezes Głównego Urzędu Cel polecił przekazanie w określonym terminie ujednoliconych informacji dotyczących zatrudnienia w administracji celnej małżonków, krewnych i powinowatych w postaci wypełnionego druku „Informacja”. Druk

²¹⁶ GI-DP-139/99, GI-DP-162/99, GI-DP-701/99, GI-DIS-186/99

²¹⁷ Podstawą jest, np. ustawa z dnia 16 września 1982 r. o pracownikach urzędów państwowych (Dz. U. Nr 31, poz. 214 z późn. zm.); sprawa GI-DP-370/99, GI-DP-1492/99.

zawierał dane takie jak imię i nazwisko, stopień pokrewieństwa lub powinowactwa, miejsce pracy, stanowisko, komórkę organizacyjną osób zatrudnionych w administracji celnej, pozostających ze sobą w związku małżeńskim, pokrewieństwa lub powinowactwa do III stopnia włącznie. Zgodnie z pismem, informacje te miały być wykorzystywane na bieżąco przy awansowaniu i przenoszeniu pracowników, aby zapobiegać naruszeniom art. 9 ustawy z dnia 16 września 1982 r. o pracownikach urzędów państwowych.²¹⁹ Zebranie powyższych danych miało służyć, wedle wyjaśnień Prezesa GUC, realizacji polityki kadrowej i zapobieganiu naruszeniom prawa w związku z powiązaniami rodzinnymi w administracji celnej. Ponadto, jak wyjaśnił Prezes GUC, zebrane informacje miały charakter dokumentu statystycznego nie zawierającego jakichkolwiek danych chronionych przez ustawę o ochronie danych osobowych, a przedsięwzięcie miało jedynie charakter doraźny i związane było z potrzebą uzyskania określonych informacji w ujęciu statystycznym, w celu ich ewentualnego wykorzystania w prowadzonych pracach legislacyjnych nad ustawą o Służbie Celnej. Zdaniem Prezesa GUC, zbieranie danych odbywało się na zasadzie kierowanej do pracowników prośby a nie polecenia służbowego. Generalny Inspektor stwierdził, że ustawa o ochronie danych osobowych dopuszcza przetwarzanie danych m.in. wtedy, gdy zezwalają na to przepisy prawa lub osoba, której dane dotyczą wyrazi na to zgodę. W świetle art. 9 ustawy o pracownikach urzędów państwowych, nie mogą być zatrudnieni w tym samym urzędzie małżonkowie oraz osoby pozostające ze sobą w stosunku pokrewieństwa do drugiego stopnia włącznie lub powinowactwa pierwszego stopnia, jeżeli powstałby między tymi osobami stosunek służbowej podległości. Generalny Inspektor uznał zatem, że polecenie ujawnienia danych w druku „Informacja”, wykracza poza dyspozycję art. 9 ustawy o pracownikach urzędów państwowych i narusza w związku z tym art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych. Stwierdzono również naruszenie art. 24 ust. 1 pkt 4 ustawy ponieważ pracownicy nie zostali poinformowani o dobrowolności lub obowiązku podania danych. W ocenie Generalnego Inspektora nie można zgodzić się ze stwierdzeniem Prezesa GUC, że przedmiotowe dane osobowe służyły do jednorazowego wykorzystania i miało ono jedynie charakter statystyczny i doraźny. W wydanej w maju ubiegłego roku decyzji Generalny Inspektor nakazał usunięcie kwestionowanych danych osobowych ze zbioru danych przetwarzanych przez Główny Urząd Celn.

Szczególne unormowanie ustawy o ochronie danych osobowych dotyczy danych szczególnie chronionych oraz danych o karalności.

Art. 27 ustawy, który zawiera wykaz danych szczególnie chronionych wylicza m.in. dane o ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, generalnie zabraniając ich przetwarzania. Wśród przesłanek dopuszczalności przetwarzania danych szczególnie chronionych, określonych w art. 27 ust. 2, znajduje się zgoda na piśmie osoby, której dane dotyczą, oraz ustawowa podstawa do przetwarzania danych (również wówczas, gdy przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzania jest określony w ustawie). Także art. 28 ustawy o ochronie danych osobowych wymaga, aby przetwarzanie danych dotyczących skazań, orzeczeń o ukaraniu, mandatów karnych a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym prowadzone było wyłącznie na podstawie ustawy, a zatem tylko wówczas, gdy ustawa wyraźnie stawia warunek wcześniejszej niekaralności pracownika.²²⁰

Właśnie zagadnienia podstaw i zasadności przetwarzania danych o karalności stanowiły znaczną część spraw zgłaszanych do Generalnego Inspektora.

Podstawą do uzyskania danych o wcześniejszej karalności jest, np. ustawa z dnia 29 sierpnia 1997 r. o warunkach wykonywania krajowego przewozu osób (Dz. U. Nr 141, poz. 942 z późn. zm.), która stawiała warunek niekaralności osobie zatrudnionej w transporcie w charakterze kierowcy.²²¹ W związku z tym nie mogła być uwzględniona skarga kierowcy o nieuzasadnionym uzyskaniu i wykorzystaniu informacji o wcześniejszej karalności, z którym pracodawca rozwiązał stosunek pracy, powołując się na wcześniejszą, nie zatartą, karalność pracownika.²²² Natomiast w odpowiedzi na pytanie, czy funkcjonariusz Straży Miejskiej ma prawo powiadomić zakład pracy o popełnieniu wykroczenia przez obywatela zatrudnionego w tym zakładzie, w szczególności, jeśli osobą, która popełniła wykroczenie jest funkcjonariusz Straży Miejskiej, udzielona została odpowiedź, iż ani ustawa z dnia 29

219 Dz. U. Nr 31, poz. 214

220 GI-DP- 259/99, GI-DP-745/99, GI-DP- 483/99, GI-DP-1115/99

221 Powoływany przepis ustawy o warunkach wykonywania krajowego drogowego przewozu osób uchylony został wyrokiem Trybunału Konstytucyjnego z dnia 26.04.1999 r. Trybunał uznał, iż przepis ten jest niezgodny z art. 22 i 65 ust. 1 w związku z art. 31 ust. 3 Konstytucji RP przez to, że wprowadza nadmierne ograniczenie w zakresie korzystania z wolności działalności gospodarczej oraz z wolności wyboru i wykonywania zawodu.

222 GI-DIS-142/99

sierpnia 1997 r. o Strażach Miejskich,²²³ ani kodeks wykroczeń, nie przewidują takiej możliwości.²²⁴

Niewątpliwie art. 28 ustawy o ochronie danych osobowych ograniczył możliwość dowolnego sprawdzania karalności pracowników i osób ubiegających się o zatrudnienie, przez pracodawców. Reakcją na tak sformułowany przepis są próby obejścia warunków art. 28, poprzez żądanie od kandydatów na pracowników przedstawienia zaświadczenia z Centralnego Rejestru Skazanych, bez późniejszego włączania zaświadczenia do akt pracowniczych.²²⁵

Z kolei w innej sprawie²²⁶ osoba ubiegająca się o zatrudnienie w firmie Centrum DAEWOO w Warszawie złożyła skargę w związku z żądaniem udzielenia przez pracodawcę w toku rekrutacji do pracy informacji na temat wyznania. W związku z podjęciem postępowania wyjaśniającego firma wyjaśniła, iż powołany w skardze przypadek miał charakter incydentalny i wynikał z niezajomości polskiego prawa przez jednego z koreańskich prezesów firmy, natomiast w ankietach personalnych w ogóle nie uwzględnia się informacji o wyznaniu kandydatów do pracy i pracowników firmy.

Nieco innej kwestii dotyczyły pytania co do zakresu danych zawartych w zaświadczeniach wymaganych przez pracodawcę na temat sytuacji życiowej, rodzinnej i materialnej pracownika, w związku z ubieganiem się tego pracownika o świadczenie z zakładowego funduszu świadczeń socjalnych (np. w związku z dofinansowaniem wypoczynku letniego dzieci pracownika).²²⁷ Generalny Inspektor udzielił odpowiedzi, że na podstawie art. 23 ust. 1 pkt 2 ustawy przetwarzanie danych osobowych dopuszczalne jest między innymi wtedy, gdy zezwalają na to przepisy prawa. Wymaganie przedmiotowych danych przez pracodawcę jest uzasadnione na podstawie przepisów ustawy o zakładowym funduszu świadczeń socjalnych,²²⁸ zgodnie z którymi przyznawanie ulgowych usług i świadczeń oraz wysokość dopłat uzależnia się od sytuacji życiowej, rodzinnej i materialnej osoby uprawnionej do korzystania z funduszu, zaś regulamin wewnętrzny zakładu powinien określać szczegółowe zasady i kryteria przyznawania świadczeń socjalnych.

223 Dz. U. Nr 123, poz. 779; powoływana ustawa o Strażach Miejskich wśród przesłanek, które musi spełnić osoba, aby być strażnikiem wymienia jedynie: korzystanie z pełni praw publicznych, niekaralność sądowa (art. 24).

224 GI-DP-158/99

225 Np. pismo GI-DIS-218/99

226 GI-DIS-74/99

227 GI-DP-553/99

228 Ustawa z dnia 4 marca 1994 r. (Dz. U. z 1996 r. Nr 70, poz. 118 z późn. zm.).

Kategoryczne dookreślenia zasad przetwarzania danych szczególnie chronionych w ustawie o ochronie danych osobowych, a w szczególności wymagana w art. 27 i 28 podstawa ustawowa żądania danych, np. o przynależności partyjnej i związkowej, skazań czy orzeczeń o ukaraniu, zrodziła pytania o zasady postępowania z dokumentami znajdującymi się w aktach osobowych pracowników zbieranymi przed wejściem w życie ustawy o ochronie danych osobowych na podstawie obowiązujących wówczas przepisów, zawierającymi powyższe informacje. W odpowiedzi na powtarzające się pytania informowano, iż zasady przetwarzania danych szczególnie chronionych obowiązują od momentu wejścia w życie ustawy o ochronie danych osobowych, tj. od 30 kwietnia 1998 r. Jeśli zbieranie wcześniej dokumentacji pracowniczej odbywało się w ramach i na podstawie przepisów prawa (np. obowiązujących kwestionariuszy osobowych) nie ma przesłanek, aby żądać usunięcia określonych dokumentów z akt osobowych.²²⁹

Z problemem gromadzenia określonych danych wiązało się pytanie o dopuszczalność wprowadzenia systemu kontroli czasu pracy pracowników w oparciu o zbieranie i przechowywanie odcisków palców pracowników przez kierownictwo placówki.²³⁰ Zagadnienie rejestracji czasu pracy w oparciu o komputerową rejestrację linii papilarnych pracowników nie budzi wątpliwości prawnych, w tym przypadku bowiem przesłanki legalne przetwarzania danych wskazane są w art. 129¹¹ ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 1998 r. Nr 21, poz. 94 z późn. zm.), który nakłada na pracodawcę obowiązek prowadzenia ewidencji czasu pracy. Sposób prowadzenia tej ewidencji jest dowolny. Z uwagi na szczególny rodzaj danych gromadzonych przez pracodawcę, w odpowiedzi na pytanie, zwrócono uwagę na szczególny obowiązek właściwego zabezpieczenia zbioru przed dostępem osób trzecich.²³¹

II. Obowiązki administratora danych, w tym dopełnianie obowiązku informacyjnego przez pracodawców

W odniesieniu do obowiązku informacyjnego w przewidzianego w art. 24 i 25 ustawy o ochronie danych osobowych, najczęściej zadawane pytania dotyczyły samego obowiązku informacyjnego, ale także momentu i formy dopełniania tego obowiązku.

229 Np. w sprawach GI-DP-149/99, GI-DP-463/99, GI-DP-1346/00.

230 GI-DP-827/99

231 Także ze względu na precedensowy charakter sprawy, w 2000 r., a zatem poza okresem sprawozdawczym, u pracodawcy przeprowadzona została inspekcja w zakresie właściwego zabezpieczenia zbioru.

W skardze skierowanej za pośrednictwem Rzecznika Praw Obywatelskich²³² zwrócona została uwaga na zbieranie szczegółowych danych osobowych o pracowniku przez pracodawcę (szkołę wyższą), bez uprzedniego poinformowania, w jakim celu i na podstawie jakich przepisów pracownik zobowiązany jest udzielić powyższych informacji. W wyniku wszczęcia postępowania treść ankiety osobowej została zmodyfikowana, w tym usunięta została rubryka dotycząca narodowości pracownika, natomiast do pracowników przekazana została informacja o podstawach prawnych żądania danych przez pracodawcę.

Generalnie, pracodawca powinien dopełnić obowiązku informacyjnego w momencie zawierania umowy, w szczególności co do zakresu zbieranych danych, podstaw prawnych zbierania oraz obowiązku lub dobrowolności przekazywania danych przez pracownika. Obowiązek ten istnieje od momentu wejścia w życie ustawy o ochronie danych osobowych.²³³ Ustawodawca nie przesądził o formie poinformowania, ani o formie potwierdzenia faktu, iż pracownik został poinformowany zgodnie z ustawą o ochronie danych osobowych.

Fakt poinformowania przez pracodawcę w momencie zbierania danych pracowników na potrzeby zatrudnienia nie przesądza o wykonaniu obowiązku informacyjnego na żądanie osoby, której dane dotyczą, w oparciu o art. 33 ustawy o ochronie danych osobowych. Zgodnie z ustawą o ochronie danych, każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, a zwłaszcza prawo do uzyskania informacji, jakie dane zawiera zbiór, w jaki sposób dane zostały zebrane, w jakim celu i zakresie dane są przetwarzane oraz w jakim zakresie i komu zostały udostępnione. W razie wykazania, że dane są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy, albo zbędne do realizacji celu, dla którego zostały zebrane, osobie przysługuje prawo żądania uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych.

W przypadku przetwarzania danych osobowych na potrzeby zatrudnienia, jeśli dane gromadzone są w oparciu o przepisy prawa, nie ma obowiązku wyrażania zgody przez pracowników na przetwarzanie ich danych.²³⁴ Nie ma także podstaw, aby żądać wyrażenia zgody na przetwarzanie danych osobowych osób poszukujących pracy, ponieważ urzędy pracy przetwarzają dane osobowe na podstawie ustawy z dnia 14 grudnia 1994 r. o zatrudnieniu i przeciwdziałaniu bezrobociu (Dz. U. 1997 r., Nr 25, poz. 128 z późn. zm.).²³⁵

232 GI-DIS-51/99

233 GI-DP-80/99, GI-DP-1478/99

234 GI-DP-474/99

235 GI-DP-541/99

Jest natomiast obowiązek uzyskania zgody, z zachowaniem formy pisemnej, gdy pracodawca przetwarza dane pracownika o jego przynależności związkowej. Art. 27 ustawy o ochronie danych osobowych dopuszcza bowiem przetwarzanie danych szczególnie chronionych, do których należą m.in. dane o przynależności związkowej (jeśli nie występują inne przesłanki przetwarzania, np. podstawa ustawowa), wyłącznie na podstawie pisemnej zgody osoby, której dane dotyczą. W związku z tym, w sprawie,²³⁶ w której związek zawodowy kwestionował potrzebę uzyskiwania pisemnej zgody na przetwarzanie danych o przynależności związkowej przez pracodawcę, skoro związkowcy wyrazili zgodę na potrącanie składek z ich wynagrodzeń, udzielona została odpowiedź, iż w świetle ustawy o ochronie danych osobowych, uzyskanie takiej zgody przez pracodawcę jest niezbędne. Ustawa zastrzega bowiem, iż zgoda nie może być dorozumiana z oświadczenia woli innej treści (np. wystawionego upoważnienia).²³⁷

W odniesieniu do pracodawcy nie obowiązują ponadto przepisy określające uprawnienia osoby, której dane dotyczą, w zakresie usuwania danych ze zbioru, jeśli przetwarzanie danych przez pracodawcę oparte jest na przepisach prawa. Przykładem mogą być sprawy zgłaszane do Generalnego Inspektora zawierające żądanie nakazania usunięcia akt pracowniczych ze zbiorów byłego pracodawcy.²³⁸ Żądanie takie nie miało podstawy prawnej ponieważ art. 94 pkt. 9a Kodeksu pracy, jak i przepisy wykonawcze²³⁹ nakładają na pracodawcę obowiązek prowadzenia dokumentacji w sprawach związanych ze stosunkiem pracy oraz akt osobowych pracowników, nakazując zachowanie w aktach osobowych byłego pracownika odpowiednich dokumentów, m.in. oświadczenia o wypowiedzeniu lub rozwiązaniu umowy o pracę, czy kopii świadectwa pracy.

III. Udostępnianie danych osobowych pracowników

Kwestie poruszane w związku z tą problematyką odnosiły się przede wszystkim do stosunków między związkami zawodowymi a pracodawcami. Dotyczyły głównie wzajemnego przekazywania danych o pracownikach zrzeszonych i nie zrzeszonych,

236 GI-DP-133/99

237 W sprawie tej związek zawodowy stawiał również pytanie, czy - jeśli pracodawca nie otrzyma wymaganej zgody na piśmie, i w związku z tym usunie dane o przynależności związkowej ze zbiorów – będzie mógł bez konsultacji ze związkiem skutecznie wypowiedzieć pracownikowi umowę o pracę. Jak podkreślono w odpowiedzi, sprawy te są niezależne od siebie. Pracodawca zawsze ma obowiązek konsultacji ze związkami zawodowymi wypowiedzenia umowy nawet, jeśli nie dysponuje danymi o przynależności związkowej pracownika. Podobne zagadnienia w sprawie GI-DP-150/99.

238 GI-DIS-200/99

dopuszczalności przetwarzania danych o przynależności związkowej (przy czym prezentowane były w tej kwestii różne stanowiska, niezależnie od tego, kto zadawał pytania: od obowiązku do niedopuszczalności gromadzenia danych przez pracodawcę), czy udostępniania związkom zawodowym do wglądu list płac i danych o wynagrodzeniach.

Przykładem w tym zakresie może być pytanie dyrektora Miejskiego Zakładu Energetyki Ciepłej, czy może udostępnić indywidualne dane kadrowe związkom zawodowym bez zgody pracowników, których te dane dotyczą. Generalny Inspektor udzielił odpowiedzi, że uchwała Sądu Najwyższego z dnia 16 lipca 1993 r.²⁴⁰ stanowi, że zawarte w art. 8 i art. 23 ust. 1 oraz art. 26 pkt 3 ustawy z dnia 23 maja 1991 r. o związkach zawodowych (Dz. U. Nr 55, poz. 234 z późn. zm.) uprawnienie do kontrolowania przez związki zawodowe przestrzegania prawa pracy oznacza także uprawnienie do kontrolowania wysokości wynagrodzeń pracowników; nie oznacza natomiast uprawnienia do żądania od pracodawcy udzielenia informacji o wysokości wynagrodzenia konkretnego pracownika bez jego zgody. Sąd Najwyższy dodał jednocześnie, że ujawnienie przez pracodawcę bez zgody pracownika wysokości jego wynagrodzenia za pracę może stanowić naruszenie jego dobra osobistego w rozumieniu art. 23 i 24 kodeksu cywilnego. Uchwała ta zachowuje swoją aktualność pod rządami ustawy o ochronie danych osobowych.²⁴¹

Nie będzie natomiast naruszać ustawy o ochronie danych osobowych udzielanie związkom zawodowym informacji dotyczących wynagrodzeń podstawowych w poszczególnych zawodach i na poszczególnych stanowiskach pracy (także sumy wynagrodzeń podstawowych w danym zawodzie lub na danym stanowisku pracy z uwzględnieniem ilości pracowników w każdej grupie zawodowej), bez powiązania tych informacji z nazwiskami konkretnych osób, w celu opracowania zakładowego układu zbiorowego pracy. Odmowa udzielania informacji w takim zakresie przez pracodawcę z powołaniem się na ustawę o ochronie danych osobowych jest nadinterpretacją ustawy.²⁴² Nie będzie też naruszeniem ustawy przekazywanie organizacji związkowej, na jej żądanie, informacji o wysokości składek związkowych potrącanych poszczególnym członkom związku. Organizacje związkowe są bowiem upoważnione do otrzymywania interesujących je

239 Rozporządzenie MPiPS z dnia 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych (Dz. U. Nr 62, poz. 286).

240 Sygn. I PZP 28/93, (OSNC 1994/1/2).

241 GI-DP-107/99, GI-DP-147/99, GI-DP-518/99, GI-DP-637/99, GI-DP-1172/99, GI-DP-1466/99, GI-DP-1533/99; podobnie w sprawie GI-DP-507/99, w której z pytaniem o możliwość kontrolowania list płac i nagród pracowników zwrócił się przedstawiciel rady zakładowej.

242 GI-DP-147/99

danych, gdyż art. 28 ustawy z dnia 23 maja 1991 r. o związkach zawodowych (Dz. U. Nr 55, poz. 234 z późn. zm.) zobowiązuje pracodawcę do udzielania organizacji związkowej informacji niezbędnych do prowadzenia działalności związkowej; do nich należą informacje o płaceniu składek przez poszczególnych członków związku oraz informacje o globalnej wysokości składek wpływających na konto związku zawodowego.²⁴³

Inaczej traktowane są dane o wysokości wynagrodzenia osób pełniących funkcje publiczne. Odpowiadając na pytanie o zasadność udzielania dziennikarzom informacji o wysokości wynagrodzenia za pracę członków zarządu gminy, udzielona została odpowiedź, że w sprawie tej wypowiedział się Naczelny Sąd Administracyjny w orzeczeniu z dnia 5 grudnia 1995 r.²⁴⁴ orzekając, iż dane płacowe burmistrza, sekretarza i skarbnika gminy nie stanowią tajemnicy państwowej i służbowej i nie leżą w sferze życia prywatnego; informacje o wynagrodzeniu tych osób związane są z ich działalnością publiczną i muszą być jawne dla społeczności lokalnej. W szczególności nie można odmówić takich informacji, powołując się na ustawę o ochronie danych osobowych.²⁴⁵

Związki zawodowe zwracały się również z pytaniem, czy nie narusza ustawy o ochronie danych osobowych żądanie związków zawodowych przedstawienia, przez osoby ubiegające się o świadczenie z zakładowego funduszu świadczeń socjalnych, zaświadczenia o uzyskanych wynagrodzeniach argumentując, iż świadczenia z zakładowego funduszu są przyznawane ze względu na sytuację materialną, rodzinną lub życiową, czyli na podstawie kryteriów socjalnych i z tego względu żądanie wymienionego dokumentu jest zasadne.²⁴⁶ Związki podnosiły, iż spotykają się z odmową przedstawienia zaświadczenia, z powołaniem się na ustawę o ochronie danych osobowych. Generalny Inspektor podzielił argumentację związków, wskazując na istnienie również podstawy prawnej do żądania powyższych zaświadczeń na mocy art. 8 ustawy o zakładowym funduszu socjalnym, który wskazuje na konieczność ustalenia sytuacji życiowej, rodzinnej i materialnej osoby uprawnionej i podjęciu stosownej decyzji.

Nie istnieje natomiast przepis nakładający na pracodawcę obowiązek posiadania list osób należących do związku i pobierania składek na rzecz związku. Przetwarzanie danych w tym zakresie musi zatem odbywać się za zgodą osoby, której dane dotyczą.²⁴⁷ Z uwagi na

243 GI-DP-1046/99

244 Orzeczenie z 1993 r., sygn. I SA. 1254/92.

245 GI-DP- 518/99, GI-DP-910/99, GI-DP- 1644/99

246 GI-DP-301/99, GI-DP-543/99, GI-DP-917/99

247 GI-DP-19/99

treść art. 27 ustawy o ochronie danych osobowych dotyczącego zasad przetwarzania danych szczególnie chronionych, zgoda ta musi być wyrażona na piśmie.²⁴⁸

Natomiast przedmiotem skargi, której skutkiem było wszczęcie postępowania administracyjnego, było udostępnienie imiennego wykazu członków jednej organizacji związkowej na rzecz członków – założycieli innej organizacji związkowej w tym samym przedsiębiorstwie.²⁴⁹ Przeprowadzone postępowanie wyjaśniające nie dostarczyło dowodów na potwierdzenie faktów wykorzystania list członków związku zawodowego przez inną organizację związkową, w związku z czym postępowanie zostało umorzone.

W odniesieniu natomiast do pytań dotyczących udostępniania akt osobowych organom kontrolującym, w tym organom kontrolnym rad gmin, regionalnej izbie obrachunkowej (np. dane o wynagrodzeniach konkretnych osób, korzystania przez osoby zatrudnione ze zwolnień lekarskich, innych informacji znajdujących się w aktach osobowych, np. kwalifikacji zawodowych urzędników), w ocenie Generalnego Inspektora – jeśli brak jest konkretnej podstawy prawnej (ustawowej – w odniesieniu do danych szczególnie chronionych), udostępnienie danych podmiotom nieuprawnionym stanowiłoby naruszenie ustawy o ochronie danych osobowych.²⁵⁰ Musi istnieć bowiem wyraźna postawa ustawowa, nie ogólna klauzula ustanawiająca, np. prawo rady nadzorczej do kontroli przedsiębiorstwa spółki we wszystkich jego gałęziach,²⁵¹ która będzie upoważniała odpowiednie organy do kontrolowania akt osobowych pracowników. Brak jest również podstaw prawnych do wglądu w akta osobowe wszystkich pracowników urzędu gminy przez komisję rewizyjną gminy, która może żądać informacji – w ramach swoich uprawnień – ile miesięcznie (zbiorczo) przeznaczają się środków na wynagrodzenia pracowników. Nie ma natomiast uprawnień do wglądu w teczki osobowe poszczególnych „szeregowych” pracowników, ponieważ do tego uprawniony jest jedynie pracodawca (np. wójt, burmistrz). Natomiast posiada prawo do przeglądania akt osobowych lustrator wydelegowany z Krajowej Rady Spółdzielczej, jednakże brak jest podstaw prawnych do umieszczenia w protokole polustracyjnym

248 Zagadnienie to zostało omówione wcześniej.

249 GI-DIS-280/99

250 GI-DP-187/99, GI-DP-1314/99. Natomiast w sprawie GI-DP-393/99 przedstawiciel wojewody żądał udostępnienia dokumentacji osobowej pracowników szpitala w celu skontrolowania prawidłowości wydatkowania dotacji z budżetu wojewody. Zdaniem GODO ogólne upoważnienie do kontrolowania prawidłowości wydatkowania dotacji finansowych, w dodatku z powołaniem się na samoistną uchwałę Rady Ministrów z dnia 23 maja 1983 r. (budzącą wątpliwości co do jej legalności z punktu widzenia Konstytucji RP), jako upoważniającą do przeprowadzania kontroli, nie daje prawa wglądu w teczki osobowe pracowników, które – z uwagi na zawartość dokumentacji personalnej, zawierającej także dane szczególnie chronione – mogłyby być kontrolowane jedynie w oparciu o upoważnienie ustawowe.

251 Na takie ogólne upoważnienie zawarte w art. 212 kodeksu handlowego powoływała się Rada Nadzorcza Przedsiębiorstwa Usług Komunalnych w sprawie GI-DP-1314/99.

szczegółowych informacji o przebiegu kariery zawodowej osoby zatrudnionej w lustrowanej spółdzielni.²⁵²

Nieprecyzyjność przepisów ustawy z dnia 6 marca 1981 r. o Państwowej Inspekcji Pracy (Dz. U. z 1985 r. Nr 54, poz. 276 z późn. zm.) sprawia, że uprawnienie do formułowania żądania przez inspektorów PIP wglądu we wszystkie teczki osobowe pracowników w kontrolowanym zakładzie pracy nie znajduje umocowania prawnego. W art. 8 i 20 ustawy o PIP określone są zadania i uprawnienia Inspekcji, w tym m.in. nadzór i kontrola przestrzegania przez zakład pracy przepisów prawa pracy, w szczególności przepisów i zasad bezpieczeństwa i higieny pracy, przepisów dotyczących stosunku pracy, wynagrodzenia za pracę. Jednakże uprawnienia inspektorów PIP, określone w art. 20 ustawy o Państwowej Inspekcji Pracy, obejmują jedynie prawo żądania od kierownika zakładu pracy oraz wszystkich osób, które zakład zatrudnia lub zatrudniał, pisemnych i ustnych informacji w sprawach objętych kontrolą oraz wzywania i przesłuchiwanie tych osób w związku z przeprowadzaną kontrolą. W toku wykonywania czynności kontrolnych inspektor pracy może sprawdzać tożsamość osób wykonujących pracę, inspektor ma ponadto m.in. prawo żądania okazania dokumentów dotyczących budowy i przebudowy (modernizacji) oraz uruchomienia zakładu, planów i rysunków technicznych. Z wyliczonych enumeratywnie w przepisie ustawy czynności, jakie mogą być wykonywane przez inspektora PIP, nie wynika prawo wglądu w teczki osobowe pracowników zakładu. Z tego też względu, w odpowiedzi na pytanie dotyczące możliwości udostępnienia do kontroli całej dokumentacji osobowej pracowników jednej z kopalni węgla kamiennego na żądanie inspektora PIP²⁵³ udzielona została odpowiedź, iż w świetle obowiązujących przepisów żądanie takie nie ma podstawy prawnej.

Natomiast – zdaniem Generalnego Inspektora – szerokie uprawnienia kontrolne posiada Najwyższa Izba Kontroli, której uprawnienia określone zostały nie tylko w ustawie z 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 1995 r. Nr 13, poz. 59 z późn. zm.), ale także w Konstytucji. W ramach nadanych uprawnień kontrolnych mieści się także kontrola dokumentów zawierających dane osobowe (np. imienny wykaz osób objętych zakazem prowadzenia działalności gospodarczej, dokumenty zawierające informacje dotyczące zajmowanego stanowiska, w tym zajmowanej funkcji, daty objęcia i opuszczenia stanowiska, a także datę złożenia oświadczenia majątkowego).²⁵⁴ Jednakże również w tym

252 GI-DP-774/99, GI-DP-798/99, GI-DP-826/99

253 GI-DP-805/99

254 GI-DP-307/99, GI-DP-952/99

przypadku tylko wyraźne upoważnienie ustawowe mogłoby stanowić podstawę wglądu w akta osobowe konkretnych pracowników.

Brak jest również podstaw do przekazywania do wglądu akt pracowników gminnego ośrodka kultury, w którym pracodawcą jest kierownik tego ośrodka osobowych, wójtowi gminy. W odpowiedzi na zadane pytanie udzielona została odpowiedź, że do akt osobowych dostęp powinien mieć jedynie pracodawca, albowiem żaden z przepisów ani ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 1998 r. Nr 21, poz. 94 z późn. zm.), ani 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, poza § 9, który dotyczy wszakże innej sytuacji (Dz. U. Nr 62, poz. 286) nie przewidują przekazania akt innemu podmiotowi.²⁵⁵

Dużo wątpliwości w praktyce budziło udostępnianie danych osobowych pracowników innym jeszcze osobom i podmiotom. Jest tak, że tylko zgoda osoby, której dane dotyczą – wobec braku regulacji prawnych w tym zakresie - powinna stanowić podstawę udostępnienia danych osobowych pracowników placówki opiekuńczo-wychowawczej, zbieranych na potrzeby wydania monografii o historii placówki.²⁵⁶

Kierowane do Generalnego Inspektora pytania i skargi dotyczyły także przypadków udostępniania danych osobowych pracowników określonym instytucjom i podmiotom, np. sądom, prokuraturze, czy zakładom opieki zdrowotnej w związku z prowadzonymi postępowaniami sądowymi. W innej sprawie²⁵⁷ skarżący zwrócił się z prośbą o udzielenie informacji, czy pracodawca miał prawo udostępnić jego dane o stanie zdrowia szpitalowi oraz sądowi, w związku z prowadzoną przez skarżącego sprawą z zakresu prawa pracy. Natomiast w sprawie GI-DIS -275/99, w której skarżący wnosił o wszczęcie postępowania w związku z nieuprawnionym udostępnianiem dokumentów pracowniczych przez kierownika placówki oświatowej, w której wcześniej był zatrudniony, prowadzone postępowanie administracyjne doprowadziło do wyjaśnienia, iż w przedmiotowej sprawie dokumenty udostępniane były sądowi pracy w związku ze sprawą rozstrzyganą z powództwa byłego pracownika przeciwko pracodawcy. W związku z powyższym postępowanie administracyjne zostało umorzone.

Udzielanie informacji sądowi w sprawach z zakresu prawa pracy, znajduje podstawę w art. 248 § 1 k.p.c. zgodnie z którym każdy jest zobowiązany przedstawić na zarządzenie sądu dokument stanowiący dowód w sprawie, chyba, że dokument stanowi tajemnicę

255 GI-DP-350/99, GI-DP-1355/99

256 GI-DP-1356/99

257 GI-DS-197/99

państwową.²⁵⁸ W świetle art. 9 i 525 k.p.c. akta sprawy, także zawierające dokumenty dotyczące zatrudnienia, są udostępniane stronom postępowania, które mają także uprawnienie do otrzymywania wyciągów z tych akt. Z tego względu skarga²⁵⁹ na nieuprawnione udostępnianie dokumentów pracowniczych stronie postępowania sądowego, po wyjaśnieniu okoliczności sprawy, nie została uwzględniona. Również z powodu istnienia podstaw prawnych udostępnienia danych, nie zostało wszczęte postępowanie dotyczące skargi na udostępnienie orzeczenia o grupie inwalidzkiej skarżącego lekarzowi wojewódzkiego ośrodka medycyny pracy oraz sądowi pracy. W odpowiedzi na skargę, po ustaleniu stanu faktycznego, poinformowano skarżącego, iż zgodnie z art. 27 ust. 2 pkt 5 ustawy o ochronie danych osobowych udostępnienie danych dotyczących stanu zdrowia jest dopuszczalne, jeżeli dotyczy danych niezbędnych do dochodzenia praw przed sądem, zaś na podstawie art. 27 ust. 2 pkt 7 ustawy, jeżeli przetwarzanie tych danych prowadzone jest w celu ochrony stanu zdrowia przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych.²⁶⁰

Istnieje również podstawa prawna udostępnienia przez pracodawcę życiorysu pracownika Zakładowi Ubezpieczeń Społecznych. Życiorys został przekazany do Zakładu Ubezpieczeń Społecznych w związku z wnioskiem w sprawie przyznania wcześniejszej emerytury, ponieważ życiorys jest istotnym dla zatrudnionego dokumentem stwierdzającym okresy zatrudnienia uzasadniające prawo do świadczeń.²⁶¹ W sprawie udostępniania ZUS dokumentów (m.in. życiorysu i ankiety personalnej) bliższa analiza zgłaszanych skarg oraz przepisów spowodowała zmianę stanowiska prezentowanego w pismach przez Generalnego Inspektora, który w jednej ze spraw,²⁶² udzielił odpowiedzi, iż żaden z ustawowych obowiązków pracodawców, określonych w ustawie z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz. U. Nr 162, poz. 118 z późn. zm.) nie obejmuje przekazywania organom rentowym ankiety personalnej i życiorysu pracownika. Wobec tego, ewentualne udostępnienie powyższych dokumentów jest możliwe jedynie po uzyskaniu zgody pracownika.

Spraw ubezpieczeń pracowniczych dotyczyło również pytanie o konieczność uzyskania zgody pracowników, których dane przekazywane są do ZUS w celu ustalenia

258 GI-DP-41/99, GI-DP-1143/99, GI-DIS-275/99

259 GI-DIS-172/99

260 GI-DIS-197/99

261 GI-DP-334/99

262 GI-DP-1143/99

„wynagrodzenia zastępczego” dla osób, które pracowały w ramach kontraktów za granicą i których zarobki ustalane są na podstawie zarobków pracowników zatrudnionych w kraju na równorzędnym stanowisku lub o podobnym charakterze.²⁶³ Analiza przepisów dała podstawę do stwierdzenia, iż § 10 pkt 2 rozporządzenia Rady Ministrów z 1985 r.²⁶⁴ w istocie wymaga przedstawienia kwoty wynagrodzenia, którą otrzymywał pracownik zatrudniony w kraju w takim samym lub podobnym charakterze, w jakim pracownik był zatrudniony przed wyjazdem za granicę. Jednakże przepisy dotyczące ustalania „wynagrodzenia zastępczego” nie dają podstawy do żądania dokładnych danych osobowych, łącznie z imieniem i nazwiskiem osoby, której wynagrodzenie przedstawiane jest do ustalenia „wynagrodzenia zastępczego”. Żądanie dokładnych danych dwóch osób przez ZUS jest zatem nieuprawnione.²⁶⁵ Ewentualnie dane mogłyby być przekazane po wyrażeniu zgody przez pracowników. ZUS nie jest również upoważniony do żądania, np. odpisów wyroków alimentacyjnych w celu wydania decyzji o zasiłku rodzinnym. Przepisy szczególne, stanowiące podstawę do żądania dokumentów uzasadniających przyznanie zasiłku rodzinnego oraz ustalenie jego wysokości uprawniają jedynie do przyjęcia wniosku oraz oświadczenia o dochodach rodziny ubiegającej się o zasiłek.²⁶⁶ Podkreślić należy, iż do żądania udostępnienia odpisu wyroku (np. alimentacyjnego) w celu włączenia go do akt osoby ubiegającej się o zasiłek rodzinny, niezbędna byłaby podstawa ustawowa. Zgodnie bowiem z art. 28 ustawy o ochronie danych, przetwarzanie danych z orzeczeń wydanych w postępowaniu sądowym lub administracyjnym, dopuszczalne jest wyłącznie na podstawie ustawy.

Z kolei w pytaniu skierowanym do Biura GIODO zawarta była prośba o odpowiedź, czy pracodawca ma prawo wglądu do akt ZUS dotyczących orzeczeń ustalających procentowy uszczerbek na zdrowiu pracowników poszkodowanych wskutek wypadku przy pracy bądź choroby zawodowej.²⁶⁷ W odpowiedzi udzielona została informacja, iż zagadnienie to częściowo regulują przepisy rozporządzenia Rady Ministrów z 1998 r. oraz rozporządzenia MPiPS i MZiOS z 1975 r.²⁶⁸, które upoważniają pracodawcę do pozyskiwania

263 GI-DP-896/99

264 Rozporządzenie Rady Ministrów z dnia 1 kwietnia 1985 r. w sprawie szczegółowych zasad ustalania podstaw emerytur i rent (Dz. U. z 1989 r. Nr 11, poz. 63 z późn. zm.).

265 Ponieważ podobne pytania, potwierdzające nie mającą uzasadnienia w przepisach prawa praktykę ZUS, powtarzały się, Generalny Inspektor w roku 2000, czyli po okresie sprawozdawczym, zwrócił się z pismem do Prezesa ZUS.

266 GI-DP-619/99

267 GI-DP-1139/99

268 Rozporządzenie Rady Ministrów z dnia 28 lipca 1998 r. w sprawie ustalania okoliczności i przyczyn wypadków przy pracy oraz sposobu ich dokumentowania, a także zakresu informacji zamieszczanych w rejestrze wypadków przy pracy (Dz. U. Nr 115, poz. 744); rozporządzenie MPiPS oraz MZiOS z dnia 17 października 1975 r. w sprawie zasad i trybu orzekania uszczerbku na zdrowiu oraz wypłacania świadczeń z

informacji od ZUS orzeczenia o ustaleniu stałego lub długotrwałego uszczerbku na zdrowiu. Uprawnienie to wiąże się m.in. z obowiązkami pracodawcy wynikającymi z kodeksu pracy zapewnienia odpowiedniego miejsca pracy dla pracownika. Pracodawca nie ma natomiast uprawnienia do wglądu w dokumentację medyczną, bowiem takie uprawnienie wprost musiałoby być przewidziane w przepisach rangi ustawowej. Zgodnie bowiem z art. 27 ust. 2, pkt. 2 i 6 ustawy o ochronie danych osobowych, dane o stanie zdrowia mogą być przetwarzane, jeśli przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą.

Podstawa prawna istnieje również w przypadku udostępniania osobie składającej zamówienie danych osobowych pracowników zatrudnionych u wykonawców zamówień publicznych. Zakres żądanych informacji dotyczących osób zatrudnionych u „dostawców” lub „wykonawców” zamówień publicznych został określony w art. 22 ustawy z dnia 10 czerwca 1994 r. o zamówieniach publicznych (Dz. U. z 1998 r. Nr 119, poz. 773 z późn. zm.), jak też w przepisie wykonawczym do tejże ustawy. Podkreślenia wymaga jednakże, iż udostępnienie danych może nastąpić wyłącznie w zakresie, w jakim przewiduje to przepis.²⁶⁹

Znaczna część spraw dotyczyła prawa wglądu członków spółdzielni w akta osobowe i wynagrodzenia zatrudnionych pracowników. W odpowiedzi wskazywano, iż prawa spółdzielców dokładnie określa ustawa z dnia 16 września 1982 r. Prawo spółdzielcze (Dz. U. z 1995 r. Nr 54, poz. 288 z późn. zm.), która dając uprawnienia członkom spółdzielni do wglądu w statut, regulaminy, uchwały, a w odniesieniu do sytuacji innych członków spółdzielni, również w rejestr spółdzielni, nie uprawnia do szczegółowej kontroli akt osobowych zatrudnionych pracowników, ani do szczegółowej informacji o wysokości wynagrodzenia poszczególnych pracowników.²⁷⁰

Zupełnie inną kategorię problemów prezentowały pytania dotyczące dopuszczalności noszenia w miejscu pracy przez pracowników identyfikatorów. M.in. na pytanie naczelnika jednego z urzędów skarbowych odnośnie obowiązku noszenia przez pracowników identyfikatorów zawierających imię, nazwisko, stanowisko, nazwę urzędu oraz zdjęcie Generalny Inspektor stwierdził, iż jest to dopuszczalne, jeżeli jest to przewidziane przez przepisy wewnętrzne danej jednostki.²⁷¹ Zgodnie z art. 104 § 1 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 1998 r. Nr 21, poz. 94 z późn. zm.) regulamin pracy ustala

tytułu wypadków przy pracy, w drodze do pracy i z pracy oraz z tytułu chorób zawodowych (Dz. U. Nr 36, poz. 199).

269 GI-DP-1226/99

270 GI-DP-55/99, GI-DP-762/99, GI-DP-696/99

271 GI-DP-112/99, GI-DP-322/99, GI-DP- 968/99, GI-DP-1136/99

organizację i porządek w procesie pracy oraz związane z tym prawa i obowiązki pracodawcy i pracowników. Stanowi on podstawę obowiązku noszenia identyfikatorów, w celu usprawnienia załatwiania spraw u urzędzie. Jednocześnie ustawa o ochronie danych osobowych nie może stanowić podstawy do odmowy ujawnienia, np. nazwiska nauczyciela rodzicom uczniów.²⁷²

Osobna grupa pytań dotyczyła udostępniania danych na potrzeby badań i publikacji naukowych.²⁷³ W świetle ustawy o ochronie danych osobowych udostępnienie danych w celu innym, niż ten, dla którego zostały zebrane, jest możliwe jeżeli nie narusza praw i wolności osób, których dane dotyczą oraz następuje w celach badań naukowych, dydaktycznych, historycznych lub statystycznych. W takim przypadku podmiot, który uzyskał dane może być zwolniony nawet z obowiązku informacyjnego wynikającego z art. 25 ustawy o ochronie danych osobowych, gdy przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą, a spełnienie obowiązku informacyjnego wymagałoby nadmiernych nakładów lub zagrażało realizacji celu badania.

W pytaniach powtarzały się również zagadnienia udzielania informacji, w tym informacji osobowych, na żądanie dziennikarzy. W świetle obowiązującego prawa prasowego organy państwowe, przedsiębiorstwa państwowe i inne państwowe jednostki organizacyjne, a w zakresie działalności społeczno-gospodarczej również organizacje społeczne i osoby prowadzące działalność gospodarczą na własny rachunek są obowiązane do udzielania prasie informacji o swojej działalności.²⁷⁴ Niewątpliwie informacją o działalności jest informacja zawierająca nazwiska osób zatrudnionych (bez wkraczania w szczegółowe dane dotyczące tych osób); podanie samych nazwisk osób zatrudnionych w instytucjach publicznych (np. nazwisk doradców prezesów PFRON) nie narusza ustawy o ochronie danych osobowych, ani dóbr osobistych tych osób i jest możliwe w trybie art. 29 ustawy o ochronie danych osobowych. Dlatego nieuprawniona – zdaniem Generalnego Inspektora – jest odpowiedź skierowana do dziennikarzy, iż informacja taka może być udzielona wyłącznie za zgodą osób, których dane dotyczą.²⁷⁵ Nie ma natomiast podstaw do udzielania dziennikarzom szczegółowych informacji o „zwykłych” pracownikach (np. o ich kwalifikacjach zawodowych, zajmowanym stanowisku, zakresie obowiązków, wysokości wynagrodzenia) nie będących osobami publicznymi.²⁷⁶ W przypadku jednak skarg na dziennikarzy, którzy

272 GI-DP-338/99

273 GI-DP-56/99, GI-DP-609/99

274 Art. 4 ustawy z dnia 26 stycznia 1984 r. Prawo prasowe (Dz. U. Nr 5, poz. 24 z późn. zm.).

275 GI-DP-789/99

276 GI-DP-781/99

powołując się na prawo prasowe uzyskiwali informacje o pracownikach wkraczające w sferę ich dóbr osobistych, w sytuacji, kiedy nie można było ze względów dowodowych jednoznacznie stwierdzić, iż informacje te udzielane były przez osobę odpowiedzialną za zabezpieczenie danych, osobom skarżącym udzielana była odpowiedź o możliwości dochodzenia odszkodowania za naruszenie dóbr osobistych w procesie cywilnym.²⁷⁷

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.²⁷⁸

Wśród pytań zgłaszanych przez pracodawców, znajdowały się także pytania dotyczące formy wniosku o udostępnienie danych. Sprawy dotyczyły m.in. udostępniania danych o podanie wysokości wynagrodzenia w związku z egzekucją świadczeń alimentacyjnych na podstawie wyroku sądowego.²⁷⁹

W odpowiedzi udzielana była informacja, iż wzór wniosku, stanowiący załącznik nr 1 do rozporządzenia MSWiA z dnia 3 czerwca 1998 r. w sprawie określenia wzoru wniosku o udostępnienie danych /.../²⁸⁰ znajduje zastosowanie – zgodnie z art. 29 ustawy o ochronie danych osobowych w sytuacji, gdy udostępnianie danych następuje w celach innych, niż włączenie do zbioru. Każdy organ działający w ramach i na podstawie przepisów prawa posiada zbiór danych prowadzonych spraw. Dopuszczona jest zatem inna forma wniosku (np. na formularzach opracowanych dla określonych podmiotów, bądź dla określonego typu prowadzonych spraw), warunkiem koniecznym jest natomiast forma pisemna.

Jednoznaczne rozstrzygnięcie ustawowe, kto i w jakim zakresie upoważniony jest do dostępu do danych jest o tyle istotne, że każdy, kto administrując zbiorem danych lub obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, wypełnia znamiona czynu zabronionego z art. 51 ustawy o ochronie danych osobowych, zagrożonego karą grzywny, karą ograniczenia wolności albo pozbawienia wolności do lat 2.

277 GI-DIS-273/99

278 GI-DP-609/99, GI-DP- 630/99

279 GI-DP-914/99

280 Rozporządzenie MSWiA 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.).

Sytuacja taka miała miejsce w sprawie opisanej w skardze dotyczącej udostępnienia osobom nieuprawnionym akt osobowych pracowników przez Prezesa Zarządu Agencji Rozwoju Regionalnego S.A. W wyniku przeprowadzonego postępowania wyjaśniającego ustalono, iż są podstawy do wystąpienia do właściwej prokuratury z zawiadomieniem o popełnieniu przestępstwa z art. 51 ust. 1 ustawy o ochronie danych osobowych. W przedmiotowej sprawie 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 Przewodniczącego Komisji Zakładowej NSZZ „Solidarność” przy Koszalińskiej Agencji Rozwoju Regionalnego S.A.²⁸¹

IV. Obowiązek zgłoszenia zbiorów danych do zarejestrowania

W związku z nałożonym przez ustawę o ochronie danych osobowych na administratorów danych osobowych obowiązkiem rejestracyjnym zbioru danych, znaczna część pytań kierowanych do GODO dotyczyła dopełnienia obowiązku rejestracyjnego.

W odpowiedzi na pytania²⁸² Generalny Inspektor wyjaśniał, że ustawa, przewidując w art. 40 obowiązek zgłaszania zbiorów danych do zarejestrowania, zwolniła w art. 43 ust. 1 niektóre kategorie zbiorów. Zgodnie z art. 43 ust. 1 zwolnione z obowiązku rejestracji są zbiory osób zatrudnionych u administratora,²⁸³ przy czym pojęcie „osób zatrudnionych” rozumiane było szeroko, w sposób obejmujący zarówno zatrudnienie na podstawie kodeksu pracy, jak i pozakodeksowe formy zatrudnienia²⁸⁴. Za zbiór osób zatrudnionych uznany został również zbiór uczniów odbywających praktyki zawodowe, jako że odbywanie praktyki oznacza ze strony podmiotu zatrudniającego praktykanta konieczność spełnienia wszystkich wymagań określonych w kodeksie pracy, np. przeszkolenia w zakresie BHP, a także zbiór dotyczący osób zatrudnianych na podstawie umowy zlecenia.²⁸⁵ Zwolnienie z obowiązku zgłoszenia do zarejestrowania zbioru danych nie zwalnia z innych obowiązków wynikających z ustawy.

Nie podlegają rejestracji także zbiory informacji o firmach lub jakichkolwiek podmiotach innych, aniżeli osoby fizyczne nawet, jeśli zbiór danych o firmach zawierałby

281 GI-DIS-246/99

282 W sumie, na pytania dotyczące obowiązku, czy też zwolnienia z obowiązku rejestracyjnego osób zatrudnionych u określonego pracodawcy, udzielonych zostało 45 odpowiedzi pisemnych

283 Por. odpowiedzi, np. w sprawach GI-DP-1302/99, GI-DP-1380/99, GI-DP-1387/99, GI-DP-1395, GI-DP-1412/99, GI-DP-1425/99, GI-DP-1469/99.

284 GI-DP-1331/99

285 GI-DP-1258/99, GI-DP-1373/99

również nazwiska osób (np. zajmujących określone stanowisko w firmie lub odpowiedzialnych za kontakty z innymi firmami). Nie będzie to bowiem zbiór danych osobowych, kryterium dostępu dotyczyć będzie bowiem firmy, nie osób.²⁸⁶ Inna sytuacja jest natomiast wówczas, gdy istnieje odrębny zbiór osób, ułożony według określonego kryterium dostępu, gdzie firma, którą reprezentują dane osoby, jest jedynie informacją dodatkową.

V. Powierzenie przez pracodawcę przetwarzania danych o pracownikach innemu podmiotowi

Pracodawcy przedstawiali również pytania dotyczące możliwości powierzenia innemu podmiotowi, na podstawie umowy, danych pracowników w określonym celu, np. w celu prowadzenia akt osobowych, czy wykonywania określonych usług na rzecz pracowników.

Z pytaniem dotyczącym możliwości przekazania nazwisk oraz konieczności uzyskania uprzedniej zgody pracowników na przekazanie nazwisk, zwrócił się do Generalnego Inspektora Zarząd Komunikacji Miejskiej, uzasadniając konieczność przekazywania nazwisk pracowników firmie świadczącej usługi w zakresie szycia i dostaw umundurowania poszczególnych pracowników.²⁸⁷ Pytania dotyczyły również możliwości powierzenia przez pracodawcę prowadzenia spraw księgowych firmie rachunkowej,²⁸⁸ a także powierzenia archiwizacji akt osobowych.²⁸⁹

W odpowiedzi Generalny Inspektor informował, iż zgodnie z art. 31 ustawy o ochronie danych osobowych, administrator danych może powierzyć innemu podmiotowi w drodze umowy zawartej na piśmie, przetwarzanie danych. Powierzenie przetwarzania nie wymaga uprzedniej zgody osób, których dane dotyczą, należy jednakże podkreślić, iż podmiot przetwarzający dane na podstawie umowy powierzenia, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

Sprawa udostępnienia tych danych osobom nieuprawnionym, była również przedmiotem skargi złożonej przez pracownika na pracodawcę.²⁹⁰ W wyniku postępowania administracyjnego wyjaśniono, że pracodawca zawarł z wyspecjalizowaną firmą obsługi prawnej i doradztwa prawnego umowę powierzenia na prowadzenie spraw pracowniczych. Firma upoważniona była również do reprezentowania pracodawcy przed sądem pracy, w

286 GI-DP-943/99, GI-DP-1321/99, GI-DP-1347/99

287 GI-DP-1068/99

288 GI-DP- 794/99, GI-DP-1325/99

289 GI-DP-402/99, GI-DP-350/99

290 GI-DIS-388/99

przypadku sporów pracowniczych. W związku z tym mogła wykorzystywać dane pracowników w zakresie niezbędnym do reprezentowania pracodawcy przed sądem pracy. Z tych względów skarga została oddalona.

VI. Przetwarzanie danych osobowych kandydatów do pracy, osób poszukujących pracy

Odrębną grupę stanowiły skargi i pytania związane z przetwarzaniem danych osobowych osób składających ofertę pracy u przyszłego pracodawcy lub w firmach doradztwa personalnego.

Sygnalizowane sprawy dotyczyły m.in. formy wyrażania zgody na przetwarzanie danych w firmach doradztwa personalnego oraz zakresu gromadzonych przez te firmy danych.²⁹¹ Ponieważ dołączone do pytania kwestionariusze osobowe, wprowadzi szersze, aniżeli wynikałoby to z powoływanego wcześniej rozporządzenia MPiPS z dnia 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracowników...²⁹² nie zawierały informacji, które mogłyby budzić zastrzeżenia z punktu widzenia ustawy o ochronie danych osobowych, taka odpowiedź została udzielona. Niedopuszczalne – zdaniem Generalnego Inspektora – jest natomiast przetrzymywanie dokumentacji kandydatów na pracowników po zakończeniu procesu rekrutacji przez potencjalnego pracodawcę, bez zgody osoby, której dane dotyczyły, a jedynie na podstawie ogólnej przesłanki zawartej w art. 23 ust. 1 pkt 5 ustawy o ochronie danych, tj. jeśli podstawą miałby być „usprawiedliwiony cel administratora danych”.²⁹³ Na administratorze danych ciąży bowiem obowiązek dołożenia szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zobowiązany jest przetwarzania zgodnego z prawem, zbierania dla oznaczonych, zgodnych z prawem celów i nie poddawanie dalszemu przetwarzaniu niezgodnemu z tymi celami oraz do przechowywania w postaci umożliwiającej identyfikację osób, których dane dotyczą nie dłużej, niż jest to niezbędne do osiągnięcia celu przetwarzania.

Znaczna część spraw dotyczyła żądań zwrotu złożonych dokumentów, co najczęściej następowało na etapie wyjaśniania sprawy.²⁹⁴ W toku wyjaśniania sprawy okazywało się

²⁹¹ GI-DP-1214/99

²⁹² Pytania dotyczyły m.in. znajomości obsługi komputera, znajomości języków obcych, preferowane wynagrodzenie oraz minimalne akceptowane wynagrodzenie.

²⁹³ GI-DP-800/99, podobnie GI-DP-61/99, GI-DP-615/99, GI-DP-61/99

²⁹⁴ GI-DIS-288/99

bowiem, iż osoba zainteresowana, której dotyczyła sprawa, w chwili składania dokumentów do wybranego pracodawcy lub firmy doradztwa personalnego, nie precyzowała swoich oczekiwań co do zwrotu dokumentów, natomiast później, bez własnego wcześniejszego wyjaśniania sprawy, kierowała skargę do Generalnego Inspektora.

Wobec braku wyłączenia z obowiązku rejestracji zbioru danych, zbiory kandydatów do pracy podlegają obowiązkowi rejestracyjnemu.²⁹⁵

VII. Zabezpieczanie dokumentacji personalnej – danych pracowników

Zgodnie z ustawą o ochronie danych osobowych pracodawca, jako administrator danych winien odpowiednio zabezpieczyć akta osobowe pracowników. Ustawa nie przesądza o rodzajach zabezpieczeń organizacyjnych i technicznych, które powinny być zastosowane, w szczególności nie przesądza o miejscu przechowywania akt. Nakłada jedynie na administratora danych obowiązek zastosowania takich środków, które zabezpieczą dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem (art. 36). Ich prowadzenie winno być zgodne z rozporządzeniem MPiPS w sprawie prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt.²⁹⁶

Jeśli administratorem danych ubezpieczonych pracowników jest ZUS, to – w świetle przepisów prawa - jest on, jako administrator danych, zobowiązany nie tylko do zabezpieczenia danych zgodnie z ustawą o ochronie danych osobowych, ale dane te chronione są tajemnicą służbową, a dane medyczne gromadzone przez lekarzy orzeczników – tajemnicą lekarską.

W związku z obowiązkiem odpowiedniego zabezpieczania danych dotyczących pracowników, skargi na pracodawców kierowały do Generalnego Inspektora związki zawodowe. W jednej ze skarg,²⁹⁷ związki zawodowe zwracały uwagę na dopuszczanie przez pracodawcę wglądu w wysokość zarobków poszczególnych pracowników poprzez nie zabezpieczenie tzw. „pasków wypłat”, nie zszywanych i trzymany w miejscu powszechnie dostępnym. Po wszczęciu postępowania administracyjnego w sprawie skargi, pracodawca wdrożył wszystkie zasady zabezpieczenia danych o wynagrodzeniu pracowników, w związku z powyższym postępowanie zostało umorzone.

295 GI-DP-1346/99

296 Op. cit. GI-DP-474/99, GI-DP-1152/99

297 GI-DIS 397/99

Oceniając sprawy związane z przetwarzaniem danych na potrzeby zatrudnienia, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych stwierdzić należy, iż w przeważającej części dotyczyły one pytań nt. zakresu danych niezbędnych do zatrudnienia oraz zakresu i zasad udostępniania danych zawartych w aktach osobowych pracowników związkom zawodowym, organom kontroli i innym podmiotom. W przypadku podjętych postępowań administracyjnych, już w toku wyjaśniania sprawy przywracany był stan zgodny z prawem (np. następowało korygowanie ankiet osobowych, a dane pozyskiwane niezgodnie z przepisami były usuwane, pracodawca dopełniał obowiązku informacyjnego, związki zawodowe uzyskiwały żądane informacje).

Analiza prowadzonych spraw pozwala jednocześnie na sformułowanie ogólnej uwagi, iż niedoskonałość przepisów prawa regulujących działalność poszczególnych instytucji, (np. NIK czy Państwowej Inspekcji Pracy) sprawia, że nawet w przypadku racjonalnie uzasadnionej konieczności wglądu w akta osobowe pracowników w celu ochrony przysługujących tym pracownikom praw, organy te nie mają możliwości wglądu w niektóre dokumenty. Niezbędna jest zatem zmiana odpowiednich ustaw, w celu doprecyzowania uprawnień poszczególnych instytucji kontrolnych.²⁹⁸

G. Ubezpieczenia prywatne

W tej grupie spraw najczęściej wątpliwości budziła kwestia stosowania przez PZU „Życie” S.A. ankiety osobowej przy zawieraniu i kontynuacji grupowego ubezpieczenia pracowniczego.²⁹⁹

Skargi dotyczyły najczęściej zbyt szczegółowych danych osobowych zbieranych przez PZU „Życie” S.A. i dopuszczalności żądania przez ubezpieczyciela zgody na udostępnianie zebranych danych osobom trzecim, oraz na wykorzystywanie ich w celach marketingowych.

Waga problemu i liczba kierowanych do Generalnego Inspektora pism ujawniły potrzebę szczególnie wnikliwego zbadania tej kwestii.

Z zasady adekwatności wynika zakaz gromadzenia danych w zakresie szerszym, niż ten, jaki jest niezbędny i wystarczający do osiągnięcia celu przetwarzania tych danych. W ocenie Generalnego Inspektora Ochrony Danych Osobowych gromadzenie przez Powszechny Zakład Ubezpieczeń „Życie” S.A. danych o wykształceniu, stanie cywilnym, rodzaju

²⁹⁸ W sprawie potrzeby nowelizacji stosownych ustaw, skierowana została już w roku 2000, a zatem poza okresem sprawozdawczym, sygnalizacja do Państwowej Inspekcji Pracy i Najwyższej Izby Kontroli.

²⁹⁹ GI-DP-44/99, GI-DP-144-99, GI-DP-230/99, GI-DP-394/99, GI-DP-772/99, GI-DP-998/99

wykonywanej pracy oraz żądanie wyrażenia zgody na udostępnienie informacji o stanie zdrowia, naruszało tę zasadę.

Zgodnie z treścią §§ 13 i 14 „Ogólnych warunków ubezpieczenia pracowniczego typu P”, w celu zawarcia umowy ubezpieczenia zakład pracy składa do PZU „Życie” S.A. wnioski i deklaracje zgody pracowników. Spełnienie tych warunków jest wystarczające do zawarcia umowy ubezpieczenia. Po wystawieniu przez PZU „Życie” S.A. polisy i przekazaniu jej ubezpieczającemu, umowę grupowego ubezpieczenia pracowników uważa się za zawartą. W tego rodzaju ubezpieczeniach wysokość składki wynika z sumy ubezpieczenia i nie jest uzależniona od okoliczności, takich jak rodzaj wykonywanej pracy, wykształcenia czy stanu cywilnego.

Z uzyskanych od PZU „Życie” S.A. wyjaśnień wynikało, że wypełnienie deklaracji i ankiety osobowej było warunkiem przystąpienia do grupowego ubezpieczenia. Jednocześnie nie wypełnienie ankiety przez osoby wcześniej objęte ubezpieczeniem nie oznaczało, że umowa nie może być kontynuowana.

Poważne zastrzeżenia budziła ponadto część ankiety zatytułowana „Oświadczenie”. W punkcie 1 „Oświadczenia” osoba zamierzająca zawrzeć umowę ubezpieczenia upoważniała ubezpieczyciela do uzyskiwania informacji o stanie zdrowia tej osoby od wszystkich placówek służby zdrowia, lekarzy i innych osób dysponujących tego typu danymi.³⁰⁰

Generalny Inspektor zauważył, że w myśl art. 815 ust. 1 ustawy z dnia 18 maja 1964 r. Kodeks cywilny (Dz. U. Nr 11, poz. 93 z późn. zm.) ubezpieczający obowiązany jest podać do wiadomości zakładu ubezpieczeń wszystkie znane sobie okoliczności, o które zakład ubezpieczeń pytał w formularzu oferty, albo przed zawarciem umowy w innych pismach. Jeżeli zakład ubezpieczeń zawarł umowę ubezpieczenia mimo braku odpowiedzi ubezpieczającego na poszczególne pytania, pominięte okoliczności uważa się za nieistotne. W przypadku umowy grupowego ubezpieczenia pracowniczego stan zdrowia określonej osoby nie ma wpływu na zawarcie lub kontynuację ubezpieczenia. W ubezpieczeniach grupowych nie prowadzi się oceny ryzyka ubezpieczeniowego, a przed zawarciem umowy osoba zamierzająca zawrzeć taką umowę nie podaje informacji o swoim stanie zdrowia. Nie zachodzi zatem nawet ewentualna konieczność weryfikacji informacji udzielanych przez tę

300 Ankiety osobowe zawierały zazwyczaj oświadczenie następującej treści: „Upoważniam kierownictwo placówek służby zdrowia, wszystkich lekarzy, którzy mnie kiedykolwiek leczyli lub badali, a także inne osoby dysponujące danymi o moim stanie zdrowia, do udzielenia PZU ŻYCIE S.A. wszelkich informacji dotyczących mojego stanu zdrowia”.

osobę. Możliwość ustalania stanu zdrowia zachodzi wyłącznie w związku z zaistnieniem szkody i prowadzeniem postępowania odszkodowawczego (likwidacyjnego). Podstawą do żądania tego rodzaju informacji od jednostek będących zakładami opieki zdrowotnej jest art. 18 ust. 1 pkt 6 ustawy z dnia 30 sierpnia 1991 r. o zakładach opieki zdrowotnej (Dz. U. Nr 91, poz. 408 z późn. zm.) zobowiązujący te zakłady do udostępniania dokumentacji medycznej organom rentowym, zakładom ubezpieczeniowym oraz zespołom do spraw orzekania o stopniu niepełnosprawności, w związku z prowadzonym przez nie postępowaniem. Oznacza to, że fakt prowadzenia postępowania odszkodowawczego uprawnia firmę ubezpieczeniową do dokonywania analizy dokumentacji medycznej. Również i w tej sytuacji ubezpieczyciel może żądać udzielenia informacji w zakresie niezbędnym do realizacji celu, jakim jest ustalenie okoliczności wypadku, opieki medycznej sprawowanej w związku z wypadkiem, wcześniejszego stanu zdrowia, który ewentualnie miał wpływ na powstanie szkody. Prawo do żądania udostępnienia dokumentacji lekarskiej w tym zakresie wynika z przepisu art. 18 ust. 1 pkt 6 ustawy o zakładach opieki zdrowotnej, nie jest zatem konieczne żądanie zgody od osoby, która ma zostać objęta ubezpieczeniem.

Szczególne zastrzeżenia Generalnego Inspektora wzbudził punkt 2 oświadczenia w części dotyczącej ewentualnego wyrażenia zgody na udostępnienie danych osobowych Powszechnemu Towarzystwu Emerytalnemu PZU S.A.

Ustawa z dnia 28 sierpnia 1997 r. o organizacji i funkcjonowaniu funduszy emerytalnych (Dz. U. Nr 139, poz. 934 z późn. zm.) oraz przepisy wykonawcze do tej ustawy, tj. rozporządzenie Rady Ministrów z dnia 9 czerwca 1998 r. w sprawie sposobu i trybu zawarcia umowy, na podstawie której następuje uzyskanie członkostwa w otwartym funduszu emerytalnym, sposobu i terminu składania oświadczenia o małżeńskich stosunkach majątkowych członka otwartego funduszu emerytalnego oraz zawiadamiania otwartego funduszu emerytalnego o każdorazowej zmianie w stosunku do treści takiego oświadczenia, obejmującej środki zgromadzone na rachunku członka (Dz. U. Nr 84, poz. 534) oraz rozporządzenie Rady Ministrów z dnia 12 maja 1998 r. w sprawie szczegółowych zasad prowadzenia rejestru członków funduszu emerytalnego, szczegółowego zakresu informacji, które powinny być zawarte w rejestrze, oraz zasad sporządzania i przechowywania kopii danych zawartych w rejestrze na wypadek jego utraty (Dz. U. Nr 63, poz. 402), szczegółowo określają zakres danych, jakie mogą być przetwarzane przez fundusze emerytalne. Z treści art. 89 ust. 2 ustawy o organizacji i funkcjonowaniu funduszy emerytalnych wyraźnie wynika, że fundusz może gromadzić tylko podstawowe dane osobowe członków, szczegółowo wymienione w tym przepisie (imię, nazwisko, data urodzenia, adres zamieszkania, PESEL lub

NIP oraz serię i numer dowodu osobistego). Z treści tej ustawy oraz przepisów wykonawczych określających sposób i tryb zawarcia umowy z funduszem wynika, że fundusz ma prawo przetwarzać również dane pozwalające na identyfikację osoby lub osób, którym należy wypłacić środki po śmierci członka otwartego funduszu emerytalnego (imię, nazwisko, data urodzenia oraz adres zamieszkania). Zdaniem Generalnego Inspektora Ochrony Danych Osobowych, bez znaczenia zatem jest wyrażenie przez osobę, której dane dotyczą zgody na udostępnienie jej danych, gdyż fundusze emerytalne mają prawo gromadzić dane osobowe tylko w zakresie ustalonym przepisami prawa, co oznacza niedopuszczalność przekazywania danych pozyskiwanych przez PZU „Życie” S.A. w ankiecie personalnej funduszom emerytalnym.

Budziła również wątpliwości część oświadczenia, w której informuje się o celu zbierania danych przez PZU „Życie” S.A. Z jej treści wynika, że dane gromadzone są w celu prowadzenia prawidłowej i sprawnej obsługi ubezpieczenia i przekazywania ubezpieczonemu informacji dotyczącej ubezpieczeń. Jak zauważył Generalny Inspektor obowiązek informowania o trwającym ubezpieczeniu wynika z samego faktu zawarcia umowy. Natomiast informowanie o możliwości zawarcia również innej umowy i skorzystania z innych usług świadczonych przez PZU „Życie” S.A. rozpatrywać należy już w kategoriach działalności marketingowej, reklamowej. Udostępnianie danych osobowych w celu zawarcia umowy nie może być traktowane jako zgoda na przetwarzanie danych osobowych w celu przesyłania ulotek zawierających informacje o innych rodzajach ubezpieczeń.

W toku postępowania sprawdzającego analizowano również problem gromadzenia za pośrednictwem ankiety, informacji o osobach trzecich. PZU „Życie” S.A. udzieliło Generalnemu Inspektorowi Ochrony Danych Osobowych informacji dotyczących przetwarzania danych o członkach rodziny ubezpieczonego. Z treści wyjaśnień wynika, że zawarcie umowy grupowego ubezpieczenia wiąże się z odpowiedzialnością ubezpieczyciela, np. z tytułu śmierci osób współubezpieczonych. Posiadanie takich informacji jest zatem niezbędne do oceny ryzyka oraz ustalenia rezerwy ubezpieczeń i w tej części treść ankiety nie budzi zastrzeżeń.

Generalny Inspektor Ochrony Danych Osobowych zwrócił się do PZU „Życie” S.A. o podjęcie stosownych działań w celu przywrócenia stanu zgodnego z prawem. W odpowiedzi z dnia 16 sierpnia 1999 r. PZU „Życie” S.A. zobowiązało się do zmodyfikowania wzoru formularza „deklaracji zgody” oraz poinformowało o rezygnacji z ankiety osobowej, jako dokumentu obligatoryjnego przy zawarciu umowy.

H. Przetwarzanie danych osobowych w sektorze telekomunikacyjnym

I. Zagadnienia wstępne

W 1999 roku do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło wiele skarg i zapytań prawnych dotyczących przetwarzania danych osobowych przez podmioty występujące w sektorze telekomunikacyjnym. Osoby fizyczne skarżyły się na zbyt szeroki w ich ocenie zakres przetwarzania danych przez operatorów telefonii komórkowej i stacjonarnej. Większość pytań dotyczyła problematyki udostępniania danych osobowych przez operatorów sieci telekomunikacyjnej użytku publicznego, a także zasadności sporządzania kserokopii dokumentów tożsamości przez operatorów sieci telefonii komórkowej przy zawieraniu umów o świadczenie usług telekomunikacyjnych z osobami fizycznymi.

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

W roku sprawozdawczym do Generalnego Inspektora Ochrony Danych Osobowych wpłynęło wiele skarg i zapytań prawnych w przedmiocie zbyt szerokiego zakresu przetwarzania danych osobowych abonentów przez operatorów sieci telekomunikacyjnej. Najlichniesza grupa skarg dotyczyła legalności przetwarzania danych osobowych klientów Telekomunikacji Polskiej S.A. Szczególnie wiele wątpliwości pojawiło się w związku z odmową udostępniania informacji o numerach telefonów przez pracowników Telekomunikacji Polskiej S.A. z powoływaniem się na ustawę o ochronie danych osobowych. Generalny Inspektor informował, iż ustawa o ochronie danych osobowych nie uniemożliwia udostępniania danych osobowych w sytuacjach, gdy zezwalają na to przepisy prawa. Podmioty świadczące usługi telekomunikacyjne w sieciach telekomunikacyjnych użytku publicznego, zwane operatorami, działają na podstawie 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 (chyba że abonent zastrzeże poufność tej informacji), a także obowiązek zapewnienia własnym abonentom uzyskania informacji o numerach stacji abonenckich osiąganych z ich stacji

abonenckiej.³⁰¹ Generalny Inspektor Ochrony Danych Osobowych w piśmie z dnia 23 marca zasygnalizował Zarządowi TP S.A. wynikający z powołanych przepisów rozporządzenia obowiązek udzielania przez biura numerów informacji o numerach telefonów abonentów telekomunikacji.³⁰²

W tym samym piśmie Generalny Inspektor odniósł się do problemu upubliczniania danych osobowych, który zaistniał w związku z użyciem w rozporządzeniu pojęcia „spis abonentów”. Informacja o abonentach powinna ograniczać się do podania numeru telefonu oraz imienia i nazwiska abonenta, zaś w przypadku powtarzalności imion i nazwisk możliwe byłoby podanie także nazwy ulicy, przy której abonent mieszka, z wyjątkiem zastrzeżenia poufności tych informacji przez abonenta. Podawanie innych informacji, w ocenie Generalnego Inspektora, wykraczałoby poza zakres „informowania o abonencie”.³⁰³ Konieczność nowelizacji przedmiotowego rozporządzenia, celem uniknięcia trudności interpretacyjnych, Generalny Inspektor wskazał także w piśmie z dnia 28 maja 1999 r. skierowanym do Ministra Łączności, w którym zasygnalizował, aby przepisy rozporządzenia w sposób dokładny określały, jakie dane osobowe abonenta mogą być udostępniane.³⁰⁴

W dniu 31 marca 1999 r. Generalny Inspektor wystąpił do Przewodniczącego Komisji Transportu i Łączności Sejmu Rzeczypospolitej Polskiej w sprawie projektu ustawy – Prawo telekomunikacyjne, w którym przepis art. 72 podobnie jak dotychczasowe przepisy, nie sprecyzował zakresu danych osobowych zawartych w spisie abonentów, stwierdzając jedynie że *„Dane osobowe zawarte w publicznie dostępnym spisie abonentów, a także udostępniane za pośrednictwem służb informacyjnych operatora powinny być ograniczone do zakresu niezbędnego do identyfikacji abonenta”*. Generalny Inspektor zaproponował zapis, który w sposób precyzyjny miałby określać, jakie dane o abonencie umieszcza się w spisie abonentów, jak również umożliwiałby abonentowi złożenie zastrzeżenia dotyczącego umieszczania jego danych w publicznie dostępnym spisie abonentów. Takie sformułowanie pozwoliłoby na uniknięcie wątpliwości interpretacyjnych, pozwoliłoby także, na wniosek abonenta, na rozszerzenie zakresu danych zawartych w spisach, oprócz dokładnego adresu lub części adresu, również o inne informacje (które dotychczas znajdowały się w książkach telefonicznych) ważne dla abonenta, dotyczące, np. stopnia czy tytułu naukowego lub zawodu.³⁰⁵ Książki telefoniczne mogłyby zatem zawierać dwa rodzaje informacji o

301 GI-DP-3/99, GI-DIS-160/99/482

302 GI/317/99

303 GI-DIS-161/99/621 i 707, GI/317/99

304 GI/513/99

305 GI/343/99, GI-DP-134/99

abonentach: informacje podstawowe, dotyczące abonentów, którzy nie rozszerzyli zakresu informacji o sobie i informacje rozszerzone, gdy abonent indywidualnie określi, jakie dane o nim powinny się znaleźć w książce telefonicznej.³⁰⁶

Na początku 1999 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło pismo w sprawie publikowania list abonentów przez Telekomunikację Polską S.A. Pismo nawiązywało do planowanej przez Telekomunikację w pierwszym kwartale 1999 roku, akcji rozesłania do swoich abonentów formularzy oświadczeń o wyrażeniu zgody na umieszczenie ich danych osobowych w publikowanej liście abonentów (książce telefonicznej) oraz wykorzystanie ich w celach marketingowych. W piśmie z dnia 5 lutego 1999 r. Generalny Inspektor wyraził jednoznaczny pogląd, iż opracowanie ankiety w ten sposób, że abonent może wyrazić zgodę na umieszczenie jego danych w książce telefonicznej i biurze informacji o numerach, wyłącznie z równoczesną zgodą na przetwarzanie danych w celach marketingowych, a brak zgody będzie traktowany jako zastrzeżenie numeru, nie znajduje uzasadnienia. Mimo bowiem nieuzyskania zgody abonenta, w przypadku niezastrzeżenia numeru operator sieci telekomunikacyjnej ma obowiązek informowania o numerach telefonów swoich abonentów w omówionym zakresie.³⁰⁷ W wyniku powyższego Telekomunikacja Polska S.A. zrezygnowała z przeprowadzenia akcji rozsyłania omawianych formularzy, a swoim abonentom przesłała jedynie pisemną informację, zgodną z treścią art. 24 ustawy o ochronie danych osobowych.

W piśmie z dnia 23 grudnia 1998 r. skierowanym do Telekomunikacji Polskiej S.A. Generalny Inspektor ustosunkował się do będącej przedmiotem wielu skarg problematyki zakresu informacji zawartych w książkach telefonicznych. Operator sieci telekomunikacyjnej użytku publicznego, zgodnie z treścią § 4 ust. 1 pkt 5 rozporządzenia Ministra Łączności z dnia 8 lutego 1996 r. w sprawie ogólnych warunków świadczenia usług telekomunikacyjnych w sieci telekomunikacyjnej użytku publicznego, ma obowiązek zapewnienia publicznego dostępu do spisów własnych abonentów, chyba, że abonent zastrzeże poufność tej informacji. A zatem, jeśli brak jest wyrażonego wprost zastrzeżenia abonenta, książka telefoniczna powinna zawierać przynajmniej spis abonentów (jeśli abonent nie wypowie się, co do zakresu informacji, które powinny znajdować się w książce telefonicznej informacji) albo informacje wskazane przez abonenta, nie wykraczające poza cel, jaki ma spełniać książka telefoniczna.³⁰⁸

306 Stanowisko Generalnego Inspektora zostało omówione w artykule „Rzeczpospolitej” z dnia 2 kwietnia 1999 r.

307 GI/101/99

308 GI/562/98

Złożenie zastrzeżenia o którym wyżej mowa, powoduje, że operator sieci telekomunikacyjnej nie może podawać do publicznej wiadomości informacji dotyczących zastrzeżonych numerów telefonicznych.³⁰⁹ Opublikowanie w książce telefonicznej, będącej spisem abonentów, np. Telekomunikacji Polskiej S.A. zastrzeżonego przez abonenta numeru jego telefonu wraz z jego danymi osobowymi stanowi naruszenie ustawy o ochronie danych osobowych i w takim wypadku Generalny Inspektor - poprzez wydanie decyzji - nakazywał zgodnie z art. 18 ust. 1 ustawy przywrócić stanu zgodnego z prawem, a w szczególności usunięcie uchybień.

W przekonaniu Generalnego Inspektora, każdy z abonentów, realizując konstytucyjną zasadę prawa do prywatności, polegającą również na tym, iż każda osoba ma prawo decydować o tym w jakim zakresie udziela informacji o sobie (o ile nakaz udzielania informacji nie wynika z przepisów prawa), ma prawo podjęcia samodzielnie decyzji i określenia, jakie bliższe informacje na temat jego osoby mają znaleźć się w książce telefonicznej.

Duża liczba skarg dotyczyła umieszczenia w książce telefonicznej danych osobowych bez zgody osoby, której dane dotyczą. Generalny Inspektor uznał, iż skargi takie są bezzasadne z uwagi na fakt, że operator sieci telekomunikacyjnej użytku publicznego jest prawnie zobowiązany do zapewnienia publicznego dostępu do spisu własnych abonentów, którzy nie zastrzegli poufności takich informacji.³¹⁰ Bezzasadna okazała się również skarga, dotycząca opublikowania w książce telefonicznej zastrzeżonego numeru telefonu, ze względu na brak dokumentów potwierdzających, iż skarżący wystąpił o zastrzeżenie numeru.³¹¹ Jak wykazały niektóre z przeprowadzonych postępowań wyjaśniających, zastrzeżone numery telefoniczne skarżących były wskutek nieprawidłowego wypełnienia umowy o świadczenie usług telekomunikacyjnych udostępniane przez służby informacyjne TP S.A., jak również znajdowały się w spisie telefonów Abonentów Telefonów Telekomunikacji Polskiej S.A., albowiem nie przedstawiono skarżącym wniosku o zastrzeżenie numeru telefonu. W wyniku interwencji samych skarżących dane te zostały usunięte z baz Komputerowego Biura Numerów. W takim przypadku Generalny Inspektor uznawał za niecelowe wszczynanie postępowania administracyjnego, zaś w kwestiach związanych z niedopatrzeniem ze strony pracowników telekomunikacji odsyłał do uregulowań zawartych w kodeksie cywilnym.³¹²

309 GI-DIS-100/99/262, GI-DP-126/99/173

310 GI-DIS-68/99, GI-DIS/86/99/412

311 GI-DIS-67/99/552

312 GI-DIS-87/99/415, GI-DIS-192/99/730

Do Generalnego Inspektora wpłynęła również skarga dotycząca udostępnienia zastrzeżonego numeru abonenta pracownikom Policji i prokuratury. Jak wynikało z wyjaśnień udzielonych przez telekomunikację, zastrzeżony numer telefoniczny nie był udostępniany organom prokuratury, Policji, jak też i innym podmiotom. Administrator danych wyjaśnił ponadto, że dostęp do bazy numerów zastrzeżonych jest chroniony elektronicznie i każda operacja przeprowadzana przez osoby uprawnione byłaby automatycznie zarejestrowana. Generalny Inspektor poinformował, iż w związku z prowadzonym postępowaniem karnym, organy prokuratury i Policji mają prawo przetwarzania danych osobowych danych abonentów Telekomunikacji Polskiej S.A. i m.in. uzyskiwania informacji o numerach zastrzeżonych. Zgodnie z art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych, ustawodawca dopuścił możliwość przetwarzania danych osobowych, jeśli zezwalają na to przepisy prawa. Art. 15 § 2 ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (Dz. U. Nr 89, poz. 555) stanowi, że wszystkie instytucje państwowe, samorządowe i społeczne są obowiązane w zakresie swego działania do udzielania pomocy organom prowadzącym postępowanie karne. Zgodnie z art. 14 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. Nr 30, poz. 179 z późn. zm.), w granicach swych zadań Policja w celu rozpoznania, zapobiegania i wykrywania przestępstw i wykroczeń wykonuje czynności operacyjno-rozpoznawcze, dochodzeniowo-sledcze i administracyjno-porządkowe. Policja wykonując w/w czynności ma prawo żądania niezbędnej pomocy – w zakresie obowiązujących przepisów prawa – od instytucji państwowych, organów administracji rządowej i samorządu terytorialnego oraz jednostek gospodarczych prowadzących działalność w zakresie użyteczności publicznej. Ma również prawo zwracania się do innych jednostek gospodarczych oraz organizacji społecznych, a w nagłych wypadkach do każdej osoby o udzielenie doraźnej pomocy, w ramach obowiązujących przepisów prawa. W związku z powyższym należy stwierdzić, iż Policja z mocy uprawnień nadanych jej przez ustawę ma prawo do uzyskania informacji o zastrzeżonym numerze telefonu abonenta. Generalny Inspektor poinformował ponadto, iż nie jest uprawniony lub zobowiązany do dokonania oceny działalności Policji i wymiaru sprawiedliwości, zaś na sposób prowadzenia powołanych wyżej czynności przez Policję, przysługuje skarżącym na podstawie art. 15 ust. 7 ustawy o Policji zażalenie do miejscowo właściwego prokuratora.³¹³

Wśród zapytań pojawiła się również kwestia legalności udostępniania przez operatorów sieci wykazu zrealizowanych połączeń telefonicznych, tzw. bilingu. Generalny

313 GI-DIS-329/99/1005, GI-DP-620/99/626

Inspektor wyjaśnił, iż ustawa o ochronie danych osobowych znajduje zastosowanie do ochrony danych pozwalających na identyfikację osoby fizycznej. Zgodnie bowiem z art. 6 ustawy, za dane osobowe uważa się każdą informację dotyczącą osoby fizycznej pozwalającą na określenie tożsamości tej osoby. Wykaz zrealizowanych połączeń telefonicznych wystawiany na wniosek abonenta przez operatora sieci telekomunikacyjnej na podstawie § 5 cytowanego wyżej rozporządzenia Ministra Łączności z dnia 8 lutego 1996 r. w sprawie ogólnych warunków świadczenia usług telekomunikacyjnych użytku publicznego, zawiera szczegółowy wykaz usług, z których abonent skorzystał wraz z danymi umożliwiającymi ich identyfikację, a więc numer abonenta wybranego, czas rozpoczęcia i zakończenia połączenia. Nie zawiera natomiast żadnych informacji stanowiących dane osobowe, w związku z czym ustawa o ochronie danych osobowych nie znajduje tu zastosowania.³¹⁴

Osobnym zagadnieniem często pojawiającym się w treści skarg i zapytań prawnych była zasadność odmowy udzielania informacji o rozmowach telefonicznych przychodzących na numer stacji abonenckiej skarżących. W ocenie Generalnego Inspektora działanie takie znajduje uzasadnienie w przepisach prawa. Stosownie do § 4 ust. 1 pkt. 6 cytowanego wyżej rozporządzenia, operator jest zobowiązany do zapewnienia własnym abonentom uzyskania informacji o numerach stacji abonenckich osiąganych z ich stacji abonenckiej. Zgodnie zaś z § 5 ust. 1 rozporządzenia operator zobowiązany jest także do rejestracji i przechowywania co najmniej przez 12 miesięcy danych zawierających szczegółowy wykaz usług, z których abonent skorzystał, wraz z danymi umożliwiającymi identyfikację usługi, numer abonenta wybranego, czas rozpoczęcia i zakończenia połączenia, a na wniosek abonenta – do dostarczania szczegółowego wykazu zrealizowanych połączeń za okres objęty fakturą. Tym samym operator sieci nie jest zobowiązany przepisami prawa do dostarczania abonentowi wykazu numerów przychodzących do jego stacji abonenckiej.

Udostępnienie danych, zależy od arbitralnego rozstrzygnięcia właściwego organu, który decyduje o zasadności skierowanego wniosku, postanawiając ewentualnie o udostępnieniu bądź nie udostępnieniu danych. Dane osobowe, na podstawie art. 29 ust. 2 ustawy udostępnia się na pisemny, umotywowany wniosek, w celu innym niż włączenie do zbioru, chyba że przepis szczególny innej ustawy stanowi inaczej. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie. Udostępnione dane można wykorzystywać wyłącznie zgodnie z przeznaczeniem, dla którego zostały zebrane. Wzór wniosku, określony został jako

314 GI-DP-1605/99/88, GI-DP-1665/99/19

załącznik nr 1 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.). Urząd administracji publicznej jako administrator danych, może postanowić o nieudostępnianiu danych ze zbioru, jeżeli zachodzą przesłanki z art. 30 ustawy. Wydane przez organ administracji publicznej postanowienie o odmowie udostępnienia żądanych danych osobowych stanowi - w rozumieniu przepisów kodeksu postępowania administracyjnego, odmowę wydania zaświadczenia. Na takie postanowienie wydane przez urząd administracji publicznej służy (osobie wnioskującej o udostępnienie danych osobowych) zażalenie do organu wyższego stopnia.³¹⁵

W omawianym okresie sprawozdawczym do Biura Generalnego Inspektora Ochrony Danych Osobowych wpływało wiele sygnałów dotyczących niezgodnego z prawem przetwarzania danych osobowych przez operatorów sieci komórkowej.³¹⁶ Operatorzy ci przy zawieraniu umów o świadczenie usług telekomunikacyjnych sporządzali kserokopie dokumentów tożsamości osób fizycznych – stron umowy. Nadto przy kserowaniu dowodu osobistego dochodziło do udostępniania danych osobowych osób trzecich. Praktyka ta wzbudziła wątpliwości Generalnego Inspektora z uwagi na fakt, iż sporządzanie 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, jak też dane osób trzecich. Tymczasem ustawa o ochronie danych osobowych nakłada na administratora danych obowiązek dołożenia 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 (art. 26 ust. 1 ustawy).

Sporządzanie kserokopii dokumentów prowadzi również do udostępnienia danych osób trzecich. Generalny Inspektor Ochrony Danych Osobowych zwrócił uwagę, iż przetwarzanie danych osobowych powinno ograniczać się do minimum niezbędnego do zawarcia umowy o świadczenie usług telekomunikacyjnych, a więc imienia, nazwiska, adresu i numeru PESEL abonenta. Dane te są zawarte w dokumencie tożsamości obowiązującym na

315 GI-DP-1432/99/1594

316 GI-DIS-130/99/539, GI-DIS-245/99/654, GI-DP-445/99/451, GI-DIS-479/99/151/00, GI-DP-534/99/582, GI-DP-1117/99/1368

terenie Rzeczypospolitej, jakim jest dowód osobisty, tymczasowy dowód osobisty, tymczasowe zaświadczenie tożsamości, czy paszport (ustawa z dnia 10 kwietnia 1974 roku o ewidencji ludności i dowodach osobistych, Dz. U. Nr 32 poz. 174 z późn. zm.). Z tego punktu widzenia nie ma potrzeby weryfikacji danych abonenta, poprzez okazywanie innych dodatkowych dokumentów, czego wymagało jedno z postanowień regulaminu świadczenia usług telekomunikacyjnych o charakterze powszechnym, obowiązującego w sieci operatora telefonii. Szczególna ochrona abonenta wynikać powinna z faktu, iż umowa do której przystępuje klient 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. Zbieranie danych w zakresie żądanym przez jednego z operatorów telefonii komórkowej, jest w ocenie Generalnego Inspektora naruszeniem zasady adekwatności, o której mowa w cytowanym już artykule 26 ustawy o ochronie danych osobowych.³¹⁷ Powyższa problematyka była przedmiotem szerokiej publikacji na łamach czasopisma „Rzeczpospolita” z dnia 10 czerwca 1999 roku.

Ponadto Generalny Inspektor Ochrony Danych Osobowych w dniu 11 października zwrócił się do Prezesa Urzędu Ochrony Konkurencji i Konsumentów o dokonanie analizy, czy opisane wyżej praktyki nie stanowią nadużycia przez operatorów sieci komórkowej pozycji dominującej na rynku i czy nie są praktykami monopolistycznymi w rozumieniu art. 5 ust. 1 pkt 6 ustawy z dnia 24 lutego 1990 r. o przeciwdziałaniu praktykom monopolistycznym i ochronie interesów konsumentów (Dz. U. Z 1999 r. Nr 52, poz. 547), który przewiduje, że praktyką monopolistyczną jest nadużycie pozycji dominującej na rynku, poprzez narzucanie uciążliwych warunków umów przynoszącym przedsiębiorcy narzucającemu takie warunki nieuzasadnione korzyści. Wiceprezes Urzędu Ochrony Konkurencji i Konsumentów wyjaśnił, iż zgodnie z art. 2 pkt. 7 ustawy antymonopolowej pozycję dominującą może posiadać przedsiębiorca, który nie spotyka się z istotną konkurencją. Każdy z operatorów komórkowych działających w Polsce spotyka się z konkurencją, którą w ocenie Urzędu można określić jako istotną ze strony pozostałych dwóch firm. Ponieważ polska ustawa antymonopolowa nie przewiduje tzw. kolektywnej pozycji dominującej, którą mogłyby mieć, np. trzy firmy jako jedyne działające na rynku, żadnemu z operatorów nie można zarzucić pozycji dominującej. Brak również przesłanek na to, że działania operatorów komórkowych

317 GI-DEC/52/99/DIS-4/99/DP-11/99/926

są wynikiem jakichkolwiek uzgodnień między nimi.³¹⁸ Do Generalnego Inspektora kierowano również skargi dotyczące niewłaściwego zabezpieczenia danych osobowych przetwarzanych przez operatorów sieci telefonii komórkowej poprzez udostępnienie osobie nieuprawnionej wykazu rozmów telefonicznych. Zgodnie z art. 36 ustawy o ochronie danych osobowych, administrator danych jest zobowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem. W przypadku stwierdzenia naruszenia przedmiotowego obowiązku Generalny Inspektor wydawał decyzję nakazującą usunięcie uchybień poprzez zastosowanie dodatkowych środków zabezpieczających zgromadzone dane osobowe.³¹⁹

W zapytaniach prawnych i skargach podnoszone były także kwestie wykorzystania przez operatora sieci komórkowej danych osobowych abonenta w loterii promocyjnej i tworzonego na jej potrzeby raportu zawierającego informacje o charakterze osobowym. Jak wynikało z wyjaśnień administratora danych zbiór danych osobowych o nazwie „raport” był utworzony jedynie doraźnie, ze względów technicznych – w celu przyznania nagrody. Skarżących poinformowano, iż zgodnie z art. 2 ust.1 pkt 3 ustawy, w odniesieniu do zbiorów danych osobowych sporządzanych doraźnie, wyłącznie ze względów technicznych, szkoleniowych lub w związku z dydaktyką w szkołach wyższych, a po ich wykorzystaniu niezwłocznie usuwanych albo poddanych anonimizacji, przepisy ustawy o ochronie danych osobowych nie mają zastosowania, z wyjątkiem przepisów rozdziału 5 dotyczących obowiązku zabezpieczenia zbioru danych przez administratora zbioru. Wskazano ponadto, że jeżeli skarżący nie wyraził zgody na przetwarzanie danych w celach marketingowych, jego dane nie mogą być przetwarzane w tym celu przez operatora.³²⁰

Generalny Inspektor był adresatem skargi na operatora telefonii sieci komórkowej. Jak wynikało z treści pisma skarżącego, pracownicy sklepów firmowych powyższego przedsiębiorstwa żądali przy dokonywaniu zakupów w tych sklepach podania numerów komórkowych działających w ich sieci, gdyż tylko pod tym warunkiem można było nabyć żądany towar. Na otrzymywanej wówczas fakturze znajdowały się takie dane osobowe jak nazwisko oraz adres zamieszkania osoby, będącej abonentem odpowiedniego numeru. W związku z powyższym Biuro GODO zwróciło się do operatora sieci o wyjaśnienie

318 GI-DP-1574/99

319 DEC/GI/DIS/31/99/441 i 442

320 GI-DIS-326/99/1253

przedmiotowej sytuacji. Na skutek tej interwencji PTC Sp. z o. o. stwierdziła naruszenie obowiązujących w przedsiębiorstwie procedur, zaś osoby winne zostały ukarane dyscyplinarnie. Ponadto podjęto niezbędne działania zapobiegające wystąpieniu podobnych zdarzeń w przyszłości.³²¹

Niektóre z zapytań dotyczyły zasadności pobierania, przez operatorów sieci komórkowej, opłat za zastrzeżenie danych osobowych abonenta. Generalny Inspektor poinformował, że stosownie do art. 39 ust. 1 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 komórkowej, w którym jest określony zakres, sposób oraz zasady świadczenia usług. Podstawa pobierania opłat za świadczenie usługi zastrzeżenia danych abonenta zazwyczaj określona jest w takich regulaminach. Regulaminy te stanowią, iż opłaty za usługi i szczegółowe zasady ich naliczania zawarte są w cenniku. Cennik zawiera opłaty zarówno z tytułu świadczenia usług podstawowych, jak i dodatkowych, w tym usług zastrzeżenia danych. 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. Abonent, zawierając więc umowę z operatorem sieci komórkowej wyraził równocześnie zgodę na proponowane przez nią warunki i zobowiązał się do ich przestrzegania. W świetle powyższego Generalny Inspektor stwierdził, że nie jest uprawniony lub zobowiązany do dokonania oceny treści umów cywilnoprawnych, a zwłaszcza do stwierdzenia zasadności pobierania opłat za zastrzeżenie numeru przez operatorów telefonii komórkowej.³²²

Generalnemu Inspektorowi Ochrony Danych Osobowych wielokrotnie sygnalizowano naruszenie przepisów o ochronie danych osobowych przez operatorów telefonii komórkowej w postaci przetwarzania danych osobowych ich pracowników dotyczących karalności. Wyniki przeprowadzonej kontroli dały podstawy do wszczęcia postępowania administracyjnego w celu zapewnienia stanu zgodnego z prawem. W myśl art. 28 ust. 1 ustawy, przetwarzanie danych dotyczących m.in. skazań, można prowadzić wyłącznie na podstawie ustawy. Rozporządzenie 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), stanowi w § 12 ust. 2 pkt 3, że

321 GI-DP-14449/99

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. Wynika z tego, że jeżeli przepisy szczególne dotyczące zatrudnienia na danym stanowisku lub w danej służbie uzależniają podjęcie pracy (służby), od stwierdzenia niekaralności kandydata, istnieje prawna podstawa do występowania przez pracodawców z zapytaniem o karalność pracownika. Takich przepisów szczególnych, które pozwalałyby operatorom telefonii komórkowej na przetwarzanie danych osobowych o karalności swoich pracowników nie ma. Spółka wyjaśniła, że zaprzestano przetwarzania danych o karalności pracowników.

III. Inne zagadnienia

Odrębna grupa zagadnień dotyczyła kwestii przesyłania rachunków telefonicznych listem zwykłym oraz niezakodowania numeru telefonicznego skarżącego w przesyłanych mu rachunkach telefonicznych. Po przeprowadzeniu postępowania wyjaśniającego stwierdzono, że Zakład Telekomunikacji nie ma obowiązku przesyłania rachunków telefonicznych listami poleconymi, a zupełnie wystarczającą formą zabezpieczenia informacji przesyłanych abonentom jest forma listu zwykłego, zaś co do dalszej części wniosku poradzono skarżącym złożenie skargi do Zakładu Telekomunikacji.³²³

W jednym z pism jakie wpłynęły do Biura Generalnego Inspektora Ochrony Danych Osobowych Zakład Telekomunikacji zwrócił się z wnioskiem o zobligowanie jednego z podmiotów samorządu terytorialnego do udostępniania danych osób zadłużonych w stosunku do TP S.A. Jak wykazał przedstawiony w piśmie stan faktyczny, przedmiotowe dane Zakład Telekomunikacji chciał pozyskać w celu włączenia do zbioru. Generalny Inspektor wyjaśnił, iż analiza ustawy o ochronie danych osobowych, a w szczególności wykładnia celowościowa i systemowa jej przepisów pozwala na przypuszczenie, iż w przypadku pozyskiwania danych w celu włączenia do zbioru muszą zostać spełnione podobne wymogi jakie są określone w art. 29 ustawy o ochronie danych osobowych, tzn. wniosek o udostępnienie danych powinien w sposób wiarygodny uzasadniać potrzebę ich posiadania, a udostępnienie nie naruszy praw i wolności osób, których dane dotyczą. Jednocześnie Generalny Inspektor zauważył, iż podstawę do przetwarzania, więc także pozyskiwania danych osób zadłużonych może w przedmiotowej sprawie stanowić art. 23 ust. 1 pkt 3 lub 5 ustawy, zgodnie z którym przetwarzanie jest dozwolone, gdy jest niezbędne osobie, której dane dotyczą w celu wywiązania się z umowy, której jest stroną lub jest niezbędne do wypełnienia

322 GI-DIS-20/99/272, GI-DP-566/99/588

usprawiedliwionych celów administratora danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.³²⁴

Indywidualne zapytania dotyczyły przetwarzania przez telefonie komórkowe informacji o firmach będących spółkami z o. o. takich jak wypis z rejestru sądowego, czy nazwiska właściciela firmy. W odpowiedzi na powyższe Generalny Inspektor zauważył, że zarząd spółki z ograniczoną odpowiedzialnością zgłasza zawiązanie spółki celem wpisania jej do rejestru. Stosownie do art. 166 pkt 1 i 4 kodeksu handlowego wpis powinien obejmować firmę, siedzibę, adres i przedmiot przedsiębiorstwa oraz imiona i nazwiska członków zarządu. Powyższe informacje są jawne, tzn. każdy może pod nadzorem sekretarza sądowego w godzinach urzędowych przeglądać rejestr handlowy i dokumenty złożone do rejestru. Równocześnie zaznaczono, iż dane przedsiębiorców w zakresie prowadzonej przez nich działalności, nawet jeśli pozwalają na ustalenie ich tożsamości, nie podlegają ochronie wynikającej z przepisów ustawy o ochronie danych osobowych, a dochodzenie roszczeń z tytułu poniesionej szkody może odbywać się ewentualnie w drodze procesu cywilnego.³²⁵ Dane ujawnione w ewidencji działalności gospodarczej są danymi podmiotu gospodarczego, nie zaś danymi osobowymi w rozumieniu ustawy o ochronie danych osobowych.³²⁶

Spośród licznych pytań prawnych, które napłynęły w omawianym okresie sprawozdawczym do Biura Generalnego Inspektora Ochrony Danych Osobowych pojawiło się również zagadnienie dotyczące legalności ujawniania numeru telefonicznego abonenta inicjującego połączenie telefoniczne, bez jego zgody, abonentowi do którego to połączenie jest kierowane, przy zastosowaniu specjalnych urządzeń technicznych. Urządzenia te nie są w Polsce dopuszczone do dołączenia do sieci telekomunikacyjnej użytku publicznego, a zasadność uchylenia zakazu jest przedmiotem rozważań Ministra Łączności, który zgodnie z art. 7 ustawy o łączności decyduje o dopuszczeniu do stosowania urządzeń telekomunikacyjnych. Generalny Inspektor poinformował, iż 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. W ocenie Generalnego Inspektora zestaw numerów telefonicznych nie tworzy takiego zbioru. Numer telefonu nie jest zwykle daną osobową w rozumieniu art. 6 ustawy, nie pozwala bowiem na ustalenie tożsamości

323 GI-DIS-150/99/392, GI-DIS-152/99/529

324 GI-DP-454/99/534

325 GI-DP-510/99/589

326 GI-DP-1515/99/1687

osoby fizycznej. Nie ma także określonej struktury i kryterium dostępności do danych. Tak więc zagadnienie ujawniania numeru abonenta inicjującego połączenie jest z punktu widzenia ustawy o ochronie danych osobowych obojętne. W takiej sytuacji dopuszczalność rozwiązania technicznego, będącego przedmiotem rozważań, należałoby rozważyć na gruncie innych przepisów prawa.³²⁷

Generalny Inspektor wielokrotnie zwracał uwagę na konieczność przystosowania prawa polskiego do wymogów Unii Europejskiej, w tym do wymogów Dyrektywy Parlamentu Europejskiego i Rady nr 97/66/WE w sprawie przetwarzania danych osobowych i ochrony prywatności w sektorze telekomunikacji. Wprowadzenie przedmiotowych urządzeń nie tylko nie kolidowałoby z ustawą o ochronie danych osobowych, ale także odpowiadałoby treści art. 8 cytowanej Dyrektywy. Z punktu widzenia zgodności prawa polskiego z ustawodawstwem unijnym należy postulować taką zmianę polskiego prawa telekomunikacyjnego, która uwzględni wszystkie wymogi wynikające z postanowień Dyrektywy.

I. Przetwarzanie danych osobowych przez banki, Związek Banków Polskich i instytucje współpracujące z bankami

I. Podstawy prawne przetwarzania danych osobowych

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 przede wszystkim 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

327 GI-DP-356/99/445

ustawie. Regulacja ustawy z 29 sierpnia 1997 r. Prawo bankowe znacznie rozszerzyła zakres tajemnicy bankowej w stosunku do ustawy z 31 stycznia 1989 r. (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.).

I.1 Definicja administratora danych osobowych

Do Generalnego Inspektora Ochrony Danych Osobowych zwrócono się z prośbą o wyjaśnienie wątpliwości związanych z ustaleniem administratora danych klientów, którym bank udziela kredytów ratalnych i pożyczek konsumpcyjnych przy udziale firmy, która współpracuje przy udzielaniu tych kredytów.³²⁸ Bank w ramach swojej statutowej działalności, zawierając z klientami umowy pozyskiwał i przetwarzał ich dane bezpośrednio przez swoich pracowników, jak też w przypadku kredytów i pożyczek konsumpcyjnych zlecał pozyskanie tych danych firmie leasingowej. Współpraca ta polegała ponadto na sporządzaniu umów kredytowych, pożyczek i umów zabezpieczeń prawnych spłat kredytów i pożyczek, prowadzeniu ewidencji zawartych umów, rejestru rzeczy przewłaszczonych na rzecz banku, ewidencjonowaniu spłat, archiwizacji dokumentów, prowadzeniu korespondencji z kredytobiorcami i pożyczkobiorcami, prowadzeniu czynności wyjaśniających w związku z zawartymi umowami, podejmowaniu czynności windykacyjnych. Generalny Inspektor przypomniał, że administratorem danych jest podmiot, który decyduje o celach i środkach przetwarzania danych osobowych. Wobec tego, jeżeli do banku należy ostateczna decyzja o przyznaniu środków pieniężnych, a firma z którą bank podpisał umowę o współpracy wykonuje jedynie czynności poprzedzające zawarcie umowy, za administratora danych należy uznać bank. W przypadku natomiast, gdy całość procesu przetwarzania należy do firmy przetwarzającej, a bank nie dysponując swobodą decyzyjną co do celów jakim służą dane i środków wykorzystywanych przy przetwarzaniu będzie udzielał, po opracowaniu i weryfikacji przez firmę współpracującą wniosku kredytobiorcy, administratorem będzie firma współpracująca z bankiem.

328 GI-DP-782/99

I.2 Legalność przetwarzania

Z napływających do Generalnego Inspektora pism wynika, że wiele wątpliwości wywołuje kwestia pozyskiwania przez banki danych osobowych kredytobiorców, zakresu gromadzonych danych i zmiany celu przetwarzania zbieranych danych osobowych.

Banki przed przyznaniem kredytu przedkładają do wypełnienia klientom ankiety przeznaczone dla kredytobiorców i poręczycieli zawierające podstawowe dane o stanie majątkowym i sytuacji finansowej tych osób. Podanie tych informacji jest niezbędnym warunkiem uzyskania kredytu.³²⁹ Generalny Inspektor przypominał, że zgodnie z art. 70 ustawy prawo bankowe bank uzależnia przyznanie kredytu od zdolności kredytowej kredytobiorcy.³³⁰ Kredytobiorca, na żądanie banku, jest obowiązany przedstawić dokumenty i informacje niezbędne do dokonania oceny tej zdolności. Czynności bankowe takie, jak: udzielanie pożyczek, kredytów, gwarancji, regwarancji i inne są czynnościami prawa cywilnego (umowami) i jako takie odbywają się za zgodą wszystkich stron danej czynności. Dane o sytuacji finansowej podawane są przez klientów dobrowolnie, w celu zawarcia umowy z bankiem i są niezbędne do prawidłowego wykonania postanowień umowy zarówno przez bank, jak i przez jego klientów oraz do prawidłowej oceny zdolności kredytowej potencjalnego klienta. Z uwagi na to, dane osób, które chciałyby uzyskać kredyt są przez bank przetwarzane na podstawie jednej z przesłanek określonych w art. 23 ustawy o ochronie danych osobowych. Zgodnie z art. 23 ustawy o ochronie danych osobowych przetwarzanie danych jest dopuszczalne m.in. za zgodą osoby, której dane dotyczą, albo jeżeli jest niezbędne osobie, której dane dotyczą w celu wywiązania się z umowy, której jest stroną, lub na jej życzenie, w celu podjęcia niezbędnych działań przed zawarciem umowy.³³¹ Stosownie do art. 7 pkt 5 ustawy o ochronie danych osobowych zgoda na przetwarzanie danych musi być wyrażona wprost i nie może być dorozumiana z oświadczenia woli o innej treści. Jedynie w odniesieniu do danych osobowych tzw. wrażliwych (oraz w wypadkach określonych w art. 47 ustawy) zgoda musi być wyrażona pisemnie. W pozostałych przypadkach ustawodawca nie określił żadnej szczególnej formy, należy zatem uznać, że forma pisemna jest zalecana wyłącznie *ad probationem*. Na pytanie zatem, czy w świetle ustawy o ochronie danych osobowych jest dopuszczalne nagrywanie zgody na przetwarzanie danych osoby dzwoniącej

329 GI-DIS-68/99

330 Przez zdolność kredytową rozumie się zdolność do spłaty zaciągniętego kredytu wraz z odsetkami w terminach określonych w ustawie.

na infolinię prowadzoną przez bank, Generalny Inspektor odpowiadał, że działanie takie nie narusza przepisów ustawy o ochronie danych osobowych.³³²

Do Generalnego Inspektora zwrócono się z pytaniem o zgodność z prawem praktyki umieszczania kodu paskowego w okienku adresowym koperty, w której przesyłane są miesięczne wyciągi operacji bankowych posiadacza konta przez Bank PKO S.A.³³³ Zwracano przy tym uwagę, że jest to tajna dla posiadacza konta informacja, która może sugerować wykorzystanie jej w ściśle określonych terminach na potrzeby „hakerów”. Generalny Inspektor Ochrony Danych Osobowych zwrócił uwagę, że zgodnie z art. 28 ust. 3 ustawy o ochronie danych osobowych, zabronione jest nadawanie ukrytych znaczeń elementom numerów porządkowych w systemach ewidencjonujących osoby fizyczne. Generalny Inspektor otrzymał w tej sprawie od Banku PKO S.A. wyjaśnienia, z których wynikało, że system kodu paskowego wykorzystywany jest wyłącznie na potrzeby linii druku i przygotowania korespondencji, nie zawiera natomiast ukrytych znaczeń elementów numerów porządkowych w systemie. Z uwagi na to, zdaniem Generalnego Inspektora, nie doszło do naruszenia przepisów ustawy o ochronie danych osobowych.

Zakres przetwarzanych przez bank danych osobowych określa ustawa Prawo bankowe oraz wydane na jej podstawie regulaminy. W jednej ze skarg zarzucono, że sporządzanie przez bank fotokopii niektórych stron dowodu tożsamości podczas likwidacji rachunku terminowego stanowi naruszenie ustawy o ochronie danych osobowych, jako zbieranie danych osobowych nieadekwatnych do celu, dla którego są gromadzone.³³⁴ W odpowiedzi, po uzyskaniu odpowiednich wyjaśnień, stwierdzono, że praktyka taka ma na celu potwierdzenie dokonania wypłaty środków z rachunku bankowego osobie uprawnionej, co wobec narastającej fali wyłudzeń wydaje się uzasadnione. Zwrócono także uwagę, że kopiowane strony dowodu osobistego nie zawierają żadnych danych, które już nie znajdowałyby się w posiadaniu banku.

Zgodnie z art. 106 ustawy Prawo bankowe, bank jest obowiązany przeciwdziałać wykorzystywaniu swojej działalności do celów mających związek z przestępstwem określonym w art. 299 ustawy z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U.

331 GI-DP-643/99, GI-DP-730/99

332 GI-DP-845/99; warto wspomnieć, że w myśl art. 7 ustawy Prawo bankowe, oświadczenia woli składane w związku z dokonywaniem czynności bankowych mogą być wyrażane za pomocą elektronicznych nośników informacji. Związane z czynnościami bankowymi dokumenty mogą być sporządzane na takich nośnikach, jeżeli dokumenty te zostaną w należyty sposób utrwalone i zabezpieczone. Ponadto, jeżeli ustawa zastrzega dla czynności prawnej formę pisemną, uznaje się, że czynność dokonana w formie elektronicznej spełnia wymagania formy pisemnej.

333 GI-DP-1624/99

Nr 88, poz. 553 z późn. zm.) lub w celu ukrycia działań przestępczych. W związku z tym, bank jest także obowiązany prowadzić rejestr wpłat gotówkowych powyżej określonej kwoty, oraz danych o osobach dokonujących wpłaty i na których rzecz wpłata została dokonana. Tryb postępowania banków w przypadkach, o których mowa w art. 299 kodeksu karnego, oraz wysokość kwoty i warunki prowadzenia rejestru wpłat gotówkowych określa Komisja Nadzoru Bankowego.

Do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło pismo z zapytaniem, czy zgodne z prawem jest żądanie okazania dowodu osobistego przy zakupie w banku obcej waluty.³³⁵ Generalny Inspektor odpowiedział, że na podstawie § 2 ust. 1 uchwały Nr 4/98 Komisji Nadzoru Bankowego z dnia 30 czerwca 1998 r. w sprawie trybu postępowania banków w przypadkach prania pieniędzy oraz ustalenia wysokości kwoty i warunków prowadzenia rejestru wpłat gotówkowych powyżej określonej kwoty oraz danych o osobach dokonujących wpłaty i na rzecz których wpłata została dokonana (Dz. Urz. NBP z dnia 5 sierpnia 1998 r. Nr 18, poz. 40), banki zobowiązane są do prowadzenia w oddziałach oddzielnych rejestrów wpłat gotówkowych, których wartość przekracza równowartość 10000 EURO. W pkt 2 § 2. tej uchwały stwierdzono, że *„obowiązek określony w § 2 ust. 1 uchwały dotyczy także zamiany papierów wartościowych lub zagranicznych środków płatniczych na złote polskie, zamiany złotych polskich na papiery wartościowe lub zagraniczne środki płatnicze, w tym pośrednictwa w wymienionych wyżej transakcjach, a także każdego przypadku, gdy okoliczności transakcji wskazują, że środki mogą pochodzić lub mają związek z praniem pieniędzy, bez względu na wartość transakcji lub jej charakter”*. Rejestry te prowadzone są przez banki od dnia 1 lipca 1998 r., a zamieszcza się w nich dane określone w § 3 uchwały. W przypadku osób fizycznych identyfikacja obejmuje okazanie dowodu osobistego lub paszportu, w celu ustalenia i zarejestrowania cech dokumentu (seria i numer) oraz imienia i nazwiska, daty urodzenia, a także adresu zamieszkania posiadacza dokumentu tożsamości. W związku z tym, Generalny Inspektor nie dopatrywał się naruszenia ustawy o ochronie danych osobowych.

Problem przesłanek legalności przetwarzania danych osobowych pojawiał się również w odniesieniu do instytucji udzielających kredytów, nie będących bankami.³³⁶ Odpowiadano, że kwestia zawierania powyższych umów uregulowana została w przepisach ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. Nr 16, poz. 93 z późn. zm.). W

334 GI-DIS-408/99

335 GI-DIS-309/99

336 GI-DP-105/99

szczegółności art. 353¹ k.c. wyraża fundamentalną w prawie cywilnym zasadę swobody umów. Oznacza ona, że strony zawierające umowę mogą ułożyć stosunek prawny według swego uznania, byleby jego treść lub cel nie sprzeciwiały się właściwości (naturze) stosunku, ustawie ani zasadom współżycia społecznego. Ze względu na to, że art. 23 ust. 1 pkt 1 ustawy o ochronie danych osobowych jako jedną z przesłanek przetwarzania danych wymienia zgodę osoby, której dane dotyczą, działalność takich podmiotów nie narusza przepisów o ochronie danych osobowych.

I.3 Zmiana celu przetwarzania danych osobowych

Zmiana systemu emerytalno-rentowego i wprowadzenie tzw. II filaru ubezpieczeń, wywołały intensywną kampanię reklamową prowadzoną przez towarzystwa emerytalne. Szczególnie wiele skarg dotyczyło przetwarzania danych niezgodnie z celem, dla którego zostały one zebrane.³³⁷ Klienci Banku Śląskiego będącego udziałowcem Powszechnego Towarzystwa Emerytalnego Nationale-Nederlanden Polska S.A. otrzymali wypełnione formularze „Deklaracji przystąpienia do Otwartego Funduszu Emerytalnego Nationale-Nederlanden Polska S.A.” W formularzach tych zostały zamieszczone takie dane, jak imię i nazwisko, numer PESEL oraz oznaczenie płci. Przedstawiciele Banku Śląskiego wywodzili prawo do przetwarzania kwestionowanych danych osobowych stąd, że osoby uprawnione nie zastrzegły niedopuszczalności przetwarzania danych w celach marketingowych.³³⁸ W toku przeprowadzonego postępowania ustalono, że Bank Śląski otrzymał od Powszechnego Towarzystwa Emerytalnego Nationale-Nederlanden Polska S.A. niewypełnione druki deklaracji przystąpienia do OFE Nationale-Nederlanden. W ramach prowadzonej akcji akwizycyjnej Bank kierował oferty zawarcia umowy o uzyskanie członkostwa w Otwartym Funduszu Emerytalnym Nationale-Nederlanden wpisując w otrzymane druki imię, nazwisko oraz numer PESEL pochodzące z umów zawartych z własnymi klientami. Jedynie w przypadku przystąpienia danej osoby do Funduszu, dane osobowe klientów przekazywane były do OFE Nationale-Nederlanden. Generalny Inspektor uznał, że Bank Śląski S.A. jest administratorem danych swoich klientów z tytułu umów zawartych na gruncie prawa bankowego i przetwarzanie danych osobowych tych klientów może wynikać tylko i wyłącznie z tego rodzaju działalności. Nie jest możliwe wykorzystanie tych danych do celów marketingowych w zupełnie innej dziedzinie działalności Banku, jeżeli klient nie został wcześniej poinformowany o możliwości wykorzystywania jego danych osobowych także w

337 GI-DIS-202/99, GI-DIS-207/99, GI-DIS-209/99

338 GI-DIS-195/99

innym celu, w tym w celu marketingowym i nie wyraził na to zgody w sposób wyraźny. Zgodnie z art. 24 ust. 1 pkt 2 ustawy o ochronie danych osobowych, administrator danych jest obowiązany poinformować osobę, której dane dotyczą o celu zbierania tych danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych kategoriach odbiorców. Bank Śląski nie informował swoich klientów w czasie podpisywania z nimi umów bankowych o możliwości wykorzystania ich danych osobowych w celu marketingowym (dla potrzeb Powszechnego Towarzystwa Emerytalnego Nationale-Nederlanden Polska S.A.), ani nie uzyskał zgody tych klientów na takie przetwarzanie. Generalny Inspektor zwrócił uwagę na jeszcze inny aspekt tej sprawy. Z uwagi na to, że klient korzysta z usług Banku odpłatnie, nagannym jest wykorzystywanie przez Bank jego danych osobowych w celach marketingowych, a więc zarobkowych,³³⁹ co stanowi kolejną możliwość pomnażania własnych środków przez Bank kosztem klienta. Stąd, Generalny Inspektor uznał, że wykorzystywanie danych osobowych przez Bank Śląski w celu innym niż ten, dla którego dane zostały zebrane, stanowi naruszenie ustawy o ochronie danych osobowych i w wydanej decyzji nakazał zaprzestania przetwarzania danych osobowych w sposób niezgodny z przepisami ustawy o ochronie danych osobowych.³⁴⁰ Generalny Inspektor zauważył, że niezbywalnym prawem każdej osoby, która udostępnia administratorowi swoje dane osobowe jest podjęcie decyzji o tym, w jakim zakresie i celu administrator będzie mógł te dane przetwarzać, natomiast obowiązkiem administratora jest zastosowanie się do decyzji podjętej przez klienta.³⁴¹ Bank Śląski nie zgadzając się z decyzją Generalnego Inspektora złożył wniosek o ponowne rozpatrzenie sprawy, Generalny Inspektor utrzymał jednak poprzednią decyzję w mocy.³⁴²

Generalny Inspektor otrzymał skargę dotyczącą przetwarzania danych osobowych niezgodnie z celem, którego dane zostały zebrane.³⁴³ W przedmiotowej sprawie GE Capital Bank S.A. zawarł z wnoszącymi skargę umowę o udzielenie kredytu. Dane kredytobiorców zostały przez Bank wykorzystane w celach marketingowych. Z uzyskanych wyjaśnień wynikało, że dane skarżących zostały zebrane dnia 31 stycznia 1998 r., tj. jeszcze przed

339 Tym bardziej, że działalności tej nie sposób uznać za niezbędną dla wypełniania usprawiedliwionych celów administratora danych, ani tym bardziej za nie naruszającą praw i wolności osób, których dane dotyczą.

340 Por. DEC/48/GI-DIS-217/99; także na łamach prasy Generalny Inspektor podkreślał, że klient musi wyrazić zgodę na wykorzystywanie tych danych w innym celu niż ten, dla którego dane zostały zebrane, a wykorzystywanie jego danych do innych celów i bez zagwarantowania uprawnień wynikających z ustawy o ochronie danych osobowych, należy uznać za niezgodne z przepisami ustawy; por. np.: „Bank na cenzurowanym”, Rzeczpospolita z dnia 2 sierpnia 1999 r.

341 GI-DP-1079/99

342 Zob. GI-DEC/55/DIS-217/99-DP-17/99.

343 GI-DIS-132/99

wejściem w życie ustawy o ochronie danych osobowych. Z tego powodu Bank nie uzyskał zgody osób zainteresowanych na przetwarzanie ich danych osobowych w celach marketingowych, jednakże sprzeciw złożony przez skarżących został przez Bank uwzględniony i zaprzestano przetwarzania tych danych w tych celach.

W ubiegłym roku na skutek skargi Generalny Inspektor Ochrony Danych Osobowych wszczął postępowanie kontrolne dotyczące zgodności z prawem przetwarzania danych osobowych przez firmę Lukas S.A. i Lukas Bank.³⁴⁴ Pomimo, że postępowanie obecnie jest jeszcze w toku, to na podstawie wyników kontroli można już stwierdzić, że działania tych firm naruszały przepisy ustawy o ochronie danych osobowych. Lukas S.A. jako agent niektórych banków, przetwarzał dane klientów, którym banki te udzieliły kredytów. Równocześnie przetwarzał dane wybranych osób (tych, które wywiązały się należycie z umowy kredytowej) w celach marketingowych, polegających na oferowaniu tym osobom usług finansowych firm Lukas S.A. i Lukas Banku. W toku kontroli stwierdzono, że nie został dopełniony obowiązek informacyjny w stosunku do klientów tych podmiotów, w szczególności nie poinformowano tych klientów o zamiarze przetwarzania danych w celu marketingowym (co stało się właśnie powodem skargi), niektórym klientom nie udzielono wszystkich informacji wymaganych przez art. 24 ustawy o ochronie danych osobowych, inni nie zostali poinformowani o prawie wglądu do danych i ich poprawiania.

Do Generalnego Inspektora wpłynęło pismo, z którego wynikało, że już po zawarciu z klientem umowy o udzielenie kredytu, Bank Zachodni bez zgody tego klienta na egzemplarzu umowy umieścił adnotację, która rozszerzała możliwość przekazywania danych osobowych innym podmiotom.³⁴⁵ Przedstawiciel Banku Zachodniego wyjaśnił, że adnotacja o możliwości przekazywania danych osobowych innym podmiotom znajdowała się na formularzu umowy już w chwili jej podpisywania. Biorąc jednak pod uwagę brak zgody klienta wobec takiego przetwarzania jego danych osobowych, podjęto decyzję o usunięciu adnotacji z formularza umowy.

I.4 Udostępnianie danych osobowych innym podmiotom

Do Biura Generalnego Inspektora wpłynęła skarga, z treści której wynikało, że jeden z banków udostępnił oryginały polecenia przelewów jego wynagrodzenia na konto we wskazanym banku, pełnomocnikowi procesowemu żony skarżącego, który następnie

344 GI-DIS-425/99

345 GI-DIS-220/99

wykorzystał je jako dowody w postępowaniu sądowym.³⁴⁶ W toku postępowania ustalono, że powyższą dokumentację dotyczącą stanu rachunku bankowego skarżącego przekazała swojemu pełnomocnikowi żona skarżącego. Z uwagi na to, że żona skarżącego była uprawniona do posiadania tych dokumentów (ponieważ była pełnomocnikiem do wszystkich czynności bankowych dotyczących wskazanego rachunku), nie stwierdzono naruszenia przepisów ustawy o ochronie danych osobowych.

Wątpliwości budziła kwestia wzajemnego stosunku przepisów ustawy Prawo bankowe i ustawy o ochronie danych osobowych. Pytano w szczególności, czy art. 166 ustawy Prawo bankowe jest podstawą do udostępniania danych osobowych dłużników masy upadłości i czy działanie takie nie narusza ustawy o ochronie danych osobowych.³⁴⁷ W odpowiedzi podkreślono, że zgodnie z art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych przetwarzanie danych jest dopuszczalne m.in. wtedy, gdy zezwala na to przepis prawa. Na podstawie art. 168 ustawy Prawo bankowe w sprawach nie uregulowanych w tej ustawie do postępowania w przedmiocie upadłości banku stosuje się przepisy rozporządzenia Prezydenta Rzeczypospolitej Polskiej z dnia 24 października 1934 r. Prawo upadłościowe (Dz. U. 1991 r. Nr 118, poz. 512 z późn. zm.) z wyjątkiem art. 13 oraz art. 218 § 1 pkt 1. Zgodnie z art. 81 tego rozporządzenia obwieszczenia przewidziane w prawie upadłościowym, wywieszane są w budynku sądowym oraz umieszczone co najmniej w jednym poczytnym dzienniku. Na wniosek syndyka sędzia-komisarz może zarządzić umieszczenie obwieszczenia także w innych dziennikach krajowych i zagranicznych. Na żądanie upadłego lub wierzyciela obwieszczenie może zostać opublikowane na ich koszt w dziennikach, przez nich wskazanych. W związku z tym, Generalny Inspektor uznał, że przytoczone przepisy mogą stanowić podstawę przetwarzania danych osobowych.³⁴⁸

W innej skardze zarzucono Bankowi Śląskiemu niezgodne z prawem prowadzenie akcji marketingowej.³⁴⁹ Generalny Inspektor wszczął w tej sprawie postępowanie, w toku którego ustalono, że Bank Śląski zlecił spółce ABC Direct Contact personalizację przesyłek promocyjnych. Została ona przeprowadzona przez firmę Ogólnopolski Bank Oznakowanych Pojazdów COID, z którą ABC Direct Contact zawarła stosowną umowę. Materiały reklamowe zostały spakowane i przygotowane do wysłania przez ABC Direct Contact, podczas gdy personalizacją i wysyłką zajmowała się firma COID. W związku z tym, że

346 GI-DIS-305/99

347 GI-DP-791/99

348 Wypada zauważyć, że przepisy te stanowią też swoisty przypadek uchylenia tajemnicy bankowej określonej w art. 104 ustawy Prawo bankowe.

349 GI-DIS-15/99

przetwarzane w celach marketingowych dane osobowe nie zostały udostępnione Bankowi Śląskiemu, nie doszło do naruszenia ustawy o ochronie danych osobowych.

1.5 Biuro Informacji Kredytowej

W myśl art. 105 ust. 4 ustawy Prawo bankowe, banki, wspólnie z bankowymi izbami gospodarczymi, mogą 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. Instytucja ta ma stosunkowo niedługi rodowód w polskim systemie prawa (podobnie zresztą jak i sama ustawa o ochronie danych osobowych), pomimo jednak, że niektóre problemy związane z jej funkcjonowaniem nie różnią się od problemów dotyczących przetwarzania danych osobowych przez banki ze względu na specyfikę tego podmiotu, jego charakter i znaczenie, zasadne wydaje się odrębne omówienie grupy spraw związanych z przetwarzaniem danych osobowych przez Biuro Informacji Kredytowej i Związek Banków Polskich, niezależnie od kwestii poruszanych w innym miejscu tego sprawozdania.

1) Podstawy prawne funkcjonowania

W ramach tej problematyki szczególnie wiele pytań i kontrowersji budziła kwestia przekazywania danych osobowych przetwarzanych przez banki Związkowi Banków Polskich. Na skutek licznych skarg Generalny Inspektor Ochrony Danych Osobowych wszczął postępowanie, którego przedmiotem było ustalenie zgodności z prawem przetwarzania danych osobowych przez Związek Banków Polskich.³⁵⁰ W toku postępowania ustalono, że Związek Banków Polskich działa na podstawie przepisów ustawy Prawo bankowe oraz regulaminu wewnętrznego. Wewnętrzne uregulowania, które przyjęły banki wyznaczają Związkowi Banków Polskich wyłącznie rolę pośredniczącą w dystrybucji danych przetwarzanych w „Systemie międzybankowej wymiany informacji o klientach czasowo nie wywiązujących się ze swych zobowiązań wobec banków”. Zgodnie z art. 105 ust. 1 prawa bankowego, bank ma obowiązek udzielenia informacji stanowiących tajemnicę bankową m.in. innym bankom. Informacja ta może dotyczyć wierzytelności oraz obrotów i stanu rachunków w zakresie, w jakim informacje te są niezbędne w związku z udzielaniem kredytów, pożyczek pieniężnych, gwarancji bankowych i poręczeń oraz czynnościami obrotu dewizowego. Dane osobowe klienta banku mogą być umieszczane w zbiorze wyłącznie na

pisemny wniosek banku i są przetwarzane, aż do czasu ich usunięcia na podstawie decyzji banku. Usunięcie danych klientów polega na rzeczywistym usunięciu określonych informacji ze zbioru (a nie, np. na dokonaniu odpowiedniej adnotacji) i następuje w szczególności w razie śmierci dłużnika, po umorzeniu postępowania egzekucyjnego, a także po upływie dwóch lat od uregulowania zobowiązań lub ustania przyczyny zgłoszenia do systemu. Ten międzybankowy system wymiany informacji o niesolidnych dłużnikach prowadzony przez Związek Banków Polskich ma zostać przekazany Biuru Informacji Kredytowej, gdy tylko rozpocznie ono swoją działalność. Zgodnie z treścią art. 32 ust. 1 pkt 6 ustawy o ochronie danych osobowych, osoba, której dane dotyczą ma prawo 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.³⁵¹ Ponieważ dane te są przetwarzane zgodnie z upoważnieniem wynikającym z przepisów ustawy Prawo bankowe, osobie której dane dotyczą nie przysługuje prawo żądania zaprzestania przetwarzania danych osobowych określone w art. 32 ust. 1 pkt 8 ustawy o ochronie danych osobowych.³⁵²

Do Generalnego Inspektora Ochrony Danych Osobowych zwrócono się z pytaniem, czy dopuszczalne jest utworzenie instytucji analogicznej do określonej w art. 105 ust. 4 prawa bankowego przez podmioty prowadzące działalność leasingową.³⁵³ Generalny Inspektor uznał jednak, że wymianę informacji dotyczących wiarygodności dłużników reguluje ustawa Prawo bankowe, która dopuszcza możliwość wymiany powyższych informacji wyłącznie w stosunku do Banków. Zdaniem Generalnego Inspektora nie istnieje zatem podstawa prawna prowadzenia podobnej działalności przez firmy leasingowe i przetwarzania danych kontrahentów nie wywiązujących się z zaciągniętych zobowiązań bez ich zgody.

2) Obowiązki wynikające z przetwarzania danych

Możliwość wskazania podstawy prawnej przetwarzania danych osobowych nie zwalnia administratora danych z obowiązków wynikających z ustawy o ochronie danych osobowych. Generalny Inspektor zwracał uwagę, że konieczne jest rzetelne wypełnienie obowiązku informowania osób, których dane dotyczą. Osoba taka powinna zostać poinformowana przede wszystkim o tym, że jej dane zostały Związkowi Banków Polskich

350 GI-DP-1365/99

351 GI-DIS-9/99

352 GI-DP-764/99

przekazane przez bank, którego jest dłużnikiem i że dokonano tego na podstawie przepisów prawa, oraz o pozostałych okolicznościach wymienionych w art. 25 ust. 1 ustawy o ochronie danych osobowych.³⁵⁴ W pismach kierowanych do Generalnego Inspektora podnoszono, że istotą przepisu art. 105 ust. 4 prawa bankowego jest przekazywanie informacji o klientach banków za pośrednictwem utworzonego podmiotu bez informowania o tym fakcie osób, których dane dotyczą. Generalny Inspektor odrzucił tę argumentację podkreślając zarazem, że obowiązek informacyjny wobec osób, których dane dotyczą stanowi jedną z podstawowych zasad ochrony danych osobowych, ponieważ w znacznym stopniu umożliwia efektywne jej wykonywanie. Wszelkie odstępstwa od tej zasady, jako wyjątkowe powinny wynikać z treści przepisu ustawy. Tego typu wyjątków obniżających poziom ochrony danych osobowych nie można w żadnym wypadku domniemywać.³⁵⁵ Ustawodawca wyposażył w możliwość przetwarzania danych osobowych bez wiedzy osoby, której dane dotyczą, tylko określone podmioty o pewnych specjalnych zadaniach. Charakter tych zadań uzasadnia wyjątkową regulację w zakresie obowiązku informacyjnego. W przypadku natomiast zarówno banków jak i instytucji utworzonej na podstawie art. 105 ust. 4 ustawy Prawo bankowe przetwarzanie danych bez wiedzy osoby, której dotyczą dane, nie znajduje merytorycznego uzasadnienia, a co ważniejsze nie wynika wprost z przepisów. Stąd, zdaniem Generalnego Inspektora nie ma podstaw przyjmować, że na administratorach tych nie ciąży obowiązek informacyjny określony w ustawie o ochronie danych osobowych.³⁵⁶

Zaniepokojenie Generalnego Inspektora wzbudził również zapis w ankiecie z danymi poręczycieli o przechowywaniu przez BIK S.A. danych zawartych w tej ankiecie przez okres pięciu lat.³⁵⁷ W ocenie Generalnego Inspektora, z uwagi na to, że brak jest regulacji prawnych ustalających taki właśnie okres przechowywania, oraz na fakt, że tak długiego okresu przechowywania danych osobowych nie uzasadnia cel przetwarzania danych zapis przewidujący pięcioletni okres przechowywania danych osobowych poręczycieli pozostaje w sprzeczności z przepisami ustawy o ochronie danych osobowych. Zgodnie z art. 26 tej ustawy dane powinny być przechowywane nie dłużej, niż jest to niezbędne do osiągnięcia celu, dla którego zostały one zebrane.

353 GI-DP-684/99

354 GI-DP-1365/99

355 Przykładem wyraźnego upoważnienia do przetwarzania danych osobowych bez wiedzy osoby, której dane dotyczą jest art. 20 ust. 1 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. Nr 30, poz. 179 z późn. zm.).

356 GI-DP-629/99

357 GI-DP-876/99

II. Obowiązki banków

II.1 Obowiązek usunięcia danych zbędnych do realizacji celu, dla którego zostały zebrane

Zgodnie z art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych administrator danych przetwarzający dane jest obowiązany zapewnić, aby dane te były przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

Generalny Inspektor podjął sprawę niezgodnego z prawem przetwarzania danych przez LG Petro Bank S.A.³⁵⁸ Jak ustalono w toku kontroli, do Wydziału Centrum Hipoteczne LG Petro Banku S.A. - Centrala w Łodzi, wpływają kopie wypełnionych formularzy wniosków o przyznanie kredytu hipotecznego, przesyłane przez poszczególne oddziały celem zaopiniowania. W Wydziale tym została opracowana karta urodzinowa skierowana do klientów, którym został udzielony kredyt. Ustalono także, że w omawianej sprawie wysłanie karty nastąpiło omyłkowo, ponieważ do Centrali nie dotarła informacja o rezygnacji skarżącej osoby z usług banku. W związku z interwencją Generalnego Inspektora Ochrony Danych Osobowych, Bank podjął decyzję o zniszczeniu wszystkich wniosków osób, które nie zostały klientami banku, usunięte zostały również dane osoby wnoszącej skargę.

Generalny Inspektor zwracał również uwagę, że po wygaśnięciu umowy dane są przetwarzane dla celów archiwalnych na podstawie ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. Nr 121 poz. 591 z późn. zm.) oraz uchwały nr 1/98 Komisji Nadzoru Bankowego z dnia 3 czerwca 1998 r. w sprawie szczególnych zasad rachunkowości banków i sporządzania informacji dodatkowych (Dz. Urz. NBP Nr 14, poz. 27).³⁵⁹

II.2 Obowiązek odpowiedniego zabezpieczenia danych

W przypadku banków obowiązek odpowiedniego zabezpieczenia danych nabiera szczególnej wagi, chodzi bowiem o ochronę informacji objętych tajemnicą bankową. W tym zakresie przepisy ustawy wzmacniają ochronę danych dotyczących osób, które dokonują czynności bankowych, przewidzianą w ustawie Prawo bankowe. Bank zbiera i przetwarza dane osobowe, gdyż jest to konieczne dla dokonywania czynności bankowych, będących przedmiotem jego działalności. Jednak jako administrator danych swoich klientów Bank zobowiązany jest zgodnie z art. 36 ustawy o ochronie danych osobowych do zastosowania środków technicznych i organizacyjnych zapewniających ochronę danych osobowych.

358 GI-DIS-315/99

359 GI-DIS-408/99

Przetwarzaniem danych osobowych mogą zajmować się wyłącznie osoby upoważnione przez administratora danych. Są one zobowiązane do zachowania danych osobowych w tajemnicy, a obowiązek ten istnieje również po ustaniu zatrudnienia. Bank ponosi również odpowiedzialność za szkody wynikające z ujawnienia tajemnicy bankowej.³⁶⁰ Niezależnie od tego, brak właściwego zabezpieczenia wypełnia znamiona typu czynu zabronionego określonego w art. 51 ustawy o ochronie danych osobowych. W myśl tego przepisu, 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 albo pozbawienia wolności do lat 2.³⁶¹ Ponadto zgodnie z art. 171 ust. 5 ustawy Prawo bankowe, kto będąc obowiązany do zachowania tajemnicy bankowej ujawnia lub wykorzystuje informacje stanowiące tajemnicę bankową niezgodnie z upoważnieniem określonym w ustawie, podlega grzywnie do 1. 000. 000. zł. oraz karze pozbawienia wolności do lat 3.³⁶²

W ubiegłym roku niepokojąco często powtarzały się przypadki uchybień w zabezpieczaniu przez banki dokumentów zawierających dane osobowe. W maju 1999 r. na jednej z ulic Wrocławia znaleziono dokumenty z nazwiskami, adresami oraz numerami telefonów klientów Banku Zachodniego S.A., w czerwcu w Warszawie znaleziono niezabezpieczone dokumenty o klientach Kredyt Banku PBI S.A. zawierające m.in. kserokopie ich dowodów osobistych, adresy oraz numery i stan rachunków bankowych, również w czerwcu znaleziono m.in. wezwania do zapłaty oraz zestawienia kredytów udzielanych przez Invest - Bank S.A. Zdaniem Generalnego Inspektora Ochrony Danych Osobowych wydarzenia te świadczą o nieprzestrzeganiu lub braku stosownych procedur oraz odpowiednich zabezpieczeń w odniesieniu do dokumentów zawierających dane osobowe, co stanowi nie tylko rażące uchybienie przepisom prawa, ale jest także istotnym naruszeniem interesów klientów banków.

Ponieważ, zgodnie z art. 25 ust. 2 pkt 2 ustawy Prawo bankowe, nadzorowanie banków w zakresie przestrzegania ustaw, statutu i innych przepisów prawa należy do Komisji Nadzoru Bankowego, Generalny Inspektor Ochrony Danych Osobowych zwrócił się do

360 GI-DIS-354/99

361 GI-DP-71/99, GI-DP-417/99, GI-DP-422/99

362 Obydwa typy czynu zabronionego stanowią tzw. przestępstwa indywidualne, ponieważ ich sprawcą nie może być każdy, ale jedynie określone osoby, odpowiednio: osoba administrująca danymi lub obowiązana do zabezpieczenia danych osobowych, oraz osoba obowiązana do zachowania tajemnicy bankowej (czyli osoby zatrudnione w bankach lub z którymi bank współpracuje).

Przewodniczącego tej Komisji z prośbą o podjęcie stosownych działań.³⁶³ W odpowiedzi z dnia 16 sierpnia 1999 r. stwierdzono, że nadzór bankowy podjął działania zmierzające do zapewnienia skuteczniejszego przestrzegania przez banki tajemnicy bankowej. Poinformowano Generalnego Inspektora Ochrony Danych Osobowych, wystosowaniu pisma do prezesów wszystkich banków, w którym przypomniano, że nieuprawnione ujawnianie lub udostępnianie informacji o klientach banków rodzi odpowiedzialność karną i cywilną. Zalecono ponadto, aby problematyka ochrony danych osobowych została uwzględniona w corocznych planach kontroli wewnętrznych. Równocześnie Generalny Inspektorat Nadzoru Bankowego zwrócił się do Banku Zachodniego S.A. we Wrocławiu o ustosunkowanie się do informacji przekazywanych przez media, świadczących zaistnieniu uchybień w zabezpieczaniu dokumentów bankowych. Na podstawie uzyskanych wyjaśnień ustalono, że w wyniku podjętych przez bank działań stwierdzono, które osoby ponoszą odpowiedzialność za zaistniałe nieprawidłowości. Wobec tych osób zastosowano kary dyscyplinarne, podjęte zostały także działania organizacyjne mające wyeliminować podobne wypadki w przyszłości. Podobne kroki podjęto w stosunku do Kredyt Banku PBI S.A. w Warszawie oraz Invest-Banku S.A. w Poznaniu. Banki te wszczęły postępowania wyjaśniające mające na celu ustalenie okoliczności zdarzeń oraz osób winnych ich zaistnieniu. W przypadku Kredyt Banku PBI S.A. nastąpiło ukaranie Dyrektora Oddziału i pracowników winnych zaniedbania obowiązków służbowych poprzez pozbawienie premii kwartalnych oraz udzielenie nagany z wpisaniem do akt personalnych. W czasie, gdy udzielano Generalnemu Inspektorowi Ochrony Danych Osobowych wyjaśnień, w Invest-Banku S.A. trwało postępowanie mające na celu ustalenie osób winnych naruszenia przepisów.

Generalny Inspektor Ochrony Danych Osobowych skierował również pismo podobnej treści do Prezesa Związku Banków Polskich.³⁶⁴ W odpowiedzi z dnia 27 sierpnia 1999 roku Prezes Związku Banków Polskich stwierdził, że zwrócił się do banków ze stosownym apelem oraz wskazał na konieczność przeprowadzenia odpowiednich szkoleń dla ich pracowników.

W związku z sygnałami, jakie napłynęły do Biura GIODO, Generalny Inspektor podjął sprawę przesyłania klientom banku PKO BP kart bankowych i numerów identyfikacyjnych (PIN) listem zwykłym.³⁶⁵ Generalny Inspektor zauważył, że zbyt daleko idącą interpretacją przepisów ustawy o ochronie danych osobowych byłoby kwestionowanie

363 GI-662/99

364 GI/663/99

365 GI-DIS-304/99

listu zwykłego, jako formy przesyłania dokumentów zawierających dane osobowe. Kluczową natomiast kwestią jest rozważenie, czy w omawianej sytuacji nie doszło do naruszenia przepisów prawa bankowego. Fakt wydania Numeru Identyfikacyjnego (PIN) wynika z umowy zawieranej z bankiem przez klienta, natomiast sposób dostarczenia tego numeru jest zwykle określony w obowiązującym w danym banku regulaminie, dotyczącym wydawania i używania kart bankowych. Uprawnienie banku do wydawania ogólnych warunków umów lub regulaminów określających m.in. warunki otwierania i prowadzenia rachunków bankowych, oraz wykonywania innych czynności usługowych wynika z art. 109 ustawy Prawo bankowe.³⁶⁶ Z treści art. 49 tej ustawy wynika, że bank prowadząc rachunki bankowe swobodnie dysponuje powierzonymi środkami pieniężnymi, a w zamian dokłada wszelkich starań w zakresie bezpieczeństwa powierzonych bankowi środków pieniężnych. O ile przesyłane listem zwykłym numery PIN są dość skutecznie zabezpieczane, a w przypadku uszkodzenia tych zabezpieczeń przed doręczeniem adresatowi istnieje obowiązek powiadomienia o tym fakcie banku, o tyle przesyłanie listem zwykłym kart bankowych, a tym bardziej przesyłanie ich łącznie z numerami PIN można już rozpatrywać w kategoriach naruszenia obowiązku zachowania tajemnicy bankowej. Generalny Inspektor Ochrony Danych Osobowych podkreślał jednak, że organem właściwym do spraw nadzorowania banków jest, zgodnie z art. 25 ust. 2 pkt 2 ustawy z dnia 29 sierpnia 1997 r. o Narodowym Banku Polskim (Dz. U. Nr 140, poz. 938 z późn. zm.) Komisja Nadzoru Bankowego.

W ubiegłym roku Generalny Inspektor otrzymał informację o nieprawidłowościach w przetwarzaniu danych polegających na niewłaściwym ich zabezpieczeniu.³⁶⁷ Jak ustalono, podczas księgowania przez bank PKO BP obciążeń wynikających z korzystania przez klientów z bankomatów, nastąpił błąd polegający na zakwalifikowaniu wypłat tym klientom, których one nie dotyczyły. W wyniku ujawnienia tej pomyłki zastosowano system storn, mający ją naprawić i przesłano posiadaczom rachunków noty memoriałowe, zawierające m.in. ich dane osobowe takie jak: imię i nazwisko, adres, nazwę i numer konta. Skutkiem tego było udostępnienie osobom nieuprawnionym danych osobowych klientów. Generalny Inspektor stwierdził w tej sytuacji naruszenie ustawy o ochronie danych osobowych. W wyniku podjętych przez Generalnego Inspektora działań bank przedsięwziął kroki mające na celu dostosowanie sposobu dokonywania storn księgowych do wymogów ustawy o ochronie danych osobowych oraz skierował pismo z przeprosinami do klienta, którego dane osobowe zostały ujawnione w notcie memoriałowej.

³⁶⁶ Por. GI-DIS-319/99.

Wśród omawianej grupy spraw na uwagę zasługują działania kontrolne Inspektora Ochrony Danych Osobowych. W wybranych bankach przeprowadzono inspekcje pod kątem właściwego zabezpieczenia zbiorów danych. Zasadnicze uchybienia dotyczyły niedostosowania systemów informatycznych, w których przetwarzane były dane do wymogów przewidzianych 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 większości przypadków nieprawidłowości ujawnione przez Generalnego Inspektora Ochrony Danych Osobowych zostały usunięte jeszcze przed wydaniem stosownych decyzji.³⁶⁸

II.3 Obowiązek informacyjny

Generalny Inspektor Ochrony Danych Osobowych wielokrotnie podkreślał, że informowanie osoby, której dane dotyczą, o przetwarzaniu jej danych osobowych stanowi istotny instrument ochrony poprawnego, zgodnego z prawem przetwarzania danych osobowych. Obowiązek informacyjny w znacznym stopniu ułatwia sprawowanie przez osobę, której dane dotyczą, realnej kontroli procesu przetwarzania jej danych. Jest to jedno z zasadniczych założeń ustawy.³⁶⁹

Do Generalnego Inspektora kierowano pytania, czy na banku jako administratorze danych, ciąży obowiązek wynikający z art. 24 ust. 1 i art. 32 ust. 1 ustawy o ochronie danych osobowych.³⁷⁰ Generalny Inspektor zwracał uwagę, że bank winien dopełnić obowiązku informacyjnego. Obowiązek ten jednak, odnosi się wyłącznie do osób, których dane zostały zebrane od dnia wejścia w życie ustawy. Poinformowanie może nastąpić w dowolnej formie dającej pewność, że dana osoba zapoznała się z informacją. W opinii Generalnego Inspektora Ochrony Danych Osobowych wykonanie obowiązku informacyjnego poprzez ogłoszenia prasowe nie daje gwarancji, że każda z osób uprawnionych faktycznie zapozna się z ogłoszeniem.³⁷¹

Ustawodawca obowiązek informacyjny nałożył także na administratorów danych zbierających dane nie od osoby, której dane dotyczą. Również i w tym przypadku, jeżeli bank będący administratorem uzyskał dane przed wejściem w życie ustawy nie ma obowiązku

367 DEC/GI/DIS/1999

368 Por. np. GI-DEC/54/99/DIS-K-17/DP-12/99, por. także GI-DP-DEC/3/00/60.

369 GI-DP-629/99

370 GI-DP-945/99

371 GI-DP-1169/99

informowania osoby, której dane dotyczą. Generalny Inspektor otrzymał skargę na niezgodne z prawem udostępnienie danych osobowych przez firmę marketingową Bankowi Śląskiemu, oraz nie poinformowanie o tym fakcie osoby zainteresowanej.³⁷² Stwierdzono, że z uwagi na to, że podpisanie umowy sprzedaży bazy danych nastąpiło przed wejściem w życie ustawy o ochronie danych osobowych, nie istniał wymóg informowania osób, których dotyczyły dane osobowe.

Dokonywanie przelewów na zlecenie klienta jest uregulowane w przepisach szczególnych, m.in. w prawie bankowym, oraz w kodeksie cywilnym. Dla dokonania przelewu na rachunek wierzyciela niezbędne jest poznanie jego tożsamości. Dane te uzyskuje się w tej sytuacji od dłużnika. W praktyce powstały wątpliwości, czy w przypadku, gdy bank realizuje dyspozycję klienta związaną z rozliczeniem pieniężnym istnieje obowiązek spełnienia obowiązku informacyjnego określonego w art. 25 ust. 1 ustawy o ochronie danych osobowych.³⁷³ Generalny Inspektor odpowiedział, że ustawodawca nakładając na administratorów danych obowiązek informowania osób o przetwarzaniu ich danych osobowych przewidział jednocześnie sytuację, w których są oni zwolnieni z tego obowiązku. Zgodnie z art. 25 ust. 2 pkt 4, nie stosuje się obowiązku informacyjnego określonego w art. 25 ust. 1 ustawy o ochronie danych osobowych, gdy administrator nie przetwarza dalej zebranych danych po ich jednorazowym wykorzystaniu. Jeżeli więc dane nie są następnie wykorzystywane w innym celu, nie trzeba informować osób o przetwarzaniu ich danych osobowych.

W związku ze skargą klienta banku na odmowę udzielenia informacji, Generalny Inspektor Ochrony Danych Osobowych wszczął postępowanie w toku którego ustalono, że Citibank S.A. odmówił skarżącemu otwarcia rachunku oszczędnościowo-rozliczeniowego, motywując to faktem umieszczenia danych osobowych klienta na liście niesolidnych dłużników.³⁷⁴ Skarżący zwrócił się do Citibanku S.A. o udzielenie wyjaśnień, jakie dane osobowe bank ten przetwarza, w jaki sposób zostały zebrane, oraz w jakim zakresie i komu zostały przekazane. W odpowiedzi na pismo Generalnego Inspektora bank wyjaśnił, że osoba ubiegająca się o konkretny produkt składa oświadczenie o przyjęciu do wiadomości informacji o prawie wglądu do swoich danych oraz prawie ich poprawiania, a ponadto osoba ta już w chwili składania wniosku wie, jakie dane zawiera zbiór, ponieważ ich zakres ściśle określa druk wniosku. Według przedstawicieli banku cel i zakres zbieranych danych jest

372 GI-DIS-5/99

373 GI-DP-1014/99, GI-DP-1365/99

374 GI-DIS/DP-285/99

niezbędny do podjęcia działań na życzenie osoby, której dane dotyczą, to jest do wykonania czynności jakich musi dopełnić bank, bądź na mocy wewnętrznych regulacji, bądź to w związku z przepisami Narodowego Banku Polskiego regulującymi działalność i postępowanie banków w celu zawarcia umowy kredytu, umowy rachunku bankowego lub umowy o korzystanie z karty kredytowej. W związku z tym Generalny Inspektor powziął podejrzenie, że działanie banku wypełnia znamiona typu czynu zabronionego i skierował do prokuratury zawiadomienie o popełnieniu przez Citibank S.A. przestępstwa z art. 54 ustawy o ochronie danych osobowych.

W związku z licznie wpływającymi do Biura Generalnego Inspektora Ochrony Danych Osobowych pismami dotyczącymi przetwarzania danych osobowych przez PKO BP, Generalny Inspektor prowadził postępowanie, w trakcie którego ustalono, że bank występował do swoich klientów, z którymi miał zawarte umowy w ramach wykonywania czynności bankowych określonych w przepisach prawa bankowego, o wyrażenie zgody na przetwarzanie ich danych osobowych również w celach marketingowych.³⁷⁵ Druk zgody na przetwarzanie danych nie był sformułowany precyzyjnie, wprowadzając klientów w błąd polegający na tym, że składający oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych nie byli poinformowani o dobrowolności lub obowiązku wyrażenia takiej zgody. Wiele osób przekonanych było w związku z tym o obowiązku wyrażenia zgody. Na skutek interwencji Generalnego Inspektora Ochrony Danych Osobowych PKO BP zmodyfikował wzór oświadczenia w ten sposób, że z jego treści wynika możliwość zawarcia przez klienta umowy z bankiem a jednocześnie nie wyrażenia zgody na przetwarzanie jego danych osobowych w celach marketingowych (poprzez skreślenie części oświadczenia). Informacja o prawie wykreślenia tej części treści oświadczenia, która mówi o wyrażeniu zgody na przetwarzanie danych osobowych została w sposób jednoznaczny wyszczególniona we wzorze oświadczenia

Nowy wzór oświadczenia wprowadzony został zarządzeniem nr B/26/I/99 Prezesa Zarządu PKO BP z dnia 28 lipca 1999 r. Jednocześnie bank poinformował pracowników o zmianie treści oświadczenia oraz zobowiązał pracowników do wycofania starych druków i zbierania oświadczeń wyłącznie na nowych drukach, zgodnych z zasadami ochrony danych osobowych.

375 GI-DEC67/DP-426/99

II.4 Obowiązek rejestracji zbiorów danych

Wiele wątpliwości budziła kwestia obowiązku zgłoszenia do rejestracji zbioru danych byłych kredytobiorców, wobec których bank prowadzi postępowanie egzekucyjne i sądowe.³⁷⁶ Generalny Inspektor uznał, że jeżeli zbiór taki jest wykorzystywany wyłącznie w celu prowadzenia tego postępowania, przyjąć należy, że podlega on zwolnieniu z obowiązku rejestracji na podstawie art. 43 ust. 1 pkt 2 ustawy o ochronie danych osobowych. Zgodnie z tym przepisem od obowiązku rejestracji zwolnieni są administratorzy danych przetwarzanych przez właściwe organy dla potrzeb postępowania sądowego. Szczególne uprawnienia banku (np.: prawo do wystawiania bankowego tytułu egzekucyjnego na podstawie art. 96 i nast. ustawy Prawo bankowe) uzasadniają przyjęcie, że w tej sytuacji zachodzi przesłanka określona w art. 43 ust. 1 pkt 2.

Podnoszono wątpliwości, czy w świetle art. 105 ustawy Prawo bankowe jest dopuszczalne zgłaszanie zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, a także dokonywanie aktualizacji zgłoszenia, o której mowa jest w art. 41 ust. 2 ustawy o ochronie danych osobowych.³⁷⁷ Odpowiedziano, że treść zbioru danych nie podlega rejestracji ani przesłaniu Generalnemu Inspektorowi. Nie zachodzi więc konflikt pomiędzy przepisami ustawy Prawo bankowe a przepisami ustawy o ochronie danych osobowych. Nie ma również potrzeby rozpatrywania kwestii uchylenia tajemnicy bankowej i udostępniania informacji objętych tą tajemnicą Generalnemu Inspektorowi. Podkreślono również, że nie podlega zgłoszeniu zgodnie z art. 41 ust. 2 ustawy o ochronie danych osobowych fakt, że zbiór zmienił objętość, zmianą podlegającą zgłoszeniu byłoby natomiast objęcie przetwarzaniem nowej kategorii danych.

Nie podlegają także rejestracji „Księga wizyt gości zagranicznych” oraz „Księga interesantów”, które mogą zostać zakwalifikowane jako zbiory zawierające dane przetwarzane w zakresie drobnych spraw życia codziennego, podlegają zatem zwolnieniu z obowiązku rejestracji na podstawie art. 43 ust. 1 pkt 11 ustawy o ochronie danych osobowych.³⁷⁸

Generalny Inspektorat Nadzoru Bankowego otrzymał niewiadomego pochodzenia zbiór danych w formie dokumentu pisemnego „Lista rzeczoznawców upoważnionych do

³⁷⁶ GI-DP-750/99

³⁷⁷ GI-DP-759/99

³⁷⁸ GI-DP-997/99

wycen dla potrzeb sektora bankowego - stan na 16 listopada 1998 r.”, na który żaden z pracowników GINB nie zgłaszał zapotrzebowania. Do Generalnego Inspektora zwrócono się w związku z tym z pytaniem, czy GINB jest obowiązany zgłosić, zgodnie z art. 40 ustawy o ochronie danych osobowych taki zbiór do rejestracji.³⁷⁹ Generalny Inspektor Ochrony Danych Osobowych uznał, że ponieważ zarówno przechowywanie jak i usuwanie są formami przetwarzania danych osobowych, a o dokonaniu tych czynności w stosunku do posiadanego przez NBP zbioru danych osobowych o nazwie „Lista rzeczoznawców upoważnionych do wycen dla potrzeb sektora bankowego - stan na 16 listopada 1998 r.” decyduje Generalny Inspektor Nadzoru Bankowego należy uznać, że to właśnie on jest administratorem danych. Z uwagi na to, że zbiór ten nie jest i nie będzie, jak wynika z oświadczenia GINB, wykorzystywany w przyszłości, można przyjąć, że dane w nim zawarte, są wykorzystywane doraźnie. W odniesieniu do takiego zbioru mają zastosowanie jedynie przepisy rozdziału 5 ustawy o ochronie danych osobowych dotyczące zabezpieczenia zbiorów danych osobowych. Nie zachodzi natomiast konieczność zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, ani też informowania osób, których dane dotyczą o usunięciu ich danych ze zbioru.

J. Działalność marketingowa

I. Zagadnienia wstępne

W roku 1999 do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło około 200 skarg i zapytań prawnych dotyczących problematyki przetwarzania danych osobowych przez spółki i inne podmioty w celach marketingowych. Problematiczne było samo rozstrzygnięcie zakresu pojęcia „marketing” oraz zakresu praw i obowiązków podmiotów uczestniczących w reklamie i promocji. Wielość i różnorodność skarg i zapytań, a także wyniki przeprowadzonych przez Generalnego Inspektora postępowań wyjaśniających i administracyjnych ujawniły, że przetwarzanie danych osobowych w ramach obrotu marketingowego dokonywane było niejednokrotnie niezgodnie z przepisami ustawy o ochronie danych osobowych.

379 GI-DP-229/99

II. Podstawy prawne przetwarzania danych osobowych

W 1999 r. Generalny Inspektor Ochrony Danych Osobowych podejmował szereg działań w sprawach dotyczących udostępniania danych osobowych przez podmioty zajmujące się marketingiem.

Przedmiotem szczególnie wielu skarg była niezgodna z prawem działalność firm zajmujących się działalnością marketingową. Skargi dotyczyły przede wszystkim przesyłania materiałów marketingowych oraz przekazywania danych osobowych innym podmiotom bez zgody osób, których dane dotyczą, nawet po złożeniu przez nie sprzeciwu.

Zgodnie z art. 2 ustawy z dnia 29 sierpnia 1997 r. (Dz. U. Nr 133, poz. 883 z późn. zm.), zwanej dalej ustawą, przetwarzaniem danych są jakiekolwiek operacje wykonywane na danych osobowych, a pośród innych wymienionych przykładowo przez ustawodawcę form przetwarzania znajduje się także udostępnianie danych. Przesłanki legalności przetwarzania danych osobowych określiła ustawa w art. 23, art. 27 i art. 28. Jedną z przesłanek dopuszczalności udostępniania danych osobowych jest, zgodnie z art. 23 ust. 1 pkt. 1, zgoda osoby, której dane dotyczą. Każdy administrator danych przetwarzający dane na podstawie zgody, powinien wykazać istnienie w stosunku do siebie tej przesłanki. Pod pojęciem zgody na przetwarzanie danych, ustawa rozumie oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie, oraz że zgoda na przetwarzanie danych osobowych nie może być domniemana lub dorozumiała z oświadczenia woli innej treści.

Generalny Inspektor poinformował skarżących, iż w przypadku braku przedmiotowej zgody lub braku umowy dopuszczającej przetwarzanie danych, skarżący mają prawo wniesienia do danej firmy sprzeciwu wobec przetwarzania danych w celach marketingowych. 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. 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 tego przepisu. Sprzeciw taki w ocenie Generalnego Inspektora 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. Jak wynikało z pism skarżących wielokrotnie zwracali się z żądaniem zaprzestania przetwarzania ich danych osobowych, jednakże żądania te nie zostały potraktowane jako sprzeciw.³⁸⁰

Z uwagi na to, że dane osobowe skarżących, pomimo wielokrotnie wnoszonych przez nich sprzeciwów, były nadal przetwarzane w celach marketingowych przez niektóre firmy marketingowe, Generalny Inspektor powiadomił prokuraturę o popełnieniu przez nie przestępstwa określonego w art. 49 ust. 1 ustawy o ochronie danych osobowych.³⁸¹

Na skutek szeregu skarg, interwencja Generalnego Inspektora Ochrony Danych Osobowych w postaci przeprowadzonych postępowań administracyjnych doprowadziła do uznania przez firmy faktu takiego sprzeciwu i umieszczenia danych osobowych w bazie osób, które złożyły sprzeciw, co było równoznaczne z zaprzestaniem przetwarzania danych osoby w celach marketingowych (§ 16 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). Wobec przywrócenia stanu zgodnego z prawem wydano decyzje umarzające postępowanie administracyjne.³⁸²

Generalny Inspektor wielokrotnie otrzymywał zapytania dotyczące zasad udostępniania przez jedną firmę danych osobowych innej firmie dla przetwarzania przez nią danych w celach marketingowych. Odpowiadając, Generalny Inspektor zauważył, że zgoda wyrażona przez osobę na przetwarzanie jej danych przez określony podmiot nie może być przeniesiona na drugi podmiot wraz z udostępnieniem bazy danych. Zgoda ta musi być wyrażona wprost, w sposób nie budzący wątpliwości i nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. Zgodnie z dyspozycją cytowanego art. 26 ust. 2 ustawy, na administratorze bazy danych ciąży obowiązek zachowania szczególnej staranności ochrony danych. Podmiot zbywający bądź udostępniający dane osobowe, powinien dochować więc należytej staranności przy sprawdzeniu, do jakich celów wykorzystuje je nabywca. W jego interesie jest również, aby umowa przekazania w jasny sposób precyzowała cel przetwarzania danych.³⁸³

Do Generalnego Inspektora wpływały również zapytania dotyczące udostępniania danych osobowych innym podmiotom na innej podstawie, niż zgoda osoby, której dane

380 GI-DIS-38/99/863, GI-DIS-42/99/131, GI-DP-139/99/381,382, GI-DIS-147/99, GI-DIS-163/99/584

381 GI-DIS-43/99/967, GI-DIS0234/99/120, GI-DIS-363/99/1460, GI-DIS-443/99/1463

382 DEC-GI-DIS-59/99/1132,1133, GI-DP-DEC-65/99/1187,1188

383 GI-DIS-225/99/699, GI-DIS-357/99/1377, GI-DP-521/99/556, GI-DP-688/99/890

dotyczą. Pytania dotyczyły zastosowania art. 23 ust. 1 pkt 5 ustawy o ochronie danych osobowych. Zgodnie z treścią tego artykułu przetwarzanie danych jest dopuszczalne, gdy jest to niezbędne do wypełnienia usprawiedliwionego celu administratora danych, a przetwarzanie nie naruszy praw i wolności osoby, której dane dotyczą. Generalny Inspektor podkreślił, iż przepis ten został wprowadzony do ustawy jako odpowiednik przepisu art. 7 lit. f) Dyrektywy 95/46/WE w tym celu, aby usprawiedliwić prawnie przetwarzanie danych osobowych przez podmioty, które nie mogą skutecznie powoływać się na inne podstawy. Charakter przepisu art. 23 ust. 1 pkt. 5 uzasadniającego przetwarzanie danych na zasadzie *ultima ratio*, jest z tego powodu szczególny – nie można z jego treści wyciągać wniosku, że każda operacja na danych, potrzebna administratorowi dla osiągnięcia określonego celu, jest dopuszczalna. Ustawa wymaga bowiem, aby cel ten był usprawiedliwiony, nie zaś technicznie dopuszczalny. Warunkiem *sine qua non* zastosowania tego przepisu jest bowiem zapewnienie, aby przetwarzanie danych nie naruszało praw i wolności osób, których dane dotyczą. Sformułowanie to powszechnie interpretuje się w ten sposób, że naruszenie tych praw i wolności podmiotu danych zachodzi, gdy przeważają one nad interesami administratora. Dla właściwej wykładni przedmiotowego przepisu Generalny Inspektor przywołał postanowienia punktu III 1 Rekomendacji R(85)20 Komitetu Ministrów Rady Europy o ochronie danych osobowych wykorzystywanych dla potrzeb marketingu bezpośredniego³⁸⁴: „(..) *listy marketingowe winny móc być udostępniane osobom trzecim dla potrzeb marketingu bezpośredniego, o ile osoba zainteresowana została poinformowana – bezpośrednio bądź za pośrednictwem innych środków, przy okazji zbierania danych lub w jakimkolwiek innym momencie – o możliwości przekazania danych osobom trzecim i nie zgłosiła sprzeciwu co do tego (..)*”. Ocena, czy przepis art. 23 ust. 1 pkt. 5 ustawy może mieć zastosowanie w danej sytuacji należy co prawda do administratora danych, ale ocena ta nie może być zupełnie dowolna i sprzeczna z *ratio legis* ustawy, jakim jest skuteczna ochrona danych osobowych.³⁸⁴ Skarżący wielokrotnie zwracali się do Generalnego Inspektora o podjęcie działań zapobiegających naruszaniu ustawy o ochronie danych osobowych w postaci nielegalnego, w ich ocenie, udostępniania bazy danych podmiotom, które wykorzystywały dane osobowe skarżących bez ich zgody w kampaniach marketingowych. Podmioty te uzasadniając podstawy prawne przetwarzania danych osobowych powoływały przesłankę określoną w art. 23 ust. 1 pkt. 5 ustawy. Jak wykazały niektóre z przeprowadzonych postępowań wyjaśniających, administratorzy danych często prowadzili akcję marketingową,

384 GI-DP-DEC-61/99/1172,1173

nie mieszczącą się w zakresie określonym celami działania. W takim wypadku, Generalny Inspektor w wydanych przez siebie decyzjach nakazywał przywrócenie stanu zgodnego z prawem poprzez wykorzystanie posiadanych w zbiorze danych osobowych tylko zgodnie z celem, dla którego zostały zebrane.³⁸⁵

Wiele zapytań dotyczyło legalności przetwarzania danych osobowych w celach marketingowych przez banki i instytucje maklerskie. Zgodnie z art. 26 ust. 1 ustawy, administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest zobowiązany zapewnić, aby dane te zbierane były dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami. Oznacza to, że instytucje maklerskie mogą przetwarzać dane swoich klientów tylko w celu związanym z działalnością maklerską, określoną w umowie o świadczeniu usług maklerskich. W ocenie Generalnego Inspektora prowadzenie marketingu określonych produktów, jako wykraczające poza pierwotny cel zebrania danych, może się odbywać tylko na podstawie zgody klientów (art. 23 ust. 1 pkt. 1 ustawy). W związku z tym konieczne jest uzyskanie odrębnej, wyraźnej zgody osób, których dane dotyczą na oferowane im przez firmę usługi.³⁸⁶ Odnośnie działań marketingowych podejmowanych przez banki Generalny Inspektor stwierdził, iż instytucje te działają realizując przesłankę określoną w art. 23 ust. 1 pkt. 2 ustawy, w związku z wykonywaniem czynności bankowych określonych w art. 5 ustawy z dnia 29 sierpnia 1997 r. prawo bankowe (Dz. U. Nr 140, poz. 939 z późn. zm.) jak również ich działanie może opierać się na podstawie art. 23 ust. 1 pkt. 5 ustawy o ochronie danych osobowych w przypadku marketingu własnych produktów.³⁸⁷

III. Obowiązki administratora danych

III.1 Obowiązek informacyjny

W omawianym okresie sprawozdawczym Generalny Inspektor otrzymał wiele sygnałów dotyczących niedopełnienia przez administratora danych obowiązku informacyjnego, określonego w art. 24 i 25 ustawy o ochronie danych osobowych. Zastrzeżenie budził brak informacji o dobrowolności bądź obowiązku podania danych, a także nieprecyzyjne określenie celów marketingowych, jako często celów własnych

385 DEC40/GI-DIS-145/98/DP-6/99/578 i 579

386 GI-DP-1238/99/1408, GI-DP-1291/99/1305

387 GI-DP-1238/99/1408, GI-DP-1291/99/1305

podmiotów wysyłających ankiety, ulotki informacyjne czy kwestionariusze.³⁸⁸ Wyniki kontroli i postępowań wyjaśniających, przeprowadzonych przez Generalnego Inspektora Ochrony Danych Osobowych wykazały istotne uchybienia w przedmiotowym zakresie przetwarzania danych osobowych, do usunięcia których firmy prowadzące działalność marketingową zostały niezwłocznie zobowiązane.³⁸⁹

Generalny Inspektor Ochrony Danych Osobowych wielokrotnie informował, iż zgodnie z artykułem 23 ustawy przetwarzanie danych przez administratora jest dopuszczalne, gdy zostanie spełniona którakolwiek z przesłanek dopuszczalności przetwarzania danych tam wymienionych. Jedną z nich jest zgoda osoby, której dane dotyczą, chyba że chodzi o usunięcie dotyczących jej danych. Ponadto na administratorze danych spoczywa obowiązek informacyjny określony w ustawie. 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. Trudno sobie wyobrazić skuteczne działanie ustawy o ochronie danych osobowych bez prawnie usankcjonowanego obowiązku poinformowania osoby, której dane są przetwarzane o zakresie i celu ich przetwarzania. 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.

388 GI-DP-631/99/641, GI-DP-1144/99/1106, GI-DP-169/99/1075

389 DEC-40/GI-DIS-145/98/DP-6/99/578,579, DEC/45/GI-DIS-K/2/99/DP-4/99, GI-DEC/50/DIS-K-16/99/DP-13/99/921

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 utrwaleniu 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.

Ustawa zwolniła administratorów danych z obowiązku informacyjnego jedynie w sytuacjach określonych w art. 25 ust. 2.³⁹⁰ Generalny Inspektor poinformował 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.

390 GI-DIS-216/99/542, GI-DIS-266/99/778, GI-DP-1169/99/1075

Zastrzeżenia Generalnego Inspektora budził również zbyt szeroki zakres przetwarzania danych przez podmioty prowadzące działalność marketingową, w przesyłanych klientom ankietach osobowych i kwestionariuszach produktów i usług. Zgodnie z art. 26 cytowanej ustawy na administratorze danych przetwarzającym dane spoczywa obowiązek szczególnej ich ochrony. Powinien on dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a zwłaszcza jest zobowiązany zapewnić, aby dane te były zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami. Przetwarzanie danych w innym celu niż ten, dla którego zostały zebrane, jest dopuszczalne, jeśli nie narusza praw i wolności osoby, której dane dotyczą oraz następuje w celach określonych w ustępie 2 wspomnianego artykułu. Administrator danych jest więc zobowiązany do wykorzystania danych wyłącznie w celu, dla którego zostały zebrane. I tak, administrator danych zbieranych, np. w celu wykonania badań diagnostycznych, nie może uzależniać wykonania przedmiotowego świadczenia od wyrażenia przez pacjenta zgody na przetwarzanie danych w innym celu, np. promocji innych usług lub produktów oferowanych przez tę samą lub inną firmę.³⁹¹ W ocenie Generalnego Inspektora nie wydaje się dopuszczalne wykorzystywanie danych osobowych klientów w celach marketingowo – promocyjnych, o ile wcześniej nie wyrazili oni zgody na przetwarzanie swoich danych w tym właśnie celu. Wnikliwa analiza przedstawionych ankiet i kwestionariuszy pozwoliła Generalnemu Inspektorowi na stwierdzenie, iż niezbędna jest modyfikacja treści niektórych dokumentów, albowiem brak jest adekwatności zakresu danych do celu ich przetwarzania. Wątpliwości wzbudzała również forma informacji i pouczeń istotnych z punktu widzenia ochrony danych osób, które otrzymują przedmiotowy kwestionariusz, czy ankietę, jak również sposób ich rozpowszechniania. W tym celu, sygnalizując dostrzeżone nieprawidłowości Generalny Inspektor zwracał się do firm o podjęcie stosownych działań zmierzających do przywrócenia stanu zgodnego z prawem.³⁹²

Liczna grupa zagadnień rozpatrywanych przez Generalnego Inspektora dotyczyła zakresu przetwarzania danych w imiennych ofertach osób uczestniczących w różnych konkursach i loteriach. Generalny Inspektor poinformował, że zgodnie z art. 32 ustawy o ochronie danych osobowych, każdej osobie przysługuje prawo do kontroli przetwarzania (m.in. zbierania, przechowywania i usuwania) swoich danych osobowych, zawartych w zbiorach danych, a w szczególności osoby, których dane są przetwarzane w ramach marketingu mają prawo do uzyskania wyczerpujących informacji o celu, zakresie i sposobie

391 GI-DP-648/99/639

ich przetwarzania. Skarżący zostali pouczeni o przysługującym im prawie wystąpienia z wnioskiem o udzielenie powyższych informacji do firmy, która przysyła imienne oferty dotyczące udziału w konkursach, jak również o prawie wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania ich danych osobowych przez przedmiotowe firmy (art. 32 ust. 1 pkt 2 i 7 ustawy). W przypadku, gdy skarżący nie wyrazili zgody na przetwarzanie ich danych, lub nie podpisali umowy dopuszczającej przetwarzanie danych osobowych przez firmę w ramach prowadzonej działalności marketingowej, na podstawie art. 32 ust. 1 pkt 8 przysługuje im prawo wniesienia sprzeciwu. Jednocześnie Generalny Inspektor nie uznał się uprawniony lub zobowiązany do oceny wiarygodności firm organizujących konkursy i oceny szans na otrzymanie nagród z tytułu uczestnictwa w konkursach i loteriach.³⁹³

Odrębna grupa zagadnień dotyczyła przetwarzania przez firmy, w ramach prowadzonego przez nie marketingu, danych osób nieżyjących. Członkowie rodzin osób zmarłych skarżyli się na to, że administratorzy danych odmawiają im udzielenia informacji, o których mowa w art. 32 ust. 1 ustawy o ochronie danych osobowych, a także usunięcia przedmiotowych danych ze zbioru. W literaturze prawa nie budzi wątpliwości pogląd, że z chwilą śmierci danej osoby fizycznej, ustaje jej podmiotowość prawna (art. 8 kodeksu cywilnego). Zgodnie z art. 6 ustawy o ochronie danych osobowych za dane osobowe uważa się każdą informację dotyczącą osoby fizycznej. Tak więc informacje o osobie zmarłej, nie mogą być uznane w świetle cytowanej ustawy za dane osobowe. Potwierdzeniem tego stanowiska jest sama konstrukcja ustawy o ochronie danych osobowych, w której treści przewidziano szereg instytucji, przysługujących wyłącznie osobom żywym (np. prawo wglądu do swoich danych oraz ich poprawiania, prawo wniesienia sprzeciwu). Ponadto Generalny Inspektor zauważył, iż w myśl art. 922 § 1 kodeksu cywilnego na spadkobiercę zmarłego przechodzą jedynie prawa i obowiązki o charakterze majątkowym. Gdyby prawa wynikające z art. 32 powołanej ustawy potraktować jako prawa niemajątkowe, wygasłyby one w chwili śmierci osoby, której dane dotyczą. Skarżący, jako spadkobiercy osób, których dane są przetwarzane mogą jedynie poinformować administratorów o fakcie śmierci, nie mogą natomiast żądać udzielenia informacji, o których mowa w art. 32 ust. 1 ustawy oraz usunięcia danych osobowych członków ich rodzin.³⁹⁴

392 GI-DIS-203/99/1181, GI-DP-814/99/1276, GI-DP-879/99/1031

393 GI-DIS-386/99/1068, GI DIS-444/99/1329,1402, GI-DP-631/99/641, GI-DP-1625/99/38

394 GI-DIS-240/99/634

III.2 Obowiązek rejestracji

W omawianym okresie sprawozdawczym do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło wiele zapytań dotyczących sposobu i warunków rejestracji zbiorów danych osobowych, które administrator tworzył z myślą ich wykorzystania w celach marketingowych. Zgodnie z treścią art. 40 ustawy o ochronie danych osobowych administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi. Od przedmiotowego obowiązku zwolnieni zostali administratorzy danych objętych dyspozycją art. 43 ust. 1 ustawy. Obowiązek rejestracji spoczywa na administratorze danych, a więc podmiocie decydującym o celach i środkach przetwarzania danych osobowych. 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. Zgodnie z art. 46 ustawy administrator danych może rozpocząć przetwarzanie w zbiorze danych po zgłoszeniu tego zbioru Generalnemu Inspektorowi do rejestracji, chyba że ustawa zwalnia go z tego obowiązku. Zakres informacji zawartych w zgłoszeniu określa art. 41 ustawy, natomiast samego zgłoszenia dokonuje się na formularzu, którego wzór został opublikowany 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.). 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.³⁹⁵

Szczególnie wiele zapytań dotyczyło problematyki zbiorów doraźnych. 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

395 GI-DP-799/99/937, GI-DP-941/99/943, GI-DP-1562/99/1625

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. W przypadku przewidywania możliwości dalszego przetwarzania danych, zbiór taki należy zgłosić do rejestracji. I tak w przypadku, gdy firma wykorzystuje jednorazowo dane osobowe 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. 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.³⁹⁶

Zagadnieniem, które wywołało wiele wątpliwości był termin zgłoszenia do rejestracji danych osobowych w systemach informatycznych, istniejących w dniu wejścia w życie ustawy. Na podstawie art. 61 ust. 1 wniosek o zarejestrowanie przedmiotowych zbiorów, istniejących w dniu wejścia w życie ustawy, powinien zostać złożony w terminie 18 miesięcy od dnia jej wejścia w życie. W związku z faktem wejścia w życie ustawy w dniu 30 kwietnia 1998 r., tj. po ponad siedmiu miesiącach *vacatio legis*, ostateczny termin składania wniosków przypadł na dzień 30 października 1999 r. Dla zbiorów danych osobowych zawartych w systemach innych, niż informatyczne, obowiązek rejestracji zaistniał z dniem wejścia w życie ustawy. Ponadto Generalny Inspektor informował, iż wniosek o rejestrację

396 GI-DP-621/99/678, GI-DP-941/99/943, GI-DP-868/99/993, GI-DP-1106/99/1075

zbiorów danych osobowych powstałych po dniu wejścia w życie ustawy, powinien być zgłoszony niezwłocznie po zaistnieniu zbioru.³⁹⁷

Indywidualne zapytania dotyczyły zgłoszenia zbioru danych osobowych, prowadzonego w celach marketingowych, przez podmioty mające swoją siedzibę poza terytorium Rzeczypospolitej Polskiej, jednakże przy wykorzystaniu środków technicznych znajdujących się na jej terytorium. Art. 7 pkt 4 ustawy definiuje administratora danych jako organ, instytucję, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3 ust. 1 i 2, decydujące o celach i środkach przetwarzania danych osobowych. Generalny Inspektor uznał, że jeżeli dany podmiot przetwarzający dane, wyczerpuje ustawowe znamiona definicji administratora danych określonej w art. 7 pkt 4 i przetwarza dane przy użyciu środków technicznych znajdujących się na terenie Rzeczypospolitej Polskiej, podlega tym samym w myśl art. 3 ust. 3 przepisom ustawy o ochronie danych osobowych i jest zobowiązany zgłosić taki zbiór do rejestracji.³⁹⁸

Szereg zapytań, odnośnie rejestracji zbiorów, wyłoniło się w związku z interpretacją art. 31 ustawy o ochronie danych osobowych. Pytania dotyczyły określenia podmiotu zobowiązanego do rejestracji zbiorów danych w sytuacji, gdy dane osobowe zostały przekazane przez administratora innemu podmiotowi - w drodze umowy powierzenia – w celu związanym z działalnością marketingową. Generalny Inspektor poinformował, że zgodnie z art. 31 cytowanej ustawy, administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych osobowych. W interesie administratora leży to, aby w umowie ze zleceniobiorcą obowiązki tego ostatniego zostały określone na tyle szeroko i precyzyjnie, żeby dawało to gwarancję wykonania zobowiązań wynikających z umowy zgodnie z ustawą, a ponadto zabezpieczało możliwość dochodzenia roszczeń wobec zleceniobiorcy w razie wyrządzenia przez niego szkód osobom trzecim. Cytowany przepis szczegółowo określił zasady przekazania danych osobowych innemu podmiotowi, który w imieniu i na rzecz administratora, przetwarzałby dane osobowe. Nie zmienia to jednak sytuacji w tym znaczeniu, iż administratorem nadal pozostaje podmiot, który przekazał dane. Podmiot, któremu powierzono przetwarzanie danych może wykonywać wszelkie czynności, do wykonania których został upoważniony w umowie zawartej na piśmie i to na nim spoczywa obowiązek rejestracji zbioru danych. Potwierdza to nazwa części B wzoru zgłoszenia zbioru danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, stanowiącego załącznik do cytowanego rozporządzenia

397 GI-DP-1205/99/1288

Ministra Spraw Wewnętrznych i Administracji w sprawie określenia wzorów wniosków o udostępnienie danych osobowych, zgłoszenia zbioru do rejestracji oraz imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych. Ze wzoru tego wynika, iż zbiór danych zgłasza do rejestracji administrator danych, który w punkcie 15 zobowiązany jest poinformować o tym, czy przewiduje zlecenie przetwarzania danych innemu podmiotowi. Wprawdzie art. 31 ust. 3 ustawy o ochronie danych osobowych zobowiązuje podmiot, któremu powierza się przetwarzanie danych, do podjęcia środków zabezpieczających zbiór danych, o którym mowa w artykułach 36-39, jednakże nie zmienia to faktu, iż nadal odpowiedzialność za przestrzeganie przepisów ustawy o ochronie danych osobowych ponosi administrator. 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.³⁹⁹

III.3 Obowiązek zabezpieczenia danych

Generalny Inspektor wielokrotnie spotykał się z sygnałami dotyczącymi niewłaściwego zabezpieczenia danych osobowych przez firmy zajmujące się działalnością marketingową. Celem sprawdzenia zasadności napływających licznie skarg i zapytań zostały wszczęte postępowania administracyjne, mające na celu wyjaśnienie okoliczności sprawy, warunków i sposobu przetwarzania osobowych przez zaskarżone firmy. Wyniki postępowań ujawniły, iż niektóre firmy dopuściły się istotnych uchybień w postaci: braku nadzoru nad niszczeniem materiałów zawierających dane osobowe, braku programu szkolenia osób zatrudnionych przy przetwarzaniu danych osobowych, braku ewidencji tych osób i określenia zakresu ich obowiązków oraz odpowiedzialności za przetwarzanie danych, braku stosownych instrukcji nakazanych przez przepisy wykonawcze, czy braku w systemie informatycznym funkcji udostępniania na piśmie stosownych, określonych przez przepisy wykonawcze informacji.

Ustawa o ochronie danych osobowych nałożyła na administratora danych obowiązek zabezpieczenia zbioru danych, znajdujących się w jego posiadaniu. Zgodnie z dyspozycją art. 36 ustawy, administrator danych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych,

398 GI-DP-1162/99/1369

399 GI-DP-806/99/838, GI-DP-895/99/1326

a w szczególności powinien zabezpieczyć dane przed ich udostępnianiem osobom nieupoważnionym, zabranie przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem. Odpowiedzialność za przestrzeganie przepisów ustawy, jak podkreślał Generalny Inspektor, spoczywa w każdym wypadku na administratorze danych i to on powinien bezwzględnie dopilnować, aby przetwarzane dane osobowe skutecznie zanonimizować, w sytuacji, gdy przestają one służyć celowi dla którego zostały zebrane. Obowiązek taki obciąża administratora nawet w razie zawarcia na podstawie art. 31 ustawy, odrębnej, pisemnej umowy o przetwarzanie danych, jak również, gdy takiej umowy nie zawarto.⁴⁰⁰

Z prowadzonych kontroli oraz skarg kierowanych do Generalnego Inspektora wynikało również, że niektóre spośród kontrolowanych firm, nie spełniały wymogów określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. (Dz. U. Nr 80, poz. 522 z późn. zm.) w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informacyjne służące do przetwarzania danych osobowych. W takich sytuacjach Generalny Inspektor wydawał decyzje nakazujące przywrócenie stanu zgodnego z prawem.⁴⁰¹

IV. Inne zagadnienia

Indywidualne skargi i zapytania, które wpłynęły do Biura Generalnego Inspektora Ochrony Danych Osobowych dotyczyły legalności przysyłanych skarżącym przez firmy marketingowe bezimiennych ankiet. 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.⁴⁰² Okazały się niezasadne skargi na działalność firm, które przed rozpoczęciem akcji promocyjnych (np. wysyłanych ankiet, ulotek reklamowych), spełniły wymogi zawarte w art. 24, a mianowicie podały pełną nazwę i adres swojej siedziby,

400 GEC-GI-38/DIS-K-1/99/DP-7/99/524, DEC-GI-44/DIS-K-1/99/DP-7/99

401 DEC/37/GI/DIS-K-8/99/DP-3/99/518, GI/DEC/41/DIS-K-14/99/DP-9/99/646, DEC/45/GI/DIS-K-2/99/DP-4/99, GI-DP-DEC/64/99/1181, GI-DP-DEC-68/99/1212, GI-DP-DEC/71/99/1229

cel zbierania danych osób skarżących oraz kategorie ich odbiorców, a także wyraźnie poinformowały o dobrowolności podania danych.⁴⁰³

Do Generalnego Inspektora wpływały również pisma, w których skarżący 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 do przedmiotowej sytuacji należałoby raczej odnieść cywilnoprawne reguły kształtowania więzi prawnych między stronami, wynikające przede wszystkim z zastosowania 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.⁴⁰⁴

Zgodnie z art. 2 ust. 1 ustawy, jej przepisy stosuje się do przetwarzania danych osobowych w zbiorach danych. Definicję zbioru danych określił art. 7 pkt 1 ustawy, jako każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonego kryterium, niezależnie od tego, czy zestaw ten jest rozproszony, czy podzielony funkcjonalnie. Kluczowym zagadnieniem dla oceny zasadności zastosowania ustawy, w wielu opisywanych przez skarżących stanach faktycznych, było ustalenie, czy administrator zbioru utworzył zbiór danych osobowych w rozumieniu ustawy, zawierający dane osób biorących udział w organizowanym konkursie.⁴⁰⁵ W przypadku pozytywnego rozstrzygnięcia powyższej okoliczności, administratora danych zobowiązywała zasada zabezpieczenia zbioru przed dostępem osób nieupoważnionych, a także zasada niezmienności celu przetwarzania danych, o których już była mowa w części wstępnej sprawozdania. W sytuacji, gdy administrator nie stworzył dla potrzeb konkursu zbioru danych, ujawnienie danych osobowych skarżących nie

402 GI-DIS-362/99/1033, GI-DP-1020/99/1243, GI-DP-1167/99/1238

403 GI-DP-62/99/111, GI-DIS-193/99/497, GI-DIS-381/99/1096

404 GI-DP-1561/99/59, GI-DP-1625/99/38

405 GI-DP-261/99

będzie podlegało przepisom ustawy, ale może zostać objęte innymi przepisami prawa, np. prawa cywilnego (art. 23 i 24 kodeksu cywilnego).

Odrębna grupa zapytań, kierowanych do Biura dotyczyła legalności przetwarzania danych osobowych zawartych w książkach telefonicznych, w celu przeprowadzenia akcji promujących produkty danej firmy. Jedno z pytań dotyczyło możliwości przeprowadzenia akcji wysyłania bezpłatnych egzemplarzy gazety z kuponem prenumeraty, z wykorzystaniem danych zawartych w książce telefonicznej. Generalny Inspektor zauważył, iż ustawa o ochronie danych osobowych nie stoi na przeszkodzie wykorzystaniu danych osobowych w sposób wyżej wskazany. Książki telefoniczne są bowiem jawne i można korzystać z danych tam ujawnionych. Oczywiście jest, iż wysłanie oferty zawarcia umowy nie powoduje stworzenie zbioru danych osobowych w rozumieniu art. 7 pkt 1 ustawy, o ile jednak dane osób, którym wysłano bezpłatny egzemplarz gazety i złożono ofertę zawarcia umowy zostaną ujęte w formę zbioru będzie miał on prawdopodobnie charakter tylko tymczasowy, techniczny – służący sporządzeniu docelowego zbioru prenumeratorów. Obowiązek rejestracji dotyczy właśnie zbioru docelowego, na administratorze zbioru doraźnego, określonego w art. 2 ust. 3 ustawy spoczywa jedynie obowiązek jego należytego zabezpieczenia.⁴⁰⁶

Należy jednak zaakcentować, że fakt jawności informacji zawartych w książce telefonicznej nie może oznaczać, iż posługując się tymi danymi można wprowadzać potencjalnego klienta w błąd co do oferowanego produktu lub usługi. Generalny Inspektor wielokrotnie podkreślał, że tylko wnikliwe badanie proponowanych umów przed ich podpisaniem może ustrzec w przyszłości przed kontrahentami usiłującymi stosować nieuczciwe metody socjotechniczne w marketingu. Rozstrzygnięcie tej sprawy nie leży w zakresie kompetencji Generalnego Inspektora.⁴⁰⁷

Indywidualne zapytania dotyczyły kwestii przekazywania za granicę danych w celach marketingowych. Zagadnienie przekazywania danych za granicę zostało uregulowane w rozdziale 7 ustawy o ochronie danych osobowych. Przekazywanie danych osobowych za granicę może nastąpić jedynie wtedy, gdy kraj docelowy daje gwarancje ochrony danym osobowym na swoim terytorium przynajmniej takie, jak obowiązujące na obszarze Rzeczypospolitej Polskiej (art. 47 ustawy). O tym, czy ochrona taka jest zapewniona, decyduje administrator mający zamiar dokonać przekazania. Jeżeli nie jest możliwe przekazanie na podstawie tej przesłanki, administrator może się posilkować przepisami ust. 2 i 3 art. 47.

406 GI-DP-1106/99/1075

Zgodnie z art. 48 ustawy dopiero przy braku w/w przesłanek i w odniesieniu do przekazania do kraju, który nie daje odpowiednich gwarancji ochrony danych osobowych niezbędna jest zgoda Generalnego Inspektora.⁴⁰⁸

Niezależnie od konkretnego stanu faktycznego przedstawionego Generalnemu Inspektorowi Ochrony Danych Osobowych przez osoby skarżące, 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, prawie do wniesienia pisemnego umotywowanego żądania zaprzestania przetwarzania danych ze względu na ich szczególną sytuację. Ponadto podmioty, których przedmiotem skarg było przetwarzanie ich danych dla celów marketingowych, zostały poinformowane o prawie złożenia sprzeciwu wobec przetwarzania ich danych w tym celu, a w razie jego bezskuteczności, o dalszych przysługujących im środkach prawnych. Ponadto, 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. Natomiast wobec firm, które w dalszym ciągu odmawiały zastosowania się do przepisów ustawy o ochronie danych osobowych Generalny Inspektor Ochrony Danych Osobowych złożył zawiadomienie o popełnieniu przestępstwa określonego w art. 49 ustawy o ochronie danych osobowych.⁴⁰⁹

K. Pozostałe zagadnienia

W omawianym okresie sprawozdawczym do Biura Generalnego Inspektora Ochrony Danych Osobowych napływały pisma, w których dyrekcje domów dziecka zwracały się z pytaniami o zasadność i legalność udostępnienia przez nie zbiorów danych ich wychowanków do celów naukowych. Zgodnie z dyspozycją art. 6 ustawy z dnia 29 sierpnia 1997 r o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.), zwanej dalej ustawą, przez dane osobowe należy rozumieć każdą informację dotyczącą osoby fizycznej pozwalającą na określenie tożsamości tej osoby. Tak więc w przypadku udostępnienia

407 GI-DP-1672/99/55

408 GI-DP-248/99/271

409 GI-DIS-127/99, GI-DP-128/99, GI-DP-208/99, GI-DP-211/99, GI-DP-353/99

ogólnych informacji o podopiecznych domu dziecka, bez podawania ich danych osobowych ustawa nie będzie miała zastosowania. Jeżeli natomiast dom dziecka zamierzałby udostępniać dane osobowe swoich wychowanków w celu wykorzystania tych danych w celach badań naukowych, to zastosowanie znajdzie przepis art. 26 ust. 2 ustawy. Przepis ten dopuszcza przetwarzanie danych osobowych w celu innym niż ten, dla którego zostały zebrane, jeśli nie narusza to praw i wolności osoby, której dane dotyczą oraz następuje w celach badań naukowych, dydaktycznych, historycznych lub statystycznych, z zachowaniem przepisów art. 23 i 25 ustawy. W ocenie Generalnego Inspektora przy spełnieniu powyższych warunków udostępnienie danych wychowanków domów dziecka, np. studentom w celu napisania prac magisterskich nie będzie stanowić naruszenia przepisów ustawy o ochronie danych osobowych.⁴¹⁰

W związku z wprowadzonym obowiązkiem, wynikającym z przepisu art. 40, zespoły miejskich komisji rozwiązywania problemów alkoholowych wielokrotnie zwracały się o wyrażenie opinii w sprawie zasadności rejestracji zbiorów danych osób objętych wnioskiem o leczenie.⁴¹¹

Generalny Inspektor zauważył, iż zebrane w trakcie wywiadu środowiskowego informacje są niewątpliwie danymi osobowymi, przetwarzanymi w zbiorze i tym samym podlegają przepisom ustawy. Jak wynikało z uzyskanych informacji dane te przekazywane były do miejskich komisji rozwiązywania problemów alkoholowych. Zgodnie z art. 4¹ ustawy z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi (Dz. U. Nr 35, poz. 230 z późn. zm.) do zadań gminnych komisji rozwiązywania problemów alkoholowych należy podejmowanie czynności zmierzających do orzeczenia o zastosowaniu wobec osoby uzależnionej obowiązku poddania się leczeniu. W przypadku odmowy poddania się takiemu obowiązkowi, zgodnie z art. 26 powołanej wyżej ustawy komisje upoważnione są do złożenia w sądzie wniosku o wszczęcie postępowania mającego orzec przymus leczenia. Zebrane w trakcie wywiadu informacje służą więc ocenie stanu faktycznego i ewentualnemu złożeniu wniosku o wszczęcie postępowania sądowego, co pozwala na przyjęcie, że miejskie komisje, jako administrator danych, zwolnione są z obowiązku rejestracji na podstawie art. 43 ust. 1 pkt 2 ustawy o ochronie danych osobowych.

Do Generalnego Inspektora Ochrony Danych Osobowych wpływały również pisma od organizacji społecznych i stowarzyszeń z prośbą o wykładnię przepisów określających podstawy ich funkcjonowania w świetle ustawy o ochronie danych osobowych.

410 GI-DP-1474/99/1649

Zarząd Główny Polskiego Czerwonego Krzyża zwrócił się z zapytaniem o legalność przetwarzanych przez niego danych dotyczących osób poszukiwanych, w tym osób nieżyjących. Generalny Inspektor informował, że koncentruje się na wykładni przepisów ustawy o ochronie danych osobowych tylko w odniesieniu do konkretnego stanu faktycznego, nie dokonuje zaś całościowej wykładni ustaw. Zgodnie z treścią art. 6 ustawy definicja danych osobowych odnosi się jedynie do osób fizycznych. Osobą fizyczną jest każdy człowiek od chwili urodzenia do chwili śmierci.⁴¹² W związku z tym należy przyjąć, że przepisów ustawy o ochronie danych osobowych nie stosuje się do osób nieżyjących. Ponadto Generalny Inspektor poinformował, że działania PCK, znajdując oparcie w przepisach ustawy z dnia 16 listopada 1964 r. o Polskim Czerwonym Krzyżu (Dz. U. Nr 42, poz. 182) i statutem PCK, są zgodne tym samym z treścią art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych.⁴¹³

Wiele z wpływających od stowarzyszeń pytań dotyczyło formy uzyskania zgody w przypadku spraw zgłaszanych telefonicznie i listownie. Zgodnie z art. 23 ust. 1 pkt 1 ustawy zgoda jest jedną z przesłanek dopuszczalności przetwarzania danych. Nie może być ona domniemana lub dorozumiała z oświadczenia woli o innej treści, gdyż tak stanowi art. 7 pkt 5 ustawy. W przypadku zbierania danych przed wejściem w życie ustawy i ich dalszym przetwarzaniu administrator danych powinien uzyskać przedmiotową zgodę od osoby zainteresowanej, chyba że przetwarzanie danych odbywa się na innej podstawie, np. jest niezbędne do wypełnienia usprawiedliwionych celów administratora danych, a wykorzystanie danych nie narusza praw i wolności osoby, której dane dotyczą. Wobec braku istnienia jakiegokolwiek przesłanki dopuszczającej przetwarzanie danych należy je zniszczyć lub zanonimizować. W ocenie Generalnego Inspektora zgoda na przetwarzanie danych może zostać wyrażona w dowolnej formie, jednak należy podkreślić, że w razie sporu to na administratorze danych będzie spoczywał ciężar dowodowy w tej sprawie.⁴¹⁴

411 GI-DP-741/99/1033

412 Por. art. 8 kodeksu cywilnego.

413 GI-DP-110/99/237

414 GI-DP-692/00/726

Część II. REJESTRACJA ZBIORÓW DANYCH OSOBOWYCH

W ramach realizacji ustawowych zadań związanych z prowadzeniem rejestru zbiorów danych oraz udzielaniem informacji o zarejestrowanych zbiorach (art. 12 pkt 3) Generalny Inspektor Ochrony Danych Osobowych przyjmuje zgłoszenia zbiorów danych, wpisuje do rejestru prawidłowe zgłoszenia i wydaje decyzje administracyjne w przypadku spełnienia przesłanek odmowy rejestracji, a także udostępnia informacje z jawnego rejestru zbiorów danych oraz wydaje zaświadczenia o zarejestrowaniu.

Ustawa o ochronie danych osobowych w art. 40 nakłada na administratora danych obowiązek zgłoszenia prowadzonego zbioru danych do rejestracji Generalnemu Inspektorowi. Administratorem danych, w rozumieniu cytowanej ustawy, jest „organ, instytucja, jednostka organizacyjna, podmiot lub osoba, (...) decydujące o celach i środkach przetwarzania danych osobowych” (art. 7 pkt 4). Stosownie do treści art. 3 ust. 1 ustawy o ochronie 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. Pozycja administratora danych, w przypadku administracji publicznej, zdeterminowana jest ustawami szczególnymi stanowiącymi podstawę tworzenia poszczególnych zbiorów danych osobowych, zgodnie z zasadą wynikającą z art. 6 kodeksu postępowania administracyjnego, iż administracja państwowa działa na podstawie przepisów prawa.

Administratorami danych w sferze prywatnej (art. 3 ust. 2) 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.

Ustawa o ochronie danych osobowych wprowadza następujące terminy dopełnienia obowiązku rejestracyjnego:

1. do dnia 30 października 1999 r. powinny zostać zgłoszone zbiory danych osobowych, które były prowadzone w momencie wejścia w życie ustawy o ochronie danych osobowych (tj. 30 kwietnia 1998 r.); art. 61 ustawy stanowi „podmioty (...) prowadzące w dniu wejścia w życie ustawy zbiory danych osobowych w systemach informatycznych, mają obowiązek złożenia wniosków o zarejestrowanie tych zbiorów w trybie określonym w art. 41, w terminie 18 miesięcy od dnia jej wejścia w życie”,
2. przed rozpoczęciem przetwarzania danych osobowych w zbiorze; art. 46 ustawy dotyczy zbiorów danych tworzonych po dniu wejścia w życie ustawy („administrator

danych może rozpocząć ich przetwarzanie w zbiorze danych po zgłoszeniu tego zbioru Generalnemu Inspektorowi Ochrony Danych Osobowych do rejestracji”).

Należy podkreślić, iż okres przejściowy, o którym mowa w art. 61 ust. 1 nie odnosił się do zbiorów danych prowadzonych w tzw. systemach manualnych (kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych).

Działalność Generalnego Inspektora Ochrony Danych Osobowych w roku 1999 została zdeterminowana wpływem okresu przejściowego, dla zbiorów przetwarzanych w systemach informatycznych, oraz związanym z tym zwiększeniem ilości zgłoszeń zbiorów danych osobowych do rejestracji.

I. Ilościowe przedstawienie dynamiki procesu rejestracyjnego

Liczba zgłoszeń zbiorów danych osobowych do rejestracji w roku 1999 wzrosła w porównaniu z poprzednim okresem sprawozdawczym prawie tysiąckrotnie, gdyż do dnia 1 stycznia 1999 r. ilość zgłoszeń wynosiła jedynie 76 zbiorów danych osobowych. Ilość 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. Do 31 grudnia 1999 roku zarejestrowano 6 626 zbiorów danych osobowych, natomiast w stosunku do 1604 zgłoszeń przeprowadzono postępowania wyjaśniające.

Do zgłoszeń zbiorów danych do rejestracji w szczególności zobligowani są administratorzy danych, o których mowa w art. 3 ust. 1 ustawy o ochronie danych osobowych, tj. organy państwowe i samorządu terytorialnego, państwowe i komunalne jednostki organizacyjne oraz podmioty niepaństwowe realizujące zadania publiczne.

Gminy zgłosiły do rejestracji 30 390 zbiorów danych osobowych, powiaty natomiast 4 765 zbiorów. Jednostki organizacyjne, czyli np.:

- ośrodki pomocy społecznej - 2 272 zgłoszenia zbiorów danych osobowych,
- powiatowe centra pomocy rodzinie - 686 zgłoszeń zbiorów danych osobowych,
- biblioteki - 1 960 zgłoszeń zbiorów danych osobowych,
- powiatowe urzędy pracy - 336 zgłoszeń zbiorów danych osobowych do rejestracji.

Ilość zgłoszeń na szczeblu województwa (administracji rządowej i samorządowej) wynosiła 602 zgłoszenia. Szczegółowe zestawienie przedstawiono w załączniku nr 1.

Na szczeblu centralnym organy władzy ustawodawczej i wykonawczej zgłosiły 183 zbiory danych. Wykaz zgłoszeniodawców stanowi załącznik nr 2.

W szczególności Generalnemu Inspektorowi Ochrony Danych Osobowych zostały zgłoszone zbiory danych o istotnym znaczeniu dla funkcjonowania państwa: PESEL (wnioskodawca – Minister Spraw Wewnętrznych i Administracji), Krajowa Ewidencja Podatników (Minister Finansów), Centralny Rejestr Skazanych (Minister Sprawiedliwości), centralna ewidencja pojazdów oraz właścicieli i posiadaczy pojazdów (Minister Spraw Wewnętrznych i Administracji).

Szczególna sytuacja zaistniała w przypadku Centralnego Rejestru Skazanych, ponieważ w okresie sprawozdawczym prowadzono prace nad projektem ustawy o Krajowym Rejestrze Skazanych, której celem jest dostosowanie przepisów w tym zakresie do art. 51 Konstytucji i ustawy o ochronie danych osobowych. Zgodnie bowiem z art. 28 ust.1 ustawy o ochronie danych osobowych, przetwarzanie danych dotyczących skazań można prowadzić wyłącznie na podstawie ustawy. Natomiast w chwili obecnej kwestie tą reguluje rozporządzenie Ministra 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). W związku z powyższym, na wniosek Ministra Sprawiedliwości Rzeczypospolitej Polskiej, Generalny Inspektor Ochrony Danych Osobowych postanowił zawiesić postępowanie w sprawie rejestracji tego zbioru do czasu wejścia w życie przedmiotowej ustawy.⁴¹⁵

Jednym z największych zbiorów danych osobowych w kraju jest zbiór materiałów archiwalnych wchodzących do narodowego zasobu archiwalnego.

415 GI/DRZDO/POST/3/00

Ogółem można podać, że według stanu na dzień 31.12.1998 r. zasób archiwów państwowych liczył 62 829 zespołów, czyli 208 846 m. b.-18 018 330 jednostek inwentarzowych. Zasób ten przechowywany jest w 32 archiwach państwowych (3 archiwa centralne i 29 terenowych) podlegających Naczelnemu Dyrektorowi Archiwów Państwowych oraz ich 56 oddziałom zamiejscowym. System zabezpieczenia materiałów archiwalnych oraz organizacji dostępu do nich jest zróżnicowany w zależności od warunków lokalowych.

W zasobie archiwalnym, który nie ma postaci elektronicznej, znajdują się niesamoistne zbiory danych, stanowiące część zespołów archiwalnych. Do nich należy zaliczyć, np. akta sądów, prokuratur, szkół, Policji, Państwowego Urzędu Repatriacyjnego, Służby Polsce, Nadzwyczajnej Komisji do Walki z Nadużyciami, komisji rewizyjnych i kontroli PZPR i innych organizacji, akta stanu cywilnego przekazywane do archiwów po 100 latach od wytworzenia, rejestry mieszkańców, wykazy i kartoteki więźniów, wreszcie akta pracownicze i płacowe nielicznych zlikwidowanych zakładów pracy. Zbiory danych stanowią jednostkowe ankiety, ale i zbiorcze formularze spisów powszechnych połączone w poszyty, a także komplety teczek osobowych, oraz pojedyncze karty spisów włączone do grubych tomów.

Wszystkie wymienione rodzaje dokumentów nie są tworzone przez archiwa państwowe, lecz przejmowane i przechowywane przez nie (art. 25 ust. 2 i art. 26 ust. 2 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach). W chwili obecnej nie jest dokładnie rozpoznana ilość archiwaliów zawierająca dane osobowe, nie można też przewidzieć w jakim terminie i jakim nakładem pracy można by było przeprowadzić kwerendę zmierzającą do ustalenia, jakiego rodzaju zbiory danych osobowych oraz w jakich jednostkach i w ilu jednostkach archiwalnych się one znajdują.

W dotychczasowej praktyce, zgodnej z metodyką archiwalną, w celu lepszego opisanie zasobu archiwalnego i udzielania użytkownikom szybszej i dokładniejszej informacji, archiwa tworzą pomoce archiwalne wyższego rzędu, do zespołów archiwalnych - indeksy geograficzne, rzeczowe i osobowe. Indeksy osobowe, do niedawna tworzone w tradycyjnej papierowej postaci, ostatnio coraz częściej powstają w postaci elektronicznej. Jedne i drugie, podobnie jak archiwalia, zawierają podstawowe informacje o osobach fizycznych, zarówno żyjących, jak i zmarłych, i odsyłają do konkretnych archiwaliów.

Poszczególne archiwa zgłaszają Generalnemu Inspektorowi Ochrony Danych Osobowych do rejestracji najczęściej dwa zbiory „Zasób archiwum państwowego zewidencjonowany według kryteriów dostępu” oraz „System udostępniania materiałów archiwalnych”.

Do rejestracji zgłaszane także były zbiory danych osobowych, które nie podlegały temu obowiązkowi, ponieważ administratorzy danych na podstawie art. 43 ust. 1 ustawy są zwolnieni z obowiązku zgłoszenia zbioru danych osobowych do rejestracji.

Spośród rozpatrzonych do końca 1999 r. wniosków rejestracyjnych taka sytuacja miała miejsce w 527 przypadkach. Szczegółowe zestawienie wyłączeń z punktu widzenia poszczególnych przesłanek, o których mowa w art. 43 ust. 1 ustawy 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 221 pism zawiadamiających, iż zgłoszenie zostało dokonane przez podmiot nieuprawniony.

Do podmiotów tych należy w szczególności zaliczyć agentów ubezpieczeniowych lub osoby reprezentujące otwarte fundusze emerytalne. Składali oni trzy rodzaje dokumentów:

- oświadczenia, że przetwarzają dane osobowe (128 oświadczeń),
- pisemne zgody osób, z którymi podpisane zostały umowy na przetwarzanie ich danych osobowych (8 agentów przesłało tego typu zgody),
- zgłoszenia zbiorów danych do rejestracji.

Dwie pierwsze kategorie Generalny Inspektor uznał za błędne zrozumienie obowiązku rejestracyjnego, o czym poinformowani zostali wnioskodawcy. Natomiast w trzecim przypadku stwierdził on, 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 w rozumieniu art. 31 ustawy o ochronie danych osobowych (szczegółowe omówienie w punkcie 4). Do końca 1999 r. agenci ubezpieczeniowi, czyli osoby reprezentujące otwarty fundusz emerytalny, zgłosili do rejestracji 15 108 zbiorów danych.

II. Jakościowe i ilościowe omówienie pozostałej korespondencji kierowanej do Departamentu Rejestracji Zbiorów Danych Osobowych

Oprócz zgłoszeń zbiorów danych osobowych, w roku 1999 r. skierowano do Departamentu Rejestracji Zbiorów Danych Osobowych jako jednostki właściwej do rozpatrywania wniosków rejestrowych, przedstawione poniżej kategorie pism.

1. Wnioski o przesłanie wzoru zgłoszenia zbioru danych osobowych do rejestracji (4). W odpowiedzi przesłano wzory zgłoszeń w formie papierowej lub elektronicznej.
2. W trybie art. 29 ustawy o ochronie danych osobowych przesyłano wnioski o udostępnienie danych ze zbioru (20). Ponieważ rejestr zbiorów danych, o którym mowa w art. 42 ust. 1 nie zawiera konkretnych danych osobowych, wnioski przesyłano administratorom danych odpowiednich zbiorów danych. W przypadku niemożliwości ustalenia właściwego administratora informowano o tym wnioskodawcę.
3. Oświadczenia o przetwarzaniu danych osobowych (130). Agenci ubezpieczeniowi przesyłali „oświadczenia”, w których informowali iż przetwarzają dane osobowe jako „osoby współpracujące z Commercial Union Towarzystwem Ubezpieczeń na Życie”.
4. Wzory zgody osób ubezpieczonych (132). Siedmiu agentów, pomimo, że ustawa o ochronie danych osobowych nie wprowadza takiego wymogu, przesłało zgody na przetwarzanie danych osobowych składane przez osoby ubezpieczone.
5. Zawiadomienia o zwolnieniu z obowiązku rejestracyjnego (15). Administratorzy danych przesyłali zawiadomienia, iż są zwolnieni z obowiązku rejestracyjnego. Ustawa o ochronie danych osobowych nie przewiduje obowiązku składania tego typu oświadczeń, jeżeli zachodzą przesłanki wyłączenia obowiązku rejestracyjnego.

III. Zawiadomienia o zwolnieniach i zgłoszeniach przez nieuprawnione podmioty

III.1 Zwolnienia z obowiązku zgłoszenia zbioru danych osobowych do rejestracji

Ustawa o ochronie danych osobowych w art. 40 przewiduje obowiązek zgłaszania zbioru danych osobowych do rejestracji Generalnemu Inspektorowi. Zwolnienia z tego

obowiązku określono w art. 43 ust. 1 ustawy. Mają one charakter przedmiotowy, a ich wyliczenie jest wyczerpujące. Odnoszą się do administratorów zbiorów danych osobowych:

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 do rejestracji zbiory danych osobowych zawarte w katalogu z art. 43 ust. 1 są zawiadamiani o zwolnieniu z tego obowiązku.

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)

a) zbiory danych przetwarzanych przez komisje rozwiązywania problemów alkoholowych

Gminne komisje rozwiązywania problemów alkoholowych zgłaszają Generalnemu Inspektorowi Ochrony Danych Osobowych do rejestracji zbiory danych osobowych wynikające z realizacji działań związanych z profilaktyką i rozwiązywaniem problemów alkoholowych.

Zgodnie z art. 26 ustawy z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi (Dz. U. Nr 35, poz. 230 z późn. zm.) gminne komisje rozwiązywania problemów alkoholowych, obok prokuratury, są uprawnione do występowania do sądu rejonowego z wnioskiem o zastosowanie obowiązku poddania się leczeniu w zakładzie leczenia odwykowego (np.: zgłoszenia nr R 005898/99, nr R 006532/99).

b) zbiory danych osobowych przetwarzanych w związku z umieszczeniem dziecka w rodzinie zastępczej

Zbiory danych osobowych zgłaszane Generalnemu Inspektorowi Ochrony Danych Osobowych przez ośrodki adopcyjno-opiekuńcze związane w szczególności z pozyskiwaniem i kwalifikowaniem osób wyrażających gotowość zapewnienia dziecku zastępczego wychowania rodzinnego, m.in. w formie przysposobienia.

Zgodnie z treścią przepisu art. 31d ust. 2 ustawy z dnia 29 listopada 1990 r. o pomocy społecznej (Dz. U. z 1998 r. Nr 64, poz. 414 z późn. zm.) umieszczenie dziecka w rodzinie zastępczej następuje na podstawie orzeczenia sądu opiekuńczego. Na podstawie art. 31d ust. 3 tej ustawy, dziecko może być umieszczone w rodzinie zastępczej bez orzeczenia sądu opiekuńczego, lecz nawet wtedy istnieje obowiązek zawiadomienia w/w sądu (np.: zgłoszenia nr R 000293/99, nr R 004617/99).

c) zbiory danych osobowych będące rejestrem testamentów

Generalnemu Inspektorowi Ochrony Danych Osobowych gminy zgłaszały zbiory stanowiące rejestr testamentów.

Zgodnie z art. 951 ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. Nr 16, poz. 93 z późn. zm.) „spadkodawca może sporządzić testament także w ten sposób, że w obecności dwóch świadków oświadczy swoją ostatnią wolę ustnie wobec przewodniczącego zarządu jednostki samorządu terytorialnego, sekretarza powiatu albo gminy lub kierownika urzędu stanu cywilnego”. Spadkobierca, względem osoby trzeciej, która nie rości sobie praw do spadku z tytułu dziedziczenia, może udowodnić swe prawa wynikające z dziedziczenia tylko stwierdzeniem nabycia spadku (art. 1027 kodeksu cywilnego), natomiast zgodnie z art. 1025 § kodeksu cywilnego nabycie spadku przez spadkobiercę stwierdza sąd na wniosek osoby mającej w tym interes.

Wobec powyższego, rejestr testamentów jest zbiorem prowadzonym dla potrzeb postępowania sądowego (np. nr R 003243/99).

d) 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 sporządza go i wnosi do właściwego sądu oraz popiera go przed tym sądem (np. nr R 012088/99).

e) zbiory danych osobowych dotyczące mandatów karnych nakładanych przez strażników gminnych

Wyłączenie to stosuje się do zgłoszonych przez Straże Gminne zbiorów danych osobowych dotyczących mandatów karnych. Zgodnie z art. 10 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o Strażach Gminnych (Dz. U. Nr 123, poz. 779) Straż wykonuje zadania w zakresie ochrony porządku publicznego wynikające z ustaw i aktów prawa miejscowego. Wykonując powyższe zadania strażnik ma prawo m.in. do nakładania grzywien w postępowaniu mandatowym za wykroczenia określone w trybie przewidzianym przepisami o postępowaniu w sprawach o wykroczenia oraz kierowanie 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 4 i 5 powołanej ustawy). Postępowanie mandatowe normuje dział V ustawy z dnia 20 maja 1971 r. Kodeks postępowania w sprawach o wykroczenia (Dz. U. Nr 12, poz. 116 z późn. zm.). W myśl art. 66 § 2 kodeksu, funkcjonariusz nakładający grzywnę w drodze mandatu karnego obowiązany jest pouczyć sprawcę o prawie odmowy przyjęcia mandatu oraz o tym, że w razie odmowy sporządzony zostanie wniosek o ukaranie. Wniosek taki stanowi podstawę do wszczęcia postępowania przed kolegium do spraw wykroczeń. Kolegia do spraw wykroczeń wydając orzeczenia w przedmiocie popełnienia przez obwinionego wykroczenia, stosują procedurę nawiązującą do zasad klasycznej procedury sądowej, a orzeczenia kolegium podlegają kontroli na drodze sądowej po wniesieniu środka zaskarżenia - rozdział 54 k.p.k.

Wobec powyższego, należy uznać, że prowadzone przez Straże zbiory danych osobowych osób ukaranych za popełnienie wykroczenia w postępowaniu mandatowym, przetwarzane są przez właściwe organy dla potrzeb postępowania sądowego (np. zgłoszenia nr R 003112/99, nr R 007641).

2) Zbiory danych osobowych dotyczących osób zatrudnionych, zrzeszonych lub uczących się (art. 43 ust. 4)

a) 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 000585/99, nr R 007628, nr R 014806/99).

b) 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 006171/99, nr R 009270/99).

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 005850/99, nr R 011379/99).

c) zbiory danych osobowych dotyczące osób zrzeszonych

(np.: zgłoszenia nr R 011036/99, nr R 011299/99, nr R 001476/99, nr R 007006/99).

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 Prawo spółdzielcze „spółdzielnia jest dobrowolnym zrzeszeniem nieograniczonej liczby osób, o zmiennym składzie osobowym i zmiennym funduszu udziałowym, która w interesie swoich członków prowadzi wspólną działalność gospodarczą”.
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)

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).

3. 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 zrzeczeniem o celach niezarobkowych (np. zgłoszenie nr R 001476/99, nr R 011299/99).

3) Zbiory danych osobowych dotyczące osób korzystających z usług medycznych, obsługi notarialnej, adwokackiej lub radcy prawnego

a) 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 z leczeniem, badaniem i poradą lekarską, badaniem i terapią psychologiczną (np. zgłoszenia nr R 006400/99, nr R 008105/99, nr R 008426/99).

b) zbiory danych osobowych poradni psychologiczno-pedagogicznych

Zgodnie z § 1 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), usługi w zakresie diagnozy i terapii psychologicznej świadczą poradnie psychologiczno-pedagogiczne (np. zgłoszenia nr R 009133/99, nr R 010867/99).

c) zbiory danych osobowych aptek

Zgłoszone przez apteki zbiory danych związane z realizacją recept Generalny Inspektor Ochrony Danych Osobowych uznał za zbiory osób korzystających z usług medycznych w rozumieniu art. 43 ust. 1 pkt 5 ustawy o ochronie danych osobowych (np. zgłoszenie nr R 014687/99).

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

Generalnemu Inspektorowi Ochrony Danych Osobowych zgłaszane były do rejestracji zbiory danych osobowych stanowiące listy osób wybranych do pełnienia funkcji radnego. Zbiory danych osobowych radnych gmin, powiatów i sejmików wojewódzkich tworzone są na podstawie ustawy z dnia 16 lipca 1998 r. Ordynacja wyborcza do rad gmin, rad powiatów i sejmików wojewódzkich (Dz. U. Nr 95, poz. 602 z późn. zm.).

Ustawa Ordynacja wyborcza do rad gmin, rad powiatów i sejmików wojewódzkich w art. 125, 182 i 184 stanowi, że wyniki wyborów do rad gmin są podawane do wiadomości publicznej przez komisje wyborcze, a w formie zbiorczej przez wojewódzkiego komisarza wyborczego i Państwową Komisję Wyborczą. Wobec powyższego, przedmiotowe zbiory danych osobowych na podstawie art. 43 ust. 1 pkt 6 i 9 ustawy o ochronie danych osobowych nie podlegają obowiązkowi zgłoszenia do rejestracji.

5) Zbiory danych osobowych przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub sprawozdawczości finansowej (art. 43 ust. 1 pkt 8), (np.: zgłoszenia nr R 009087/99, nr R 007688/99, nr R 005191/99).

6) Zbiory danych osobowych powszechnie dostępnych (art. 43 ust. 1 pkt 9)

a) 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), wydanym 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 (zgłoszenia nr R 002192/99, nr R 012682/99).

b) 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 008697/99, nr R 008698/99).

7) Zbiory danych osobowych przetwarzanych w zakresie drobnych bieżących spraw życia codziennego

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 024765/99).

III.2 Zgłoszenia zbiorów danych osobowych do rejestracji dokonane przez podmioty nieuprawnione

W związku z bardzo dużą liczbą zgłoszeń od agentów ubezpieczeniowych lub osób reprezentujących otwarte fundusze emerytalne, temat ten wymaga szerszego odrębnego omówienia. Z charakteru czynności wykonywanych przez wyżej wskazane podmioty (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.

Pomimo upublicznienia tego stanowiska w prasie („Rzeczpospolita” z dnia 03.11.1999 r.) i na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych oraz poinformowania o nim osób i podmiotów, które zwróciły się z zapytaniami prawnymi w tym zakresie,⁴¹⁶ zgłoszenia od w/w podmiotów składane były do końca okresu sprawozdawczego.

W zdecydowanej większości przypadków wnioskodawcami są agenci ubezpieczeniowi Commercial Union Towarzystwa Ubezpieczeń na Życie lub osoby uprawnione do wykonywania czynności akwizycyjnych na rzecz Commercial Union Otwarty Fundusz Emerytalny BPH CU WBK, a zgłaszanie przez nich zbiorów danych do rejestracji na jednolitych szablonach z wypełnionymi polami odpowiedzi ma charakter zorganizowanej akcji.

Podobna sytuacją zgłoszenia zbioru danych osobowych przez podmiot nie będący administratorem danych dotyczy zbioru danych o nazwie „Produkcyjna, pośrednia i poprodukcyjna baza danych służąca do drukowania dokumentów stwierdzających uprawnienia do kierowania pojazdami” (zgłoszenie nr R 000877/99). Została ona zgłoszona przez Polską Wytwórnę Papierów Wartościowych S.A. z siedzibą w Warszawie, którą zawiadomiono, że nie jest administratorem danych przedmiotowego zbioru.⁴¹⁷

Zgodnie bowiem treścią art. 97 ust. 1 i 3 ustawy z dnia 20 czerwca 1997 r. Prawo o ruchu drogowym (Dz. U. Nr 190, poz. 1086 z późn. zm.) dokument stwierdzający uprawnienie do kierowania pojazdami wydaje starosta właściwy ze względu na miejsce zamieszkania osoby ubiegającej się, a w pewnych sytuacjach również Wojewoda Mazowiecki. Szczegółowe czynności organów w sprawach związanych z wydawaniem uprawnień do kierowania pojazdami określa rozporządzenie Ministra Transportu i Gospodarki Morskiej z dnia 19 czerwca 1999 r. w sprawie wydawania uprawnień do kierowania pojazdami (Dz. U. Nr 58, poz. 621). Z treści § 3 ust 1 rozporządzenia wynika, iż blankiety prawa jazdy wykonuje producent na podstawie zamówienia składanego przez organ, tj. starostę lub Wojewodę Mazowieckiego. Jednocześnie rozporządzenie zobowiązuje organ wydający, do prowadzenia ewidencji kierowców w postaci akt ewidencyjnych osób. Na podstawie tego przepisu, w dniu 22 grudnia 1998 r. Polska Wytwórnia Papierów Wartościowych S.A. zawarła z Ministerstwem Transportu i Gospodarki Morskiej umowę nr DMM/056/98, które w imieniu zleceniodawców, jakimi są „odpowiednie organy administracji, wymienione w ustawie Prawo o ruchu drogowym”, powierzyło wytworzenie wypełnionych blankietów dokumentów Polskiej Wytwórni Papierów Wartościowych S.A. W tym celu zleceniodawca zobowiązał się do dostarczenia Polskiej Wytwórni Papierów Wartościowych S.A. zamówień zawierających informacje niezbędne do wypełnienia blankietów dokumentów. Działanie takie jest zgodne z przepisami ustawy o ochronie danych osobowych, a w szczególności z art. 31 ust. 1 dotyczącym powierzenia innemu podmiotowi w drodze umowy zawartej na piśmie, przetwarzania danych.

Prowadzenie przedmiotowego zbioru danych osobowych przez Polską Wytwórnę Papierów Wartościowych S.A. w ramach wykonywania umowy powierzenia nie powoduje zmiany administratora zbioru. Administratorem danych, czyli podmiotem decydującym i odpowiedzialnym za gromadzenie, przechowywanie, udostępnianie danych ze zbioru są starostowie, bądź Wojewoda Mazowiecki. Polska Wytwórnia Papierów Wartościowych,

416 Np. DRZDO/3604/99, DRZDO/3260/99.

przez fakt wykonywania pewnych czynności na danych osobowych i prowadzenia zbioru na podstawie powierzenia, nie stała się administratorem zbioru danych osobowych i nie jest podmiotem właściwym do zgłoszenia zbioru danych o nazwie „Produkcyjna, pośrednia i poprodukcyjna baza danych służąca do drukowania dokumentów stwierdzających uprawnienia do kierowania pojazdami” do rejestracji.

IV. Postępowania wyjaśniające

IV.1 Postępowania wyjaśniające zakończone rejestracją zbioru danych osobowych

Ustawa o ochronie danych osobowych w art. 44 ust. 1 zawiera przesłanki, których spełnienie powoduje wydanie 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.

Do końca 1999 r. przeprowadzono 1604 postępowania wyjaśniające. Najczęściej powtarzające się nieprawidłowości można podzielić na:

- wady formalne
- wady merytoryczne

Ad 1) Zgłoszenie zbioru danych osobowych jest podaniem w rozumieniu art. 63 kodeksu postępowania administracyjnego i w szczególności powinno 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 006226/99, nr R 013457/99, nr R 009722/99).

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. (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, nr R 013949/99), bądź też zgłaszano zbiór do rejestracji na druku niezgodnym z obowiązującym wzorem, najczęściej opracowanym przez wnioskodawcę (np.: zgłoszenia nr R 000029/99, nr R 000043/99). Zbiory danych osobowych zgłaszano też na niekompletnym formularzu, tzn. zgłoszenia nie zawierały jednej lub kilku stron wzoru (np.: zgłoszenia nr R 000528/99, nr R 000480/99), lub w zgłoszeniu nie wypełniono poszczególnych części formularza (np. zgłoszenia nr R 010207/99, nr R 006653/99).

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 (np.: zgłoszenia nr R 000029/99 nr R 000043/99, nr R 005290/99, nr R 000528/99, nr R 000480/99).

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 odmówią rejestracji zbioru danych, jeżeli przetwarzanie danych w przedmiotowym zbiorze narusza zasady określone w art. 23-30 ustawy, np.:

- w przypadku naruszenie zasady legalności przetwarzania danych zwykłych - art. 23 ust 1 ustawy o ochronie danych osobowych (zgłoszenie nr R 016476/99),
- w przypadku naruszenie zasady zachowania szczególnej staranności przy przetwarzaniu danych osobowych w celu ochrony interesów osób, których dane dotyczą - art. 26 ust. 1 ustawy (zgłoszenia nr: R 003469/99, R 003474/99),
- naruszenie zasady legalności przetwarzania danych „wrażliwych” - art. 27 ust. 2 ustawy (zgłoszenia nr: R 002590/99, R 006065/99, R 006312/99),

- 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 002074/99, R 007570/99, R 005141/99).

Z analizy zgłoszeń wynika również, że została spełniona przesłanka 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 z jednej strony 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. Drugim powodem, dla którego administratorzy danych pozostawiali pusta część F zgłoszenia, było rzeczywiste nie dopełnianie wymogów wynikających z rozporządzenia. W trakcie postępowań 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 001563/99, nr R 000683/99, nr R 000781/99).

Działania Generalnego Inspektora w ramach postępowań rejestracyjnych wywołują zmianę nieprawidłowych praktyk. Przykład stanowi zgłoszenie nr R 001275/99 zbioru danych o nazwie „Powszechny elektroniczny system ewidencji ludności PESEL” dokonane przez Dyrektora Ośrodka Informatyki Dolnośląskiego Urzędu Wojewódzkiego we Wrocławiu ustanowionego na podstawie decyzji Wojewody Dolnośląskiego administratorem danych przedmiotowego zbioru. W trakcie podjętego postępowania wyjaśniającego Generalny Inspektor Ochrony Danych osobowych zwrócił się do Wojewody Dolnośląskiego, jako administratora danych wyżej wskazanego zbioru, o prawidłowe dopełnienie obowiązku rejestracyjnego.⁴¹⁸ W odpowiedzi na pismo Generalnego Inspektora Ochrony Danych

418 DRZDO/222/00

Osobowych Wojewoda Dolnośląski anulował decyzję ustanawiającą Dyrektora Departamentu Informatyki administratorem danych zbioru „Powszechny Elektroniczny System Ewidencji Ludności PESEL” i w sposób prawidłowy dokonał zgłoszenia do rejestracji.⁴¹⁹

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.

IV.2 Postępowania wyjaśniające zakończone wydaniem decyzji odmawiającej rejestracji

Generalny Inspektor Ochrony Danych Osobowych w 1999 roku wydał 15 decyzji administracyjnych odmawiających rejestracji zbioru danych osobowych dotyczących:

- 1) Zgłoszenia zbioru danych o nazwie „Baza osobowa Mars International I”, złożonego przez Reemtsma Polska S.A. Zgłoszenie to nie spełniało wymogów, o których mowa w art. 41 ust. 1 pkt 5 i 6 ustawy o ochronie danych osobowych, tj. nie zawierało kompletnego opisu środków technicznych i organizacyjnych zastosowanych w celach określonych w art. 36-39 ustawy oraz informacji o sposobie wypełnienia wymagań technicznych i organizacyjnych, o których mowa w wymienionym rozporządzeniu. Tym samym, została spełniona przesłanka odmowy rejestracji określona w art. 44 ust. 1 pkt 1 ustawy o ochronie danych osobowych.

W związku z tym, zwrócono się do Reemtsma Polska S.A. o złożenie pisemnych wyjaśnień w tej sprawie. Mimo pouczenia w tym samym piśmie, iż w przypadku niezłożenia wymaganych wyjaśnień, Generalny Inspektor Ochrony Danych Osobowych odmówi rejestracji przedmiotowego zbioru danych i wyznaczenia 14-dniowego terminu do złożenia wyjaśnień. Reemtsma Polska S.A. nie złożyła żądanych wyjaśnień.

Wobec powyższego, Generalny Inspektor Ochrony Danych Osobowych, w drodze decyzji administracyjnej, odmówił rejestracji przedmiotowego zbioru danych osobowych i nakazał usunięcie danych ze zbioru.⁴²⁰

419 OI.10/0717/15/2000

420 GI/DRZDO/DEC/13/99

- 2) Zgłoszenia zbioru danych o nazwie „Kartoteka danych osobowych kandydatów” złożonego przez Business Consulting Sp. z o. o. Zgłoszenie to spełniało przesłankę, o której mowa w art. 44 ust. 1 pkt 2 w związku z art. 28 ust. 1 ustawy - w spółka oświadczyła bowiem, iż przetwarza dane osobowe dotyczące karalności, nie podając ustawowej podstawy przetwarzania takich danych.

Przeprowadzone w tej sprawie postępowanie potwierdziło, iż Business Consulting Sp. z o. o. przetwarza dane dotyczące karalności (formułowane jako „karany” lub „nie karany”), natomiast we wzorze standardowego kwestionariusza osobowego, wykorzystywanego przez spółkę przy zbieraniu danych osobowych, znajduje się rubryka do wypełniania - „Karalność”. Jednocześnie administrator nie podał ustawowej podstawy przetwarzania tego typu danych.

Wobec powyższego Generalny Inspektor Ochrony Danych Osobowych w drodze decyzji administracyjnej odmówił rejestracji przedmiotowego zbioru danych osobowych i nakazał usunięcie danych ze zbioru.⁴²¹

Wnioskodawca usunął wady zgłoszenia, które były przyczyną odmowy rejestracji, tj. z kwestionariusza osobowego wykreślono pytanie dotyczące skazań, a dane uprzednio uzyskane zostały protokolarnie zniszczone i w trybie art. 44 ust. 4 ustawy o ochronie danych osobowych zgłosił zbiór ponownie do rejestracji. Ponownie zgłoszony zbiór danych zarejestrowano (numer księgi 86).

- 3) Zgłoszenia zbioru danych o nazwie „Baza osobowa Mars International II”, złożonego przez Reemtsma Polska S.A. Zgłoszenie to nie spełniało wymogów, o których mowa w art. 41 ust. 1 punkt 5 i 6 ustawy o ochronie danych osobowych. Tym samym, została spełniona przesłanka odmowy rejestracji określona w art. 44 ust. 1 pkt 1 ustawy o ochronie danych osobowych.

W związku z tym, zwrócono się do Reemtsma Polska S.A. o złożenie pisemnych wyjaśnień w tej sprawie. Ponieważ wyjaśnienia te nie zostały złożone, Generalny Inspektor Ochrony Danych Osobowych, w drodze decyzji administracyjnej, odmówił rejestracji przedmiotowego zbioru danych osobowych i nakazał usunięcie danych ze zbioru.⁴²²

⁴²¹ GI/DRZDO/DEC/14/99

⁴²² GI/DRZDO/DEC/15/99

- 4) Zgłoszenia zbioru danych o nazwie "Ogólnopolskie badania socjologiczne młodzieży szkolnej" złożonego przez Guliwer Sp. z o. o. Zgłoszenie to spełniało przesłankę odmowy rejestracji zbioru danych określoną w art. 44 ust. 1 pkt 3 ustawy o ochronie danych osobowych, tj. urządzenia i system informatyczny służące do przetwarzania danych osobowych nie spełniały podstawowych warunków technicznych i organizacyjnych, o których mowa w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji.

W związku z tym, zwrócono się do Guliwer Sp. z o. o. o złożenie pisemnych wyjaśnień w tej sprawie. Mimo pouczenia w tym samym piśmie, iż w przypadku niezłożenia wymaganych wyjaśnień, Generalny Inspektor Ochrony Danych odmówi rejestracji przedmiotowego zbioru danych i wyznaczenia 14-dniowego terminu do złożenia wyjaśnień, Guliwer Sp. z o.o. nie złożyła żądanych wyjaśnień. Wobec powyższego, Generalny Inspektor Ochrony Danych Osobowych, w drodze decyzji administracyjnej odmówił rejestracji przedmiotowego zbioru danych osobowych i nakazał usunięcie danych ze zbioru.⁴²³

- 5) Zgłoszenia zbioru danych o nazwie „PDD” złożonego przez Polski Dom Dystrybucji Sp. z o. o. Ze zgłoszenia wynikało, iż przetwarzanie danych w tym zbiorze spełniało przesłankę wydania decyzji odmownej wymienioną w 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 ramach przeprowadzonego postępowania wyjaśniającego dwukrotnie zażądano złożenia pisemnych wyjaśnień, odebrano ustne wyjaśnienia od przedstawiciela firmy, a także przeprowadzono inspekcję w siedzibie podmiotu, któremu wnioskodawca powierzył przetwarzanie danych. Postępowanie w tej sprawie wykazało, iż Polski Dom Dystrybucji Sp. z o.o. spełnił wymogi techniczne i organizacyjne, ale jednocześnie przetwarzając dane w zgłoszonym zbiorze nie dopełnił obowiązków informacyjnych zawartych w art. 24 ustawy o ochronie danych osobowych w częściach dotyczących adresu siedziby administratora danych i dobrowolności lub obowiązku podania danych osobowych. Tym samym została spełniona przesłanka odmowy rejestracji określona w art. 44 ust. 1 pkt 2 ustawy o ochronie danych osobowych. Z uwagi na to Generalny Inspektor Ochrony Danych Osobowych w drodze decyzji administracyjnej odmówił rejestracji

423 GI/DRZDO/DEC/90/99

przedmiotowego zbioru danych osobowych i nakazał wstrzymanie przetwarzania danych w zgłoszonym zbiorze, tj. zaniechanie operacji, o których mowa w art. 7 pkt 2 ustawy o ochronie danych osobowych, za wyjątkiem przechowywania danych.⁴²⁴

- 6) Zgłoszenia zbioru danych o nazwie „Dom Eli” złożonego przez Dom Eli Sp. z o. o. Ze zgłoszenia wynikało, iż przetwarzanie danych w tym zbiorze spełniało przesłankę wydania decyzji odmownej wymienioną w art. 44 ust. 1 pkt 3 ustawy, tj. urządzenia i systemy informatyczne 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 ramach przeprowadzonego postępowania wyjaśniającego dwukrotnie zażądano złożenia pisemnych wyjaśnień, odebrano ustne wyjaśnienia od przedstawiciela firmy, a także przeprowadzono inspekcję w siedzibie podmiotu, któremu wnioskodawca powierzył przetwarzanie danych. Postępowanie w tej sprawie wykazało, iż Polski Dom Dystrybucji Sp. z o.o. spełnił wymogi techniczne i organizacyjne, ale jednocześnie przetwarzając dane w zgłoszonym zbiorze nie dopełnił obowiązków informacyjnych zawartych w art. 24 ustawy o ochronie danych osobowych, w częściach dotyczących adresu siedziby administratora danych i dobrowolności lub obowiązku podania danych osobowych Tym samym została spełniona przesłanka odmowy rejestracji określona w art. 44 ust. 1 pkt 2 ustawy o ochronie danych osobowych.

W związku z tym, 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.⁴²⁵

- 7) Zgłoszenia zbioru danych o nazwie „Acti-Vita” złożonego przez Acti-Vita Sp. z o. o. Ze zgłoszenia wynikało, iż przetwarzanie danych w tym zbiorze spełniało przesłankę wydania decyzji odmownej wymienioną w art. 44 ust. 1 pkt 3 ustawy, tj. urządzenia i systemy informatyczne 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.

424 GI/DRZDO/DEC/101/99

425 GI/DRZDO/DEC/102/99

W ramach przeprowadzonego postępowania wyjaśniającego dwukrotnie zażądano złożenia pisemnych wyjaśnień, odebrano ustne wyjaśnienia od przedstawiciela firmy, a także przeprowadzono inspekcję w siedzibie podmiotu, któremu wnioskodawca powierzył przetwarzanie danych. Postępowanie w tej sprawie wykazało, iż Polski Dom Dystrybucji Sp. z o.o. spełnił wymogi techniczne i organizacyjne, ale jednocześnie przetwarzając dane w zgłoszonym zbiorze nie dopełnił obowiązków informacyjnych zawartych w art. 24 ustawy o ochronie danych osobowych, w częściach dotyczących adresu siedziby administratora danych i dobrowolności lub obowiązku podania danych osobowych Tym samym została spełniona przesłanka odmowy rejestracji określona w art. 44 ust. 1 pkt 2 ustawy o ochronie danych osobowych. Mając na uwadze powyższe Generalny Inspektor Ochrony Danych Osobowych, w drodze decyzji administracyjnej, odmówił rejestracji przedmiotowego zbioru danych osobowych i nakazał wstrzymanie przetwarzania danych w zgłoszonym zbiorze.⁴²⁶

- 8) Zgłoszenia zbioru danych o nazwie „Salon Nowości” złożonego przez Salon Nowości Sp. z o. o. Ze zgłoszenia wynikało, iż przetwarzanie danych w tym zbiorze spełniało przesłankę wydania decyzji odmownej wymienioną w art. 44 ust. 1 pkt 3 ustawy, tj. urządzenia i systemy informatyczne 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 ramach przeprowadzonego postępowania wyjaśniającego dwukrotnie zażądano złożenia pisemnych wyjaśnień, odebrano ustne wyjaśnienia od przedstawiciela firmy, a także przeprowadzono inspekcję w siedzibie podmiotu, któremu wnioskodawca powierzył przetwarzanie danych. Postępowanie w tej sprawie wykazało, iż Polski Dom Dystrybucji Sp. z o.o. spełnił wymogi techniczne i organizacyjne, ale jednocześnie przetwarzając dane w zgłoszonym zbiorze nie dopełnił obowiązków informacyjnych zawartych w art. 24 ustawy o ochronie danych osobowych w częściach dotyczących adresu siedziby administratora danych i dobrowolności lub obowiązku podania danych osobowych 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

⁴²⁶ GI/DRZDO/DEC/103/99

przedmiotowego zbioru danych osobowych i nakazał wstrzymanie przetwarzania danych w zgłoszonym zbiorze, za wyjątkiem przechowywania danych.⁴²⁷

- 9) Zgłoszenia zbioru danych o nazwie „World Marketing” złożonego przez World Marketing Sp. z o. o. Ze zgłoszenia wynikało, iż przetwarzanie danych w tym zbiorze spełniało przesłankę wydania decyzji odmownej wymienioną w art. 44 ust. 1 pkt 3 ustawy, tj. urządzenia i systemy informatyczne 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 ramach przeprowadzonego postępowania wyjaśniającego dwukrotnie zażądano złożenia pisemnych wyjaśnień, odebrano ustne wyjaśnienia od przedstawiciela firmy, a także przeprowadzono inspekcję w siedzibie podmiotu, któremu wnioskodawca powierzył przetwarzanie danych. Postępowanie w tej sprawie wykazało, iż Polski Dom Dystrybucji Sp. z o.o. spełnił wymogi techniczne i organizacyjne, ale jednocześnie przetwarzając dane w zgłoszonym zbiorze nie dopełnił obowiązków informacyjnych zawartych w art. 24 ustawy o ochronie danych osobowych w częściach dotyczących adresu siedziby administratora danych i dobrowolności lub obowiązku podania danych osobowych. Tym samym została spełniona przesłanka odmowy rejestracji określona w art. 44 ust. 1 pkt 2 ustawy o ochronie danych osobowych. Generalny Inspektor Ochrony Danych Osobowych w drodze decyzji administracyjnej odmówił rejestracji przedmiotowego zbioru danych osobowych i nakazał wstrzymanie przetwarzania danych w zgłoszonym zbiorze.⁴²⁸

- 10) Zgłoszenia zbioru danych o nazwie "Baza Danych Osobowych CRDP Sp. z o. o." złożonego przez spółkę z ograniczoną odpowiedzialnością pod firmą "CRDP". 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 przedmiotowym zbiorze naruszałoby art. 26 ust. 1 i 3 ustawy - dane były nieadekwatne w stosunku do celów, w jakich były przetwarzane (administrator przetwarzał dane ujawniające pochodzenie

⁴²⁷ GI/DRZDO/DEC/174/99
⁴²⁸ GI/DRZDO/DEC/175/99

rasowe i etniczne, przekonania filozoficzne, stan zdrowia oraz nałogi w celu prowadzenia doradztwa personalnego);

- art. 28 ust. 1 ustawy, ponieważ przetwarzanie danych o skazaniach oraz orzeczeń o ukaraniu nie znajduje podstawy ustawowej;
- art. 44 ust. 1 pkt 3 ustawy, tj. urządzenia i systemy informatyczne 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.

Przeprowadzone w tej sprawie postępowanie wykazało, iż urządzenia i systemy informatyczne służące do przetwarzania danych osobowych w przedmiotowym zbiorze spełniają wymagania określone przepisami prawa, a przetwarzanie danych wrażliwych dotyczących pochodzenia rasowego i etnicznego, przekonań filozoficznych, stanu zdrowia oraz nałogów odbywa się na wyraźne życzenie osób, których dane dotyczą i za ich pisemną zgodą.

Jednocześnie w złożonych wyjaśnieniach spółka pod nazwą CRDP potwierdziła, iż przetwarza w przedmiotowym zbiorze dane dotyczące skazań i orzeczeń o ukaraniu. 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 usunięcie danych ze zbioru.⁴²⁹ Wnioskodawca usunął wady zgłoszenia, które były przyczyną odmowy rejestracji, tj. z kwestionariusza osobowego wykreślono pytanie dotyczące skazań, a dane uprzednio uzyskane nie zostały wprowadzone do zbioru i w trybie art. 44 ust. 4 ustawy o ochronie danych osobowych zgłosił zbiór ponownie do rejestracji. Ponownie zgłoszony zbiór danych zarejestrowano (numer księgi 3855).

11) Zgłoszenia zbioru danych o nazwie „Willemse” złożonego przez spółkę z ograniczoną odpowiedzialnością pod firmą „Willemse-Ogrody”.

W ramach postępowania wyjaśniającego przeprowadzono inspekcję w siedzibie Willemse-Ogrody Sp. z o.o., która wykazała, że wnioskodawca nie dopełnił obowiązku

⁴²⁹ GI/DRZDO/DEC/176/99

informacyjnego, o którym mowa w art. 25 ust. 1 ustawy, a także obowiązków dotyczących technicznych i organizacyjnych aspektów przetwarzania danych w systemach informatycznych. Informacje zawarte w zgłoszeniu przedmiotowego zbioru do rejestracji pozostawały w sprzeczności z ustaleniami poczynionymi w trakcie kontroli.

Wobec powyższego Generalny Inspektor Ochrony Danych Osobowych w drodze decyzji administracyjnej odmówił rejestracji przedmiotowego zbioru danych osobowych i nakazał usunięcie danych ze zbioru.⁴³⁰

Do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynął wniosek Willemse-Ogrody Sp. z o.o. o ponowne rozpatrzenie sprawy i o wstrzymanie natychmiastowego wykonania decyzji. W uzasadnieniu wnioskodawca wyjaśniał, że w okresie pomiędzy inspekcją a wydaniem decyzji odmownej zostały usunięte nieprawidłowości wskazane w decyzji.

W toku postępowania odwoławczego ponownie przeprowadzono czynności kontrolne w siedzibie zgłoszeniodawcy, które wykazały, że administrator danych usunął wady, które były powodem wydania decyzji.⁴³¹ Tym samym zbiór danych o nazwie „Willemse” należało uznać za podlegający rejestracji. Wobec powyższego uchylono zaskarżoną decyzję w całości, a przedmiotowy zbiór danych zarejestrowano (księga rejestrowa nr 7401).

- 12) Zgłoszenia zbioru danych o nazwie „Baza Klientów Nemetschek” złożonego przez spółkę z ograniczoną odpowiedzialnością pod firmą „Nemetschek Polska”.

Przeprowadzone postępowanie wyjaśniające w tej sprawie jednoznacznie wykazało, iż dane przetwarzane są w przedmiotowym zbiorze w celach marketingowych bez zgody osoby, której dotyczą. Administrator nie podał żadnej innej podstawy prawnej przetwarzania danych w zbiorze.

W związku z tym przetwarzanie danych osobowych w zgłoszonym zbiorze 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 przedmiotowego zbioru danych osobowych i nakazał wstrzymanie przetwarzania danych w zgłoszonym zbiorze, tj. zaniechanie

⁴³⁰ GI/DRZDO/DEC/187/99

operacji, o których mowa w art. 7 pkt. 2 ustawy o ochronie danych osobowych, za wyjątkiem przechowywania danych.⁴³²

- 13) Zgłoszenia zbioru danych o nazwie „Baza danych osobowych wydawnictwa G+J RBA Sp. z o. o. & Co. Spółka Komandytowa złożonego przez spółkę komandytową pod firmą „Wydawnictwo G+J RBA Sp. z o. o. & Co.”.

Przeprowadzone w powyższej sprawie postępowanie, tj. odebranie pisemnych wyjaśnień od strony oraz czynności kontrolne przeprowadzone w siedzibie administratora, wykazały, iż w przedmiotowym zbiorze przetwarzane są również dane osób pozyskane z innych źródeł, niż od osób, których dane dotyczą, a także, iż w stosunku do tych osób nie dopełniono obowiązku informacyjnego wynikającego z art. 25 ustawy o ochronie danych osobowych, pomimo że nie zachodzą przesłanki wyłączające ten obowiązek.

Ustalenia poczynione w trakcie kontroli w siedzibie administratora danych pozostawały w sprzeczności z pisemnymi wyjaśnieniami strony w tej kwestii.

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, tj. zaniechanie operacji, o których mowa w art. 7 pkt. 2 ustawy o ochronie danych osobowych, za wyjątkiem przechowywania danych.⁴³³

Do Generalnego Inspektora Ochrony Danych Osobowych wpłynął wniosek wydawnictwa G+J RBA Sp. z o. o. & Co. Spółka Komandytowa o ponowne rozpatrzenie sprawy i wstrzymanie natychmiastowego wykonania decyzji. W uzasadnieniu wnioskodawca wyjaśniał, iż wstrzymanie natychmiastowego wykonania decyzji umożliwi mu dopełnienie czynności, których brak stanowił podstawę wydania decyzji odmownej.

Generalny Inspektor Ochrony Danych Osobowych postanowił wstrzymać natychmiastowe wykonanie decyzji.⁴³⁴ Następnie administrator danych zwrócił się do Generalnego Inspektora Ochrony Danych Osobowych o wycofanie wniosku o ponowne rozpatrzenie sprawy. Po usunięciu wad, które były przyczyną odmowy rejestracji, na podstawie art. 44 ust. 4 ustawy o ochronie danych osobowych zgłosił zbiór ponownie do rejestracji. Ponownie zgłoszony zbiór danych zarejestrowano (numer księgi 7420).

431 GI/DRZDO/DEC/187/99

432 GI/DRZDO/DEC/190/99

433 GI/DRZDO/DEC/192/99

434 GI/DRZDO/POST/2/00

- 14) Zgłoszenia zbioru danych o nazwie „Hostessy, modelki, fotomodelki” złożonego przez Ewę Kowalską, prowadzącą działalność gospodarczą pod firmą „Media Group”.

Celem przetwarzania danych osobowych w tym zbiorze była rekrutacja i pozyskiwanie hostess, modelek i fotomodelek oraz stałe pośredniczenie przy zawieraniu w ich imieniu i na ich rzecz umów o świadczenie pracy w kraju lub poza jego granicami.

W zgłoszonym zbiorze przetwarzane były natomiast dane ujawniające życie intymne. Naruszało to zasadę art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych, tzn. zakres przetwarzanych danych był nieadekwatny w stosunku do celu przetwarzania. Tym samym została spełniona przesłanka odmowy rejestracji określona w art. 44 ust. 1 pkt 2 ustawy.

W ramach postępowania wyjaśniającego odebrano od strony pisemne wyjaśnienia. Przeprowadzone postępowanie potwierdziło przetwarzanie w zgłoszonym zbiorze danych ujawniających bezpośrednio lub w kontekście życia seksualne, między innymi dotyczących momentu inicjacji seksualnej. Administrator danych w pisemnych wyjaśnieniach oświadczył także, iż przetwarzanie tego typu informacji w założeniu służyć ma wyborowi takich kandydatek, które swoim zachowaniem nie wpłyną negatywnie na dotychczasowy wizerunek firmy. Generalny Inspektor nie uznał wyjaśnień strony w tym zakresie i jednocześnie stwierdził, iż spełniona została przesłanka odmowy rejestracji, o której mowa w art. 44 ust. 1 pkt 2 ustawy o ochronie danych osobowych, ponieważ informacje ujawniające życie seksualne nie są adekwatne do celu przetwarzania, którym w tym przypadku była rekrutacja i pozyskiwanie hostess, modelek i fotomodelek.

Wobec powyższego Generalny Inspektor Ochrony Danych Osobowych w drodze decyzji administracyjnej odmówił rejestracji przedmiotowego zbioru danych osobowych i nakazał usunięcie danych ze zbioru.⁴³⁵ Wnioskodawca usunął wady zgłoszenia, które były przyczyną odmowy rejestracji i w trybie art. 44 ust. 4 ustawy o ochronie danych osobowych zgłosił zbiór ponownie do rejestracji.

- 15) Zgłoszenia zbioru danych o nazwie "Duo-Tour" złożonego przez spółkę z ograniczoną odpowiedzialnością pod firmą „Duo-Tour”.

Zgłoszenie to nie spełniało wymogów, o których mowa w art. 41 ust. 1 pkt 5 i 6 ustawy, tj. nie zawierało opisu środków technicznych i organizacyjnych zastosowanych w celach określonych w art. 36-39 ustawy oraz informacji o sposobie wypełnienia wymagań

⁴³⁵ GI/DRZDO/DEC/193/99

technicznych i organizacyjnych, o których mowa w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji. Tym samym spełniona została przesłanka odmowy rejestracji zbioru danych określona w art. 44 ust. 1 pkt 1 ustawy o ochronie danych osobowych.

W toku prowadzonego postępowania administrator uzupełnił braki formalne dotyczące części E i F zgłoszenia. Ze złożonych wyjaśnień wynikało jednak, 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.

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, t.j. zaniechanie operacji, o których mowa w art. 7 pkt. 2 ustawy o ochronie danych osobowych, za wyjątkiem przechowywania danych.⁴³⁶

V. 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 1999 r. wydano 1065 zaświadczeń, z czego 143 zaświadczenia dotyczyły zarejestrowania zbiorów danych zgłoszonych przez administratorów, o których mowa w art. 3 ust. 2 ustawy o ochronie danych osobowych, natomiast 922 zgłoszonych przez podmioty określone w art. 3 ust. 1 ustawy. Żaden wniosek o wydanie zaświadczenia nie został załatwiony odmownie.

VI. Wnioski

Ze względu na szeroki katalog wyłączeń (art. 43 ust. 1) i zakres przedmiotowy obowiązku, który obejmuje wyłącznie zbiory danych, bardzo trudne jest określenie ilości zbiorów, które powinny być zgłoszone do rejestracji, w celu porównania jej z rzeczywistą liczbą zgłoszonych zbiorów. Trudności te występują nawet w przypadku administracji publicznej, która co do zasady przetwarza dane osobowe realizując obowiązki nałożone przez przepisy prawa. Jednakże organy administracyjne samodzielnie kształtują w ramach

⁴³⁶ GI/DRZDO/DEC/209/99

zakreślonych przez przepisy prawa ilość prowadzonych i zgłaszanych zbiorów danych. Na przykład gmina może prowadzić nie tylko jeden zbiór danych osobowych związanych z opłatami i podatkami lokalnymi, ale również w tym samym zakresie kilka zbiorów danych (np. zbiór danych związany z podatkiem od posiadanych psów, środków transportu itd.). Administrator danych w sposób indywidualny określa więc ilość prowadzonych zbiorów, dokonując podziału na konkretne zbiory danych ze względów prawnych, funkcjonalnych lub terytorialnych.

Obowiązujący wzór zgłoszenia sprawiał wnioskodawcom problemy z jego prawidłowym wypełnieniem, czego konsekwencjami w poszczególnych sprawach były postępowania wyjaśniające prowadzone przez organ rejestracyjny. Wobec powyższego w czerwcu 1999 r. Generalny Inspektor Ochrony Danych Osobowych zdecydował o umieszczeniu na swojej stronie internetowej (www.giodo.gov.pl) wskazówek dotyczących wypełniania zgłoszeń zbiorów danych do rejestracji (zostały one przedrukowane m.in. w „Gazecie Samorządowej” nr 21-22/1999). Ponadto Generalny Inspektor Ochrony Danych Osobowych i pracownicy jego Biura przeprowadzili szereg szkoleń, podczas których szczegółowo omówiono problematykę prawidłowej realizacji obowiązku rejestracyjnego.

W związku z potrzebą docelowego rozwiązania problemu wzoru zgłoszenia Generalny Inspektor Ochrony Danych Osobowych pismem z dnia 14 lipca 1999 r. (GI/723/99) wystąpił do Ministra Spraw Wewnętrznych i Administracji o zmianę właściwego rozporządzenia wykonawczego i jednocześnie przedstawił projekt jego nowelizacji, którego podstawowym założeniami były:

- uproszczenie części F wzoru zgłoszenia, poprzez podzielenie jej na pola do wypełnienia lub zakreślania odpowiednich wariantów,
- korekta pozostałych części wzoru pozwalająca na lepszą identyfikację wnioskodawcy i podmiotu, któremu zlecił on przetwarzania danych osobowych, a także usuwająca sprzeczności występujące w formularzu.

Propozycje Generalnego Inspektora zostały uwzględnione w rozporządzeniu MSWiA z dnia 2 listopada 1999 r. zmieniającym rozporządzenie 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 83, poz. 1091).

Zorganizowana nawet przez jeden podmiot akcja wysyłania wniosków rejestracyjnych na jednolicie wypełnionych formularzach może zaciemnić faktyczny obraz: zarówno w zakresie informacji o prowadzonych zbiorach danych, jak i warunkach przetwarzania danych osobowych. Tego typu akcja przeprowadzona przez Commercial Union Towarzystwo Ubezpieczeń na Życie S.A. i Powszechne Towarzystwo Emerytalne BPH CU WBK S.A. dodatkowo utrudnia sprawne przeprowadzenie procesu rejestracyjnego (weryfikację wszystkich wniosków rejestracyjnych), ze względu na znaczną ilość zgłoszonych zbiorów danych.

Część III. ZAWIADOMIENIA DO PROKURATURY

W 1999 r. w 18 przypadkach Generalny Inspektor skierował sprawy do organów ścigania. Niniejsze 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.

Generalny Inspektor zawiadamiając organy ścigania wypełniał obowiązek nałożony art. 19 ustawy o ochronie danych osobowych, zgodnie z którym 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 organów ścigania dotyczyły nie dopełnienia obowiązku rejestracyjnego, tj. popełnienia przestępstwa z art. 53 ustawy o ochronie danych osobowych (3 sprawy), nieodpowiedniego zabezpieczenia danych osobowych pochodzących ze zbioru, a w związku z tym dopuszczenie do udostępnienia danych osobom nieuprawnionym oraz nieuprawnionego udostępnienia danych osobowych ze zbioru danych, tj. popełnienia przestępstwa z art. 51 ustawy o ochronie danych osobowych (8 spraw), niedopełnienia obowiązku informacyjnego, tj. popełnienia przestępstwa z art. 54 ustawy (7 spraw).

W trzech przypadkach, po przeprowadzeniu postępowania, do sądów skierowane zostały akty oskarżenia. W pozostałych przypadkach następowało umorzenie dochodzenia (4 przypadki), wydawane było postanowienie o odmowie wszczęcia dochodzenia (2 przypadki) bądź też brak jest informacji o prowadzonym (lub umorzonym) postępowaniu.

1. Sprawy, w wyniku których zostały skierowane do sądów akty oskarżenia.

- 1.1. W związku ze skargami kierowanymi do Biura GODO, Generalny Inspektor wszczął postępowanie administracyjne w sprawie działalności firmy CLARITAS Polska Sp. z o. o. Firma ta, w ramach prowadzonej działalności gospodarczej, zbiera dane dotyczące preferencji konsumentów odnośnie produktów i usług oferowanych na rynku polskim, lub takich, które mają być wprowadzone na ten rynek, a także takich danych konsumentów, które umożliwiają podział rynku na sektory. W trakcie postępowania okazało się, iż mimo rozpoczęcia działalności w okresie listopad - grudzień 1998 r., w którym to terminie do firmy zaczęły napływać pierwsze wypełnione kwestionariusze osobowe, firma nie dopełniła obowiązku

rejestracyjnego zbioru danych osobowych. W związku z powyższym o niedopełnieniu obowiązku zgłoszenia zbioru do zarejestrowania zawiadomiona została prokuratura, która uznała przedstawioną argumentację i podjęła postępowanie.⁴³⁷

Natomiast w analogicznych sprawach, niezgłoszenia do zarejestrowania zbiorów danych osobowych, mimo rozpoczęcia działalności przez AIG Powszechne Towarzystwo Emerytalne S.A. oraz przez Powszechne Towarzystwo Emerytalne DOM, wydane zostały przez prokuraturę – w pierwszym przypadku postanowienie o odmowie wszczęcia dochodzenia, mimo stwierdzenia, iż „rzeczywiście Zarząd AIG Powszechne Towarzystwo Emerytalne S.A. swoim zachowaniem wypełniło znamiona czynu zabronionego, nie dopełniając wskazanego w ustawie obowiązku, jednakże ujemna zawartość czynu jest typowo niska i osiąga poziom znikomego stopnia społecznej szkodliwości, przez co wyłącza jego karygodność”.⁴³⁸ W drugim zaś, wydane zostało postanowienie o umorzeniu dochodzenia, „wobec braku ustawowych znamion czynu zabronionego”. Bowiem prokuratura stwierdziła, iż mimo rozpoczęcia działalności Powszechne Towarzystwo Emerytalne DOM i przyjmowania umów o przystąpienie do PTE, umowy te nie były włączane w zbiór danych osobowych klientów PTE, ponieważ PTE nie było jeszcze organizacyjnie przygotowane do przetwarzania danych, gdyż „pisanie programu informatycznego umożliwiającego dostęp do tych danych rozpoczęto w ostatnich dniach marca. Zdaniem PTE DOM podmiot ten dysponował zbiorem danych, dopiero od momentu, kiedy to napisany został program umożliwiający dostęp do danych” (Postanowienie Prok. Rejonowej Warszawa Wola 6 Ds. 608/99). Brak zbioru danych – co miało być przeszkodą do zgłoszenia zbioru w momencie rozpoczęcia działalności – nie stanowiło przeszkody w zgłoszeniu zbioru (mimo nieposiadania stosownego programu komputerowego) do zarejestrowania Generalnemu Inspektorowi w dniu 24 marca 1999 r.

- 1.2. W wyniku informacji dziennikarskiej wszczęte zostało postępowanie dotyczące udostępnienia nieograniczonej liczbie osób danych osobowych klientów firmy Frito Lay Poland Sp.z o.o., w postaci imion, nazwisk i dokładnych adresów osób biorących udział w zorganizowanej przez tę firmę loterii „Graj w zielone”, uczestników V Wielkiej Loterii Przeglądu Reader’s Digest oraz dokumentów

⁴³⁷ Sprawa prowadzona przez Prokuraturę Rejonową Warszawa-Mokotów, sygn. 6 Ds. 251/99/III.

departamentu rejestrów Państwowych, Łączności i Informatyki MSWiA (zawierających wydruki komputerowe PESEL, wypełnione druki zgłoszenia pobytu czasowego i wypełnione druki zgłoszenia zmian w danych osobowo-adresowych) poprzez wyrzucenie znacznej ilości kopert z powyższymi danymi osobowymi (w paczkach, kartonach i luzem) oraz dokumentów urzędowych z MSWiA na składowisko makulatury Warszawskich Zakładów Papierniczych S.A. z siedzibą w Konstancinie – Jeziornej, tj. o naruszenie art. 51 ustawy o ochronie danych osobowych.

W powyższych sprawach, prowadzonych przez tę samą Prokuraturę Rejonową, do sądu skierowany został akt oskarżenia przeciwko Firmie Przegląd Reader's Digest,⁴³⁹ natomiast przeciwko osobom odpowiedzialnym za zabezpieczenie danych w Departamencie Rejestrów Państwowych, Łączności i Informatyki MSWiA postępowanie najpierw zostało zawieszone, a na skutek zażalenia Generalnego Inspektora podjęte na nowo i umorzone „z powodu znikomej szkodliwości społecznej czynu”.⁴⁴⁰

- 1.3. W związku ze skargą mieszkańców miejscowości Cz. na osobę piastującą funkcję burmistrza, która w trakcie kampanii wyborczej przed wyborami samorządowymi w 1998 r. bezprawnie wykorzystwała dane osobowe znajdujące się w zbiorze urzędowym danych mieszkańców gminy, wszczęte zostało postępowanie administracyjne, mające na celu wyjaśnienie wszystkich okoliczności sprawy. Postępowanie potwierdziło, iż w rzeczywistości mogło dojść do nieuprawnionego wykorzystania danych, a ponadto, iż burmistrz, jako administrator danych, nie dopełnił obowiązków organizacyjnych i nie zapewnił zabezpieczeń technicznych wynikających z ustawy o ochronie danych osobowych w celu zabezpieczenia danych. Poprzez niezabezpieczenie zbioru umożliwiono dostęp do zbioru osobom nieuprawnionym. W wyniku zawiadomienia skierowanego do prokuratury przez Generalnego Inspektora, Prokuratura podjęła postępowanie i skierowała akt oskarżenia do sądu.⁴⁴¹

2. *Pozostałe sprawy zakończone umorzeniem postępowań przez prokuraturę oraz odmową wszczęcia postępowania.*

438 Postanowienie Prokuratury Rejonowej Warszawa – Śródmieście 6 Ds. 1928/99/III.

439 Sprawa prowadzona przez Prokuraturę Rejonową w Piasecznie, nr 2 Ds. 470/99/V.

440 Postanowienie Prokuratury Rejonowej w Piasecznie, nr 2 Ds. 515/00/V.

441 Sprawa prowadzona przez Prokuraturę Rejonową w Śremie, nr sprawy Ds. 598/99.

W dwóch przypadkach umorzenia postępowania, zawiadomienie ze strony Generalnego Inspektora Ochrony Danych Osobowych dotyczyło niedopełnienia wobec osoby, której dane dotyczyły, obowiązku informacyjnego.

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, której dotyczą – o nazwie i siedzibie administratora danych, celu i zakresie zbierania, źródle danych, uprawnieniach wynikających z ustawy o ochronie danych osobowych. Art. 54 ustawy o ochronie danych osobowych przewiduje odpowiedzialność karną za niedopełnienie obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w ustawie o ochronie danych osobowych. Zarówno prawny obowiązek poinformowania, jak i sankcje karne mają zagwarantować osobom, których dane dotyczą, realizację przysługujących im konstytucyjnie praw.

Natomiast we wszystkich przypadkach, gdy umorzenie postępowania dotyczyło zawiadomień o niedopełnieniu obowiązku informacyjnego, mimo potwierdzenia niedopełnienia obowiązku informacyjnego, podstawą umorzenia było stwierdzenie o znikomości społecznej szkodliwości czynu,⁴⁴² lub o braku ustawowych znamion czynu zabronionego.⁴⁴³

Podobne rozstrzygnięcia zapadały w związku z zawiadamianiem organów ścigania o nieuprawnionym udostępnieniu danych osobowych.⁴⁴⁴ W jednym przypadku wydane zostało postanowienie o odmowie wszczęcia postępowania z powodu „powagi rzeczy osądzonej” mimo, iż prowadzone wcześniej i umorzone przez prokuraturę postępowanie dotyczyło naruszenia innego przepisu ustawy o ochronie danych osobowych.⁴⁴⁵

Doświadczenia z pierwszego pełnego roku kalendarzowego działalności Generalnego Inspektora Ochrony Danych Osobowych wskazują, iż mimo powtarzających się przypadków stwierdzenia naruszenia ustawy o ochronie danych osobowych, zebrania materiału dowodowego i przekazania wraz z zawiadomieniem do organów ścigania, w niewielu przypadkach organy ścigania kierują sprawy na drogę sądową.

442 Postanowienie Prokuratury Rejonowej Łódź-Górna, Ds.-7825/99.

443 Postanowienie Prokuratury Rejonowej Warszawa-Mokotów, KP-Ds- 5792/99.

444 Sprawa prowadzona przez Prokuraturę Rejonową Warszawa-Ochota, sprawa 154/99; sprawa Prowadzona przez Prokuraturę Rejonową w Katowicach, sprawa 2494/99.

445 Postanowienie Prokuratury Rejonowej w Gdyni, sprawa 3 Ds. 99/99.

W świetle powyższych doświadczeń w dalszym ciągu aktualna jest sformułowana wcześniej ocena, iż naruszenie ustawy o ochronie danych osobowych nie jest uznawane przez organy ścigania jako zasługujące na uwagę i nie uznaje za wskazane przeprowadzenie postępowania karnego. W wielu przypadkach, mimo zebrania w toku postępowania administracyjnego materiałów wskazujących na naruszenia przepisów ustawy o ochronie danych osobowych, przedstawiciele prokuratury uznają, iż „z powodu znikomej szkodliwości społecznej czynu” należy umorzyć postępowanie.

Działania prokuratury w przeważających przypadkach potwierdzają iluzoryczność prawnokarnej ochrony danych osobowych.

Część IV. PROPAGOWANIE IDEI OCHRONY DANYCH OSOBOWYCH

1. W ramach propagowania idei ochrony danych osobowych w społeczeństwie, Generalny Inspektor, bądź upoważnieni przez niego pracownicy Biura, przeprowadzili szkolenia oraz wykłady na temat stosowania przepisów ustawy o ochronie danych osobowych w instytucjach państwowych i samorządach, szkołach wyższych oraz u innych podmiotów (załącznik 6). W ramach przeprowadzanych szkoleń wśród instytucji najczęściej wymienianych były urzędy wojewódzkie w miastach takich, jak: Biłgoraj, Białystok, Bydgoszcz, Gdańsk, Łódź, Opole, Rzeszów, Szczecin czy Warszawa, urzędy miasta Łodzi i Krakowa, instytucje związane z działalnością bankową, jak Związek Banków Polskich czy Centrum Prawa Bankowego, Prokuratura Apelacyjna w Warszawie i w Gdańsku, Prokuratura Okręgowa w Gdańsku i Ostrowie Wielkopolskim, Kancelaria Prezydenta RP, Ministerstwo Spraw Wewnętrznych i Administracji oraz Ministerstwo Pracy i Polityki Socjalnej, Biuro Rzecznika Praw Obywatelskich, Biuro Zarządu Miasta Stołecznego Warszawy i inne. Generalny Inspektor Ochrony Danych Osobowych wygłaszał referaty na Uniwersytecie Warszawskim, Uniwersytecie Jagiellońskim, Uniwersytecie Łódzkim i w Akademii Teologii Katolickiej, a także w Trybunale Konstytucyjnym, na spotkaniu w Polskim Towarzystwie Socjologicznym, w Centrum Edukacji Helsińskiej Fundacji Praw Człowieka, w Biurze Rzecznika Praw Obywatelskich i u innych podmiotów.
2. Generalny Inspektor organizował również konferencje prasowe, seminaria, cyklicznie zamieszczał artykuły poświęcone ochronie danych osobowych w prasie o zasięgu ogólnopolskim, a także na utworzonej w 1999 roku stronie internetowej Biura.

W okresie sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych zorganizował trzy konferencje prasowe (załącznik 8) z udziałem wszystkich ośrodków telewizji publicznej i komercyjnej, stacji radiowych, dziennikarzy prasy codziennej i periodycznej oraz agencji informacyjnych.

Konferencje prasowe w kolejności poświęcone były działalności podmiotów prywatnych, banków i firm marketingowych w kontekście obowiązywania ustawy o ochronie danych osobowych. Stałą pozycją na konferencjach prasowych jest rozdawanie dziennikarzom materiałów z informacjami zawierającymi bieżącą statystykę skarg, zapytań prawnych, dane dotyczące rejestracji, przeprowadzonych kontroli i zawiadomień o popełnieniu przestępstw skierowanych do prokuratury, a także objaśnienia wybranych przepisów ustawy o ochronie danych osobowych.

Generalny Inspektor przedstawiał inicjatywy, z którymi wystąpił do odpowiednich instytucji, realizując w ten sposób swój ustawowy obowiązek inicjowania i podejmowania przedsięwzięć w zakresie doskonalenia ochrony danych osobowych. Szeroko omawiał przypadki nadinterpretacji ustawy oraz przykłady łamania jej przepisów przez różne instytucje, zarówno prywatne, jak i państwowe (szczególnie przez firmy ubezpieczeniowe i fundusze emerytalne). Wiele uwagi poświęcił sprawie niewłaściwego rozumienia przez instytucje publiczne zapisu art. 29 ustawy o ochronie danych osobowych, podając przykład odmowy udostępnienia przez Policję danych osobowych organizatorów blokad drogowych, mimo iż była ona jedynym dysponentem tych danych, zaś ich udostępnienie miałoby służyć wyłącznie dochodzeniu spraw przed sądem. W związku z takimi sprawami Generalny Inspektor skierował pismo do Ministra Spraw Wewnętrznych i Administracji z prośbą o przekazanie podległym ministrowi podmiotom informacji o powyższej sprawie, w celu umożliwienia (w uzasadnionych przypadkach) dostępu do informacji osobom zwracającym się w tej sprawie do Policji lub organów administracji terenowej. Na konferencji Generalny Inspektor wyjaśniał również, jak uchronić się przed agresywnymi działaniami firm marketingu bezpośredniego, podając przykłady konkretnych skarg (m.in. na Claritas i Reader's Digest) na przetwarzanie danych osobowych bez podstawy prawnej (brak zgody osoby, której dane dotyczą), niedopełnianiu obowiązku informacyjnego wynikającego z art. 24 i 25 ustawy o ochronie danych osobowych, a także nieuwzględnianiu sprzeciwów osób, których dane są przetwarzane. Wskazywał także na niewłaściwe zabezpieczenia zbiorów danych osobowych będących w dyspozycji różnych instytucji i często stosowaną przez nich praktykę wykorzystywania danych w celach innych niż te, dla których zostały zebrane, a także o podjętych przez Generalnego Inspektora działaniach w przypadkach łamania przepisów ustawy o ochronie danych osobowych.

Poruszane na konferencjach prasowych tematy zawsze spotykały się z dużym zainteresowaniem dziennikarzy, co znajdowało wyraz w licznych doniesieniach telewizyjnych, radiowych oraz w artykułach prasowych.

3. Generalny Inspektor podejmował również szereg działań na forum międzynarodowym, uczestnicząc w screeningu w związku z akcesją Polski do Unii Europejskiej i licznych międzynarodowych konferencjach.

Generalny Inspektor organizował także szkolenia dla pracowników Biura zarówno w Polsce, jak i za granicą (załącznik 6).

Między innymi na zaproszenie Generalnego Inspektora w dniu 1 grudnia 1999 r. przyjechał do Polski dr Alexander Dix, Rzecznik Ochrony Danych Osobowych i Dostępu do Informacji w Brandenburgii, który na otwartym spotkaniu z pracownikami Biura wygłosił referat, pt.: Prawo wglądu do akt i dostępu do informacji w Brandenburgii – podstawowe założenia ustawy o ochronie danych osobowych i prawie obywateli do informacji; pierwsze doświadczenia w zakresie jej funkcjonowania.

Na zaproszenie niemieckiego Rzecznika Ochrony Danych Osobowych na szkoleniu w Berlinie i Poczdamie przebywała w dniach od 19 do 22 grudnia 1999 r. pięcioosobowa grupa pracowników Biura Generalnego Inspektora Ochrony Danych Osobowych.

4. Przykładem propagowania idei ochrony danych osobowych przez Generalnego Inspektora było zorganizowanie w dniach 26 – 27 listopada 1999 r. polsko – niemieckiej konferencji, pt.: Wolność prasy a prawo do prywatności i ochrony danych osobowych. Referentami na konferencji ze strony niemieckiej byli prof. dr hab. Rainer Hamm z Uniwersytetu we Frankfurcie nad Menem, który wygłosił referat, pt.: Ochrona danych osobowych a prawo karne – sprzeczność sama w sobie, prof. dr hab. Winfried Hassemer, sędzia Trybunału Konstytucyjnego Niemiec: Konflikt pomiędzy sferą publiczną a prywatnością jednostki, dr Joachim Jacob, Związkowy Rzecznik Ochrony Danych Osobowych: Wolność prasy a ochrona danych osobowych, dr Marie - Theres Tinnefeld: Ochrona prywatności wobec naruszeń przez media.

Stronę polską na konferencji reprezentowali: prof. dr hab. Lech Garlicki, sędzia Trybunału Konstytucyjnego, który wygłosił referat, pt.: *Normy konstytucyjne dotyczące wolności prasy, prywatności i ochrony danych osobowych*, dr Ewa Kulesza, Generalny Inspektor Ochrony Danych Osobowych: *Wolność prasy a ochrona danych osobowych*, prof. dr hab. Ewa Nowińska z Uniwersytetu Jagiellońskiego miała wystąpienie, pt.: *Prywatność osób prowadzących działalność publiczną. Rzeczywistość a prawo*, prof. dr hab. Andrzej Rzepliński z Uniwersytetu Warszawskiego: *Orzecznictwo strasburskie w zakresie wolności prasy*, prof. dr hab. Marek Safjan, Prezes Trybunału Konstytucyjnego: *Prywatność osób publicznych*, prof. dr hab. Jacek Sobczak z Uniwersytetu Jagiellońskiego: *Granice wolności prasy* i prof. dr hab. Andrzej Zoll, Przewodniczący Rady Legislacyjnej przy Prezesie Rady Ministrów, który przedstawił referat, pt.: *Prawnokarna ochrona prywatności*.

W konferencji uczestniczyli posłowie i senatorowie, przedstawiciele różnych ministerstw, sędziowie Trybunału Konstytucyjnego, przedstawiciele nauki, dziennikarze,

adwokaci, pracownicy Kancelarii Sejmu i Kancelarii Prezydenta, Helsińskiej Fundacji Praw Człowieka, Rzecznik Praw Obywatelskich i przedstawiciele Biura RPO, Instytutu Spraw Publicznych, Zarządu TVP, Dyrektor Naczelnej Dyrekcji Archiwów Państwowych, a także pracownicy Biura Generalnego Inspektora Ochrony Danych Osobowych.

Konferencja stanowiła interesujące forum dla polsko – niemieckiej wymiany poglądów na temat prawa do prywatności i ochrony danych osobowych w państwach, z których jedno posiada wieloletnią już tradycję w dziedzinie ochrony tych praw, drugie zaś dopiero od niedawna wdraża je w życie. Tematyka poruszana w wystąpieniach dotyczyła szerokiego spektrum zagadnień związanych z granicami wolności prasy a prawem do prywatności i ochrony danych osobowych oraz omówieniu norm konstytucyjnych dotyczących tej problematyki, przedstawieniu prawnokarnych aspektów naruszenia prywatności, a także orzecznictwa strasburskiego w zakresie wolności prasy. Wiele kontrowersji wzbudzała definicja pojęcia *osoba publiczna*, w kontekście prawa do prywatności i wyznaczenia granicy pomiędzy sferą publiczną a prywatnością jednostki.

Zaprezentowane na konferencji stanowiska przedstawicieli różnych środowisk, w tym zwłaszcza praktyków, stanowiły doniosły wkład do ciągle aktualnej dyskusji na temat prawnych granic ingerencji w sferę prywatności jednostki, w zależności od funkcji, jaką pełni ona w społeczeństwie.

Konferencja zaowocowała szeregiem zainicjowanych przez Generalnego Inspektora spotkań z przedstawicielami mediów i środowisk naukowych, w celu zharmonizowania przepisów ustawy o ochronie danych osobowych z przepisami prawa prasowego.

5. Generalny Inspektor Ochrony Danych Osobowych, zgodnie ze swoimi obowiązkami statutowymi, uczestniczy w pracach wielu organizacji międzynarodowych. Swoją udział w tych pracach ma również Departament Informatyki. Do ważniejszych inicjatyw międzynarodowych, w których Generalny Inspektor uczestniczył w 1998 r. należały:
 - 8th Meeting of Working Group on New Technologies (GT-NT), które odbyło się w Strasburgu w ramach projektu Project Group On Data Protection (CJ-PD), Strasburg, 17 - 21.05.1999 r.
 - Konferencja „Data Protection – Bridge Between Privacy and the Global Market” oraz spotkanie grupy roboczej: „26th Meeting International Working Group on Data Protection in Telecommunication”, Berlin 30.08 – 1.09.1999 r.

WNIOSKI KOŃCOWE

Sprawozdanie za rok 1999 obejmuje pierwszy pełny rok kalendarzowy działalności Generalnego Inspektora Ochrony Danych Osobowych.

Największą liczbę spraw w 1999 r. stanowiły wnioski rejestracyjne (69 974 zgłoszeń) w związku z wykonaniem obowiązku rejestracyjnego, którego ostateczny termin ustawowy w odniesieniu do zbiorów danych prowadzonych w dniu wejścia w życie ustawy o ochronie danych osobowych mijał 30 października 1999 r. W związku z tym, że obowiązek zgłoszenia zbioru do zarejestrowania nie jest powtarzalny można domniemywać, iż w przyszłości nie będzie tak znaczącej liczby spraw kierowanych do Generalnego Inspektora Ochrony Danych Osobowych.

W 1999 r. podjęte zostały działania inspekcyjne, które należy ocenić jako skuteczny instrument kontroli prawidłowego przetwarzania danych oraz wdrażania ustawy o ochronie danych osobowych. W związku z tym, w kolejnych latach działalności Generalnego Inspektora działania inspekcyjne zostaną zintensyfikowane.

Pozytywnie należy ocenić również uprawnienie Generalnego Inspektora w zakresie opiniowania aktów prawnych, co w wielu przypadkach pozwoliło na zwrócenie szczególnej uwagi na ochronę danych osobowych i wyeliminowało sprzeczności z Konstytucją (art. 51) i ustawą o ochronie danych osobowych. W roku sprawozdawczym sporządzone zostały 262 opinie pisemne oraz prowadzona była bezpośrednia współpraca zarówno przy formułowaniu projektów aktów prawnych w poszczególnych resortach, jak i w komisjach sejmowych, na etapie czytania projektów aktów prawnych w Sejmie.

I. Z oceny przeprowadzonych inspekcji wynika, że stopień dopełnienia obowiązków w zakresie spełnienia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych jest w znacznym stopniu uzależniony od wielkości jednostki organizacyjnej.

W **małych jednostkach**, liczących od kilku do kilkudziesięciu pracowników, bardzo często obserwuje się brak jakichkolwiek działań organizacyjnych wymaganych przez ustawę o ochronie danych osobowych. Zdarzało się, iż w niektórych podmiotach „nie zauważono” ustawy o ochronie danych osobowych lub odczytano zapisane tam wymagania, jako nie odnoszące się do tych podmiotów. Podczas kontroli przeprowadzonej u jednego z administratorów danych pracownik działu kadr stwierdził, iż reprezentujący ich radca prawny po powrocie ze szkolenia w zakresie przepisów ustawy o ochronie danych osobowych

skomentował, że ustawa ta nie dotyczy ich jednostki organizacyjnej. Była to jednostka, w której przetwarzane zbiory danych osobowych, zgodnie z postanowieniami art. 43 ustawy, zwolnione były z obowiązku rejestracji. Zwolnienie to utożsamiono ze zwolnieniem od wszelkich innych obowiązków, jakie ustawa o ochronie danych osobowych nakłada na administratorów danych osobowych. Konsekwencją takiego rozumowania było to, iż nie podjęto w jednostce organizacyjnej żadnych działań w kierunku właściwego zarządzania przetwarzanymi zbiorami danych, ani też działań w zakresie zabezpieczenia użytego do ich przetwarzania systemu informatycznego, o którym, mowa w § 2 rozporządzenia MSWiA w sprawie warunków technicznych i organizacyjnych /.../.⁴⁴⁶

Charakterystyczne dla małych jednostek 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 jest mowa w § 11 rozporządzenia. W jednostkach takich nie przeprowadzono na ogół żadnej inwentaryzacji posiadanych zbiorów danych osobowych, ani identyfikacji zagrożeń i ryzyka, na jakie mogą być narażone przetwarzane przez nich dane osobowe. W wielu przypadkach administracją systemów informatycznych zajmują się tam firmy zewnętrzne, na podstawie umowy outsorsingu, które na ogół nie dostarczają swojemu klientowi żadnej dokumentacji zarządzania administrowanym systemem. Natomiast same jednostki będące formalnie administratorem przetwarzanych danych osobowych, z uwagi na to, że działania techniczno-organizacyjne w zakresie technicznej obsługi systemu zleciły innemu podmiotowi, nie zwracają należytej uwagi na wymagane przez ustawę działania techniczno-organizacyjne. 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 zleceniobiorca dopełnić w związku z wejściem w życie ustawy o ochronie danych osobowych.

Większość z kontrolowanych w małych firmach systemów informatycznych nie spełniało podstawowych warunków określonych w § 16 rozporządzenia. Tylko nieliczne użytkowane tam systemy dostosowane są do realizacji wymogów określonych w punktach 2, 4 i 5 § 16 wymienionego wyżej rozporządzenia. Podobnie jest z realizacją wymogów określonych w § 17, gdzie administratorzy starają się często wykazać, iż określone tam

446 Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, op.cit.

warunki spełniają ich systemy, uzasadniając to możliwością wydruku formatek z danymi prezentowanymi na monitorze, poprzez wykorzystanie opcji systemowej umożliwiającej „przeniesienie” obrazu monitora na drukarkę (opcja Print Scrn). O ile jednak niedociągnięcia wynikające z niedostosowania eksploatowanych systemów można usprawiedliwiać brakiem środków na ich modyfikację lub wymianę, to **zaniepokojenie budzi fakt zaniedbania podstawowych obowiązków organizacyjnych, w tym przede wszystkim w zakresie prowadzenia ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych, braku instrukcji postępowania na wypadek naruszenia ochrony danych osobowych oraz przeprowadzenia odpowiednich szkoleń.**

W małych jednostkach organizacyjnych obserwuje się również duże niedociągnięcia w realizacji takich wymagań, jak: dopełnienie obowiązków w zakresie właściwego zabezpieczenia fizycznego posiadanych zasobów, stosowanie odpowiednich urządzeń do podtrzymywania zasilania komputerów przed zanikami napięcia, zarządzanie wykonywaniem kopii awaryjnych oraz ich monitoringiem.

W **dużych jednostkach organizacyjnych**, takich jak towarzystwa emerytalne, banki, przedsiębiorstwa telefonii komórkowej, itp. obserwuje się na ogół, iż w zakresie zarządzania systemami informatycznymi starały się one wypełnić podstawowe wymagania organizacyjne i techniczne określone przez ustawę o ochronie danych osobowych. W przedsiębiorstwach tych nie można mieć najczęściej żadnych zastrzeżeń odnośnie zastosowanych środków bezpieczeństwa fizycznego oraz bezpieczeństwa dostępu do systemów informatycznych, w których przetwarzane są dane osobowe. Podmioty te zazwyczaj mają również opracowane dokumenty dotyczące polityki bezpieczeństwa (§ 2 powoływanego rozporządzenia MSWiA). W wielu przypadkach są to dokumenty, w których oddzielnie mówi się o bezpieczeństwie systemów informatycznych i oddzielnie o pozostałych aspektach bezpieczeństwa. Niektóre z ocenianych dokumentów były na bardzo dobrym poziomie merytorycznym. **Wiele zastrzeżeń w dużych jednostkach budzą natomiast takie zagadnienia, jak:**

- ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych,
- instrukcja zarządzania systemem informatycznym, w którym są przetwarzane dane osobowe,
- funkcjonalność stosowanych systemów informatycznych w zakresie dotyczącym głównie wymagań określonych w § 16 i 17 rozporządzenia,

- brak ewidencji posiadanych zbiorów danych osobowych.

Jak wykazały inspekcje, w wielu przypadkach ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych była prowadzona w różnej formie. Zazwyczaj były to ewidencje prowadzone lokalnie przez administratorów poszczególnych aplikacji. W konsekwencji prowadziło to do tego, że była ona niekompletna i niespójna. W ewidencji tej pomijano często administratorów systemów baz danych oraz administratorów aplikacji, czyli osoby, które miały w rzeczywistości najwyższe uprawnienia do przetwarzania zgromadzonych tam danych. Zdarzały się również przypadki, że nie wszystkie z użytkowanych w danym przedsiębiorstwie danych uznano za zbiory danych osobowych, pomimo, że fakt ten nie budził wątpliwości. Jako przykład można tutaj wskazać firmę, która do zbiorów danych osobowych nie zakwalifikowała hurtowni danych, w której zawarte były dane osobowe.

Z przeprowadzonych w dużych jednostkach organizacyjnych inspekcji wynika również, że w wielu przypadkach niewłaściwie została opracowana instrukcja zarządzania systemem informatycznym, o której mówi § 11 rozporządzenia. Występują tutaj najczęściej dwa skrajne przypadki. W pierwszym opracowuje się jedną instrukcję, bardzo ogólną, którą można zastosować praktycznie do wszystkich eksploatowanych w danej firmie aplikacji, w których są przetwarzane dane osobowe. W instrukcjach tych nie ma natomiast informacji, jakie aplikacje rzeczywiście są eksploatowane i jak ze sobą współpracują, jeżeli taka współpraca (wymiana danych) ma miejsce. W drugim przypadku, który wydaje się być bardziej odpowiedni, instrukcje dotyczą poszczególnych aplikacji bez wskazania jednak „środowiska”, w jakim zostały usytuowane i jak przekazywane są między nimi dane. W obydwu przypadkach brak jest najczęściej syntetycznego opisu eksploatowanych systemów informatycznych, który określałby zasady ich współpracy oraz administracji w zakresie zarządzania danymi osobowymi, jakie są w nich przetwarzane.

Zbiory danych osobowych, zwłaszcza te, które dotyczą klientów firm ubezpieczeniowych, banków i przedsiębiorstw telekomunikacyjnych, przetwarzane są najczęściej przy wykorzystaniu profesjonalnych narzędzi do budowy aplikacji oraz systemów baz danych. Narzędzia te posiadają zazwyczaj odpowiednie mechanizmy ułatwiające implementację niektórych wymagań określonych w rozporządzeniu, a zwłaszcza tych dotyczących odnotowania identyfikatora użytkownika, który po raz pierwszy wprowadza dane osobowe do zbioru oraz daty tego wprowadzenia. Znacznie gorzej jest natomiast z wypełnieniem pozostałych wymagań, a szczególnie tych o których mowa w punktach 2, 4 i 5

§ 16 oraz w § 17 rozporządzenia. W wielu przypadkach wymagania dotyczące odnotowywania informacji o udostępnieniach danych osobowych innym podmiotom realizowane są metodami tradycyjnymi, co z uwagi na rozproszony sposób przetwarzania niektórych zbiorów danych osobowych, nie w pełni odpowiada wymogom określonym w przepisach prawa. 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.

Interpretując literalnie ustawową definicję danych osobowych, wielu administratorów uważa, że do danych osobowych zalicza się tylko te dane, które mogą posłużyć do ustalenia tożsamości osoby. Tym samym do kategorii danych osobowych nie zaliczają takich danych, jak: zainteresowania, przynależność do organizacji, cechy charakteru, posiadane zasoby majątkowe itp. Jednakże biorąc pod uwagę intencje ustawodawcy i inne okoliczności,⁴⁴⁷ a także przepisy Konwencji 108 oraz Dyrektywy 95/46/WE Parlamentu Europejskiego oraz Rady z 24 października 1995 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych oraz swobodnym obiegiem tychże danych, należy przyjąć, iż dane, np. o przynależności do sekty X należy zaliczyć do kategorii danych osobowych, szczególnie chronionych. Nasuwa się jednak wniosek o potrzebie zmodyfikowania obecnej, ustawowej definicji danych osobowych do postaci bardziej przejrzystej i jednoznacznej tak, aby nie było wątpliwości, iż także dane, które nie identyfikują osoby, ale określają jej cechy, traktowane były jako dane osobowe. Najważniejsza definicja w ustawie o ochronie danych osobowych, czyli definicja *danych osobowych*, powinna być tak skonstruowana, aby dla osiągnięcia zamierzonego celu ustawodawcy nie było konieczne stosowanie specjalnych komentarzy wyjaśniających. Dobrym wzorem wydaje się być na przykład definicja danych osobowych przedstawiona w Dyrektywie 95/46/WE powoływanej wyżej, w której definiuje się dane osobowe w sposób następujący: „Dane osobowe – oznaczają wszelkie informacje dotyczące zidentyfikowanej lub dającej się zidentyfikować osoby fizycznej (podmiotu danych); osobą dającą się zidentyfikować jest osoba, której tożsamość można określić bezpośrednio lub pośrednio,

447 Por. Andrzej Szewc: Z problematyki ochrony danych osobowych, Radca Prawny 3/99.

szczególnie poprzez odniesienie się do numeru identyfikacyjnego lub innych wskaźników charakterystycznych dla jej fizycznej, fizjologicznej, umysłowej, gospodarczej, kulturowej lub społecznej tożsamości”. Innym, również dobrym wzorem dla definicji danych osobowych jest definicja sformułowana w dokumencie „Zalecenie Rady dotyczące Wytocznych w Sprawie Prywatności i Przepływu Danych Osobowych przez Granice” z dnia 23 września 1980 r., w którym dane osobowe definiuje się jako „wszelkie informacje odnoszące się do osoby zidentyfikowanej lub możliwej do zidentyfikowania (obiektu danych)”. Zgodne z treścią tej ostatniej definicji były początkowe propozycje ustawodawcy. W artykule „Prawna ochrona danych osobowych, Uzasadnienie projektu ustawy przyjętego przez radę Ministrów 13 sierpnia br.”,⁴⁴⁸ czytamy: „Zaproponowano, aby przez dane osobowe rozumieć każdą informację dotyczącą osoby fizycznej, której tożsamość jest określona lub można ją ustalić na podstawie tej informacji”. Takie brzmienie definicji danych osobowych było jak najbardziej zbieżne i adekwatne do celu, któremu ustawa ma służyć, czyli ograniczeniu niebezpieczeństwa zagrażającego prywatności życia osobistego.

Wiele problemów interpretacyjnych stwarza również określenie systemu informatycznego zawarte w rozporządzeniu MSWiA. W rozporządzeniu tym system informatyczny definiuje się, jako system przetwarzania informacji wraz ze związanymi z nimi ludźmi oraz zasobami technicznymi i finansowymi, który dostarcza i rozprowadza informacje. Definicja taka pozwala uniknąć zawężenia tego pojęcia tylko do sprzętu i oprogramowania, natomiast nie charakteryzuje zasobów technicznych, które są w istocie podstawą odróżniającą systemy informatyczne od systemów informacyjnych.⁴⁴⁹ Konsekwencją tak sformułowanej definicji systemu informatycznego jest ograniczenie możliwości egzekwowania od administratorów danych osobowych funkcjonalności systemów informatycznych, które są niezbędne w celu spełnienia wymogów określonych w § 16 i § 17 rozporządzenia. Zgodnie z aktualną definicją systemu informatycznego, wymienioną w § 16 i § 17 rozporządzenia, wymagania mogą być odnotowywane (sporządzane) w sposób tradycyjny bez jakiegokolwiek ich skojarzenia ze zbiorem danych przetwarzanych na komputerze. Co oznacza w takiej sytuacji zapis w § 17 rozporządzenia, który brzmi: „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 (...)”. Czy należy to rozumieć, jako

448 Przegląd Rządowy nr 10/96.

449 Por. również G. Szpor: Publicznoprawna ochrona danych osobowych, Przegląd Ustawodawstwa Gospodarczego, 1999 r. Nr 12.

konieczność odnotowywania niezbędnych danych, aby możliwe było ręczne lub automatyczne sporządzenie odpowiedniego raportu.⁴⁵⁰ Na pewno nie, gdyż o tym stanowi § 16 rozporządzenia. Domyślać się zatem należy, że w § 17 rozporządzenia chodzi o to, aby system informatyczny, rozumiany jako program komputerowy (aplikacja) posiadał wbudowaną funkcjonalność, czyli odpowiednią procedurę programową, która na polecenie użytkownika (operatora) spowoduje automatyczne sporządzenie wymaganego raportu.

II. 1. W związku z wejściem w życie ustawy o ochronie danych osobowych, przeważająca liczba spraw kierowanych do Generalnego Inspektora Ochrony Danych Osobowych zawierała pytania dotyczące możliwości udostępniania dokumentów i informacji zawierających dane osobowe. Pytania pochodziły m.in. od pracodawców i związków zawodowych, organów samorządowych, radnych, parlamentarzystów, dziennikarzy.

Zakres pytań kierowanych do Generalnego Inspektora Ochrony Danych osobowych, a także przywoływane przypadki odmowy udzielania informacji z powołaniem się na ustawę o ochronie danych osobowych wskazuje, iż ustawa o ochronie danych osobowych ograniczyła dostęp do informacji w sytuacjach, gdy brak jest dostatecznie precyzyjnej podstawy prawnej dla uzyskania informacji. Ustawa o ochronie danych osobowych wykorzystywana była m.in. dla świadomego ograniczenia kontroli społecznej, realizowanej również przez prasę, nad działalnością organów samorządowych i rządowych, ale częściowo również wynikała z niezrozumienia przepisów prawa oraz z braku klarowności przepisów określających powinności administratorów zbiorów danych osobowych. Przepisy ustawy o ochronie danych, niezbyt jasno określające niektóre obowiązki administratorów zbiorów danych oraz świadomość grożącej tym administratorom odpowiedzialności karnej, nie ułatwiała podjęcia decyzji o udostępnieniu żądanych danych.

Niewątpliwie na stan „zamknięcia” dostępu do danych po wejściu w życie ustawy o ochronie danych osobowych miał fakt, iż konstytucyjnie zagwarantowane w art. 51 prawo każdego do ochrony danych dotyczących jego osoby zostało uszczegółowione i rozwinięte w ustawie o ochronie danych, natomiast konstytucyjne prawo obywateli do informacji, wynikające z art. 61 Konstytucji RP, nie znalazło odzwierciedlenia w odrębnym akcie prawnym, równoważącym gwarancje w zakresie ochrony danych osobowych. Podkreślenia wymaga, iż zgodnie z art. 61 Konstytucji obywatel ma nie tylko prawo do uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje

⁴⁵⁰ Jeżeli odpowiednie dane są dostępne, nie można stwierdzić, że sporządzenie jakiegoś raportu na piśmie (w tym przypadku wykazu danych o wskazanej osobie wraz z informacjami, o których mowa w § 16 rozporządzenia) jest niemożliwe.

publiczne, informacji o działalności organów samorządu gospodarczego i zawodowego, a także innych osób oraz jednostek organizacyjnych w zakresie, w jakim wykonują one zadania władzy publicznej i gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa, ale prawo to obejmuje również dostęp do dokumentów oraz wstęp na posiedzenia kolegiałnych organów władzy publicznej pochodzących z powszechnych wyborów .

Z tego względu niezbędne jest stworzenie *prawnych podstaw dostępu obywateli do informacji*.

2. W związku z wejściem w życie ustawy o ochronie danych osobowych niezbędna jest nowelizacja przepisów prawa określających *uprawnienia organów kontrolnych*. Obowiązujące ustawodawstwo, stanowiące podstawę działalności organów kontrolnych, zawiera normy określające uprawnienia sformułowane w sposób generalny, nie precyzujący zakresu działania bądź konkretnych uprawnień organu kontrolnego. Pytania i sygnały kierowane do Generalnego Inspektora Ochrony Danych Osobowych wskazują na żądania udostępniania dokumentów wykraczające poza określony prawem zakres działania organów kontroli, jak też na sytuację wykorzystywania do utrudniania lub uniemożliwiania kontroli z powołaniem się na ustawę o ochronie danych osobowych.

Uwagi te dotyczą wszystkich organów kontrolnych, jakkolwiek klasycznym przykładem w tym zakresie może być Najwyższa Izba Kontroli. Podstawą działania NIK jest ustawa z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 1995 r. Nr 13, poz. 59 z późn. zm.), która w sposób generalny określa uprawnienia tego organu. Przepisy wspomnianej ustawy, szeroko określające uprawnienia NIK jako organu kontrolującego pod względem legalności, gospodarności, celowości i rzetelności działania wskazanych w ustawie podmiotów, nie stanowią podstawy do wglądu w dokumenty zawierające dane szczególnie chronione (np. dane o stanie zdrowia), czego z kolei domagają się inspektorzy NIK.

Podobnie nieprecyzyjnie określa uprawnienia inspektorów pracy ustawa z dnia 6 marca 1981 r. o Państwowej Inspekcji Pracy (Dz. U. z 1985 r., Nr 54, poz. 276 z późn. zm.). Jak wynika ze spraw kierowanych do Generalnego Inspektora, inspektorzy PIP żądają w trakcie prowadzonych kontroli udostępniania akt osobowych pracowników kontrolowanych zakładów pracy, powołując się na kompetencje określone w art. 8, zgodnie z którymi do zakresu działania należy nadzór i kontrola przestrzegania przez zakład 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 inicjowania przedsięwzięć w sprawach ochrony pracy w rolnictwie indywidualnym. Ustawa o Państwowej Inspekcji Pracy nie uprawnia jednak do wglądu w dokumenty osobowe pracowników kontrolowanych zakładów pracy, zezwalając inspektorom PIP jedynie na przeprowadzanie kontroli przestrzegania przepisów prawa pracy, żądania pisemnych i ustnych informacji w sprawach objętych kontrolą oraz wzywania i przesłuchiwanie tych osób w związku z przeprowadzaną kontrolą (art. 20). Gdyby inspektorzy PIP mieliby być wyposażeni w prawo wglądu w dokumenty osobowe pracowników w trakcie kontroli, co – jak argumentują inspektorzy PIP pozwalałoby na zebranie całości materiałów w zakresie przestrzegania przepisów prawa pracy. Takie uprawnienie musiałoby wprost wynikać z przepisów ustawy.

Z tego względu niezbędne jest ściśle określenie w przepisach prawa zakresu uprawnień przysługujących poszczególnym organom kontrolnym w szczególności, jeśli uprawnienia kontrolne miałyby wiązać się z dostępem organów kontrolnych do dokumentów zawierających dane szczególnie chronione.

3. Problemy ochrony danych osobowych nie są w dalszym ciągu w pełni uwzględniane w toku prac legislacyjnych. Akty normatywne, w częściach dotyczących danych osobowych, w dalszym ciągu cechuje niespójność, fragmentaryczność rozwiązań, a nawet wewnętrzna sprzeczność.

Klasycznym przykładem w tym zakresie są przepisy z zakresu ubezpieczeń zdrowotnych.

Ustawa z dnia 6 lutego 1997 r. o powszechnym ubezpieczeniu zdrowotnym (Dz. U. Nr 28, poz. 153 z późn. zm.) przewiduje w art. 16 szerszy zakres danych gromadzonych przez ZUS i Kasę Rolniczego Ubezpieczenia Społecznego wymaganych w zgłoszeniu do ubezpieczenia zdrowotnego, niż zakres danych, do przetwarzania którego upoważniona jest Kasa Chorych. W zgłoszeniu do ubezpieczenia winny znajdować się m.in. informacje wykraczające poza zakres danych przetwarzanych przez Kasę Chorych na podstawie art. 141a ustawy o powszechnym ubezpieczeniu zdrowotnym., obejmujący m.in. drugie imię, nazwisko rodowe, numer NIP oraz – gdy osoba zgłaszana do ubezpieczenia nie posiada numeru PESEL i numeru NIP – serię i numer dowodu tożsamości. W rezultacie Kasy Chorych przetwarzają dane, do przetwarzania których nie są upoważnione przepisami prawa.

W dalszym ciągu, wbrew wymogom Konstytucji, nieprawidłowo i w sposób zbyt ogólny formułowane są delegacje ustawowe i wydawane przepisy prawa na podstawie tych delegacji. Przykładem są niektóre przepisy wykonawcze do kodeksu postępowania karnego i

kodeksu karnego wykonawczego, upoważniające bez podstawy ustawowej do przetwarzania danych szczególnie chronionych (np. o stanie zdrowia).

4. Uregulowania przepisami prawa wymaga zagadnienie **udostępniania** dla potrzeb prowadzonych postępowań niektórym organom i instytucjom **danych osobowych z urzędowych zbiorów danych za pomocą systemów teletransmisji**.

Nie ulega wątpliwości, iż niektóre organy (np. prokuratura, Policja, Straż Graniczna) dla zapewnienia sprawności działania winny posiadać możliwość uzyskiwania bezpośrednio, np. za pomocą systemów teletransmisji, dane osobowe niezbędne dla prowadzenia postępowania. W chwili obecnej jedynie nowo tworzone przepisy (np. znowelizowana ustawa z dnia 20 czerwca 1997 r. Prawo o ruchu drogowym, Dz. U. Nr 98, poz. 602 z późn. zm.) przewiduje możliwość udostępniania danych za pomocą systemów teleinformatycznych pod warunkiem zachowania określonych norm bezpieczeństwa danych i kontroli przetwarzania danych osobowych. W pozostałych ustawach (np. ustawie z dnia 6 kwietnia 1990 r. o Policji Dz. U. Nr 30, poz. 602 z późn. zm.) brak jest stosownych zapisów, co sprawia, że dane mogą być udostępniane w sposób przewidziany w obecnie obowiązujących przepisach, tj. na pisemny wniosek funkcjonariusza organów celnych, Policji czy UOP.

5. Pierwszy rok wdrażania przepisów o ochronie danych osobowych ujawnił niedoskonałości ustawy z dnia 29 sierpnia 1997 r., której nowelizacja w zasadniczych punktach winna dotyczyć wskazanych poniżej kwestii.

Przede wszystkim powinna doprowadzić do pełnej implementacji Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych oraz swobodnego przepływu tych danych, w szczególności w zakresie objętym regulacją przez Dyrektywę, a nie uregulowanym przez polską ustawę. Ustawa w szczególności powinna być uzupełniona o odpowiednik zapisu art. 15 Dyrektywy, tj. o zakaz podejmowania indywidualnych rozstrzygnięć wyłącznie na podstawie przetwarzania danych w systemach automatycznych.

Nowelizacja ustawy, przygotowana w oparciu o doświadczenia zebrane w toku działalności Generalnego Inspektora, winna poszerzać uprawnienia Generalnego Inspektora m.in. o możliwość składania do Trybunału Konstytucyjnego wniosku o stwierdzenie zgodności aktu normatywnego z Konstytucją oraz o możliwość zwracania się do Sądu Najwyższego z wnioskiem o podjęcie uchwały mającej na celu wyjaśnienie przepisów

prawnych budzących wątpliwości lub których stosowanie wywołało rozbieżności w orzecznictwie. Należałoby również rozważyć, czy Generalny Inspektor jako organ ochrony danych osobowych, wzorem innych państw europejskich, nie powinien być wyposażony w prawo nakładania kar finansowych w trybie administracyjnym.

Generalny Inspektor oraz upoważnieni przez niego inspektorzy, w ramach wykonywania czynności kontrolnych, powinni być objęci ochroną, poprzez stworzenie sankcji za udaremnienie lub utrudnianie wykonywania kontroli.⁴⁵¹ W chwili obecnej bowiem inspektorzy dokonujący kontroli w zakresie ochrony danych osobowych nie są chronieni żadnymi przepisami w przypadku niedopuszczania do wykonania inspekcji przez kontrolowany podmiot.

Celowe wydaje się również dookreślenie w ustawie o ochronie danych osobowych, w sposób nie budzący wątpliwości, uprawnień inspektorskich inspektorów Generalnego Inspektora, jak też zasad ich zatrudniania i statusu zawodowego.

Zmiany wymagają również przepisy ustawy określające obowiązki administratorów danych osobowych. Nie wydaje się trafnym rozwiązaniem ustawy, nałożenie w równym zakresie obowiązków, w tym obowiązku informacyjnego, na podmioty sektora publicznego i prywatnego. Z praktyki Generalnego Inspektora Ochrony Danych Osobowych wynika, iż znaczne zagrożenie prawa do prywatności niesie działalność firm prywatnych, np. firm marketingowych. Z tego względu każda osoba, której dane są przetwarzane, powinna mieć prawo do kontroli przetwarzania jej danych, a przede wszystkim prawo do informacji o tym, kto (jaki podmiot) dane przetwarza, jakie jest źródło pozyskania tych danych oraz w jakim celu dane są wykorzystywane, także po to, aby móc skorzystać z przysługujących jej uprawnień.

Natomiast dopełnianie obowiązku informacyjnego przez podmioty sektora publicznego, zwłaszcza na podstawie art. 25 ustawy o ochronie danych osobowych, nie jest celowe, ponieważ przetwarzanie danych winno odbywać się wyłącznie w ramach i na podstawie przepisów prawa, a zatem już przepisy prawa wskazują, jakie podmioty sektora publicznego i w jakim zakresie mogą przetwarzać dane osobowe zgromadzone w określonym celu. Dlatego też nowelizacja ustawy o ochronie danych osobowych winna iść w kierunku wyłączenia obowiązku informacyjnego w odniesieniu do organów i instytucji, które

451 Np. w takim zakresie, w jakim przewiduje to art. 225 k.k.

przetwarzają dane w ramach i na podstawie przepisów prawa. Zmiana ustawy w takim zakresie odpowiadałaby filozofii Dyrektywy 95/46/WE, która kładąc nacisk na obowiązek informacyjny wobec podmiotu danych wyraźnie zastrzega, iż „(...) *nie ma konieczności nakładania tego obowiązku, kiedy podmiot danych posiada już tę informację (...)*” oraz że „(...) *obowiązek taki nie występuje wówczas, gdy rejestracja lub ujawnianie danych jest wyraźnie przewidziane przez prawo (...)*”. 452

452 Por. pkt 40, część wstępna Dyrektywy.

Załączniki

Załącznik nr 1

Ilość zbiorów danych osobowych zgłoszonych do rejestracji przez administrację publiczną szczebla wojewódzkiego w 1999 r.

L.p.	Województwo	Ogólna liczba zgłoszeń	Liczba zgłoszeń adm. Rządowej	Liczba zgłoszeń adm. samorządowej	Liczba zgłoszeń adm. Zespółonej
	dolnośląskie	22	19	0	3
	kujawsko-pomorskie	40	38	0	2
	lubelskie	37	31	1	5
	lubuskie	17	12	0	5
	łódzkie	31	22	5	4
	małopolskie	51	48	1	2
	opolskie	29	24	1	4
	mazowieckie	41	33	4	4
	podkarpackie	45	36	0	9
	podlaskie	52	31	9	12
	pomorskie	49	36	8	5
	śląskie	27	18	8	1
	świętokrzyskie	51	39	5	7
	warmińsko-mazurskie	23	16	3	4
	wielkopolskie	53	50	0	3
	zachodniopomorskie	34	25	3	6
	Ogółem	602	478	48	76

Załącznik nr 2

Centralne i naczelne organy administracji publicznej, które zgłosiły zbiory do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.

1. PREZYDENT RZECZPOSPOLITEJ POLSKIEJ

2. ADMINISTRACJA RZĄDOWA PODLEGA PREZESOWI RADY MINISTRÓW

- 2.1. Prezes Głównego Urzędu Statystycznego
- 2.2. Przewodniczący Komisji Papierów Wartościowych i Giełd
- 2.3. Prezes Państwowego Urzędu Nadzoru Ubezpieczeń
- 2.4. Prezes Urzędu Nadzoru Nad Funduszami Emerytalnymi
- 2.5. Szef Urzędu Służby Cywilnej

3. MINISTROWIE

- 3.1. Minister Edukacji Narodowej
- 3.2. Przewodniczący Komitetu Badań Naukowych
- 3.3. Minister Finansów
- 3.4. Minister Ochrony Środowiska
- 3.5. Minister Pracy i Polityki Socjalnej
- 3.6. Minister Skarbu Państwa
- 3.7. Minister Spraw Wewnętrznych i Administracji
- 3.8. Minister Sprawiedliwości
- 3.9. Minister Zdrowia

4. URZĘDY CENTRALNE

- 4.1. Przewodniczący Komitetu Kinematografii
- 4.2. Naczelny Dyrektor Archiwów Państwowych
- 4.3. Generalny Konserwator Zabytków
- 4.4. Prezes Urzędu Mieszkalnictwa i Rozwoju Miast
- 4.5. Prezes Krajowego Urzędu Pracy
- 4.6. Prezes Kasy Rolniczego Ubezpieczenia Społecznego
- 4.7. Centralny Zarząd Służby Więziennej
- 4.8. Agencja Własności Rolnej Skarbu Państwa

- 4.9. Dyrektor Generalny Lasów Państwowych
- 4.10. Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej
- 4.11. Prezes Urzędu do Spraw Kombatantów i Osób Represjonowanych
- 4.12. Prezes Głównego Urzędu Cei
- 4.13. Komendant Główny Straży Granicznej
- 4.14. Prezes Zakładu Ubezpieczeń Społecznych
- 4.15. Główny Geodeta Kraju

5. INSPEKTORZY

- 5.1. Główny Inspektor Inspekcji Handlowej
- 5.2. Główny Inspektor Nadzoru Budowlanego
- 5.3. Główny Inspektor Sanitarny
- 5.4. Główny Inspektor Inspekcji Nasiennej
- 5.5. Główny Inspektor Lotnictwa Cywilnego
- 5.6. Państwowa Inspekcja Pracy
- 5.7. Prezes Państwowej Inspekcji Telekomunikacyjnej i Pocztovej

6. . MARSZAŁEK SEJMU I SENATU

- 6.1. Marszałek Sejmu RP
- 6.2. Marszałek Senatu RP
- 6.3. . INNE ORGANY
- 6.4. Rzecznik Praw Obywatelskich
- 6.5. Rzecznik Ubezpieczonych

7. AGENCJE

- 7.1. Prezes Agencji Restrukturyzacji i Modernizacji Rolnictwa
- 7.2. Agencja Własności Rolnej Skarbu Państwa

8. INNE

- 8.1. Urząd Kultury Fizycznej i Turystyki (zgłoszenia z dnia 7 czerwca 1999 r.)
- 8.2. Archiwum Akt Nowych
- 8.3. Archiwum Główne Akt Dawnych
- 8.4. Państwowy Fundusz Rehabilitacji Osób Niepełnosprawnych

Załącznik nr 3

Liczba zwolnień od rejestracji w zależności od podstawy wyłączenia

Podstawa wyłączenia		Liczba zwolnień
Art. 43 ust. 1 pkt 1		2
Art. 43 ust. 1 pkt 2		120
Art. 43 ust. 1 pkt 3		0
Art. 43 ust. 1 pkt 4	Osoby zatrudnione	131
	Osoby zrzeszone	15
	Osoby uczące się	98
Art. 43 ust. 1 pkt 5		9
Art. 43 ust. 1 pkt 6		13
Art. 43 ust. 1 pkt 7		0
Art. 43 ust. 1 pkt 8		18
Art. 43 ust. 1 pkt 9		121
Art. 43 ust. 1 pkt 10		0
Art. 43 ust. 1 pkt 11		0
Ogółem		527

Załącznik nr 4

Wykaz wystąpień i opinii prawnych Generalnego Inspektora Ochrony Danych Osobowych

W okresie sprawozdawczym Generalny Inspektor skierował do administratorów danych (zarówno organów administracji państwowej jak i podmiotów prywatnych) 42 wystąpienia i opinie prawne dotyczące stosowania ustawy o ochronie danych osobowych.

Lp.	Numer sprawy	Adresat	Data	Przedmiot
1.	GI/6/99	Ministerstwo Zdrowia i Opieki Społecznej	05.01.1999 r.	Opinia na temat praktyki wywieszania list pacjentów w przychodniach zdrowia.
2.	GI/8/99	Najwyższa Izba Kontroli	08.01.1999 r.	Uprawnienia inspektorów NIK do uzyskiwania dokumentów zawierających dane osobowe, gdy jest to niezbędne dla przeprowadzenia postępowania kontrolnego.
3.	GI/39/99	Ministerstwo Edukacji Narodowej	13.01.1999 r.	Opinia na temat konieczności przygotowania nowelizacji ustawy Karta Nauczyciela.
4.	GI-DIS-189/99	Urząd Ochrony Konkurencji i Konsumentów	15.01.1999 r.	Informacje na temat działalności firm prowadzących działalność wysyłkową naruszającą ustawę o ochronie danych osobowych.
5.	GI/54/99	Rzecznik Praw Obywatelskich	19.01.1999 r.	Opinia na temat legalności rozpowszechniania listu gończego w Internecie.
6.	GI-DIS-157/99	Prezes Rady Krajowej Federacji Konsumentów	21.01.1999 r.	Informacje na temat działalności firmy Claritas Polska Sp. z o. o., która naruszyła ustawę o ochronie danych osobowych.
7.	GI/92/99	Ministerstwo Spraw Wewnętrznych i Administracji	02.02.1999 r.	Prośba o przedstawienie stanowiska w kwestii udostępniania bankowi danych osobowych z systemu PESEL.
8.	GI/101/99	Telekomunikacja Polska S.A.	05.02.1999 r.	Opinia na temat rozwiązania zaproponowanego przez TP S.A. przy publikowaniu list abonentów.

9.	GI/231/99	Urząd Ochrony Konkurencji i Konsumentów	05.03.1999 r.	Zwrócenie uwagi na praktykę firm ubezpieczeniowych oferujących ubezpieczenie na życie i uzależnienie zawarcia takiej umowy od wypełnienia wniosku, w którym upoważnia się lekarza i pracowników placówek leczniczych do udzielania pełnej informacji o wnioskodawcy, a także wymaganie udzielenia informacji o danych osobowych rodziny.
10.	GI/296/99	Ministerstwo Obrony Narodowej	17.03.1999 r.	Zwrócenie uwagi na przypadki odmowy udzielania Urzędowi ds. Kombatantów przez jednostki organizacyjne podległe MON, informacji wykorzystywanych w prowadzonych postępowaniach administracyjnych.
11.	GI/301/99	Urząd ds. Kombatantów	17.03.1999 r.	Opinia na temat możliwości uzyskiwania danych osobowych na potrzeby postępowań administracyjnych.
12.	GI/306/99	Urząd Nadzoru nad Funduszami Emerytalnymi	19.03.1999 r.	Uwagi dotyczące sposobu prowadzenia działalności przez fundusze emerytalne – niedopełnienie obowiązku zgłoszenia rejestrów członków funduszy.
13.	GI-DIS-91/98	Wysoki Komisarz Narodów Zjednoczonych	22.03.1999 r.	Informacje dotyczące wyników przeprowadzonego postępowania wyjaśniającego w sprawie przetwarzania danych osobowych cudzoziemców ubiegających się o udzielenie azylu.
14.	GI/314/99	Ministerstwo Spraw Wewnętrznych i Administracji	23.03.1999 r.	Poinformowanie o naruszeniu ustawy o ochronie danych osobowych przez Departament Rejestrów Państwowych i Łączności - PESEL.
15.	GI/317/99	Zarząd Telekomunikacji Polskiej S.A.	23.03.1999 r.	Prośba o interwencję w sprawie odmowy udzielania informacji przez pracowników biur informacji o numerach telefonicznych.
16.	GI/438/99	Komisja Praw Człowieka i Praworządności	11.05.1999 r.	Propozycja zmiany niektórych zapisów w ustawie o ochronie danych osobowych.

17.	GI/461/99	Ministerstwo Spraw Wewnętrznych i Administracji	17.05.1999 r.	Zwrócenie uwagi na niedopełnienie obowiązku zgłoszenia do rejestracji zbiorów danych osobowych prowadzonych przez jednostki samorządu terytorialnego.
18.	GI/476/99	Polska Telefonia Komórkowa CENTERTEL	19.05.1999 r.	Ocena postanowień Regulaminu Świadczenia Usług Telekomunikacyjnych obowiązującego w Polskiej Telefonii Komórkowej i związanej z nim praktyki stosownej przy zawieraniu umów o świadczenie usług telekomunikacyjnych.
19.	GI/496/99	Polkomtel S.A.	24.05.1999 r.	Opinia na temat postanowień Regulaminu Świadczenia Usług Telekomunikacyjnych stosowanych przez firmę Polkomtel przy zawieraniu umów o świadczenie usług telekomunikacyjnych.
20.	GI/497/99	Polska Telefonia Cyfrowa Era GSM S.A.	24.05.1999 r.	Opinia na temat postanowień Regulaminu Świadczenia Usług Telekomunikacyjnych stosowanych przez Polską Telefonię Komórkową ERA GSM przy zawieraniu umów o świadczenie usług telekomunikacyjnych.
21.	GI/513/99	Ministerstwo Łączności	28.05.1999 r.	Propozycja zmian w rozporządzeniu Ministra Łączności z dnia 8 lutego 1996 r.
22.	GI/558/99	Ministerstwo Sprawiedliwości	01.06.1999 r.	Propozycja zaniechania stosowania na potwierdzeniach odbioru przesyłek opisu sprawy – jako naruszenia ustawy o ochronie danych osobowych.
23.	GI/644/99	Ministerstwo Zdrowia i Opieki Społecznej	21.06.1999 r.	Opinia na temat kwestionariusza, który wypełniają osoby ubiegające się o leczenie uzdrowiskowe.
24.	GI/656/99	Wojewoda Śląski	24.06.1999 r.	Propozycja przeprowadzenia szkolenia jednostek gminnych i samorządowych z zakresu ustawy o ochronie danych osobowych.
25.	GI/659/99	Ministerstwo Spraw Wewnętrznych i Administracji	24.06.1999 r.	Informacja dotycząca możliwości przeprowadzenia szkoleń dla wojewodów oraz potwierdzenie obowiązku zgłaszania do zarejestrowania zbiorów przez organy administracji państwowej.

26.	GI/562/99	Ministerstwo Zdrowia i Opieki Społecznej	02.06.1999 r.	Uwagi dotyczące aktów prawnych regulujących opiekę zdrowotną obywateli.
27.	GI/662/99	Prezes Narodowego Banku Polskiego	29.06.1999 r.	Zasygnalizowanie faktów naruszenia ustawy o ochronie danych osobowych przez banki zgłaszanych do Biura Generalnego Inspektora Ochrony Danych Osobowych.
28.	GI/702/99	Komisja Finansów Publicznych	06.07.1999 r.	Opinia i uwagi do projektu Ustawy o zmianie ustawy o działalności ubezpieczeniowej.
29.	GI/687/99	Ministerstwo Spraw Wewnętrznych i Administracji	02.07.1999 r.	Opinia dotycząca możliwości udostępniania danych będących w posiadaniu Policji w celu dochodzenia praw przed sądem.
30.	GI/711/99	Prezes Zakładu Ubezpieczeń Społecznych	08.07.1999 r.	Zapytanie o możliwość zmiany wzoru odcinka emerytury i renty uwzględniający zachowanie otrzymanej kwoty tylko do wiadomości uposażonego.
31.	GI/663/99	Prezes Związku Banków Polskich	29.07.1999 r.	Informacja dotycząca naruszenia ustawy o ochronie danych osobowych przez banki.
32.	GI/808/99	PZU „Życie” SA	30.07.1999 r.	Ocena zgodności ankiety stosowanej przez Państwowy Zakład Ubezpieczeń „Życie” z ustawą o ochronie danych osobowych.
33.	GI/810/99	Rzecznik Praw Obywatelskich	30.07.1999 r.	Informacja dotycząca ankiety osobowej stosowanej przez Państwowy Zakład Ubezpieczeń „Życie” przy zawieraniu i kontynuacji grupowego ubezpieczenia pracowniczego.
34.	GI-DP-58/99	Prokurator Okręgowy	27.10.1999 r.	Wniosek o wniesienie sprzeciwu lub skargi do NSA od postanowienia Samorządowego Kolegium Odwoławczego w Olsztynie wydanego z przez Zastępcę Burmistrza Miasta Pisz w sprawie odmowy udzielenia informacji adresowej i umorzenia postępowania.
35.	GI-DP-758/99	Prokuratura Okręgowa w Olsztynie	27.10.1999 r.	Wniosek o wniesienie sprzeciwu do Naczelnego Sądu Administracyjnego od postanowienia Samorządowego Kolegium Odwoławczego w

				Olsztynie z dnia 24 czerwca 1999 r. (SKO-511-28/99).
36.	GI/1089	Szef Służby Cywilnej	27.10.1999 r.	Opinia dotycząca projektu bazy danych o korpusie służby cywilnej, która będzie tworzona w Urzędzie Służby Cywilnej.
37.	GI/1148/99	Zakład Ubezpieczeń Społecznych	17.11.1999 r.	Prośba o interwencję w związku ze skargami zgłoszonymi do Biura Generalnego Inspektora Ochrony Danych Osobowych na odmowy udzielania informacji przez jednostki organizacyjne ZUS-u.
38.	GI/1231/99	Prokurator Okręgowy	09.12.1999 r.	Zawiadomienie o popełnieniu przestępstwa przez Citibank Polska S.A.
39.	GI/1236/99	Rektor Śląskiej Akademii Medycznej	09.12.1999 r.	Interpretacja ustawy o ochronie danych osobowych w kontekście konieczności wypełniania ustawowego obowiązku, określonego w ustawie o szkolnictwie wyższym.
40.	GI/1239/99	Ministerstwo Sprawiedliwości	09.12.1999 r.	Rozporządzenie Ministra Sprawiedliwości w sprawie określenia rodzajów i zakresu informacji przekazywanych przez sądy, komorników sądowych i notariuszy oraz terminu i sposobu przekazywania organom podatkowym.
41.	GI-DIS-441/99	Posel Edward Daszkiewicz	15.12.1999 r.	Informacja o wszczęciu postępowania wyjaśniającego dotyczącego działalności firmy Reader's Digest Sp. z o. o.
42.	GI-DP-1400/99	Wojewoda Lubuski	16.12.1999 r.	Odpowiedź na pytanie o uprawnienia i zakres uzyskiwania informacji przez pracowników Urzędu Ochrony Państwa w świetle ustawy o ochronie danych osobowych.

Załącznik nr 5**Wykaz kontroli**

Lp.	Data kontroli	Podmiot i miejsce kontroli	Wynik kontroli	
			zawiadomienie o przestępstwie	decyzja
1.	07.01.1999 r.	Uniwersytet im. Mikołaja Kopernika w Toruniu		DEC 12/99
2.	24-25.03.1999 r.	Reader's Digest Przegląd Sp. z o.o. w Warszawie	18.05.1999 r.	DEC 38/99 DEC 44/99
3.	09.04.1999 r.	OTTO Sp. z o.o. w Łodzi		DEC 45/99
4.	15-16.04.1999 r.	WIZJA TV Sp. z o.o. w Warszawie		
5.	20.04.1999 r.	Urząd Dzielnicy Ochota Gminy Warszawa-Centrum	30.04.1999 r.	DEC 30/99
6.	20-21.04.1999 r.	IMP Sp. z o.o. w Warszawie		
7.	20-21.04. 1999 r.	PTE Nationale Nederlanden		
8.	22-23.04.1999 r.	Claritas Polska Sp. z o.o. w Warszawie		DEC 37/99 DEC 53/99
9.	27-28.04.1999 r.	Volkswagen Bank Polska S.A.		
10.	29-30.04.1999 r.	ART. FILE Sp. z o.o. w Warszawie		
11.	05.05.1999 r.	Spółdzielnia Mieszkaniowo- Budowlana Torwar w Warszawie		
12.	06.05.1999 r.	Uniwersytet im. Mikołaja Kopernika w Toruniu Wydział Humanistyczny – Instytut Socjologii		
13.	10.05.1999 r.	Urząd Gminy Czempin	29.05.1999 r.	DEC 35/99
14.	11-12.05.1999 r.	Frito Lay Poland Sp. z o.o. w Warszawie		DEC 41/99
15.	24-25.05.1999 r.	PTE AIG w Warszawie		
16.	27-28.05.1999 r.	Consumer Data Sp. z o.o. w Warszawie		DEC 50/99
17.	31.05.1999 r.- 02.06.1999 r.	Bank Zachodni S.A. we Wrocławiu		DEC 54/99
18.	08-09.06.1999 r.	ABC DIRECT CONTACT Sp. z o.o. w Warszawie		
19.	17-18.06.1999 r.	MediAdress Sp. z o.o. w Skierniewicach		
20.	17-18.06.1999 r.	CALL CENTER POLAND w Warszawie		
21.	24.06.1999 r.	JJ direct Sp. z o.o. w Otwocku		

22.	13-15.07.1999 r.	Kredyt Bank PBI S.A. – II/O w Warszawie		
23.	13-16.07.1999 r.	Kredyt Bank PBI S.A. – Centrala w Warszawie, Kredyt Bank PBI S.A. – Oddział Regionalny w Warszawie		
24.	27-30.07.1999 r.	COMMERCIAL UNION OFE BPH CU WBK S.A. w Warszawie, COMMERCIAL UNION Towarzystwo Ubezpieczeń na Życie Polska S.A. w Warszawie, COMMERCIAL UNION Financial Services Sp. z o.o. w Warszawie		DEC 70/99
25.	10-11.08.1999 r.	GENERAL MOTORS POLAND Sp. z o.o. w Warszawie		
26.	12-13.08.1999 r.	Wydawnictwo Verlag Dashofer Sp. z o.o. w Warszawie		DEC 64/99
27.	17-18.08.1999 r.	WILLEMSE OGRODY Sp. z o.o. w Krakowie		
28.	07-08.09.1999 r.	DIXI CAR S.A. w Raszynie		
29.	09-10.09.1999 r.	OFE Kredyt Bank PBI S.A. w Warszawie		
30.	14-15.09.1999 r.	LG PETRO BANK S.A. Centrala w Łodzi		
31.	16-17.09.1999 r.	Auto-Fapol Sp. z o.o. w Łodzi		
32.	16-17.09.1999 r.	Centrum Muzyczno- Rozrywkowe „Digital” Sp. z o.o. w Warszawie		DEC 68/99
33.	23-24.09.1999 r.	TU „WINTERTHUR ŻYCIE” S.A. – Oddział w Białymstoku		
34.	23-24.09.1999 r.	WIZJA TV Sp. z o.o. – Katowice		DEC 71/99
35.	30.09.1999 r.- 01.10.1999 r.	Volkswagen Bank Polska S.A. w Warszawie		
36.	06-08.10.1999 r.	PTK „CENTERTEL” Sp. z o.o. w Warszawie		
37.	06-08.10.1999 r.	Autoryzowany Przedstawiciel PTK „CENTERTEL” Sp. z o.o. – Centrum Peugeot w W-wie ul. Świętokrzyska 36		
38.	07.10.1999 r.	Autoryzowany		

		Przedstawiciel PTK „Centertel” Sp. z o.o. – Centrum Peugeot w Warszawie, Al. Krakowska 7		
39.	18.10.1999 r.	OTTO Sp. z o.o. w Łodzi	03.12.1999 r.	
40.	20-22.10.1999 r.	TU „WINTERTHUR ŻYCIE” S.A. Centrala w Warszawie		
41.	21-22.10.1999 r.	Zespół Szkół Mechanicznych im. St. Staszica w Tarnowie		DEC 69/99
42.	26-28.10.1999 r.	PTE „DOM” S.A. Oddział Regionalny w Krakowie		
43.	26-28.10.1999 r.	WILLEMSE OGRODY Sp. z o.o. w Krakowie		
44.	28-29.10.1999 r.	ZXY Sp. z o.o. w Otwocku		
45.	04-08.11. 1999 r.	EUROGLOB Sp. z o.o. w Sopocie		
46.	22-24.11.1999 r.	POLKOMTEL S.A. w Warszawie		
47.	09-10.11.1999 r.	Straż Miejska w Częstochowie		
48.	16-17.11.1999 r.	Miejski Ośrodek Pomocy Społecznej w Katowicach		
49.	25-29.11.1999 r.	Polska Telefonii Cyfrowa Sp. z o.o. w Warszawie		
50.	16.11.1999 r.	Autoryzowany Przedstawiciel „POLKOMTEL” S.A. w Warszawie, ul. Jasna 10		
51.	17.11.1999 r.	Autoryzowany Przedstawiciel „POLKOMTEL” S.A. w Warszawie, Pl. Defilad 1		
52.	23.11.1999 r.	Autoryzowany Przedstawiciel Polskiej Telefonii Cyfrowej Sp. z o.o. w Warszawie, Al. Jerozolimskie 11/19		
53.	24.11.1999 r.	Autoryzowany Przedstawiciel Polskiej Telefonii Cyfrowej Sp. z o.o. w Warszawie, ul. Puławska 15		
54.	29-30.11.1999 r.	Łódzka Regionalna Kasa Chorych		
55.	02-06.12.1999 r.	PTE „DOM” S.A. w Warszawie		
56.	07-09.12.1999 r.	PZU Życie S.A. Przedstawicielstwo we		

		Wrocławiu		
57.	13.12.1999 r.	Wydawnictwo G + J RBA Sp. z o.o. & Co. Sp. Komandytowa w Warszawie		
58.	16-17.12.1999 r.	Szpital św. Jana w Starogardzie Gdańskim		
59.	14.12.1999 r.	CITIBANK POLAND S.A. w Warszawie		
60.	20-22.12.1999 r.	PZU Życie S.A. Inspektorat w Suwałkach		
61.	15.12.1999 r.	NetLand Sp. z o.o. w Warszawie		
62.	17.12.1999 r.	ABC DIRECT CONTACT Sp. z o.o. w Warszawie		
63.	20-21.12.1999 r.	Telewizja Kablowa TVM S.A. w Warszawie		
64.	22.12.1999 r.	DCN DIRECT Sp. z o.o. w Warszawie		

Załącznik nr 6

Konferencje, seminaria, spotkania i szkolenia z udziałem Generalnego Inspektora Ochrony Danych Osobowych i pracowników Biura*

1. **Normalizacyjna Komisja Problemowa Nr 182, referat, pt. „Zabezpieczenia systemu i ochrony danych” (Cz. II).** Warszawa. **28.01.1999 r.**
2. **Urząd Miasta Łodzi, Wydział Spraw Obywatelskich, szkolenie, pt. „Ustawa o ochronie danych osobowych i rozporządzenia wykonawcze do niej”.** **02.02.1999 r.**
3. **Urząd Miasta Krakowa, wykład Generalnego Inspektora, pt. „Prawo obywateli do ochrony danych osobowych”;***
Wykłady pracowników Biura, pt. „Obowiązki administratorów danych w zakresie ochrony danych obywateli”, „Rejestracja zbiorów danych – podmioty zobowiązane do dokonania zgłoszenia, ustawowe zwolnienia, wymogi formalne zgłoszenia.” **12.04.1999 r..**
4. **Trybunał Konstytucyjny, referat Generalnego Inspektora, pt. „Ochrona danych osobowych w Polsce – pierwsze doświadczenia stosowania ustawy”.*** **13.04.1999 r.**
5. **Główny Urząd Geodezji i Kartografii, szkolenie, pt. „Przepisy o ochronie danych osobowych z uwzględnieniem zasad przetwarzania danych w ramach wykonywanych zadań Głównego Urzędu Geodezji i Kartografii”.** **06.05.1999 r.**
6. **Polskie Towarzystwo Socjologiczne, referat Generalnego Inspektora, pt. „Ochrona danych osobowych w badaniach społecznych”.*** **14.05.1999 r.**
7. **Ogólnopolska Konferencja Bezpieczeństwa Systemów Sieci Teleinformatycznych, Katowice.** **20 – 21.05.1999 r.**
8. **Związek Banków Polskich, szkolenie, pt. „Obowiązki administratora danych wynikające z ustawy o ochronie danych osobowych i rozporządzeń wykonawczych do niej”.*** **25.05.1999 r.**
9. **Kancelaria Prezydenta RP, Biuro Kadr i Odznaczeń, szkolenie, pt. „Obowiązek zgłoszenia danych do rejestracji – właściwe zabezpieczenia techniczno – organizacyjne zbiorów danych osobowych”,** **28.05.1999 r.**

„Przepisy ustawy o ochronie danych osobowych”.

10. **Polsko – niemiecka konferencja, zorganizowana przez Fundację im. F. Naumanna, referat Generalnego Inspektora, pt. „Ochrona danych o stanie zdrowia w przepisach polskiego prawa”, Wrocław*** **18 –19.06.1999 r.**
11. **Prokuratura Okręgowa w Ostrowie Wielkopolskim, szkolenie, pt. „Zasady przetwarzania danych osobowych w świetle ustawy o ochronie danych osobowych i rozporządzeń wykonawczych do niej”, „Przepisy karne ustawy o ochronie danych osobowych”.** **23.06.1999 r.**
12. **Urząd Wojewódzki w Biłgoraju, szkolenie, pt. „Rejestracja zbiorów danych osobowych. Zabezpieczenie zbiorów danych osobowych – określenie podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych. Szczegółowe omówienie zasad prawidłowego wypełniania zgłoszenia danych osobowych”, „Ustawa o ochronie danych osobowych”.** **29.06.1999 r.**
13. **Centrum Prawa Bankowego, szkolenie, pt. „Obowiązki administratora danych wynikające z ustawy o ochronie danych osobowych”.** **30.06.1999 r.**
14. **Urząd Wojewódzki w Białymstoku, szkolenie dla pracowników samorządowych, pt. „Rejestracja zbiorów danych osobowych. Zabezpieczenie zbiorów danych osobowych – określenie podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych. Szczegółowe omówienie zasad prawidłowego wypełniania zgłoszenia danych osobowych”.** **4.08.1999 r.**
15. **Urząd Wojewódzki w Białymstoku, szkolenie, pt. „Przepisy ustawy o ochronie danych osobowych”.** **05.08.1999 r.**
16. **Urząd Wojewódzki w Bydgoszczy, szkolenie, pt. „Obowiązek zgłoszenia zbiorów danych do rejestracji oraz właściwe zabezpieczenie techniczne i organizacyjne przetwarzania danych osobowych”, „Przepisy ustawy o ochronie danych osobowych”.** **17.08.1999 r.**
17. **Urząd Wojewódzki w Rzeszowie, szkolenie, pt. „Obowiązek zgłoszenia zbiorów danych do rejestracji oraz właściwe zabezpieczenie techniczne i organizacyjne przetwarzania danych osobowych”,** **27.08.1999 r.**

„Przepisy ustawy o ochronie danych osobowych”.

18. **Urząd Wojewódzki w Łodzi, szkolenie, pt.** *„Rejestracja zbiorów danych osobowych. Zabezpieczenie zbiorów danych osobowych – określenie podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Szczegółowe omówienie zasad dotyczących prawidłowego wypełniania zgłoszenia danych osobowych”*, *„Przepisy ustawy o ochronie danych osobowych”.* **30.08.1999 r.**
19. **Centrum Edukacji Helsińskiej Fundacji Praw Człowieka, wykład Generalnego Inspektora dla sędziów, pt.** *„Wybrane problemy ochrony danych osobowych”*. * **06.09.1999 r.**
20. **Urząd Wojewódzki w Gdańsku, wykład Generalnego Inspektora, pt.** *„Pozycja Generalnego Inspektora Ochrony Danych Osobowych”*. * **Wykłady pracowników Biura, pt.** *„Rejestracja zbiorów danych osobowych. Zabezpieczenie zbiorów danych osobowych – określenie podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Szczegółowe omówienie zasad dotyczących prawidłowego wypełniania Zgłoszenia danych osobowych”*. *„Omówienie zasad przetwarzania danych osobowych według ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych”*. **15.09.1999 r.**
21. **Dowództwo Wojsk Lądowych, Wydział Prawny, szkolenie, pt.** *„Przepisy ustawy o ochronie danych osobowych”*. **17.09.1999 r.**
22. **Spotkanie w Urzędzie Wojewódzkim w Opolu.* Wykłady pracowników Biura, pt.** *„Rejestracja zbiorów danych osobowych. Zabezpieczenie zbiorów danych osobowych – określenie podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Szczegółowe omówienie zasad dotyczących prawidłowego wypełniania zgłoszenia danych osobowych”*, *„Omówienie zasad przetwarzania danych osobowych według ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych”*. **20.09.1999 r.**
23. **Główny Inspektorat Inspekcji Nasionnej, szkolenie,** **23.09.1999 r.**

pt. „Przepisy Ustawy o ochronie danych osobowych”.

24. **Centrum Edukacji Helsińskiej Fundacji Praw Człowieka, wykład Generalnego Inspektora dla sędziów, pt. „Wybrane problemy ochrony danych osobowych”.*** 27.09.1999 r.
25. **Urząd Wojewódzki w Szczecinie, wykład Generalnego Inspektora, pt. „Założenia ochrony danych osobowych oraz uprawnienia Generalnego Inspektora Ochrony Danych Osobowych”.*** 29.09.1999 r.
26. **Seminarium: „Bezpieczne transakcje elektroniczne”.** 4-5.10.1999 r.
27. **Polskie Radio, szkolenie, pt. „Przepisy ustawy o ochronie danych osobowych”.** 12.10.1999 r.
28. **Urząd Wojewódzki w Warszawie, wykład Generalnego Inspektora, pt. „Założenia ustawy o ochronie danych osobowych. Doświadczenia z praktyki”.* Wykład pracownika Biura, pt. „Obowiązek zgłoszenia zbiorów danych osobowych do rejestracji oraz właściwe zabezpieczenie techniczne i organizacyjne przetwarzania danych”.** 12.10.1999 r.
29. **Biuro Rzecznika Praw Obywatelskich, wykład Generalnego Inspektora, pt. „Podstawowe zagadnienia ochrony danych osobowych. Doświadczenia z praktyki”.*** 14.10.1999 r.
30. **Ministerstwo Pracy i Polityki Socjalnej, Biuro Pełnomocnika Rządu ds. Osób Niepełnosprawnych; szkolenie.** 14.10.1999 r.
31. **Spotkanie w Radzie Adwokackiej, Warszawa.* Referat Generalnego Inspektora Ochrony Danych Osobowych, pt.: „Podstawowe zagadnienia ochrony danych osobowych”.** 09.11.1999 r.
32. **Ministerstwo Spraw Wewnętrznych i Administracji, Biuro Ochrony Informacji Niejawnych, referat Generalnego Inspektora Ochrony Danych Osobowych, pt.: „Podstawowe zagadnienia ochrony danych osobowych”.*** 16 – 17.11.1999 r.
33. **Prokuratura Apelacyjna w Gdańsku, referat Generalnego Inspektora Ochrony Danych Osobowych, pt. „Podstawowe zagadnienia ochrony danych osobowych”.** 17.11.1999 r.

34. **Biuro Rzecznika Praw Obywatelskich; szkolenie i wykłady pracowników Biura, pt. „Rejestracja zbiorów danych osobowych. Zabezpieczenie zbiorów danych osobowych – określenie podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urzędy i systemy informatyczne służące do przetwarzania danych osobowych. Szczegółowe omówienie zasad dotyczących prawidłowego wypełniania zgłoszenia danych osobowych”, „Omówienie zasad przetwarzania danych osobowych według ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych”.** **17 i 19.11.1999 r.**

35. **Prokuratura Okręgowa w Gdańsku, szkolenie, pt. „Podstawowe zagadnienia ochrony danych osobowych”.** **22 – 23.11.1999 r.**

36. **Prokuratura Okręgowa w Gdańsku Jastrzębia Góra, szkolenie, pt. „Podstawowe zagadnienia ochrony danych osobowych”.** **22 – 23.11.1999 r.**

37. **Polsko – niemiecka konferencja zorganizowana przez Generalnego Inspektora Ochrony Danych Osobowych, pt. „Wolność prasy a prawo do prywatności i ochrony danych osobowych”. Referat Generalnego Inspektora, pt. „Wolność prasy a ochrona danych osobowych”. *** **26 – 27.11.1999 r.**

38. **Wykład dr Alexandra Dix, Rzecznika Ochrony Danych Osobowych i Prawa Dostępu do Informacji w Brandenburgii, pt.: „Prawo wglądu do akt i dostępu do informacji w Brandenburgii – podstawowe założenia ustawy o ochronie danych osobowych i prawie obywateli do informacji; pierwsze doświadczenia w zakresie jej funkcjonowania”. *** **01.12.1999 r.**

39. **II Ogólnopolskie Forum Prawno – Medyczne w Warszawie, wykład Generalnego Inspektora, pt. „Ochrona danych o stanie zdrowia w świetle ustawodawstwa europejskiego i polskiej ustawy o ochronie danych osobowych”. *** **03.12.1999 r.**

40. **Spotkanie w Prokuraturze Apelacyjnej, Warszawa. Wykład generalnego Inspektora Ochrony Danych Osobowych, pt. „Podstawowe zagadnienia ochrony danych osobowych”. *** **07.12.1999 r.**

41. **Biuro Zarządu Miasta Stołecznego Warszawy, Zespół Promocji Zdrowia i Opieki Społecznej; szkolenie nt. „Wybranych zagadnień ochrony danych osobowych”.** **08.12.1999 r.**

42. **Uniwersytet Jagielloński, referat Generalnego Inspektora, pt. „Podstawowe zagadnienia ochrony danych osobowych”.*** **10.12.1999 r.**
43. **Zjazd Stowarzyszenia Absolwentów Uniwersytetu Łódzkiego, referat Generalnego Inspektora, pt. „Wybrane zagadnienia ochrony danych osobowych”.*** **17.12.1999 r.**
44. **Spotkanie w Kancelarii Sejmu, Biuro Prawno – Organizacyjne. Referat Generalnego Inspektora Ochrony Danych Osobowych, pt. „Założenia ochrony danych osobowych oraz uprawnienia Generalnego Inspektora Ochrony Danych Osobowych”.** **20.12.1999 r.**

* Oznaczono konferencje, seminaria, spotkania i szkolenia z udziałem Generalnego Inspektora Ochrony Danych Osobowych.

Załącznik nr 7

Działalność Generalnego Inspektora na forum międzynarodowym *

1. **Screening wielostronny w obszarze „Swoboda świadczenia usług”, Bruksela.** 01 – 02.02.1999 r.
2. **Screening dwustronny w obszarze „Swoboda świadczenia usług”, Bruksela. *** 11 – 13.02.1999 r.
3. **25 Meeting of International Working Group on Data Protection in Telecommunications, Norwegia. *** 26 – 29.04.1999 r.
z udziałem pracowników Biura Generalnego Inspektora Ochrony Danych Osobowych - referat dotyczący głównych problemów z zakresu ochrony danych osobowych w sektorze telekomunikacyjnym
4. **Udział Generalnego Inspektora Ochrony Danych osobowych w posiedzeniu Komisji ds. Ochrony Danych Osobowych przy Radzie Europy (CJ-PD), Strasburg.** 17 – 21.05.1999r.
5. **Udział Generalnego Inspektora Ochrony Danych Osobowych w konferencji nt. ochrony danych osobowych w sektorze Policji, zorganizowanej przez niemieckich inspektorów ochrony danych osobowych, Kilonia. *** 23 – 24.08.1999 r.
6. **Udział Generalnego Inspektora Ochrony Danych Osobowych w sympozjum, pt. „Ochrona danych – pomost między prywatnością a rynkiem globalnym oraz 26. Spotkanie Międzynarodowej Grupy Roboczej ds. Ochrony Danych w Telekomunikacji”, Berlin.** 30.08-01.09.1999 r.
(wystąpienie Dyrektora Departamentu Informatyki)
7. **Udział Generalnego Inspektora Ochrony Danych Osobowych w międzynarodowej konferencji dotyczącej ochrony danych osobowych w sektorze telekomunikacji, Berlin. *** 30.08.–02.09.1999 r.
8. **37. Posiedzenie Komisji ds. Ochrony Danych Osobowych przy Radzie Europy, Strasburg.** 12 –15.10.1999 r.
9. **Posiedzenie Podkomitetu ds. Rynku Wewnętrznego, Urząd Komitetu Integracji Europejskiej, Warszawa.** 18.11.1999 r.
10. **Regionalne Seminarium poświęcone ochronie danych osobowych w sektorze Policji, zorganizowane przez Radę Europy, Strasburg.** 13 –14.12.1999 r.

11. **Szkolenie pracowników Biura Generalnego
Inspektora w Biurze Rzecznika Ochrony Danych
Osobowych miasta Berlina oraz Rzecznika Ochrony
Danych Osobowych i Prawa Dostępu do Informacji w
Brandenburgii ***

19 – 22.12.1999 r

Załącznik nr 8

Konferencje prasowe Generalnego Inspektora Ochrony Danych Osobowych

1. W dniu 23 marca 1999 r., pt. Czy firmy prywatne i instytucje państwowe łamią ustawę o ochronie danych osobowych?
2. W dniu 13 lipca 1999 r., pt. Działalność banków a przestrzeganie ustawy o ochronie danych osobowych.
3. W dniu 22 września 1999 r., pt. „Firmy marketingowe łamią ustawę o ochronie danych osobowych”.