GIODO

Generalny Inspektor
Ochrony Danych Osobowych

ABC
ochrony danych osobowych

WYDAWNICTWO SEJMOWE
Warszawa 2007

BIURO GENERALNEGO INSPEKTORA
OCHRONY DANYCH OSOBOWYCH

ul. Stawki 2, 00-193 Warszawa
www.giodo.gov.pl
kancelaria@giodo.gov.pl
tel. (0 22) 860 70 81
fax (0 22) 860 70 86

Redaktor Anna Kowalik

ISBN 978-83-7059-808-2

KANCELARIA SEJMU

Wydawnictwo Sejmowe
Wydanie pierwsze
Warszawa, styczeń 2007

SPIS TREŚCI

WPROWADZENIE

Postęp gospodarczy, rozwój nowych technologii – zwłaszcza informatycznych – spotęgowały zagrożenie tej sfery prywatności człowieka, jaką stanowią jego dane osobowe. Poszerzenie zakresu danych gromadzonych o obywatelach przez różne instytucje, publiczne i prywatne, spowodowało, iż sprawowanie przez jednostkę kontroli nad obiegiem i treścią dotyczących jej informacji stało się utrudnione. Dostrzeżono więc konieczność objęcia tej sfery prywatności ochroną państwa.

Pierwszym aktem prawnym o zasięgu międzynarodowym, kompleksowo regulującym zagadnienia ochrony danych osobowych jest Konwencja nr 108 Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych. Takim aktem na poziomie europejskim jest dyrektywa Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. (95/46/EC) w sprawie ochrony osób w związku z przetwarzaniem danych osobowych oraz swobodnego przepływu tych danych. Zasady w nich wyrażone przeniosła do polskiego porządku prawnego ustawa o ochronie danych osobowych. Jej uchwalenie w 1997 r. było przejawem postępującej demokratyzacji życia publicznego w Polsce i troski o ochronę prywatności każdego obywatela. Ustawa o ochronie danych osobowych skonkretyzowała konstytucyjnie zagwarantowane każdemu prawo do decydowania o tym, komu, w jakim zakresie i w jakim celu przekazywane są jego dane osobowe. Wyposażyła osoby, których dane są wykorzystywane, w środki służące realizacji tego prawa, jak również powołała organ – Generalnego Inspektora Ochrony Danych Osobowych – który stoi na straży przysługującego każdemu prawa do ochrony danych osobowych.

I. PRZEPISY O OCHRONIE DANYCH OSOBOWYCH

Zasady przetwarzania danych osobowych oraz prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych, określa ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz.U. z 2002 r. nr 101, poz. 926, z późn. zm.; dalej jako: ustawa) oraz wydane na jej podstawie akty wykonawcze – rozporządzenia Ministra Spraw Wewnętrznych i Administracji.

1. Rozporządzenie z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. nr 100, poz. 1024) – wydane na podstawie art. 39a ustawy – określa:
   - sposób prowadzenia i zakres dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych – odpowiednią do zagrożeń oraz kategorii danych objętych ochroną;
   - podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;
   - wymagania w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzania danych osobowych.
2. Rozporządzenie z dnia 29 kwietnia 2004 r. w sprawie wzoru zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz.U. nr 100, poz. 1025) – wydane na podstawie art. 46a ustawy – określa wzór zgłoszenia, który jest załącznikiem do tego rozporządzenia.
3. Rozporządzenie z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz.U. nr 94, poz. 923) – wydane na podstawie art. 22a ustawy – określa wzory, o których mówi to rozporządzenie.

Na system ochrony danych osobowych składają się też wszystkie inne przepisy szczególne, które regulują kwestie wykorzystywania danych osobowych. Podmioty publiczne, w myśl zasady praworządności, wyrażonej w art. 7 Konstytucji Rzeczypospolitej Polskiej, działają wyłącznie na podstawie i w granicach prawa. Oznacza to, że mogą one przetwarzać dane osobowe jedynie wtedy, gdy służy to wypełnieniu określonych prawem zadań, obowiązków i upoważnień.

II. POJĘCIA UŻYTE W USTAWIE O OCHRONIE DANYCH OSOBOWYCH

1. Administrator danych

Ustawa posługuje się pojęciem „administrator danych". Jest ono zdefiniowane w art. 7 pkt 4 ustawy. Administratorem jest organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych. Między innymi może to być organ państwowy, organ samorządu terytorialnego lub państwowa albo komunalna jednostka organizacyjna.

Z praktyki stosowania ustawy wynika, że niektóre podmioty mają problem z właściwym wskazaniem administratora danych, tymczasem w przypadku podmiotów publicznych jego rozwiązanie nierzadko znajduje się w przepisach prawa stanowiących podstawę utworzenia zbioru. Zazwyczaj znajduje się tam wskazanie, kto jest odpowiedzialny za utworzenie i prowadzenie zbioru danych osobowych, oraz określone są podstawowe zasady prowadzenia zbioru.

Tytułem przykładu można wskazać przepisy ustawy z dnia 13 czerwca 2003 r. o cudzoziemcach (Dz.U. nr 128, poz. 1175). Zgodnie z art. 125 ust. 1 pkt 5, w zw. z art. 124 pkt 1 lit. h) tej ustawy, rejestr osób, którym udzielono zezwolenia na wjazd i pobyt na terytorium Rzeczypospolitej Polskiej, prowadzi, na podstawie art. 144 ust. 1 tej ustawy, Prezes Urzędu ds. Repatriacji i Cudzoziemców.

2. Zbiór danych

Zgodnie z definicją sformułowaną w art. 7 pkt 1 ustawy o ochronie danych osobowych, zbiorem danych jest taki zestaw danych o charakterze osobowym, w którym dane dostępne są według określonych kryteriów, „niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie".

Wszelkie materiały gromadzone w formie akt, w tym sądowe, prokuratorskie, policyjne i inne zawierające dane osobowe, są zbiorami danych osobowych. Typowym zbiorem danych jest zestaw informacji o pracownikach, zgromadzonych w związku z ich zatrudnieniem i świadczeniem przez nich pracy, wykorzystywany przez różne komórki organizacyjne pracodawcy, zarówno w systemach informatycznych, jak i w formie papierowej.

Ustawa chroni dane osobowe, jeśli są one uporządkowane w zestawach, aktach, księgach, skorowidzach, rejestrach i innych zbiorach ewidencyjnych. Ustawę stosuje się również do danych osobowych przetwarzanych w systemach informatycznych, nawet jeśli są to pojedyncze dane (art. 2 ust. 2 ustawy).

3. Dane osobowe

Definicja danych osobowych znajduje się w art. 6 ustawy. Danymi osobowymi są wszelkie informacje dotyczące konkretnej osoby, za pomocą których bez większego wysiłku można tę osobę zidentyfikować, chociaż nie jest ona wyraźnie wskazana. Możliwą do zidentyfikowania jest taka osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności poprzez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

Do danych osobowych zalicza się więc nie tylko imię, nazwisko i adres osoby, ale również przypisane jej numery, dane o cechach fizjologicznych, umysłowych, ekonomicznych, kulturowych i społecznych.

Danymi osobowymi nie będą zatem pojedyncze informacje o dużym stopniu ogólności, np. sama nazwa ulicy i numer domu, w którym mieszka wiele osób, czy wysokość wynagrodzenia. Informacja ta będzie jednak stanowić dane osobowe wówczas, gdy zostanie zestawiona z innymi, dodatkowymi informacjami, np. imieniem i nazwiskiem czy numerem PESEL, które w konsekwencji można odnieść do konkretnej osoby.

Przykładem pojedynczej informacji stanowiącej dane osobowe jest numer PESEL

Numer ten, zgodnie z art. 31a ust. 1 ustawy z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych (tekst jedn. Dz.U. z 2006 r. nr 139, poz. 993, z późn. zm.), jest 11-cyfrowym, stałym symbolem numerycznym, jednoznacznie identyfikującym osobę fizyczną, w którym sześć pierwszych cyfr oznacza datę urodzenia (rok, miesiąc, dzień), kolejne cztery – liczbę porządkową i płeć osoby, a ostatnia jest cyfrą kontrolną, służącą do komputerowej kontroli poprawności nadanego numeru ewidencyjnego. Numer ten, występując nawet bez zestawienia z innymi informacjami o osobie, stanowi dane osobowe, a ich przetwarzanie podlega wszelkim rygorom przewidzianym w ustawie o ochronie danych osobowych.

Adres poczty elektronicznej

Adres poczty elektronicznej – bez dodatkowych informacji, umożliwiających ustalenie tożsamości osoby – zasadniczo nie stanowi danych osobowych. Występujący samodzielnie adres poczty elektronicznej można w wyjątkowych przypadkach uznać za dane osobowe, ale tylko wtedy, gdy elementy jego treści pozwalają, bez nadmiernych kosztów, czasu lub działań – na ustalenie na ich podstawie tożsamości danej osoby. Dzieje się tak w sytuacji, gdy elementami treści adresu są np. imię i nazwisko jego właściciela.

Dane szczególnie chronione

Dane szczególnie chronione wyliczone są w art. 27 ust. 1 ustawy. Są to informacje o pochodzeniu rasowym lub etnicznym, poglądach politycznych, religijnych, filozoficznych, wyznaniu, przynależności do partii lub związku, stanie zdrowia, kodzie genetycznym, nałogach,

życiu seksualnym, skazaniach, orzeczeniach o ukaraniu, mandatach i innych orzeczeniach wydanych w postępowaniu przed sądem lub urzędem. Na administratorów tych danych ustawa nakłada bardziej rygorystyczne obowiązki niż na administratorów danych „zwykłych".

Dane „zwykłe"

Nie jest to pojęcie zdefiniowane w ustawie o ochronie danych osobowych, ale tak nazywane są dane osobowe poza wymienionymi w art. 27 ust. 1 ustawy. Zaliczamy do nich np. imię, nazwisko, adres zamieszkania, datę urodzenia, nr PESEL.

Danymi osobowymi nie są informacje o osobach zmarłych

Firmy, urzędy i instytucje publiczne, odmawiając udzielenia informacji o osobach zmarłych, powołują się na ustawę o ochronie danych osobowych. Ustawa o ochronie danych osobowych nie może jednak stanowić podstawy takiej odmowy, ponieważ nie dotyczy ona osób zmarłych.

Przepisów ustawy o ochronie danych osobowych nie stosuje się do informacji o przedsiębiorcach

Zakresem przedmiotowym ustawy o ochronie danych osobowych objęte są wyłącznie dane dotyczące osób fizycznych. Jej przepisów nie stosuje się natomiast do przetwarzania informacji o innych podmiotach, w szczególności o osobach prawnych, jednostkach organizacyjnych nieposiadających osobowości prawnej oraz podmiotach prowadzących działalność gospodarczą na podstawie przepisów ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz.U. nr 173, poz. 1807, z późn. zm.) – w takim zakresie, w jakim dane te identyfikują podmiot w obrocie gospodarczym i ściśle wiążą się z prowadzoną przez niego działalnością gospodarczą.

4. Przetwarzanie danych

Przetwarzaniem danych osobowych jest wykonywanie na nich jakichkolwiek operacji. Przetwarzaniem jest zatem już samo przechowywanie danych, nawet jeśli podmiot faktycznie z nich nie korzysta. W po-

jęciu przetwarzania mieści się także ich udostępnianie, zmienianie, modyfikowanie, przekazywanie, zbieranie, utrwalanie, opracowywanie.

Ustawa definiuje jedynie pojęcie „przetwarzania", brak jest natomiast definicji poszczególnych form przetwarzania, takich jak: udostępnianie, przekazywanie. Należy je zatem rozumieć zgodnie z ich słownikowym znaczeniem.

Ustawa definiuje wszakże jedną z operacji przetwarzania, a mianowicie – operację usuwania danych.

5. Usuwanie danych

Zgodnie z art. 7 pkt 3 ustawy usuwanie danych polega na ich niszczeniu lub modyfikacji. Aby można było mówić o usunięciu danych osobowych, należy dokonać tej czynności w sposób niepozwalający na odtworzenie ich treści, czyli tak, aby po dokonaniu usunięcia danych niemożliwe było zidentyfikowanie osób, których dotyczą.

Istnieje przy tym dowolność w wyborze środków służących usuwaniu danych. Można zatem, w celu usunięcia danych, skorzystać z niszczarki lub zanonimizować dokument, czyli usunąć z niego dane osobowe, np. zaczerniając je, tak aby nie było możliwe ich odtworzenie.

Warto zwrócić uwagę na zjawisko błędów popełnianych przez pracowników w procesie niszczenia zbędnych dokumentów zawierających dane osobowe. Częstym procederem jest wyrzucanie dokumentów na śmietnik, bez uprzedniego sprawdzenia ich treści. Stanowi to naruszenie norm o zabezpieczeniu danych osobowych, ponieważ umożliwia zapoznanie się z treścią danych osobom nieuprawnionym.

6. Zgoda

W myśl art. 7 pkt 5 ustawy o ochronie danych osobowych, przez zgodę osoby, której dane dotyczą, rozumie się oświadczenie woli, którego treścią jest zgoda składającego oświadczenie na przetwarzanie jego danych osobowych. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

Z definicji tej nie wynikają szczegółowe zasady formułowania klauzul zgody, jednakże podkreśla się, że z treści klauzul zgody na przetwarzanie danych osobowych powinno w sposób niebudzący wątpliwości wynikać, w jakim celu, w jakim zakresie i przez kogo dane osobowe będą przetwarzane. Wyrażający zgodę musi mieć pełną świadomość tego, na co się godzi.

W przypadku zgody na wykorzystywanie danych osobowych podlegających szczególnej ochronie – zgoda musi być wyrażona na piśmie.

7. Powierzenie

Instytucja powierzenia przetwarzania danych, o której mówi art. 31 ustawy, ma bardzo istotne znaczenie praktyczne. Zezwala ona administratorowi danych na skorzystanie z usług wyspecjalizowanych podmiotów zewnętrznych. Oznacza to, że administrator danych osobowych nie musi osobiście wykonywać wszystkich czynności związanych z procesem przetwarzania danych osobowych. Może powierzyć ich przetwarzanie – w całości lub w części.

Ustawa wymaga, aby umowa powierzenia zawarta była na piśmie oraz wyraźnie określała zakres i cel przetwarzania danych. Zawierając takie umowy, należy pamiętać o tym, że administrator nie może przekazać zleceniobiorcy więcej praw, niż sam posiada. Podmiot przetwarzający dane na podstawie umowy powierzenia zawartej z administratorem danych, w rozumieniu przepisów ustawy nie staje się ich administratorem.

Z faktem, że podmiot, któremu powierzono dane, nie staje się ich administratorem, związane są określone skutki. Nie spoczywają na nim obowiązki, którymi ustawodawca obciążył administratora danych, m.in. obowiązek rejestracji. Jest on jednak zobowiązany do podjęcia środków, o których mowa w art. 36–39 ustawy, zabezpieczających przetwarzane dane, oraz do spełnienia wymagań określonych w rozporządzeniu w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Zastosowanie tych środków musi nastąpić przed

przystąpieniem do przetwarzania danych, tj. np. przed ich uzyskaniem. W zakresie przestrzegania wymienionych przepisów ustawy i rozporządzenia podmiot przetwarzający dane ponosi odpowiedzialność jak administrator danych. Ponadto podmiot, któremu dane powierzono, jest odpowiedzialny wobec administratora w zakresie działań niezgodnych z umową zawartą z administratorem danych.

Generalny Inspektor Ochrony Danych Osobowych jest uprawniony do kontroli zgodności przetwarzania danych przez podmiot, któremu przetwarzanie powierzono – z przepisami o ochronie danych osobowych. Kontrola ta prowadzona jest na zasadach określonych w art. 14–19 ustawy o ochronie danych osobowych (art. 31 ust. 5 wymienionej ustawy).

8. System informatyczny

Pojęcie systemu informatycznego określone zostało w art. 7 pkt 2a ustawy o ochronie danych osobowych. Zgodnie z brzmieniem tego artykułu systemem informatycznym jest „zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych".

9. Administrator bezpieczeństwa informacji

Wyznaczenie administratora bezpieczeństwa informacji jest jednym z obowiązków administratora danych, wynikającym z art. 36 ust. 3 ustawy, służącym właściwemu zabezpieczeniu danych.

Administrator bezpieczeństwa informacji nadzoruje przestrzeganie zasad ochrony danych, określonych przez administratora, stosując odpowiednie do zagrożeń i kategorii danych objętych ochroną środki techniczne i organizacyjne, które mają zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Administrator danych sam może pełnić funkcję administratora bezpieczeństwa informacji.

III. PODSTAWOWE OBOWIĄZKI ADMINISTRATORA DANYCH

1. Spełnienie przesłanek uprawniających do przetwarzania danych osobowych

A. Przetwarzanie danych „zwykłych"

Każde przetwarzanie zwykłych danych osobowych, czyli dokonywanie na nich jakichkolwiek operacji, np. ich przechowywanie, wykorzystywanie, udostępnianie, zmienianie, należy uzasadnić spełnieniem jednego z warunków określonych w art. 23 ust. 1 ustawy o ochronie danych osobowych. Należy podkreślić, że wymienione w art. 23 ust. 1 ustawy warunki są rozłączne. Oznacza to, że aby wykorzystywanie danych można było uznać za działanie legalne, wystarczające jest spełnienie jednego z nich, a nie wszystkich łącznie. Jeśli zatem wykorzystywanie danych służy realizacji uprawnienia lub obowiązku określonego w przepisach prawa, to nie jest potrzebne dodatkowo żądanie zgody osoby na wykorzystywanie danych, ani uzasadnianie, że przetwarzanie danych służy dobru publicznemu lub niezbędnym celom administratora danych. W szczególności: żądanie zgody wówczas, gdy wykorzystywanie danych służy realizacji normy prawnej, wprowadza w błąd. Sugeruje bowiem możliwość wyboru, podczas gdy przekazanie danych jest obowiązkiem, bez którego cel pozyskania danych nie mógłby zostać zrealizowany.

Przetwarzanie danych osobowych jest możliwe, jeśli:

1) *Osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych.*

   Jeśli zgoda jest wymagana, to należy pamiętać w szczególności o jej definicji – określonej w art. 7 pkt 5 ustawy – i jasnym formułowaniu treści ewentualnych klauzul zgody na przetwarzanie danych, a także na wyodrębnianie tych klauzul z treści innych oświadczeń woli składanych przez osobę, której dane dotyczą.

Ponadto z przepisu tego nie wynika, aby zgoda na wykorzystywanie danych osobowych musiała mieć formę pisemną. Zaleca się ją jednak ze względów dowodowych oraz ze względu na wymagania przepisów szczególnych, np. Kodeksu postępowania administracyjnego. Pisemna zgoda jest natomiast wymagana w przypadku danych szczególnie chronionych.

2) *Jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.*

Warunek ten najczęściej uzasadnia wykorzystywanie danych przez podmioty publiczne. Działają one w ramach określonych przepisami prawa i podejmują czynności w celu wykonania nałożonych na nie zadań i realizacji kompetencji. Przetwarzanie przez nie danych osobowych będzie zawsze uzasadnione, jeśli będzie służyło wykonaniu prawnie określonych uprawnień i obowiązków.

Pojawia się tu zatem zagadnienie mnogości norm odnoszących się do przetwarzania danych. Okazuje się bowiem, że kwestie dopuszczalności wykorzystywania danych regulują przepisy określające kompetencje poszczególnych instytucji i podmiotów. Te szczególne wobec ustawy o ochronie danych osobowych przepisy dają odpowiedź na pytania, w jaki sposób, w jakich okolicznościach i przy zachowaniu jakich procedur podmioty publiczne mogą z danych osobowych korzystać. Np. zasady prowadzenia ewidencji ludności, udostępniania danych z ewidencji oraz właściwe w tym zakresie organy określa ustawa z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych (tekst jedn. Dz.U. z 2006 r. nr 139, poz. 993). Do określonych tam przepisów i procedur będą odwoływały się zarówno podmioty, którym ustawa ta przyznaje w związku z prowadzeniem ewidencji ludności określone uprawnienia, jak i osoby oraz podmioty zwracające się o udostępnienie danych z ewidencji.

3) *Jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą.*

4) *Jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego.*

5) *Jest to niezbędne dla wypełniania prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą. Przy czym, zgodnie z art. 23 ust. 4 ustawy o ochronie danych osobowych, tym prawnie usprawiedliwionym celem jest w szczególności marketing własnych produktów lub usług administratora danych bądź dochodzenie roszczeń z prowadzonej przez niego działalności gospodarczej.*

B. Przetwarzanie danych szczególnie chronionych

Wykorzystywanie danych podlegających szczególnej ochronie, co do zasady, jest zabronione z mocy art. 27 ust. 1 ustawy. Z danych tych może jednak korzystać ten administrator, który wykaże, że znajduje się w jednej z wyjątkowych sytuacji, opisanych w art. 27 ust. 2 ustawy.

Przetwarzanie takich danych jest dopuszczalne, jeśli wyrazi na to pisemną zgodę osoba, której one dotyczą (art. 27 ust. 2 pkt 1) lub zezwala na to przepis szczególny innej ustawy, dający pełne gwarancje ochrony tych danych (art. 27 ust. 2 pkt 2). Przetwarzanie danych szczególnie chronionych dopuszcza się również, jeśli następuje ono w celu ochrony żywotnych interesów osoby, której dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, fizycznie lub prawnie nie jest w stanie wyrazić zgody, do czasu ustanowienia opiekuna prawnego albo kuratora (art. 27 ust. 2 pkt 3); gdy jest to niezbędne do wykonania statutowych zadań kościołów i innych związków wyznaniowych, stowarzyszeń, fundacji lub innych niezarobkowych organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, pod warunkiem że przetwarzanie danych dotyczy wyłącznie członków tych organizacji lub instytucji albo osób utrzymujących z nimi stałe kontakty w związku z ich działalnością i że zapewnione są pełne gwarancje ochrony przetwarzanych danych (art. 27 ust. 2 pkt 4); gdy dotyczy danych, które są niezbędne do dochodzenia praw przed sądem (art. 27 ust. 2 pkt 5); gdy przetwarzanie jest niezbędne do wykonania zadań administratora związanych z zatrudnieniem pracowników i innych osób, a zakres danych jest określony w ustawie (art. 27 ust. 2 pkt 6); gdy jest prowadzone w celu ochrony stanu zdro-

wia, 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); gdy dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą (art. 27 ust. 2 pkt 8); gdy jest to niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego, przy czym publikowanie wyników badań naukowych nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone (art. 27 ust. 2 pkt 9); wtedy gdy przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym (art. 27 ust. 2 pkt 10).

2. Spełnienie obowiązku informacyjnego, o którym mowa w art. 24 oraz art. 25 ustawy o ochronie danych osobowych

Należy rozróżnić dwie sytuacje, w których administrator musi spełnić obowiązek informacyjny. Obowiązek ten należy spełnić zarówno w momencie gromadzenia danych, jak i na każdym dalszym etapie ich przetwarzania.

Art. 24 i art. 25 ustawy odnoszą się do pierwszej sytuacji, gdy informacji udziela się w momencie pozyskiwania danych. Wówczas poinformowanie osoby, której dane dotyczą, o zasadach ich wykorzystania jest obowiązkiem administratora, niezależnie od tego, czy osoba z wnioskiem o taką informację występuje, czy też nie. Na każdym dalszym etapie przetwarzania danych – informacji udziela się wtedy, gdy osoba o to występuje.

Obowiązek informacyjny na etapie pozyskania danych kształtuje się w zależności od źródła, z którego dane pochodzą. Dane mogą być bowiem pozyskane od osoby, której dotyczą, jak też od osoby trzeciej.

Jeśli dane zbierane są od osoby, której dotyczą, administrator danych musi spełnić obowiązek informacyjny określony w art. 24 ust. 1 ustawy o ochronie danych osobowych, a więc poinformować tę osobę o:

1) adresie swojej siedziby i pełnej nazwie administratora,
2) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych (należy w tym miejscu przypomnieć, że odbiorcą danych nie jest podmiot, który działa na podstawie umowy powierzenia),
3) prawie do dostępu do treści swoich danych oraz do ich poprawiania,
4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

Obowiązek poinformowania wynikający z art. 24 ust. 1 powinien być wykonany w momencie zbierania danych. Jest on jednak wyłączony (art. 24 ust. 2), gdy:

- przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania,
- osoba, której dane dotyczą, posiada już informacje, których udzielenia wymaga art. 24 ust. 1 ustawy.

Jeżeli osoba przychodzi do urzędu, np. w sprawie wydania dowodu osobistego, wydania decyzji o warunkach zabudowy, przyznania dodatku mieszkaniowego, to urzędnik może uznać, że posiada ona informacje, o których mowa w art. 24 ust. 1 ustawy, jeśli wie, że osoba ta ma świadomość, kto jest administratorem danych, orientuje się co do celu ich zbierania, wie o tym, czy podanie danych jest dobrowolne, czy też obowiązkowe. Osoba ta może bowiem pozostawać w kontakcie z urzędem, np. być w nim już wcześniej w tej samej sprawie. Wtedy, gdy dochodzi do ponownego zbierania danych (przez tego samego administratora, do tych samych celów), można powołać się na spełniony już wcześniej obowiązek poinformowania.

Jeśli dane zbierane są nie od osoby, której dotyczą, administrator danych musi spełnić obowiązek informacyjny określony w art. 25 ust. 1 ustawy, a więc poinformować osobę, ktrej dane dotyczą, o:

1) adresie swojej siedziby i pełnej nazwie administratora,
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 ustawy o ochronie danych osobowych.

Obowiązek poinformowania powinien zostać spełniony bezpośrednio po utrwaleniu zebranych danych, a więc po zapisaniu danych w sposób umożliwiający ich dalsze przetwarzanie.

Zwolnienia z tego obowiązku wymienia art. 25 ust. 2 ustawy, zgodnie z którym informacji udzielać nie trzeba, jeśli:

- przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą,
- dane są niezbędne do badań naukowych, dydaktycznych, historycznych, statystycznych lub badania opinii publicznej, ich przetwarzanie nie narusza praw lub wolności osoby, której dane dotyczą, a spełnienie wymagań określonych w art. 25 ust. 1 wymagałoby nadmiernych nakładów lub zagrażałoby realizacji celu badania,
- dane są przetwarzane przez podmiot publiczny lub wykonujący zadania publiczne na podstawie przepisów prawa,
- osoba, której dane dotyczą, posiada informacje, które miałyby zostać udzielone.

3. Dołożenie szczególnej staranności w celu ochrony interesów osób, których dane dotyczą (art. 26 ust. 1 ustawy)

W ramach realizacji tego obowiązku administrator przetwarzający dane jest zobowiązany w szczególności zapewnić, aby dane osobowe:

a) wykorzystywane były zgodnie z prawem;
b) były zbierane dla jasno określonych, zgodnych z prawem celów i nie były wykorzystywane do innych celów niż te, dla których zostały zebrane (zasada celowości).

   Dane mogą być wykorzystane przez administratora w innym celu niż ten, dla którego zostały zgromadzone, jeśli nie narusza to praw i wolności osoby, której dane dotyczą, i służy celom naukowym, dydaktycznym, historycznym lub statystycznym. Cel

przetwarzania można zmienić również wówczas, gdy administrator spełni jeden z warunków wymienionych w art. 23 ustawy oraz wypełni obowiązek informacyjny określony w art. 25 ustawy;

c) były aktualne, a ich treść zgodna ze stanem faktycznym (zasada merytorycznej poprawności danych);
d) były adekwatne do celu ich wykorzystania – zakres danych nie może wykraczać poza niezbędny do zrealizowania celu, jakiemu przetwarzanie danych ma służyć (zasada adekwatności);
e) nie były wykorzystywane dłużej, niż wymaga tego realizacja celu, dla którego zostały zgromadzone. Jeśli zatem cel, do realizacji którego dane osobowe pozyskano, został osiągnięty, to należy dane usunąć.

4. Zastosowanie środków technicznych i organizacyjnych zapewniających ochronę danych osobowych

Administrator jest zobowiązany do:

a) zastosowania środków technicznych i organizacyjnych odpowiednich do zagrożeń oraz kategorii danych objętych ochroną;
b) zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem niezgodnie z ustawą oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
c) prowadzenia dokumentacji opisującej sposób przetwarzania danych oraz podjęte środki organizacyjne i techniczne – na dokumentację składa się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym;
d) wyznaczenia administratora bezpieczeństwa informacji, tj. osoby odpowiedzialnej za nadzór nad procesem przetwarzania – zaleca się, aby posiadała ona wiedzę w zakresie ochrony danych osobowych, niezbędną w celu efektywnego wypełniania tej funkcji;
e) nadania upoważnień osobom mającym dostęp do danych osobowych.

Obowiązek upoważnienia osób wynika z art. 37 ustawy. Biorąc pod uwagę cele dowodowe oraz konieczność sporządzenia ewidencji upoważnień, upoważnienie powinno mieć formę pisemną i zawierać nazwę (nazwisko), imię i nazwisko osoby upoważniającej do przetwarzania danych osobowych, datę nadania i ustania upoważnienia. Należy również określić zakres danych, do których osoba ma dostęp, oraz nazwę zbioru.

W ewidencji osób upoważnionych muszą się znaleźć następujące informacje: imię i nazwisko osoby upoważnionej, data nadania, ustania oraz zakres upoważnienia do przetwarzania danych, a także identyfikator, jeśli dane przetwarzane są w systemie informatycznym. Osoby upoważnione do dostępu do danych osobowych muszą zachować je w tajemnicy;

f) zapewnienia kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane. Sposób sprawowania takiej kontroli określa administrator danych, uwzględniając przede wszystkim podjęte środki organizacyjne i techniczne.

Szczegółowe warunki zabezpieczenia danych osobowych określone są w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Opisuje ono także środki bezpieczeństwa, jakie należy zastosować w celu ochrony danych. Dobór tych środków uzależniony jest od przyjętego dla danego zbioru – poziomu bezpieczeństwa danych w systemie informatycznym.

5. Zgłoszenie zbioru do rejestracji

Na administratorze danych spoczywa wynikający z art. 40 ustawy obowiązek zgłoszenia zbioru danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych. Wyjątki od tej zasady wyliczone zostały w art. 43 ust. 1 ustawy. Każdy administrator przed zgłoszeniem zbioru powinien sprawdzić, czy prowadzony

przez niego zbiór nie podlega, w myśl tych przepisów, zwolnieniu z obowiązku zgłoszenia do rejestracji. Zwolnienie z tego obowiązku nie oznacza zwolnienia z pozostałych obowiązków wynikających z przepisów o ochronie danych osobowych.

Sposób dokonywania zgłoszenia

Zgłoszenia zbioru danych dokonuje się przez złożenie wypełnionego formularza, którego wzór opublikowany został w rozporządzeniu wykonawczym do ustawy. Formularz jest dostępny na stronie internetowej <www.giodo.gov.pl>.

Zgłoszeniu podlega również każda zmiana informacji wcześniej zgłoszonych. Jeśli zatem zmieniają się warunki i zasady prowadzenia zbioru, to taką zmianę należy zgłosić Generalnemu Inspektorowi Ochrony Danych Osobowych.

Jeśli strona działa przez pełnomocnika, do formularza zgłoszenia należy załączyć prawidłowo udzielone pełnomocnictwo. Do przedstawienia innych dokumentów, które mogą mieć znaczenie w sprawie (odpis z KRS, polityka bezpieczeństwa, instrukcja zarządzania systemem informatycznym), strona może zostać wezwana w toku postępowania administracyjnego, prowadzonego w celu rejestracji zbioru przez GIODO.

Zgłoszenie zbioru danych do rejestracji może być dokonane poprzez przesłanie formularza zgłoszenia za pośrednictwem poczty, osobiście, jak również przy wykorzystaniu elektronicznej platformy komunikacji z Generalnym Inspektorem: e-giodo, dostępnej ze strony internetowej <www.giodo.gov.pl>.

System e-giodo umożliwia zgłaszanie do rejestracji zbiorów danych i ich aktualizację poprzez internet. Formularz zgłoszenia zbioru danych jest wówczas wypełniany przy użyciu zainstalowanego na stronie internetowej <www.giodo.gov.pl> programu, który – poprzez system podpowiedzi i komunikatów o popełnionych błędach – minimalizuje możliwość niewłaściwego wypełnienia zgłoszenia przez wnioskodawcę. Po wypełnieniu formularza istnieje możliwość wysłania zgłoszenia drogą elektroniczną. Dotyczy to jednak tylko podmiotów dysponujących podpisem elektronicznym. Tak wypełniony formularz można również wydrukować i przesłać drogą tradycyjną.

Zaświadczenie o zarejestrowaniu zbioru

Administrator danych „zwykłych" podlegających rejestracji może rozpocząć ich przetwarzanie od momentu zgłoszenia zbioru Generalnemu Inspektorowi. Zaświadczenie o zarejestrowaniu zbioru jest wówczas wydawane na wniosek administratora danych.

Gromadzenie danych podlegających szczególnej ochronie administrator może rozpocząć dopiero po zarejestrowaniu zbioru. W tym przypadku zaświadczenie wydawane jest obligatoryjnie, przez Generalnego Inspektora Ochrony Danych Osobowych, niezwłocznie po dokonaniu rejestracji zbioru danych.

Przykłady zwolnienia z obowiązku zgłoszenia danych do rejestracji:

— rejestracja danych pracowników i kandydatów do pracy

Zwolnienie z obowiązku rejestracji, na podstawie art. 43 ust. 1 pkt 4 ustawy, dotyczy zbiorów danych osobowych przetwarzanych w związku z zatrudnieniem u administratora danych (tj. zbiorów aktualnych i byłych pracowników, a także kandydatów do pracy) oraz świadczeniem mu usług na podstawie umów cywilnoprawnych (np. na podstawie umowy zlecenia, umowy o dzieło). Takich zbiorów nie należy zgłaszać do rejestracji.

— rejestracja zbiorów wykorzystywanych do celów utrzymywania bieżących kontaktów

Podstawą zwolnienia z obowiązku zgłoszenia zbioru do rejestracji może być powszechna dostępność zawartych w nim danych (art. 43 ust. 1 pkt 9 ustawy) lub ich przetwarzanie w zakresie drobnych bieżących spraw życia codziennego (art. 43 ust. 1 pkt 11).

Przetwarzanie danych w celu utrzymywania kontaktu z osobą reprezentującą określony podmiot oraz w zakresie niezbędnym do realizacji tego celu służy usprawnieniu działalności administratora danych. Zatem dane zawarte w tego typu zbiorze traktować można jako przetwarzane w zakresie drobnych bieżących spraw życia codziennego.

IV. PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ

1. Prawo do informacji i kontroli przetwarzanych danych przysługujące osobie, której dane dotyczą (art. 32 ustawy); obowiązek udzielenia informacji spoczywający na administratorze (art. 33 ustawy)

Każda osoba, której dane są przetwarzane w zbiorze, ma prawo, nie częściej niż raz na 6 miesięcy, zwrócić się do administratora danych o wyczerpującą informację na temat dotyczących jej danych. Z uprawnieniem tym skorelowany jest obowiązek udzielenia takiej informacji, spoczywający na administratorze (art. 33 ustawy).

Podmiot, do którego osoba zwraca się z takim żądaniem, powinien m.in. poinformować o istnieniu zbioru, swojej nazwie i siedzibie, źródle, z którego informacje pochodzą, celu, zakresie i sposobie wykorzystywania danych zawartych w zbiorze, od kiedy wykorzystuje dane osobowe, o sposobie udostępniania danych, a w szczególności o ich odbiorcach. Administrator winien także poinformować osobę o treści posiadanych na jej temat danych. Nie oznacza to jednak prawa wglądu tej osoby do dokumentów, nie jest też podstawą ich wydania.

Obowiązek udzielenia informacji określony został w art. 33 ustawy. Odmowa może nastąpić jedynie wtedy, gdy spowodowałoby to ujawnienie wiadomości stanowiących tajemnicę państwową, zagrożenie obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego, zagrożenie podstawowego interesu gospodarczego lub finansowego państwa, istotne naruszenie dóbr osobistych innych osób.

Obowiązkiem administratora jest udzielenie żądanych informacji w terminie 30 dni. Informacja powinna być udzielona w zrozumiałej formie. Na wniosek osoby, której dane dotyczą, informacji udziela się jej na piśmie.

Należy pamiętać, że art. 54 ustawy przewiduje odpowiedzialność karną (karę grzywny, ograniczenia wolności lub pozbawienia wolności do roku) za niedopełnienie obowiązku poinformowania osoby, której dane dotyczą, o przysługujących jej prawach lub nieprzekazanie tej

osobie informacji umożliwiających korzystanie z praw przyznanych jej w ustawie.

2. Prawo do poprawiania danych, żądania wstrzymania ich przetwarzania lub ich usunięcia

Osoba, której dane dotyczą, może zwrócić się do administratora danych o uzupełnienie, uaktualnienie, sprostowanie danych, czasowe lub stałe wstrzymanie ich przetwarzania lub o ich usunięcie. Musi ona jednak wykazać, że dane są niekompletne, nieaktualne, nieprawdziwe, zostały zebrane z naruszeniem ustawy lub są już zbędne do realizacji celu, dla którego je zgromadzono. Art. 35 ustawy nakazuje w takiej sytuacji administratorowi uwzględnienie żądania bez zbędnej zwłoki, chyba że dotyczy to danych, których tryb uzupełniania, uaktualniania lub sprostowania określają odrębne ustawy.

Administrator danych jest obowiązany poinformować bez zbędnej zwłoki innych administratorów, którym udostępnił zbiór danych, o dokonanym uaktualnieniu lub sprostowaniu danych (art. 35 ust. 3 ustawy). Jeśli natomiast administrator nie uwzględni żądania osoby, której dane dotyczą, to może ona wystąpić do Generalnego Inspektora z wnioskiem o nakazanie dopełnienia tego obowiązku (art. 35 ust. 2 ustawy).

3. Prawo do wniesienia sprzeciwu (art. 32 ust. 1 pkt 8 ustawy)

W przypadku wykorzystywania danych w oparciu o przesłanki wymienione w art. 23 ust. 1 pkt 4 i 5 ustawy należy pamiętać o konieczności uwzględnienia sprzeciwu złożonego przez osobę, której dane są przetwarzane.

Sprzeciw można wnieść, jeśli administrator twierdzi, że wykorzystuje dane osobowe w oparciu o przesłankę dopuszczalności przetwarzania danych wymienioną w art. 23 ust. 1 pkt 4 ustawy (przetwarzanie danych jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego) i przesłankę wymienioną w art. 23 ust. 1 pkt 5 ustawy (przetwarzanie jest niezbędne dla wypełnienia

prawnie usprawiedliwionego celu administratora albo odbiorcy danych i nie narusza praw i wolności osoby, której dotyczy), tymczasem zaś zamierza je przetwarzać w celach marketingowych lub przekazać je innemu administratorowi danych.

Prawo sprzeciwu nie przysługuje osobie, której dane dotyczą, gdy podstawą przetwarzania danych jest zgoda tej osoby, realizacja obowiązku lub uprawnienia wynikającego z przepisu prawa albo gdy przetwarzanie danych służy zawarciu lub wykonaniu umowy między administratorem a osobą, której dane dotyczą.

Wniesienie sprzeciwu przez osobę, której dane dotyczą, oznacza konieczność zaprzestania wykorzystywania jej danych osobowych.

W razie wniesienia sprzeciwu dalsze przetwarzanie kwestionowanych danych jest niedopuszczalne. Możliwe jest jednak pozostawienie w zbiorze imienia i nazwiska osoby oraz numeru PESEL albo adresu – wyłącznie dla uniknięcia ponownego wykorzystania danych osoby w celach objętych sprzeciwem.

Zatem, w przypadku wykorzystywania danych przez podmioty publiczne, gdy przetwarzanie danych uzasadnione jest spełnieniem warunku określonego w art. 23 ust. 1 pkt 2 ustawy, czyli odbywa się wraz z wypełnianiem przez te podmioty zadań i obowiązków określonych w przepisach prawa, sprzeciwu wnieść nie można. Nie można go wnieść również wówczas, gdy podstawą wykorzystywania danych jest zgoda osoby lub łącząca strony umowa.

4. Żądanie zaprzestania przetwarzania danych, ze względu na szczególną sytuację osoby (art. 32 ust. 1 pkt 7 ustawy)

Każda osoba może wystąpić do administratora z żądaniem zaprzestania przetwarzania jej danych osobowych, uzasadniając żądanie swoją szczególną sytuacją. Przepisy nie precyzują, o jakie szczególne okoliczności chodzi. Umotywowane żądanie powinno być skierowane do administratora danych na piśmie. Z takim żądaniem można wystąpić, tak jak ze sprzeciwem, jedynie wtedy, gdy podstawą prawną przetwarzania danych jest art. 23 ust. 1 pkt 4 i 5 ustawy, czyli wtedy, gdy wykorzystywanie danych jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego, jak również wte-

dy, gdy jest to niezbędne dla wypełniania prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą. Tym prawnie usprawiedliwionym celem jest w szczególności marketing bezpośredni własnych produktów lub usług administratora danych oraz dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej.

W przypadku wniesienia takiego żądania administrator danych zaprzestaje przetwarzania kwestionowanych danych osobowych albo bez zbędnej zwłoki przekazuje takie żądanie Generalnemu Inspektorowi, celem podjęcia decyzji w tym zakresie.

V. UDOSTĘPNIANIE DANYCH OSOBOWYCH

1. Ogólne zasady udostępniania danych

Biorąc pod uwagę, że udostępnianie danych jest jedną z form ich przetwarzania, jest ono dopuszczalne wtedy, gdy spełniony jest jeden z warunków, o którym mowa w art. 23 ust. 1 ustawy (artykuł określa warunki, które uzasadniają udostępnianie danych „zwykłych") bądź w art. 27 ust. 2 ustawy (artykuł wylicza sytuacje, które uzasadniają udostępnienie danych szczególnie chronionych).

2. Udostępnianie danych na wniosek osoby, w celu innym niż włączenie do zbioru (art. 29 ustawy)

Konieczność wystąpienia z pisemnym wnioskiem o udostępnienie danych zachodzi wówczas, gdy osoba uprawniona do ich otrzymania zamierza pozyskać dane innej osoby, ze zbioru prowadzonego np. przez podmiot publiczny lub wykonujący zadania publiczne, a celem pozyskania nie jest włączenie danych do jakiegoś istniejącego lub mającego powstać zbioru.

Dopuszczalna jest każda pisemna forma zwrócenia się o dane osobowe, np. zwykły list skierowany do administratora danych należy traktować jako wniosek o udostępnienie danych, jeśli z jego treści będzie wynikało takie żądanie. Osoba zwracająca się o dane musi spełnić warunki określone w art. 29 ustawy. Przepis ten wymaga, aby wniosek był uzasadniony oraz zawierał informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych. Osoba zwracająca się o dane musi też wyraźnie określić, jakich danych żąda i do jakiego celu zamierza je wykorzystać.

Dane należy udostępnić, jeśli występujący z wnioskiem o ich udostępnienie wskaże przepis prawa, który upoważnia go do posiadania danych, bądź też uwiarygodni potrzebę ich posiadania. W tym drugim przypadku żądane dane osobowe nie mogą należeć do kategorii danych szczególnie chronionych, a ich udostępnienie nie może naruszyć praw i wolności osób, których dotyczą.

Ocena uzasadnienia wniosku należy do administratora danych osobowych.

3. Szczególne przepisy o udostępnianiu danych

Akta stanu cywilnego

Zasady i tryb wydawania odpisów aktów stanu cywilnego reguluje ustawa z dnia 29 września 1986 r. – Prawo o aktach stanu cywilnego (tekst jedn. Dz.U. z 2004 r. nr 161, poz. 1688).

Zgodnie z art. 79 tej ustawy, z ksiąg stanu cywilnego wydaje się: odpisy zupełne i skrócone aktów stanu cywilnego; zaświadczenia o dokonanych w księgach stanu cywilnego wpisach lub o ich braku; zaświadczenia o zaginięciu lub zniszczeniu księgi stanu cywilnego. Przepisy tej ustawy wymieniają dane osobowe, jakie należy zamieścić w poszczególnych dokumentach. Odpisy oraz zaświadczenia, o których mowa, wydaje się na wniosek sądu lub innego organu państwowego, osoby, której stan cywilny został w akcie stwierdzony, jej wstępnego, zstępnego, rodzeństwa, małżonka lub przedstawiciela ustawowego (art. 83 ust. 1). Zgodnie z art. 83 ust. 2 tej ustawy odpisy aktów stanu cywilnego i zaświadczenia o dokonanych w księgach stanu cywilnego wpisach lub

o ich braku mogą być również wydane na wniosek innych osób niż wymienione w ust. 1, które wykażą w tym interes prawny, oraz na wniosek organizacji społecznej, jeżeli jest to uzasadnione celami statutowymi tej organizacji i gdy przemawia za tym interes społeczny. Zaświadczenie o zaginięciu lub zniszczeniu księgi stanu cywilnego może być także wydane na wniosek innych zainteresowanych osób.

Ewidencja gruntów i budynków

Przetwarzanie danych osobowych zgromadzonych w ewidencji gruntów i budynków odbywa się w oparciu o przepisy ustawy z dnia 17 maja 1989 r. – Prawo geodezyjne i kartograficzne (tekst jedn. Dz.U. z 2005 r. nr 240, poz. 2027, z późn. zm.) oraz wydanego na jej podstawie rozporządzenia Ministra Rozwoju Regionalnego i Budownictwa z dnia 29 marca 2001 r. w sprawie ewidencji gruntów i budynków (Dz.U. nr 38, poz. 454).

Stosownie do treści art. 24 ust. 2 Prawa geodezyjnego i kartograficznego, informacje o gruntach, budynkach i lokalach zawarte w operacie ewidencyjnym są jawne. Z przepisów tej ustawy wynika, iż każdy może zapoznać się z treścią wpisów w ewidencji gruntów i budynków oraz dokumentami, na podstawie których wpisów tych dokonano. Zgodnie z art. 24 ust. 3 cytowanej ustawy „Wyrysy i wypisy z operatu ewidencyjnego są wydawane przez organ prowadzący ewidencję gruntów i budynków odpłatnie na żądanie właścicieli lub osób fizycznych i prawnych, w których władaniu znajduje się grunt, budynek lub lokal, osób fizycznych i prawnych oraz innych jednostek organizacyjnych nieposiadających osobowości prawnej, które mają interes prawny w tym zakresie, a także na żądanie zainteresowanych organów administracji rządowej i jednostek samorządu terytorialnego".

Jedynie w przypadku, gdy osoba niebędąca właścicielem i niedysponująca innym prawem dającym władztwo nad nieruchomością żąda wydania wypisów i wyrysów z ewidencji, organ prowadzący ewidencję może sprawdzić posiadanie przez nią interesu prawnego w tym zakresie, nie bada natomiast, czy osoba występująca o udostępnienie danych spełniła przesłankę legalności przetwarzania danych – wskazaną w art. 23 bądź art. 29 ustawy o ochronie danych osobowych.

Organami właściwymi do rozstrzygania spraw z zakresu udostępniania informacji zgromadzonych w ewidencji gruntów i budynków są

starosta powiatu oraz wojewoda, który sprawuje kontrolę instancyjną nad rozstrzygnięciami wydanymi przez starostę. Organem administracji geodezyjnej i kartograficznej, do którego zadań należy prowadzenie ewidencji gruntów i budynków, jest bowiem starosta powiatu, wykonujący zadania przy pomocy geodety powiatowego (art. 6a ust. 1 pkt 2 lit b i art. 7d pkt 1 Prawa geodezyjnego i kartograficznego). Kontrolę nad działaniami administracji geodezyjnej i kartograficznej sprawuje wojewódzki inspektor nadzoru geodezyjnego i kartograficznego, działający w imieniu wojewody (art. 7b ust. 1 pkt 2 cytowanej ustawy).

Ewidencja ludności

Kwestie dotyczące dopuszczalności udostępnienia bądź odmowy udostępnienia informacji ze zbioru „ewidencja ludności" należy rozpatrywać m.in. w oparciu o przepisy ustawy z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych (tekst jedn. Dz.U. z 2006 r. nr 139, poz. 993, ze zm.) oraz wydanych na jej podstawie aktów wykonawczych, w szczególności rozporządzenia Rady Ministrów z dnia 30 kwietnia 2002 r. w sprawie wysokości opłat za udostępnianie danych ze zbiorów meldunkowych, zbioru PESEL oraz ewidencji wydanych i utraconych dowodów osobistych oraz warunków i sposobu ich wnoszenia (Dz.U. nr 62, poz. 564) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 18 listopada 2002 r. w sprawie wzoru formularza wniosku o udostępnienie danych ze zbiorów meldunkowych, zbioru PESEL oraz ewidencji wydanych i utraconych dowodów osobistych (Dz.U. nr 201, poz. 1702).

Przepisy ustawy o ewidencji ludności i dowodach osobistych wskazują krąg podmiotów, którym należy udostępnić oraz tych, którym mogą być udostępnione dane ze zbiorów meldunkowych oraz zbioru PESEL, a także przesłanki, po spełnieniu których udostępnienie w przedmiotowym zakresie staje się możliwe (art. 44h tej ustawy). Zgodnie z art. 44h ust. 2 pkt 2 ustawy, dane ze zbiorów meldunkowych, zbioru PESEL oraz ewidencji wydanych i utraconych dowodów osobistych mogą być udostępnione osobom i jednostkom organizacyjnym – jeżeli wykażą w tym interes prawny; stosownie zaś do brzmienia jego pkt 4 również „innym osobom i podmiotom – jeżeli uwiarygodnią one interes faktyczny w otrzymaniu danych i za zgodą osób, których dane dotyczą".

Jak stanowi art. 44i ust. 1 tej ustawy, dane ze zbiorów meldunkowych oraz ewidencji wydanych i utraconych dowodów osobistych udostępnia organ gminy, zaś dane ze zbioru PESEL – zgodnie z ust. 3 powołanego przepisu – Minister Spraw Wewnętrznych i Administracji za pośrednictwem jednostki organizacyjnej MSWiA. Dane udostępnia się na pisemny wniosek zainteresowanego podmiotu, złożony na formularzu, którego wzór określa rozporządzenie MSWiA w sprawie wzoru formularza wniosku o udostępnienie danych ze zbiorów meldunkowych, zbioru PESEL oraz ewidencji wydanych i utraconych dowodów osobistych (art. 44h ust. 3 i 5).

Podkreślić należy, iż organ rozpatrujący wniosek może odmówić udostępnienia danych w drodze decyzji administracyjnej tylko w przypadku, gdy ich udostępnienie spowodowałoby naruszenie dóbr osobistych osoby, której dane dotyczą, lub dóbr innych osób (art. 44i ust. 5 ustawy). Stosownie zaś do brzmienia art. 44i ust. 6 tej ustawy, od decyzji odmawiającej udostępnienia danych osobowych przysługuje odwołanie, zgodnie z przepisami Kodeksu postępowania administracyjnego.

VI. GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

1. Kompetencje

Nad przestrzeganiem prawa obywateli do ochrony ich danych osobowych czuwa niezależny organ – Generalny Inspektor Ochrony Danych Osobowych. Postępowanie w sprawach uregulowanych w ustawie o ochronie danych osobowych Generalny Inspektor prowadzi według zasad określonych w przepisach Kodeksu postępowania administracyjnego, o ile przepisy ustawy o ochronie danych osobowych nie stanowią inaczej (art. 22 ustawy).

Generalny Inspektor:

1) kontroluje, czy dane wykorzystywane są zgodnie z przepisami o ochronie danych osobowych,

2) rozpatruje skargi i wydaje decyzje w sprawach dotyczących ochrony danych osobowych,
3) prowadzi ogólnokrajowy, jawny rejestr zbiorów danych osobowych,
4) opiniuje projekty ustaw i rozporządzeń dotyczących ochrony danych,
5) inicjuje i podejmuje przedsięwzięcia w zakresie doskonalenia ochrony danych osobowych,
6) uczestniczy w pracach międzynarodowych organizacji i instytucji zajmujących się ochroną danych osobowych.

A. Decyzje Generalnego Inspektora

Generalny Inspektor wyposażony został w kompetencje o charakterze władczym. Art. 12 ustawy zaliczył do jego zadań wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych.

Jeśli, w wyniku czynności podjętych z urzędu lub na wniosek osoby zainteresowanej, Generalny Inspektor Ochrony Danych Osobowych stwierdzi naruszenie przepisów o ochronie danych, nakazuje, w drodze decyzji administracyjnej, 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.

Decyzje Generalnego Inspektora nie mogą ograniczać swobody działania podmiotów zgłaszających kandydatów lub listy kandydatów w wyborach na urząd Prezydenta Rzeczypospolitej Polskiej, w wyborach do Sejmu, do Senatu i do organów samorządu terytorialnego, a także w wyborach do Parlamentu Europejskiego, pomiędzy dniem

zarządzenia wyborów a dniem głosowania. W odniesieniu do zbiorów, które zostały uzyskane w wyniku czynności operacyjno-rozpoznawczych przez funkcjonariuszy organów uprawnionych do wykonywania tych czynności – Generalny Inspektor nie może poprzez swe decyzje nakazywać usunięcia danych osobowych zebranych w toku tych czynności, jeśli prowadzone są na podstawie przepisów prawa. W przypadku, gdy przepisy innych ustaw przewidują odmienny tryb przywracania stanu zgodnego z prawem, stosuje się inne przepisy.

Strona niezadowolona z decyzji Generalnego Inspektora Ochrony Danych Osobowych może wystąpić z wnioskiem o ponowne rozpatrzenie sprawy. Odwołanie wnosi się w terminie 14 dni od dnia doręczenia decyzji stronie. Przed upływem terminu do wniesienia odwołania decyzja nie podlega wykonaniu, a wniesienie odwołania w terminie – wstrzymuje wykonanie decyzji. O wniesieniu odwołania Generalny Inspektor informuje strony postępowania. Wniosek o ponowne rozpatrzenie sprawy rozpatrywany jest na podstawie przepisów dotyczących odwołań od decyzji.

Na decyzję Generalnego Inspektora Ochrony Danych Osobowych w przedmiocie wniosku o ponowne rozpatrzenie sprawy przysługuje stronie, zgodnie z art. 21 ust. 2 ustawy, skarga do sądu administracyjnego.

B. Ogólnokrajowy, jawny rejestr zbiorów danych osobowych

Generalny Inspektor Ochrony Danych Osobowych prowadzi ogólnokrajowy, jawny rejestr zbiorów danych osobowych. Jest on dostępny w siedzibie Biura GIODO. Z informacjami zamieszczonymi w rejestrze można się również zapoznać, korzystając z systemu e-giodo, poprzez internet. System e-giodo zapewnia możliwość wyszukiwania zbiorów danych za pomocą wielu kryteriów, takich jak: nazwa zbioru, nazwa administratora danych czy jego siedziba. Rejestr zawiera informacje zgłaszane przez administratorów danych w procesie rejestracji. Nie znajdują się tam informacje o konkretnych osobach, stanowiące treść danych osobowych.

2. Kontakt z Generalnym Inspektorem

Pytania i skargi do Generalnego Inspektora należy kierować na adres:

Generalny Inspektor Ochrony Danych Osobowych
ul. Stawki 2
00-193 Warszawa

Pisma można kierować, korzystając z poczty tradycyjnej, jak i drogą elektroniczną. Ważne jest jednak, by korespondencja spełniała wymagania określone w art. 63 § 2 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, to jest zawierała co najmniej wskazanie:

1) osoby (imienia i nazwiska), od której pochodzi,
2) adresu (kodu pocztowego, miejscowości, ulicy i nr domu) tej osoby,
3) przedmiotu sprawy, której dotyczy.

Ponadto, stosownie do postanowień ustawy z dnia 16 listopada 2006 r. o opłacie skarbowej (Dz.U. nr 225, poz. 1635), opłacie skarbowej – uiszczanej gotówką lub bezgotówkowo – podlega w szczególności:

- wydanie na wniosek administratora danych zaświadczenia o zarejestrowaniu zbioru – w wysokości 17,00 zł (obowiązek zapłaty powstaje z chwilą złożenia wniosku o wydanie zaświadczenia);
- dokonanie przez Generalnego Inspektora Ochrony Danych Osobowych czynności urzędowej w postaci wydania decyzji administracyjnej – w wysokości 10,00 zł (obowiązek zapłaty powstaje z chwilą złożenia skargi do Generalnego Inspektora);
- złożenie dokumentu stwierdzającego udzielenie pełnomocnictwa albo jego odpisu, wypisu lub kopii w postępowaniu administracyjnym – w wysokości 17 zł (obowiązek zapłaty powstaje z chwilą złożenia dokumentu w organie administracji publicznej).

Uwaga! Od 1 stycznia 2007 r., w związku z wejściem w życie nowej ustawy o opłacie skarbowej, nie pobierane są opłaty za zgłoszenie zbioru danych do rejestracji, zgłoszenie zmian informacji zawartych w zgłoszeniu, a także za załączniki do tych zgłoszeń.

Uiszczenia opłaty skarbowej dokonuje się gotówką w kasie organu podatkowego lub bezgotówkowo na rachunek tego organu. Ponieważ w postępowaniach przed Generalnym Inspektorem – organem podatkowym właściwym w sprawach opłaty skarbowej jest Prezydent m.st. Warszawy (art. 12 ustawy), opłata skarbowa powinna zostać wpłacona w kasie lub na konto:

Dzielnica Śródmieście m.st. Warszawy
ul. Nowogrodzka 43
00-691 Warszawa
Nr konta: 45 1240 1066 1111 0010 0317 1881

W tytule wpłaty, poza opisem, należy zamieścić skrót – GIODO.

Składający skargę, wniosek o wydanie zaświadczenia lub pełnomocnictwo zobowiązany jest załączyć dowód zapłaty należnej opłaty skarbowej.

Więcej informacji na temat ochrony danych osobowych znajduje się na stronie internetowej <www.giodo.gov.pl>.