

Decyzja GIODO z dnia 20 września 2004 r. w sprawie dopełnienia przez Komendanta Głównego Policji, obowiązku informacyjnego wynikającego z art. 33 ustawy o ochronie danych osobowych w zakresie przetwarzania danych osobowych zawartych w zbiorach „Broń i Licencja” oraz „Ewidencja kierowców naruszających przepisy ruchu drogowego”.

Warszawa, dnia 20 września 2004 r.

GI-DEC-DS-198/04

DECYZJA

Na podstawie art. 104 § 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2000 r. Nr 98, poz. 1071 z późn. zm.) oraz art. 12 pkt 2, art. 18 ust. 1 pkt 1, art. 22 w związku z art. 23 ust. 1 pkt 2, art. 25, art. 26, art. 30 i 33 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) i w związku z art. 20 ust. 1 i 2 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2002 r. Nr 7, poz. 58 z późn. zm.) oraz z art. 20 ust. 1 pkt 2 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95 z późn. zm.) po przeprowadzeniu postępowania administracyjnego w sprawie skargi Pana A, na przetwarzanie jego danych osobowych przez Komendanta Głównego Policji,

- 1) nakazuję Komendantowi Głównemu Policji usunięcie uchybień w procesie przetwarzania danych osobowych Pana A poprzez wykonanie wobec niego obowiązku informacyjnego określonego w art. 33 ustawy o ochronie danych osobowych, w zakresie przetwarzania jego danych osobowych w zbiorze „Broń i Licencja” i „Ewidencja kierowców naruszających przepisy ruchu drogowego”,**
- 2) w pozostałym zakresie odmawiam uwzględnienia wniosku.**

Uzasadnienie

Do Generalnego Inspektora Ochrony Danych Osobowych (zwanego dalej Generalnym Inspektorem) wpłynęła skarga Pana A, zwanego dalej Skarżącym, na działanie Komendanta Głównego Policji, polegające na odmowie udostępnienia Skarżącemu dotyczących go danych osobowych. Skarżący, jako podstawę swojego działania, powołał art. 8 ust. 1 w związku z art. 12 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), zwanej dalej ustawą, w związku z art. 8 lit. d Konwencji nr 108 Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (Dz. U. z 2003 r. Nr 3, poz. 25) i art. 1 ust. 2 pkt 8 i 9, art. 5 ust. 1 i art. 20 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2002 r. Nr 7, poz. 58 z późn. zm.), zwanej dalej ustawą o Policji oraz z § 17 rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Składając skargę na Komendanta Głównego Policji Skarżący zarzucił mu: 1) odmowę udostępnienia na wniosek Skarżącego z dnia 2 grudnia 2002 r. dotyczących go danych osobowych, które przetwarza Komendant Główny Policji; 2) naruszenie art. 32 i 33 w związku z art. 3 ust. 1 i art. 1 ust. 1 i art. 25 i art. 26 ustawy, art. 51 ust. 3 Konstytucji RP oraz art. 5 lit a i art. 8 Konwencji nr 108; 3) naruszenie pkt 4 Rezolucji 45/95 Zgromadzenia Ogólnego ONZ z dnia 14 grudnia 1990 r. „Wytyczne w sprawie uregulowania kartotek skomputeryzowanych danych osobowych”, zasady 6.2 Rekomendacji R (87)15 Komitetu Ministrów Rady Europy z 17 września 1987 r. dotyczącej uregulowania wykorzystywania danych o charakterze osobistym w sektorze Policji oraz pkt 5 Rezolucji (74) 29 Komitetu Ministrów Rady Europy „Ochrona życia prywatnego osób fizycznych w kontekście elektronicznych banków danych w sektorze publicznym”; 4) błędną interpretację i wykładnię art. 20 ust. 2 ustawy o Policji.

Skarżący wniósł o nakazanie Komendantowi Głównemu Policji, w trybie art. 18 ustawy, w drodze decyzji administracyjnej przywrócenia stanu zgodnego z prawem poprzez nakazanie udzielenia pełnej odpowiedzi na wniosek Skarżącego w ciągu 30 dni i poinformowanie Skarżącego co do przetwarzanych o nim danych osobowych, oraz nakazanie przekazania Skarżącemu wszystkich danych dotyczących jego osoby, będących w posiadaniu Komendanta Głównego Policji. Jak wynika z uzasadnienia skargi:

1. Wniosek z dnia 2 grudnia 2002 r. o udzielenie informacji o przetwarzanych przez Policję danych osobowych o Skarżącym, Pan A złożył do Ministra Spraw Wewnętrznych i Administracji, wnosząc o przekazanie mu pełnego wypisu lub wydruku zawierającego wszelkie informacje, dane i zapisy dotyczące Skarżącego, a przetwarzane i gromadzone przez Policję, prowadzone w informatycznych systemach danych osobowych: 1) Podstawowy Zbiór

Informacji Policyjnych „PZIP”, 2) Podstawowy System Informacyjny Policji „POSIP”, 3) Krajowy System Informacyjny Policji „KSIP”, 4) Zintegrowany System Informacyjny Policji „ZSIP”, 5) System Analizy Kryminalnej „Alert”, 6) System Informatyczny Wspomagający Proces Wydawania Pozwoleń na Broń „BRON”, 7) System Zarządzania Bazą Danych Osobowych Krajowego Systemu Informacyjnego Policji „Oracel”, 8) Policyjny System Informacji Granicznej „POSIGRAF”. Skarżący twierdzi, iż pomimo przekazania tego wniosku do Komendanta Głównego Policji nie otrzymał informacji, jakie dane są o nim przetwarzane.

2. Następnie Skarżący wystąpił do Generalnego Inspektora ze skargą na bezczynność Komendanta Głównego Policji, a w odpowiedzi został poinformowany, iż organ ochrony danych osobowych nie posiada kompetencji do rozpatrywania skarg na bezczynność innych organów, bowiem jest to zadanie Naczelnego Sądu Administracyjnego.
3. Kolejno (na podstawie przepisu art. 34 ust. 3 ustawy o Naczelnym Sądzie Administracyjnym), Skarżący wystąpił za pośrednictwem Generalnego Inspektora, do Komendanta Głównego Policji, żądając (na podstawie art. 65 Kpa) od Generalnego Inspektora przekazanie sprawy do Komendanta Głównego Policji. Sprawa została przekazana do organu wskazanego przez Skarżącego, o czym Generalny Inspektor poinformował Skarżącego.
4. Następnie do Generalnego Inspektora wpłynęła informacja z Komendy Głównej Policji, iż pismem Dyrektora Biura Łączności i Informatyki Komendy Głównej Policji z dnia 23 listopada 2003 r., w nawiązaniu do wniosku skierowanego przez Skarżącego do Ministra Spraw Wewnętrznych i Administracji, na podstawie art. 20 ust. 2 ustawy o Policji, odmówiono Skarżącemu udzielenia informacji ze zbiorów administrowanych przez Policję, bowiem nie znaleziono podstaw do pozytywnego rozpatrzenia wniosku Skarżącego. W piśmie z dnia 30 grudnia 2003 r poinformowano Generalnego Inspektora, iż wskazano Skarżącemu komendanta wojewódzkiego Policji właściwego do miejsca zamieszkania, jako organ, od którego Skarżący może uzyskać dotyczące go informacje w przypadkach występowania o pozwolenie na broń lub w wyniku naruszenia przepisów ruchu drogowego.

W toku postępowania administracyjnego w tej sprawie Generalny Inspektor, na podstawie zebranego materiału ustalił następujący stan faktyczny:

1. Na podstawie Instrukcji - stanowiącej załącznik nr 3 do Zarządzenia nr 6 Komendanta Głównego Policji z dnia 16 maja 2002 r. w sprawie uzyskiwania, przetwarzania i wykorzystywania przez Policję informacji oraz sposobów zakładania i prowadzenia zbiorów tych informacji, które wprowadzone zostało w życie stosownie do delegacji z art. 20 ust. 19 oraz art. 7 ust. 1 pkt 2 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2002 r. Nr 7, poz. 58 i Nr 19, poz. 185) - Biuro Łączności i Informatyki KGP prowadzi Krajowy System Informacyjny

Policji (KSIP) stanowiący podstawowy zbiór informacji uzyskiwanych przez Policję w wyniku realizacji ustawowych działań. Podzbiory funkcjonujące w KSIP nie zapewniają samodzielnie pełnej funkcjonalności. Wobec zbioru KSIP, w zakresie rejestracji kryminalnych i operacyjnych zachodzą przesłanki odmowy udostępnienia danych osobowych wynikające z art. 30 pkt 2 ustawy. Dostęp do systemu KSIP w zakresie rejestracji operacyjnych regulują art. 20 ust. 1 pkt 2 w związku z art. 1 ust. 2 oraz art. 35 ust. 1 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych. Systemy teleinformatyczne, w których są przetwarzane informacje o zainteresowaniu operacyjnym oraz skierowanym do niej pytaniom, dopuszczone są do użytkowania na podstawie przepisów ustawy o ochronie informacji niejawnych. POSIGRAF jest systemem, w którym gromadzi się i przechowuje informacje zdjęciowe i tekstowe o osobach pozostających w zainteresowaniu Policji – zdjęcia te powiązane są z informacjami o osobach gromadzonymi przez system KSIP. Zbiór POSIGRAF jest modułem systemu KSIP i tworzą go informacje graficzne, zbiory zdjęć sygnalitycznych, fotografii osób poszukiwanych, rysopisy podejrzanych, prowadzone na podstawie § 14 Instrukcji o szczególnych zasadach prowadzenia zbiorów daktyloskopijnych i zdjęć sygnalitycznych oraz wzorów dokumentów w tych sprawach, stanowiącej załącznik nr 1 do Zarządzenia nr 6 Komendanta Głównego Policji.

2. ALERT jest systemem Centralnego Biura Śledczego przeznaczonym w całości do gromadzenia informacji niejawnych o charakterze tajemnicy służbowej, a dostęp do zawartych w nim informacji w całości regulują przepisy ustawy o ochronie informacji niejawnych, w tym art. 20 ust. 1 pkt 2 w związku z art. 1 ust. 2 oraz art. 35 ust. 1 tejże ustawy.
3. BRONŃ jest systemem wspomagania procesu wydawania pozwoleń na broń i licencje zintegrowanym z systemem KSIP w zakresie wprowadzania danych osobowych i rejestracji podmiotów – informacje zwarte w tym zbiorze są wprowadzane, aktualizowane i usuwane przez Komendy Wojewódzkie Policji właściwej do miejsca zamieszkania osoby ubiegającej się o pozwolenie i właściwe do udzielania informacji z tego obszaru, a więc przetwarzane na podstawie przepisów ustawy z dnia 21 maja 1999 r. o broni i amunicji (Dz. U. z 2004 r., Nr 52, poz. 525 z późn. zm.), zwanej dalej ustawą o broni.
4. Policja nie prowadzi, wskazanych przez Skarżącego, zbiorów POSIP, ZSIP i Oracel. ZSIP był funkcjonalnym poprzednikiem zbioru KSIP, wycofanym z użytkowania z końcem 2002 r. ORACLE to baza danych osobowych na podstawie której funkcjonuje system KSIP.
5. Skarżącemu odmówiono udzielenia informacji o jego danych osobowych przetwarzanych przez Policję we wskazanych zbiorach, na podstawie art. 20 ust. 2 ustawy o Policji, wywodząc z tego przepisu, że przepis prawa, który pozwala na przetwarzanie danych osobowych bez wiedzy i

zgody osób wymienionych w tym przepisie, uprawnia Policję do zachowania w tajemnicy również sam fakt przetwarzania tych danych osobowych.

6. W zbiorach administrowanych przez Policję znajdują się informacje, których ujawnienie mogłoby spowodować zagrożenie dla bezpieczeństwa i porządku publicznego. Możliwe jest jedynie udzielenie informacji ze zbioru KSIP w odniesieniu do zbiorów „Broń i Licencja” oraz „Ewidencja kierowców naruszających przepisy ruchu drogowego”, do których dane pozyskiwane są na podstawie art. 27 ust. 2 ustawy o broni i amunicji oraz art. 130 ust. 1 ustawy z dnia 20 czerwca 1997 r. Prawo o ruchu drogowym (Dz. U. z 2003 r. Nr 58, poz. 515 z późn. zm.) zwanej dalej Prawem o ruchu drogowym. Przekazano kopię pism (z dnia 13 listopada 2003 r. i z dnia 24 grudnia 2003 r.) skierowanych do Skarżącego przez Dyrektora Łączności i Informatyki Komendy Głównej Policji oraz poinformowano, iż ustalono w Komendzie Głównej Policji, iż Skarżący nie wnioskował pisemnie do właściwych miejscowo organów Policji o udostępnienie informacji o przetwarzaniu jego danych osobowych w systemach „Broń i Licencja” i „Ewidencja kierowców naruszających przepisy ruchu drogowego”.

Po przeanalizowaniu powyższego, Generalny Inspektor Ochrony Danych Osobowych zważył, co następuje:

Ochrona danych osobowych zagwarantowana jest co do zasady w art. 51 Konstytucji RP, jednakże zakres konstytucyjnego unormowania nie rozciąga się na wszelkie przejawy przetwarzania danych osobowych. Stosownie bowiem do ust. 1 i ust. 3 powołanego przepisu Konstytucji RP, nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby (ust. 1) i każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych; ograniczenie tego prawa może określić ustawa (ust. 3), jednakże zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa (ust. 5). Aktem wskazanym w art. 51 ust. 5 Konstytucji RP jest ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 101, poz. 926 z późn. zm.), zwana dalej ustawą, natomiast stosownie do zasad ochrony danych osobowych, wynikających z przepisów ustawy, na administratorze danych osobowych spoczywa szereg obowiązków.

Jednym z podstawowych obowiązków administratora danych jest wykazanie co najmniej jednej z materialnych przesłanek przetwarzania danych osobowych, określonych w art. 23 ust. 1 pkt 1-5 ustawy. Równoprawność przesłanek legalizujących proces przetwarzania danych osobowych odnosi się do wszelkich form przetwarzania danych osobowych, zdefiniowanych w art. 7 pkt 2 ustawy, a zwłaszcza ich zbierania, utrwalania, przechowywania, opracowywania, zmieniania,

udostępniania i usuwania. Zgodnie z obowiązującym od dnia 1 maja 2004 r. brzmieniem art. 23 ust. 1 pkt 2 i 4 ustawy, przetwarzanie danych jest dopuszczalne m.in. wtedy, gdy: osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych (pkt 1), jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa (pkt 1), jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego (pkt 4). Każda z przesłanek przetwarzania danych osobowych ustanowionych w art. 23 ust. 1 ustawy, ma charakter autonomiczny i niezależny, a zatem przesłanki te co do zasady są równoprawne, dlatego też spełnienie co najmniej jednej z nich stanowi o zgodnym z prawem przetwarzaniu danych osobowych. Jednocześnie, zgodnie z wykładnią ww. przepisu ustawy, zgoda osoby, której dane dotyczą jest jednym z możliwych, ale nie jedynym warunkiem legalizującym proces przetwarzania danych osobowych.

Ponadto, w myśl art. 25 ust. 1 ustawy, w przypadku zbierania danych osobowych nie od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, 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 dostępu do treści swoich danych oraz ich poprawiania, 5) uprawnieniach wynikających z art. 32 ust. 1 pkt 7 i 8. Istotne dla rozstrzygnięcia w tej sprawie jest wskazanie, iż od ww. obowiązku informacyjnego przewidziane są wyjątki, które ustanowione zostały w ust. 2 powołanego przepisu ustawy, a w szczególności, zgodnie z art. 25 ust. 2 pkt 1 ustawy przepisu ust. 1 nie stosuje się, jeżeli przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą.

Kolejnym obowiązkiem administratora danych - wynikającym z art. 26 ustawy - jest dołożenie szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności administrator obowiązany jest zapewnić, aby dane te były przetwarzane zgodnie z prawem, zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, merytorycznie poprawne i adekwatne w stosunku do celów w jakich są przetwarzane, przechowywane w postaci umożliwiającej identyfikację osób których dane dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

Jednocześnie, zgodnie z art. 1 ust. 1 ustawy, każdy ma prawo do ochrony dotyczących go danych osobowych, natomiast przepisy art. 32 ustawy, gwarantują osobom, których dane dotyczą prawo do kontroli przetwarzanych danych osobowych, które ich dotyczą, zawartych w zbiorach danych osobowych oraz precyzuje, w jaki sposób w szczególności prawo kontrolne może być realizowane.

Stosownie do art. 34 ustawy, w sprawach informowania i udostępniania danych osobie, której dane dotyczą, stosuje się przepisy art. 30. Zgodnie natomiast z art. 30 ustawy, administrator danych osobowych odmawia udostępnienia danych osobowych ze zbioru danych podmiotom i osobom innym niż wymienione w art. 29 ust. 1 ustawy, jeżeli spowodowałoby to: 1) ujawnienie wiadomości stanowiących tajemnicę państwową, 2) zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego. Jednocześnie stwierdzić należy, iż w związku z brzmieniem przepisu art. 30 ustawy osoby, których dane dotyczą - ze względu na wyżej wskazany szczególny charakter analizowanego przepisu - powinny liczyć się z tym, iż administrator posiada prawo odmowy udostępnienia danych osobowych, o ile obowiązany jest chronić inne ważne interesy. Ponadto brak jest wątpliwości, iż odmowa udostępnienia osobie, jej danych osobowych, powinna mieć charakter wyjątkowy.

Stwierdzając powyższe wskazać równocześnie należy, iż w myśl art. 33 ustawy, na wniosek osoby, której dane dotyczą, administrator danych osobowych jest zobowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić odnośnie jej danych osobowych, informacji, o których mowa w art. 32 ust. 1 pkt 1-5a, a w szczególności podać w formie zrozumiałej 1) jakie dane osobowe zawiera zbiór, 2) w jaki sposób dane zebrano, 3) w jakim celu i zakresie dane są przetwarzane, 4) w jakim zakresie oraz komu dane zostały udostępnione. Zgodnie z ust. 2 art. 33 ustawy, na wniosek osoby, której dane dotyczą, informacji, o których mowa w ust. 1, udziela się na piśmie.

Obowiązek informacyjny, wynikający z art. 33 ustawy, jest zasadniczym przedmiotem wniosku Skarżącego. Jednocześnie, niezwykle istotne w analizowanej sprawie jest podkreślenie, iż art. 30 ustawy wprowadza wyjątek od generalnej zasady swobody udostępniania danych osobowych. Tym samym, co do zasady istnieje prawo, wynikające z art. 33 ustawy, gwarantujące każdemu możliwość pozyskania informacji przetwarzanych o osobie, której dane dotyczą, jednakże jak wyżej wskazano, cytując przepisy art. 30 pkt 1 i 2 ustawy, przepisy ustawy przewidują także sytuacje, gdy obowiązek informacyjny z art. 33 nie może zostać spełniony.

Istnienie w ustawie przepisu sformułowanego w jej art. 30 jest konsekwencją wyjątku, jaki ustanawia art. 51 ust. 3 Konstytucji RP, zgodnie z którym, każdy ma prawo dostępu do dotyczących do urzędowych dokumentów i zbiorów danych osobowych, a ograniczenie tego prawa może określić ustawa. Omawiany wyjątek znajduje źródło także w art. 9 Konwencji nr 108 Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (Dz. U. z 2003 r. Nr 3, poz. 25), zwanej dalej także Konwencją Nr 108, który to akt został powołany przez Skarżącego, która jest regulacją o randze międzynarodowej, poświęconą ochronie danych osobowych. Art. 5 Konwencji nr 108 ustanawia zasady jakości danych osobowych,

jej art. 6 – szczególne kategorie danych osobowych, a art. 8 powołanego aktu - gwarancje dodatkowe dla podmiotu danych osobowych, tymczasem art. 9 Konwencji Nr 108 wprowadza wyjątki i ograniczenia. Dlatego też konieczne jest wskazanie, iż wprowadzanie danych osobowych będących przedmiotem automatycznego przetwarzania powinny być pozyskiwane oraz przetwarzane rzetelnie i zgodnie z prawem (zgodnie ze wskazanym przez Skarżącego art. 5 lit. a Konwencji nr 108) oraz każda osoba powinna mieć zapewnione prawo do ustalenia, czy istnieje zautomatyzowany zbiór danych osobowych, zawierający dane jej dotyczące, poznania podstawowych celów jego utworzenia, a także tożsamości, miejsca zamieszkania lub siedziby administratora tego zbioru (zgodnie ze wskazanym przez Skarżącego art. 8 lit. a Konwencji nr 108) - jednakże art. 9 ust. 1 Konwencji nr 108 stanowi, iż wyjątki od przepisów art. 5, 6 i 8 niniejszej Konwencji dopuszczalne są jedynie w granicach określonych w niniejszym artykule. Odstąpienie od stosowania art. 5, 6 i 8 niniejszej Konwencji jest dozwolone, jak stanowi art. 9 ust. 2 lit. b Konwencji nr 108, jeśli przewidywane jest ustawowo przez Stronę, jako środek konieczny w społeczeństwie demokratycznym w interesie ochrony Państwa, bezpieczeństwa publicznego, interesów walutowych państwa lub zwalczania przestępczości.

I. Rozważając kwestię, czy na Komendancie Głównym Policji spoczywa obowiązek informacyjny z art. 33 ustawy - w odniesieniu do prowadzonych przez niego zbiorów „Broń i Licencja” oraz „Ewidencja kierowców naruszających przepisy ruchu drogowego” - stwierdzić należy, iż Komendant Główny Policji obowiązany był uczynić zadość wnioskowi Skarżącego w tym zakresie. Brak bowiem podstaw do stwierdzenia, iż dostęp do tych zbiorów jest obwarowany wyjątkami ustanowionymi w art. 30 ustawy, w tym w szczególności, aby dostęp Skarżącego do jego danych osobowych w tym zakresie miał spowodować zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego (art. 30 pkt 2 ustawy). Na podstawie art. 27 ust. 2 ustawy o broni, Komendant Główny Policji, z zastrzeżeniem ust. 3, prowadzi rejestr zawierający dane osobowe osób posiadających pozwolenie na broń, dopuszczonych do posiadania broni, posiadających legitymację osoby dopuszczonej do posiadania broni, ubiegających się o pozwolenie na broń lub dopuszczenie do posiadania broni, posiadających kartę rejestracyjną broni; urzędowe informacje i opinie o tych osobach i podmiotach sporządzone w związku ze sprawami pozwoleń na broń. Natomiast na podstawie art. 130 ust. 1 Prawa o ruchu drogowym, Policja prowadzi ewidencję kierowców naruszających przepisy ruchu drogowego. Określonymu naruszeniu przypisuje się odpowiednią liczbę punktów w skali od 0 do 10 i wpisuje się do tej ewidencji. Jednocześnie, zgodnie z § 3 ust. 1 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 20 grudnia 2002 r. w sprawie postępowania z kierowcami

naruszającymi przepisy ruchu drogowego (Dz. U. z 2002 r. Nr 236, poz.1998 z późn. zm.), ewidencję prowadzi komendant wojewódzki Policji właściwy ze względu na miejsce zamieszkania ewidencjonowanych. Ponadto, na podstawie § 9 powołanego rozporządzenia, osoba zainteresowana ma prawo uzyskać od Policji ustną informację lub zaświadczenie o wpisach ostatecznych lub tymczasowych dotyczących punktów odpowiadających dokonany przez siebie naruszeniom. Informacji udziela się lub zaświadczenie wydaje się w siedzibie organu prowadzącego ewidencję lub, w miarę możliwości technicznych, w innej jednostce Policji. Jednocześnie, z ustaleń dokonanych w toku postępowania nie wynika, aby Komenda Główna Policji udostępniła Skarżącemu jego dane osobowe w analizowanym w tym miejscu zakresie, ponadto, nie ulega wątpliwości, iż Komendant Główny Policji, jako administrator, a tym samym Policja powinna spełnić omawiany obowiązek.

Zgodnie natomiast z art. 18 ust. 1 pkt 1-6 ustawy, w przypadku naruszenia przepisów o ochronie danych osobowych Generalny Inspektor z urzędu lub na wniosek osoby zainteresowanej, w drodze decyzji administracyjnej, nakazuje przywrócenie stanu zgodnego z prawem, a w szczególności: usunięcie uchybień; uzupełnienie, uaktualnienie, sprostowanie, udostępnienie lub nieudostępnienie danych osobowych; zastosowanie dodatkowych środków zabezpieczających zgromadzone dane osobowe; wstrzymanie przekazywania danych osobowych do państwa trzeciego; zabezpieczenie danych lub przekazanie ich innym podmiotom; usunięcie danych osobowych. Wskazany przepis wyraźnie stanowi, iż wydanie nakazu może być dokonane przez Generalnego Inspektora jedynie w przypadku stwierdzenia przez organ naruszenia przepisów o ochronie danych osobowych. Dlatego też, konieczne jest wydanie nakazu wyrażonego w pkt 1 sentencji niniejszej decyzji rozpatrując wniosek Skarżącego w tym zakresie.

II. W odniesieniu do pozostałych zbiorów przetwarzanych przez Policję w ramach Krajowego Systemu Informacyjnego Policji, w odniesieniu do zbiorów KSIP w zakresie rejestracji kryminalnych i operacyjnych oraz do ALERT i POSIGRAF będących przedmiotem niniejszego postępowania, stwierdzić należy – po analizie sprawy – iż zachodzi konieczność zastosowania wyjątku od zasady udostępnienia danych osobowych ustanowionego w art. 30 pkt 2 ustawy. Powyższe wynika z przepisów prawa obowiązujących w brzmieniu, które przedstawione zostanie w dalszej części uzasadnienia niniejszej decyzji, z których wynika konieczność uniemożliwienia Skarżącemu skorzystania z prawa wynikającego z art. 33 ustawy. Uznać bowiem należy, iż udostępnienie danych w zakresie wnioskowanym przez Skarżącego spowodowałoby naruszenie art. 30 pkt 2 ustawy, poprzez spowodowanie zagrożenia dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego.

Stwierdzić należy, iż bez wątpienia Policja jest szczególnym organem w każdym, w tym także w polskim systemie prawnym, a w myśl art. 5 ust. 1 ustawy o Policji, centralnym organem administracji rządowej, właściwym w sprawach ochrony bezpieczeństwa ludzi oraz utrzymania bezpieczeństwa i porządku publicznego, jest Komendant Główny Policji. Policja jest formacją służącą społeczeństwu i przeznaczona do ochrony bezpieczeństwa ludzi oraz do utrzymywania bezpieczeństwa i porządku publicznego (art. 1 ust. 1 ustawy o Policji). Do podstawowych zadań Policji należą m.in. ochrona życia i zdrowia ludzi oraz mienia przed bezprawnymi zamachami naruszającymi te dobra, ochrona bezpieczeństwa i porządku publicznego, wykrywanie przestępstw i wykroczeń, gromadzenie, przetwarzanie i przekazywanie informacji kryminalnych, a także prowadzenie Krajowego Systemu Informatycznego (art. 1 ust. 2 pkt 1, 2, 4, 8 i 9 ustawy o Policji). Zgodnie z art. 7 ust. 1 pkt 2 ustawy o Policji, Komendant Główny Policji określa metody i formy wykonywania zadań przez poszczególne służby policyjne, w zakresie nieobjętym innymi przepisami wydanymi na podstawie ustawy.

W dziedzinie przetwarzania różnego rodzaju informacji, w tym danych osobowych, znamieną jest funkcja Policji, bowiem zbiera ona – w celu wykonania zadań nałożonych na nią nie tylko przepisami ustawy o Policji i przepisów wykonawczych, ale także na podstawie innych ustaw w tym ustawy o ochronie informacji niejawnych – takie informacje, które podlegają szczególnemu reżimowi i ochronie. Wyrazem tych zasad jest w szczególności art. 20 ust. 1 i ust. 2 ustawy o Policji, na podstawie którego Policja, z zachowaniem ograniczeń wynikających z art. 19, może uzyskiwać informacje, w tym także niejawnie, gromadzić je, sprawdzać oraz przetwarzać (ust. 1). Policja może pobierać, przetwarzać i wykorzystywać w celach wykrywczych i identyfikacyjnych informacje, w tym dane osobowe o osobach podejrzanych o popełnienie przestępstw ściganych z oskarżenia publicznego, nieletnich dopuszczających się czynów zabronionych przez ustawę jako przestępstwa ścigane z oskarżenia publicznego, osobach o nieustalonej tożsamości lub usiłujących ukryć swą tożsamość oraz o osobach poszukiwanych, także bez ich wiedzy i zgody, a w szczególności: dane osobowe, o których mowa w art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883, z 2000 r. Nr 12, poz. 136, Nr 50, poz. 580 i Nr 116, poz. 1216 oraz z 2001 r. Nr 42, poz. 474, Nr 49, poz. 509 i Nr 100, poz. 1087), z tym że dane dotyczące kodu genetycznego, wyłącznie o niekodujących regionach genomu; odciski linii papilarnych; zdjęcia i opisy wizerunku; cechy i znaki szczególne, pseudonimy; informacje o miejscu zamieszkania lub pobytu, wykształceniu, zawodzie, miejscu i stanowisku pracy, dokumentach tożsamości, którymi się posługują, sposobie działania sprawcy, jego środowisku i kontaktach, sposobie zachowania się sprawców wobec osób pokrzywdzonych (ust. 2).

Ponadto, w wykonaniu delegacji ustawowej z art. 20 ust. 19 ustawy o Policji, obowiązuje Zarządzenie Nr 6 Komendanta Głównego Policji z dnia 16 maja 2002 r. w sprawie uzyskiwania, przetwarzania i wykorzystywania przez Policję informacji oraz sposobów zakładania i prowadzenia zbiorów tych informacji (zwane dalej Zarządzeniem). W celu realizacji ustawowych zadań Policja, wykonując czynności operacyjno-rozpoznawcze, dochodzeniowo-śledcze i administracyjno-porządkowe uzyskuje, gromadzi, sprawdza oraz przetwarza i wykorzystuje informacje (§ 1 ust. 1 Zarządzenia); pobiera, przetwarza i wykorzystuje w celach wykrywczych i identyfikacyjnych informacje, w tym dane osobowe, o: osobach podejrzanych o popełnienie przestępstw ściganych z oskarżenia publicznego, nieletnich dopuszczających się czynów zabronionych przez ustawę jako przestępstwa ścigane z oskarżenia publicznego, osobach o nieustalonej tożsamości lub usiłujących ukryć swą tożsamość, osobach poszukiwanych, także bez ich wiedzy i zgody w zakresie nie objętym innymi przepisami (§ 2 pkt 1-4 Zarządzenia); uzyskuje, pobiera, przetwarza i wykorzystuje informacje z zachowaniem przepisów o ochronie informacji niejawnych oraz przepisów o ochronie danych osobowych (§ 3 ust. 2 i § 4 ust. 1 Zarządzenia); w ramach wykonywania czynności dochodzeniowo-śledczych może pobierać informacje w sposób i na warunkach określonych w zarządzeniu (§ 4 Zarządzenia).

Stosownie do § 16 pkt 3 Zarządzenia, wprowadzona została do stosowania w Policji Instrukcja o szczegółowych zasadach prowadzenia zbiorów informacji o zdarzeniach, osobach, podmiotach, miejscach i przedmiotach, uzyskanych przez Policję podczas realizacji zadań oraz wzory dokumentów w tych sprawach (stanowiąca załącznik nr 3 do Zarządzenia), która określa szczegółowe zasady i tryb rejestrowania, przetwarzania i wykorzystywania przez Policję informacji o zdarzeniach, osobach, podmiotach, miejscach i przedmiotach uzyskanych podczas wykonywania czynności służbowych. W celu gromadzenia i przetwarzania informacji, Biuro Łączności i Informatyki KGP prowadzi krajowy system informacyjny Policji, zwany dalej „KSIP”, składający się z zapisów elektronicznych, sporządzonych oddzielnie dla każdej informacji; do czasu pełnej informatyzacji dopuszcza się prowadzenie zbiorów tematycznych w formie kartotek (§ 1 ust. 2 i § 2 ust. 1 Instrukcji). Informacje zgromadzone w KSIP przetwarzane są z zachowaniem przepisów o ochronie danych osobowych oraz o ochronie informacji niejawnych; klauzulę POUFNE przyznaje się rejestracji informacji o zainteresowaniu operacyjnym, informacji o miejscu będącym w zainteresowaniu Policji, zapytania odnoszącego się do informacji określonych w pkt 1, 2 i 3 (§ 4 ust. 1 i ust. 2 Instrukcji). Systemy teleinformatyczne, w których przetwarzane są informacje, o których mowa w ust. 2, dopuszczone są do użytkowania na podstawie ustawy o ochronie informacji niejawnych i stosownych decyzji Komendanta Głównego Policji (§ 4 ust. 5 Instrukcji). Na podstawie § 14 ust. 1 Instrukcji o szczególnych zasadach prowadzenia zbiorów daktyloskopijnych i

zdjęć sygnalitycznych oraz wzorów dokumentów w tych sprawach, stanowiącej załącznik nr 1 do Zarządzenia nr 6 Komendanta Głównego Policji, wykonuje się zdjęcia sygnalityczne osobie podejrzanej o popełnienie przestępstwa ściganego z oskarżenia publicznego; nieletniemu, który dopuścił się czynu zabronionego przez ustawę jako przestępstwo ścigane z oskarżenia publicznego; osobie, której tożsamości nie można ustalić lub usiłującej ukryć swoją tożsamość.

W związku z charakterem wykonywanych działań Policja pozyskuje i przetwarza informacje także na podstawie przepisów ustawy o ochronie informacji niejawnych, która stosownie do jej art. 1 ust. 1, określa zasady ochrony informacji, które wymagają ochrony przed nieuprawnionym ujawnieniem, jako stanowiące tajemnicę państwową lub służbową, niezależnie od formy i sposobu ich wyrażania, także w trakcie ich opracowania, zwanych dalej „informacjami niejawnymi”, a w szczególności: udostępniania informacji niejawnych; postępowania sprawdzającego, w celu ustalenia, czy osoba nim objęta daje rękojmię zachowania tajemnicy. Przepisy ustawy mają zastosowanie do organów kontroli państwowej i ochrony prawa, przepisy ustawy nie naruszają przepisów innych ustaw o ochronie tajemnicy zawodowej lub innych tajemnic prawnie chronionych (art. 1 ust. 2 pkt 1 lit f i ust. 3 ustawy o ochronie informacji niejawnych). W rozumieniu ustawy tajemnicą państwową - jest informacja niejawna określona w wykazie rodzajów informacji niejawnych, stanowiącym załącznik nr 1, której nieuprawnione ujawnienie może spowodować istotne zagrożenie dla podstawowych interesów Rzeczypospolitej Polskiej, a w szczególności dla niepodległości lub nienaruszalności terytorium, interesów obronności, bezpieczeństwa państwa i obywateli, albo narazić te interesy na co najmniej znaczną szkodę; tajemnicą służbową - jest informacja niejawna nie będąca tajemnicą państwową, uzyskana w związku z czynnościami służbowymi albo wykonywaniem prac zleconych, której nieuprawnione ujawnienie mogłoby narazić na szkodę interes państwa, interes publiczny lub prawnie chroniony interes obywateli albo jednostki organizacyjnej (art. 2 pkt 1 i 2 ustawy o ochronie informacji niejawnych). Ponadto, stosownie do art. 3 cytowanej ustawy, informacje niejawne mogą być udostępnione wyłącznie osobie dającej rękojmię zachowania tajemnicy i tylko w zakresie niezbędnym do wykonywania przez nią pracy lub pełnienia służby na zajmowanym stanowisku albo innej zleconej pracy.

Ustawa o ochronie informacji niejawnych, wskazuje m.in., jakie dane objęte są ochroną oraz precyzuje, czy i na jakich warunkach można je udostępniać, bowiem informacje te pełnią znamioną rolę w ochronie zasad, na straży których stoi m.in. Policja. Dostęp do informacji niejawnych reguluje art. 20 ust. 1 pkt 1-3 ustawy o ochronie informacji niejawnych, zgodnie z którym informacje niejawne, którym przyznano określoną klauzulę tajności, z zastrzeżeniem ust. 2, są chronione zgodnie z przepisami ustawy, które dotyczą informacji niejawnych oznaczonych daną

klauzulą tajności. Oznacza to w szczególności, że informacje takie mogą być udostępnione wyłącznie osobie uprawnionej do dostępu do informacji niejawnych o określonej klauzuli tajności; muszą być wytwarzane, przetwarzane, przekazywane lub przechowywane w warunkach uniemożliwiających ich nieuprawnione ujawnienie, zgodnie z przepisami określającymi wymagania dotyczące kancelarii tajnych, obiegu i środków fizycznej ochrony informacji niejawnych, odpowiednich dla przyznanej im klauzuli tajności; muszą być chronione, odpowiednio do przyznanej klauzuli tajności, przy zastosowaniu środków określonych w rozdziale 9. Postępowanie sprawdzające ma na celu ustalenie, czy osoba sprawdzana daje rękojmię zachowania tajemnicy (art. 35 ust. 1 ustawy o ochronie informacji niejawnych). Natomiast udostępnianie informacji niejawnych zgodnie z art. 49 ust. 1 cytowanej ustawy, w szczególnie uzasadnionych przypadkach, z zastrzeżeniem przepisu art. 4 ust. 1, udostępnienie informacji niejawnych stanowiących tajemnicę państwową określonej osobie lub instytucji może nastąpić na podstawie pisemnej zgody odpowiednio Szefów Kancelarii: Prezydenta Rzeczypospolitej Polskiej, Sejmu, Senatu lub Prezesa Rady Ministrów albo ministra właściwego dla określonego działu administracji rządowej, Prezesa Narodowego Banku Polskiego lub kierownika urzędu centralnego, a w przypadku ich braku - na podstawie pisemnej zgody właściwej służby ochrony państwa. Zgodę na udostępnienie informacji niejawnych stanowiących tajemnicę służbową może wyrazić na piśmie kierownik jednostki organizacyjnej, wyłącznie w odniesieniu do informacji wytworzonych w tej jednostce; wyrażenie zgody na udostępnienie informacji niejawnych nie oznacza zmiany lub zniesienia jej klauzuli tajności oraz musi określać zakres podmiotowy i przedmiotowy udostępnienia (ust. 2 i 3 powołanego przepisu art. 49 ustawy o ochronie informacji niejawnych).

Stan faktyczny niniejszej sprawy wskazuje, że Policja przetwarza dane na podstawie przepisów ustawy o Policji, ustawy o ochronie informacji niejawnych, a więc do każdego zbioru dostęp jest ściśle limitowany, a w konsekwencji, na skutek ustawowych ograniczeń, nie każde dane osobowe mogą być udostępnione. Zacytowane wyżej przepisy, w tym art. 20 ustawy o Policji, stanowią podstawę dla przetwarzania szeroko rozumianych, określonych w tych przepisach informacji kryminalnych w tym m.in. danych osobowych osób przez Policję, która – co jest niezwykle istotne dla rozpatrzenia niniejszej sprawy - może uzyskiwać wskazane szczegółowo informacje, także w sposób niejawnny oraz przetwarzać je prowadząc Krajowy System Informatyczny Policji (KSIP) stanowiący podstawowy zbiór informacji uzyskiwanych przez Policję w wyniku realizacji ustawowych działań. Dostęp do systemu KSIP w zakresie rejestracji operacyjnych i kryminalnych oraz do systemu ALERT i POSIGRAF regulują art. 20 ust. 1 pkt 2 w związku z art. 1 ust. 2 oraz art. 35 ust. 1 ustawy o ochronie informacji niejawnych, bowiem jak ustalono, systemy teleinformatyczne, w których są przetwarzane informacje o zainteresowaniu

operacyjnym dopuszczone są do użytkowania na podstawie przepisów ustawy o ochronie informacji niejawnych. Wobec zbioru KSIP, w zakresie rejestracji kryminalnych i operacyjnych zachodzą, jak ustalono, przesłanki odmowy udostępnienia danych osobowych wynikające z art. 30 pkt 2 ustawy. Oznacza to, iż udostępnienie tych informacji, w tym danych osobowych powodowałoby zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego. Stwierdzić jednocześnie należy, iż brak jest podstaw do uznania, iż Skarżący jest uprawniony do dostępu do informacji niejawnych stosownie do postanowień art. 20 ust. 1 ustawy o ochronie informacji niejawnych, a także, iż spełnione zostały w niniejszej sprawie przesłanki udostępniania informacji niejawnych z art. 49 ust. 1 tejże ustawy.

Ponadto – ustosunkowując się do zarzutu Skarżącego, iż nie został spełniony wobec niego obowiązek informacyjny z art. 25 ustawy – stwierdzić należy, iż wprowadzie w myśl art. 25 ust. 1 ustawy, istnieje obowiązek informacyjny, w przypadku zbierania danych osobowych nie od osoby, której dane dotyczą, jednakże stosownie do art. 25 ust. 2 ustawy przepisu ust. 1 nie stosuje się jeżeli przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą. W niniejszej sprawie wyłączenie obowiązku informacyjnego następuje na podstawie art. 20 ust. 2 ustawy o Policji, w myśl którego Policja może pobierać, przetwarzać i wykorzystywać w celach wykrywczych i identyfikacyjnych informacje, w tym dane osobowe o osobach podejrzanych o popełnienie przestępstw ściganych z oskarżenia publicznego, nieletnich dopuszczających się czynów zabronionych przez ustawę jako przestępstwa ścigane z oskarżenia publicznego, osobach o nieustalonej tożsamości lub usiłujących ukryć swą tożsamość oraz o osobach poszukiwanych, także bez ich wiedzy i zgody.

Mając zatem na względzie zasady określone w art. 9 Konwencji nr 108 oraz w wyżej cytowanych przepisach prawa, które stały się wytycznymi dla Zarządzenia, stwierdzić należy, iż nie dają one podstaw, a wręcz ograniczają dostęp Skarżącego do tych zbiorów. Udostępnienie, czy to informacji o charakterze pozytywnym (tj. poprzez wskazanie, iż dane osobowe figurują w rejestrze) lub też tych, które mogłyby mieć cechę informacji negatywnych (tj. wskazanie o braku informacji o przetwarzaniu danych osobowych), mogłyby mieć wpływ na zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego.

Jednocześnie, jak ustalono, że Policja nie prowadzi, wskazanych przez Skarżącego, zbiorów: POSIP; ZSIP, który był funkcjonalnym poprzednikiem zbioru KSIP, wycofanym z użytkowania z końcem 2002 r.; natomiast ORACLE to baza danych osobowych na podstawie której funkcjonuje system KSIP.

Z tych względów nie można przychylić się do stanowiska Skarżącego i zarzucić Komendantowi Głównemu Policji błędu w przedmiocie odmowy udostępnienia na wniosek

Skarżącego tych danych, które przetwarza Komendant Główny Policji na zasadach przewidzianych w powołanych przepisach ustawy o Policji i Zarządzenia regulującego uzyskiwanie, przetwarzanie i wykorzystywanie przez Policję informacji oraz sposobów zakładania i prowadzenia zbiorów tych informacji, a także ustawy o ochronie informacji niejawnych.

Jednocześnie uznać należy, iż wyżej przytoczone zasady obowiązują – w wykonaniu ww. przepisów art. 51 ust. 3 Konstytucji RP i art. 9 Konwencji nr 108 - m.in. dlatego, iż konieczne jest ograniczenie osobom, których dane dotyczą, dostępu do dotyczących ich danych osobowych i informacji, które mogłyby zostać przez te osoby wykorzystane w sposób nieodpowiedni, niezgodny z prawem, co z kolei narażałoby administratora na zarzut niedostatecznej, sprzecznej z zasadami wynikającymi z przepisów prawa, ochrony danych osobowych, zgromadzonych na podstawie przepisów ustawy o Policji dla potrzeb ochrony ważnych interesów, wynikających z przepisów określających kompetencje Policji.

W kontekście powyższego trudno jest uznać, aby każdy – czyje dane gromadzi Policja na podstawie wyżej szeroko przytoczonych zasad wynikających z przepisów prawa - miał być informowany, stosownie do postanowień art. 25 ust. 1 ustawy, iż zbierane są o nim dane, a także aby dane tak gromadzone miały być udostępniane osobie, której dotyczą, w trybie art. 33 ustawy. Ograniczenie praw jednostkowych, a więc także praw Skarżącego i złożonych przez niego żądań, determinują wyżej przytoczone przepisy, w tym w szczególności art. 9 Konwencji, art. 51 ust. 3 Konstytucji RP, art. 25 ust. 2 pkt 1 oraz art. 30 pkt 2 ustawy o ochronie danych osobowych.

Brak zatem podstaw do stwierdzenia w niniejszej sprawie naruszenia przez Komendanta Głównego Policji art. 32 i 33 w związku z art. 3 ust. 1 i art. 1 ust. 1 i art. 25 i art. 26 ustawy oraz postawienia mu zarzutu dokonania błędnej interpretacji i wykładni art. 20 ust. 2 ustawy o Policji w odniesieniu do zbiorów KSIP w zakresie rejestracji kryminalnych i operacyjnych oraz do ALERT i POSIGRAF. Jednocześnie, bezprzedmiotowe jest rozważanie wniosku Skarżącego w odniesieniu do wskazanych przez niego „zbiorów” POSIP i ZSIP, które nie istnieją oraz w stosunku do Oracel, bowiem ORACLE to jedynie baza danych na podstawie której funkcjonuje system KSIP.

Ponadto, mając na względzie art. 9 Konwencji nr 108, brak jest podstaw do stwierdzenia, aby przepisy te pozostawały w sprzeczności z art. 5 lit a i art. 8 Konwencji i aby wskazane przez Skarżącego przepisy Konwencji naruszył Komendant Główny Policji.

Nie może zostać także uwzględniony postawiony przez Skarżącego zarzut naruszenia przez Komendanta Głównego Policji pkt 4 Rezolucji 45/95 Zgromadzenia Ogólnego ONZ z dnia 14 grudnia 1990 r. „Wytyczne w sprawie uregulowania kartotek skomputeryzowanych danych osobowych”, zasady 6.2 Rekomendacji R (87)15 Komitetu Ministrów Rady Europy z 17 września 1987 r. dotyczącej uregulowania wykorzystywania danych o charakterze osobistym w sektorze

Policji oraz pkt 5 Rezolucji (74) 29 Komitetu Ministrów Rady Europy „Ochrona życia prywatnego osób fizycznych w kontekście elektronicznych banków danych w sektorze publicznym”, ze względu na to, iż wskazane rezolucje i rekomendacje nie posiadają charakteru wiążącego, a stanowią jedynie zalecenia odnośnie gwarancji, jakie powinny być zapewnione przez ustawodawcę w przepisach krajowych. Zatem wskazane przez Skarżącego akty prawne nie stanowią źródeł prawa w rozumieniu art. 87 Konstytucji RP, zgodnie z którym, źródłami powszechnie obowiązującego prawa Rzeczypospolitej Polskiej są: Konstytucja, ustawy, ratyfikowane umowy międzynarodowe oraz rozporządzenia. Tym samym nie ma podstaw prawnych do czynienia Komendantowi Głównemu Policji zarzutu ich naruszenia.

W tym stanie faktycznym i prawnym Generalny Inspektor Ochrony Danych Osobowych rozstrzygnął, jak we wstępie.

Decyzja niniejsza jest ostateczna. Stronie, na podstawie art. 21 ust. 1 ustawy o ochronie danych osobowych, w związku z art. 22 tej ustawy i w związku z art. 127 § 3 i art. 129 § 2 Kodeksu postępowania administracyjnego, przysługuje, w terminie 14 dni od daty doręczenia niniejszej decyzji, prawo złożenia do Generalnego Inspektora Ochrony Danych Osobowych wniosku o ponowne rozpatrzenie sprawy (adres: Biuro Generalnego Inspektora Ochrony Danych Osobowych, ul. Stawki 2, 00 – 193 Warszawa).