



GIODO

Generalny Inspektor
Ochrony Danych Osobowych

ABC

**wybranych
zagadnień
z ustawy
o ochronie
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. (022) 860 70 81
fax (022) 860 70 86

Opracowały:

Monika Krasieńska

Dyrektor Departamentu Orzecznictwa, Legislacji i Skarg

Sylwia Mizerek

Zastępca Dyrektora Departamentu Orzecznictwa, Legislacji i Skarg

Redaktor Andrzej Rudnicki

SPIS TREŚCI

Wprowadzenie	5
I. Procedura rozpatrywania skarg w sprawach ochrony danych osobowych	6
II. Zakres stosowania ustawy o ochronie danych osobowych	10
III. Zasady przetwarzania danych osobowych	12
1. Zasada legalności	13
2. Zasada celowości	16
3. Zasada merytorycznej poprawności	17
4. Zasada adekwatności	17
5. Zasada ograniczenia czasowego	18
IV. Wykonywanie obowiązku informacyjnego	19
V. Realizacja obowiązków administratora danych i praw osób, których dane dotyczą – pytania i odpowiedzi	25

© Copyright by Kancelaria Sejmu
Warszawa 2007

ISBN 978-83-7059-838-9

KANCELARIA SEJMU

Wydawnictwo Sejmowe

Wydanie pierwsze

Warszawa, październik 2007

WPROWADZENIE

Konstytucja RP z dnia 2 kwietnia 1997 r. wprowadziła do polskiego ustawodawstwa zasadę ochrony danych osobowych. Art. 51 ustawy zasadniczej stanowi: *Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby* (ust. 1). *Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa* (ust. 3). Ponadto: *Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą* (ust. 4).

Konkretyzacją normy konstytucyjnej są przepisy ustawy 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), będące jednocześnie implementacją dyrektywy Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. (95/46/WE) w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych. Dyrektywa ta ma służyć zapewnieniu jednolitego minimalnego poziomu ochrony prywatności osób fizycznych, których dane osobowe są przetwarzane oraz zapewnić swobodny przepływ tych danych pomiędzy krajami członkowskimi Unii Europejskiej.

Od chwili wejścia w życie wskazanej ustawy zostały ujednocnione standardy w zakresie przetwarzania i ochrony danych osobowych. Osoby, których dane dotyczą wyposażone zostały w instrumenty kontroli przebiegu procesu przetwarzania ich danych, zaś na administratorów danych nałożono szereg obowiązków. Precyzując zakres obowiązków podmiotów przetwarzających dane, ustawa określiła także zakres ich praw. Koncepcja ochrony danych osobowych, prezentowana w świe-

tle omawianej ustawy, opiera się bowiem na balansowaniu interesów – z jednej strony chodzi o prawo do ochrony prywatności, a z drugiej – o prawo do informacji o osobie, której dane dotyczą. Wyważenie tego jest często bardzo trudne, o czym świadczą rozbieżne stanowiska w doktrynie oraz niejednolitość orzecznictwa sądowno-administracyjnego w sprawach prowadzonych przez Generalnego Inspektora Ochrony Danych Osobowych (dalej: Generalny Inspektor).

W obliczu postępującej informatyzacji życia społecznego, rozwoju nowych technologii i globalizacji, funkcjonowanie jednostki w strukturze społeczeństwa staje się w zasadzie niemożliwe bez szerokiej ingerencji w jej sferę prywatności. Każda osoba, której prawa zostaną naruszone może jednak zwrócić się o zbadanie procesu przetwarzania jej danych, a rozpatrywanie skarg i przeprowadzanie czynności kontrolnych mających na celu zbadanie, czy nie doszło do naruszeń ustawy o ochronie danych osobowych jest jednym z naczelných zadań Generalnego Inspektora.

I. PROCEDURA ROZPATRYWANIA SKARG W SPRAWACH OCHRONY DANYCH OSOBOWYCH

Skargi

Do zadań Generalnego Inspektora należy m.in. – stosownie do art. 12 pkt 2 ustawy – *wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych*. Postępowanie wszczynane jest zwykle na wniosek osób zainteresowanych. Podejmowane są również czynności z urzędu, w związku z powzięciem informacji o naruszeniu przepisów ustawy.

Formalne warunki skargi

Wszczęcie postępowania administracyjnego na wniosek wiąże się z koniecznością dopełnienia przez osobę zainteresowaną określonych prawem wymogów. Zgodnie z art. 22 ustawy *postępowanie w sprawach uregulowanych w niniejszej ustawie prowadzi się według przepisów Ko-*

*deksu postępowania administracyjnego*¹, o ile przepisy ustawy nie stanowią inaczej.

W korespondencji kierowanej do Generalnego Inspektora drogą elektroniczną lub tradycyjną, w celu zainicjowania postępowania administracyjnego, stosownie do art. 63 § 2 k.p.a., wymagane jest wskazanie co najmniej:

- a) osoby, od której dane pochodzą (imienia i nazwiska), jej adresu (kodu pocztowego, miejscowości, ulicy i numeru domu),
- b) podpisu tej osoby,
- c) sprawy, której skarga dotyczy.

Skarga wniesiona pisemnie albo ustnie do protokołu powinna być podpisana przez wnoszącego, a protokół ponadto przez pracownika, który go sporządził. Gdy podanie wnosi osoba, która nie może lub nie umie złożyć podpisu, podanie lub protokół podpisuje za nią inna osoba przez nią upoważniona, czyniąc o tym wzmiankę obok podpisu.

Nieuzupełnienie wskazanych braków w wyznaczonym dla tej czynności terminie skutkuje pozostawieniem skargi bez rozpoznania.

Osoba składająca skargę jest zobowiązana wnieść także opłatę skarbową² do organu podatkowego (jest nim Prezydent m.st. Warszawy), a fakt ten udokumentować Generalnemu Inspektorowi w momencie wniesienia skargi. Opłata skarbową w wysokości 10 zł pobierana jest za dokonanie przez Generalnego Inspektora czynności urzędowej w postaci wydania decyzji administracyjnej. Obowiązek jej uiszczenia powstaje z chwilą złożenia skargi do Generalnego Inspektora. Ponadto pobierana jest opłata skarbową w wysokości 17 zł za złożenie dokumentu stwierdzającego udzielenie pełnomocnictwa albo jego odpisu, wypisu lub kopii w postępowaniu administracyjnym. Obowiązek zapłaty powstaje z chwilą złożenia dokumentu w organie administracji publicznej (art. 6 ust. 1 pkt 4 ustawy o opłacie skarbowej).

W przypadku nieuiszczenia opłaty (pomimo wezwania) skarga podlega zwrotowi.

¹ Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz.U. z 2000 r. nr 98, poz. 1071 ze zm.).

² Stosownie do przepisów ustawy z dnia 16 listopada 2006 r. o opłacie skarbowej (Dz.U. nr 225, poz. 135 ze zm.).

Terminy rozpatrzenia skargi

Ustawowym terminem rozpatrzenia sprawy jest okres 1 miesiąca. W przypadku szczególnie skomplikowanym może on ulec przedłużeniu do 2 miesięcy.

Pisemność postępowania

Postępowanie jest prowadzone w formie pisemnej (stosownie do art. 14 § 1 k.p.a.). W jego toku organ ochrony danych osobowych podejmuje czynności niezbędne do wyjaśnienia wszystkich istotnych okoliczności związanych ze złożoną skargą: np. zwraca się do stron o złożenie pisemnych wyjaśnień czy przysłanie dokumentów, przeprowadza czynności kontrolne w siedzibie administratora danych.

Rozstrzygnięcie i odwołanie

W przypadku naruszenia przepisów o ochronie danych osobowych GODO nakazuje, w drodze decyzji administracyjnej, przywrócić stanu zgodnego z prawem, poprzez:

- 1) *usunięcie uchybień,*
- 2) *uzupełnienie, uaktualnienie, sprostowanie, udostępnienie lub nieudostępnienie danych osobowych,*
- 3) *zastosowanie dodatkowych środków zabezpieczających zgromadzone dane osobowe,*
- 4) *wstrzymanie przekazywania danych osobowych za granicę,*
- 5) *zabezpieczenie danych lub przekazanie ich innym podmiotom,*
- 6) *usunięcie danych osobowych* (art. 18 ust. 1 ustawy).

W przypadku usunięcia uchybień w toku postępowania lub jeszcze przed jego wszczęciem, postępowanie podlega umorzeniu.

Od wydanej decyzji stronom przysługuje prawo wniesienia wniosku o ponowne rozpatrzenie sprawy w terminie 14 dni od dnia doręczenia decyzji, a następnie w razie utrzymania przez Generalnego Inspektora w mocy zaskarżonej decyzji, składana w terminie 30 dni skarga do Wojewódzkiego Sądu Administracyjnego w Warszawie. W związku z wprowadzeniem w 2004 r. w Polsce dwuinstancyjnego postępowania sądowo-administracyjnego, od wyroku wydanego w I instancji przysługuje skarga

kasacyjna do Naczelnego Sądu Administracyjnego, w terminie 30 dni od dnia doręczenia stronom odpisu orzeczenia z uzasadnieniem.

Ograniczenia w zakresie wydawania decyzji administracyjnej przez GODO

- Decyzje Generalnego Inspektora nie mogą ograniczać swobody działania podmiotów zgłaszających kandydatów lub listy kandydatów w wyborach na urząd Prezydenta Rzeczypospolitej Polskiej, do Sejmu, Senatu i organów samorządu terytorialnego, a także w wyborach do Parlamentu Europejskiego, pomiędzy dniem zarządzenia wyborów a dniem głosowania (art. 18 ust. 2 ustawy).
- W odniesieniu do zbiorów, które zostały uzyskane w wyniku czynności operacyjno-rozpoznawczych przez funkcjonariuszy organów uprawnionych do tych czynności, decyzje Generalnego Inspektora nie mogą nakazywać usunięcia danych osobowych zebranych w toku tych czynności prowadzonych na podstawie przepisów prawa (art. 18 ust. 2a ustawy).
- W przypadku, gdy przepisy innych ustaw przewidują odmienny tryb przywracania stanu zgodnego z prawem, stosuje się te przepisy a nie wydaje nakazy w oparciu o ustawę o ochronie danych osobowych (art. 18 ust. 3 ustawy).

Wykonalność decyzji

Przed upływem terminu do wniesienia odwołania decyzja nie podlega wykonaniu. Wniesienie odwołania w terminie wstrzymuje wykonanie decyzji. Decyzja podlega wykonaniu przed upływem terminu do wniesienia odwołania, gdy jest zgodna z żądaniem wszystkich stron. Sąd administracyjny może wstrzymać wykonanie decyzji.

Inne uprawnienia organu ochrony danych osobowych

W przypadku stwierdzenia naruszenia przepisów o ochronie danych osobowych Generalnemu Inspektorowi przysługuje również możliwość:

- a) zawiadomienia organów ścigania o popełnieniu przestępstw określonych w przepisach karnych ustawy,

- b) składania wniosków o ukaranie dyscyplinarne,
- c) występowania do administratorów danych o zmianę niewłaściwych praktyk (tzw. sygnalizacje).

II. ZAKRES STOSOWANIA USTAWY O OCHRONIE DANYCH OSOBOWYCH

Zakres podmiotowy

1. Podmioty publiczne
 - organy państwowe (np. NIK, Kancelaria Sejmu, Kancelaria Senatu, ZUS),
 - organy samorządu terytorialnego (np. wójt, burmistrz, prezydent miasta),
 - państwowe i komunalne jednostki organizacyjne (np. miejskie zakłady oczyszczania, miejskie zakłady komunikacji).
2. Podmioty prywatne
 - podmioty niepubliczne realizujące zadania publiczne (np. prywatne zakłady opieki zdrowotnej, prywatne szkoły itd.),
 - osoby fizyczne (bez względu na narodowość, obywatelstwo, zdolność do czynności prawnych, wiek itp.),
 - osoby prawne (np. stowarzyszenia, spółdzielnie, fundacje) i jednostki organizacyjne niebędące osobami prawnymi (np. niemające osobowości prawnej spółki prawa handlowego).

Ustawa nie ma zastosowania w przypadkach:

- osób nieżyjących – ze względu na ochronę powszechnych dóbr osobistych (kult pamięci osoby zmarłej),
- informacji o przedsiębiorcach w zakresie, w jakim identyfikują podmiot w obrocie gospodarczym i ściśle wiążą się z prowadzeniem działalności gospodarczej,
- osób fizycznych, prawnych i jednostek organizacyjnych niebędących osobami prawnymi, o ile nie przetwarzają danych w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych,

- podmiotów mających siedzibę albo miejsca zamieszkania w państwie trzecim (tj. nienależącym do Europejskiego Obszaru Gospodarczego), wykorzystujących środki techniczne znajdujące się na terytorium Rzeczypospolitej Polskiej wyłącznie do przekazywania danych,
- osób fizycznych, które wykorzystują dane wyłącznie w celach osobistych lub domowych.

Zakres przedmiotowy

1. Przetwarzanie danych osobowych w zbiorach prowadzonych w systemie papierowym (kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych).
2. Przetwarzanie danych osobowych w systemach informatycznych, także w przypadku przetwarzania danych osobowych poza zbiorem.

Ustawa nie ma zastosowania w przypadkach:

- przetwarzania danych osobowych w zbiorach doraźnych (tworzonych wyłącznie ze względów technicznych, szkoleniowych lub w związku z dydaktyką w szkołach wyższych), które po wykorzystaniu podlegają obowiązkowi niezwłocznego usunięcia albo anonimizacji – wyjątkiem są przepisy dotyczące zabezpieczenia takich zbiorów przez okres ich funkcjonowania (rozdział 5 ustawy),
- działalności dziennikarskiej w rozumieniu prawa prasowego, działalności literackiej lub artystycznej, za wyjątkiem przepisów dotyczących zabezpieczeń i umożliwiających organowi ochrony danych osobowych pozyskanie wyjaśnień oraz złożenie zawiadomienia o popełnieniu przestępstwa, o ile wolność wyrażania poglądów i rozpowszechniania informacji nie narusza istotnie praw i wolności osoby, której dane dotyczą,
- umowy międzynarodowej, której stroną jest Rzeczypospolita – jeżeli ta umowa stanowi inaczej,
- istnienia odrębnych ustaw, które odnoszą się do przetwarzania danych, a przewidują dalej idącą ich ochronę, niż wynika to z ustawy o ochronie danych osobowych (stosuje się wówczas przepisy tych ustaw).

III. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

Główne zasady postępowania przy przetwarzaniu danych osobowych wyznacza art. 26 ust. 1 ustawy, ujmując je w formę podstawowych obowiązków administratora danych. Z jego treści wynika, iż powinien on dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a co za tym idzie ma on przestrzegać pewnych zasad:

- 1) zasady legalności – przetwarzać dane zgodnie z prawem,
- 2) zasady celowości – zbierać dane dla oznaczonych, zgodnych z prawem celów i nie poddawać ich dalszemu przetwarzaniu niezgodnemu z tymi celami,
- 3) zasady merytorycznej poprawności – dbać o merytoryczną poprawność danych,
- 4) zasady adekwatności – dbać o adekwatność danych w stosunku do celów, w jakich są przetwarzane,
- 5) zasady ograniczenia czasowego – przechowywać dane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

Przetwarzanie danych w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą, oraz następuje:

- 1) w celach badań naukowych, dydaktycznych, historycznych lub statystycznych,
- 2) z zachowaniem przepisów art. 23 i 25 ustawy (art. 26 ust. 2 ustawy).

Działania administratora polegające na respektowaniu interesów (zarówno majątkowych, jak i niemajątkowych) osób, których dane dotyczą, muszą się odznaczać „szczególną starannością”, a więc większą od „zwykłej”, „przeciętnej” czy nawet „należytej”, o których mowa w Kodeksie cywilnym.

1. Zasada legalności

Pierwszym obowiązkiem wymienionym w art. 26 ust. 1 ustawy jest obowiązek przetwarzania danych zgodnie z prawem, określane także jako zasada legalności.

Przetwarzanie danych osobowych przez ich administratora powinno odbywać się z zachowaniem przynajmniej jednej z przesłanek legalności przetwarzania określonych w ustawie. W przypadku danych „zwykłych”, przesłanki te wymienia enumeratywnie art. 23 ustawy i są nimi:

- a) zgoda osoby, której dane dotyczą, chyba że chodzi o usunięcie dotyczących jej danych,
- b) niezbędność realizacji uprawnień lub spełnienia obowiązku wynikającego z przepisu prawa,
- c) konieczność realizacji umowy, gdy osoba, której dane dotyczą jest jej stroną lub gdy przetwarzanie jest niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,
- d) niezbędność przetwarzania danych do wykonania określonych prawem zadań realizowanych dla dobra publicznego,
- e) niezbędność przetwarzania danych dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów albo odbiorców danych, a przetwarzanie danych nie narusza praw i wolności osoby, której one dotyczą.

Za prawnie usprawiedliwiony cel [...] uważa się w szczególności: marketing bezpośredni własnych produktów lub usług administratora danych oraz dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej (art. 23 ust. 4 ustawy).

Odrębny reżim przetwarzania danych odnosi się do danych „szczególnie chronionych”, tj. wrażliwych. Ich przetwarzanie co do zasady jest zabronione. Zgodnie z art. 27 ust. 1 ustawy do danych szczególnie chronionych należy zaliczyć: dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną, związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach, życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

W myśl art. 27 ust. 2 ustawy przetwarzanie tej kategorii danych jest jednak dopuszczalne po spełnieniu jednej z następujących przesłanek:

- 1) osoba, której dane dotyczą wyrazi na to zgodę na piśmie, chyba że chodzi o usunięcie dotyczących jej danych,
- 2) przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony,
- 3) przetwarzanie takich danych jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora,
- 4) jest to niezbędne do wykonywania statutowych zadań kościołów i innych związków wyznaniowych, stowarzyszeń, fundacji lub innych niezarobkowych organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, pod warunkiem, że przetwarzanie danych dotyczy wyłącznie członków tych organizacji lub instytucji albo osób utrzymujących z nimi stałe kontakty w związku z ich działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych,
- 5) przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem,
- 6) przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie,
- 7) przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych,
- 8) przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą,
- 9) jest to niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego; publikowanie wyników badań naukowych nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone,

10) przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

Stosowanie zasady legalności nie oznacza tylko przetwarzania danych osobowych zgodnie z przepisami ustawy, ale także z wszelkimi obowiązującymi normami prawnymi, i to zarówno określonymi w przepisach o randze ustawy, jak i aktach niższego rzędu (przepisy wykonawcze).

W myśl zasady zabronione jest (poza wyjątkami wskazanymi w ustawach odrębnych) zbieranie danych w sposób ukryty, przez podsłuch, czy z naruszeniem tajemnicy korespondencji, a także za pomocą wariografu. W wyroku z dnia 4 marca 2002 r. NSA podkreślił, że żadne względy natury organizacyjno-finansowej nie powinny być traktowane jako podstawa do sprzecznego z prawem przetwarzania danych osobowych przez banki (sygn. akt II SA 3144/01).

Należy podkreślić, że zasada nie obejmuje postanowień umownych.

W zasadzie legalności szczególną rolę odgrywa przesłanka zgody osoby, której dane dotyczą. W myśl art. 7 pkt 5 ustawy przez zgodę rozumie się oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. Zgoda na wykorzystywanie danych osobowych podlegających szczególnej ochronie musi być wyrażona na piśmie.

Z definicji tej nie wynikają szczegółowe zasady formułowania zgody, jednakże podkreślić należy, 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 mogą być przetwarzane. Wyrażający zgodę musi mieć pełną świadomość tego, na co się godzi. Stanowisko takie wyraził także Naczelny Sąd Administracyjny w wyroku z dnia 4 kwietnia 2003 r. (sygn. akt II SA 2135/2002). W uzasadnieniu stwierdzono, iż zgoda na przekazywanie danych musi mieć charakter wyraźny, a jej wszystkie aspekty muszą być jasne dla podpisującego w momencie jej wyrażania. Czynności takiej nie legalizuje późniejsze poinformowanie o treści regulaminu, ani możliwość zgłoszenia zastrzeżeń wobec pewnych form przetwarzania danych.

Ponadto oświadczenie o wyrażeniu zgody musi być przejawem wolnej i nieskrępowanej woli osoby je składającej. Nie może ona czuć się zmuszona do jego złożenia.

Przykładowa treść klauzuli zgody na przetwarzanie danych osobowych

Wyrażam zgodę na przetwarzanie moich danych osobowych w zakresie obejmującym imię, nazwisko i adres zamieszkania, przez XYZ Sp. z o.o. z siedzibą w Warszawie (00-111), ul. Kwiatowa 1, w celach przesyłania ofert marketingowych, jak również na przekazywanie ich innym podmiotom.

Warszawa, dnia 5 lipca 2007 r.

Anna Kowalska

Wyrażenie zgody jest zbędne, gdy przetwarzanie danych jest dopuszczalne na podstawie:

- odrębnych przepisów prawa (np. w celu przeprowadzenia wywiadu środowiskowego przez pracownika pomocy społecznej),
- innych przesłanek (np. w celu realizacji umowy).

2. Zasada celowości

Zasada ta, zwana również zasadą związania z celem, oznacza, iż zbieranie danych osobowych powinno być dokonywane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami. Oznacza to, iż:

- zbierający dane nie może pominąć ani zataić tego celu,
- nie można określać celu przetwarzania danych w sposób ogólnikowy,
- cel ten powinien być zakomunikowany zainteresowanemu przed zebraniem danych osobowych,
- niedopuszczalne jest uzależnianie zawarcia umowy od wyrażenia zgody na przetwarzanie danych w zupełnie innych celach (np. marketingu produktów i usług podmiotów trzecich).

Przetwarzanie danych w celu innym niż ten, w którym zostały zebrane, jest jednak dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą, oraz następuje:

- w celach badań naukowych, dydaktycznych, historycznych lub statystycznych,
- z zachowaniem przepisów art. 23 i 25 ustawy.

3. Zasada merytorycznej poprawności

Administrator danych jest obowiązany zapewnić merytoryczną poprawność danych osobowych. Chodzi o to, aby były one zgodne z prawdą, pełne (kompletne) i aktualne.

W tym celu konieczne jest, aby w procesie przetwarzania danych administrator:

- każdorazowo oceniał wiarygodność źródła pozyskania danych,
- wypracował tryb weryfikowania prawdziwości danych (w zależności od tego, czy dane są zwykłe czy szczególnie chronione) oraz ustalił zasady postępowania w przypadku stwierdzenia ich nieprawdziwości – o dokonanych uaktualnieniu lub sprostowaniu danych administrator jest obowiązany bez zbędnej zwłoki poinformować innych administratorów, którym udostępnił zbiór danych (art. 35 ust. 3 ustawy).

Naruszeniem tej zasady jest zbieranie danych ze źródeł niewiadomego pochodzenia, które nie gwarantują ich poprawności. Również względy natury technicznej (np. konstrukcja programów informatycznych, za pomocą których przetwarzane są dane osobowe) nie mogą decydować o przetwarzaniu danych nieprawdziwych, niekompletnych czy nieaktualnych, o czym przesądził Wojewódzki Sąd Administracyjny w wyroku z dnia 5 marca 2007 r., sygn. akt II SA/Wa 2328/06 (niepublikowany).

4. Zasada adekwatności

Zgodnie z zasadą adekwatności administrator powinien przetwarzać tylko takiego rodzaju dane i tylko o takiej treści, które są niezbędne ze względu na cel zbierania danych. Relewantność (adekwatność) danych powinna być oceniana najpóźniej w momencie ich zbierania. Zatem administrator ma obowiązek dokonania w tym względzie oceny.

Zakres danych osobowych adekwatnych do celu przetwarzania oceniać trzeba każdorazowo z uwzględnieniem określonego stosunku prawnego, w związku z którym administrator przetwarza dane osobowe (wyrok NSA z dnia 27 listopada 2003 r., II SA 209/2003). W odniesieniu do umów uwzględnić należy ich charakter i znaczenie (wyrok NSA z dnia 19 grudnia 2001 r., II SA 2869/2000, ONSA 2003, nr 1, poz. 29).

Niekiedy ustawodawca wskazuje wprost w przepisach prawa na zakres danych adekwatnych do celu przetwarzania. Przepisy takie mają charakter *lex specialis* i wyłączają stosowanie zasady adekwatności. Przykładem takiej sytuacji jest art. 112b ustawy – Prawo bankowe, zgodnie z którym banki mogą przetwarzać, w celach prowadzonej działalności bankowej, informacje zawarte w dokumentach tożsamości osób fizycznych.

Z kolei za nieadekwatne należy uznać pozyskiwanie danych o wykształceniu i stanie cywilnym przy zawieraniu umów odpowiedzialności cywilnej posiadacza pojazdu mechanicznego (wyrok WSA z dnia 5 lutego 2003 r., sygn. akt II SA 3505/01) czy też zbieranie przez bank danych osobowych klientów w zakresie poprzednich adresów zameldowania, kategorii i daty nadania uprawnienia do kierowania pojazdem silnikowym oraz danych zawartych w świadectwie pracy, dotyczących przebiegu zatrudnienia (wyrok WSA z dnia 24 listopada 2005 r., sygn. akt II SA/Wa 1335/05).

Przy stosowaniu zasady adekwatności należy zwrócić uwagę, że:

- posłużenie się określoną techniką zbierania danych (np. kopiowanie dokumentów) nie przesądza o naruszeniu tej zasady (wyrok NSA z dnia 19 grudnia 2001 r., sygn. akt II SA 2869/2000, ONSA 2003, nr 1, poz. 29),
- dane osobowe nie mogą być zbierane na zapas, „na wszelki wypadek”, tj. bez wykazania celowości ich pozyskania i niezbędności dla realizacji zadań administratora danych.

5. Zasada ograniczenia czasowego

Ustawa nakłada na administratora obowiązek przechowywania danych w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż to jest niezbędne do osiągnięcia celu przetwarzania. Po osiągnięciu celu (np. wykonaniu zawartej umowy, upływie wskazanego w przepisach prawa okresu przechowywania danych) dane powinny zostać usunięte, zanonimizowane lub też przekazane podmiotowi uprawnionemu ustawowo do ich przejęcia od administratora (np. przekazane do archiwum państwowego). W tym celu administrator danych jest zobowiązany do stałego nadzorowania zawartości swoich zbiorów pod kątem

konieczności usuwania danych zbędnych, albo do których przetwarzania przestał być upoważniony ustawowo lub w drodze umowy. Przykładowo, w kontekście przetwarzania danych osobowych przez Biuro Informacji Kredytowej WSA wskazał, iż „[...] z chwilą całkowitej spłaty kredytu (zamknięcia rachunku bankowego) kończy się prawne zezwolenie na przetwarzanie danych osobowych tych osób, których rachunki zostały zamknięte. Osiągnięty zostaje wówczas cel, w jakim dane te były przetwarzane” (wyrok WSA z dnia 22 lutego 2005 r., sygn. akt II SA/Wa 2030/04, LEX nr 164935).

W razie wykazania przez osobę, której dane osobowe dotyczą, iż są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, administrator danych jest obowiązany, bez zbędnej zwłoki, do uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, chyba że dotyczy to danych osobowych, w odniesieniu do których tryb ich uzupełnienia, uaktualnienia lub sprostowania określają odrębne ustawy (art. 35 ust. 1 ustawy).

Gdy administrator odmawia wypełnienia powyższego obowiązku, na wniosek podmiotu danych, Generalny Inspektor wydaje decyzję administracyjną nakazującą przywrócenie stanu zgodnego z prawem.

IV. WYKONYWANIE OBOWIĄZKU INFORMACYJNEGO

Istotnym obowiązkiem, jaki z mocy ustawy spoczywa na administratorze jest obowiązek informacyjny, o którym mowa w art. 24 (gdy dane zbierane są bezpośrednio od osoby, której one dotyczą) i art. 25 (w przypadkach gromadzenia danych ze źródeł pośrednich, np. nie od osoby, której one dotyczą).

Chodzi o to, aby na podstawie uzyskanych informacji, zainteresowany miał możliwość właściwego oceny sytuacji i podjęcia decyzji co do udostępnienia danych, a także, aby mógł korzystać z praw przyznanych mu w art. 32 ustawy.

Dla wykonania obowiązku informacyjnego nie ma znaczenia:

- w jaki sposób dane są zbierane (drogą pisemną, telefonicznie czy też w kontaktach bezpośrednich),

- w jaki sposób są utrwalane ani też jaką postać ma zbiór, do którego są one wprowadzane (czy jest to zbiór prowadzony metodą tradycyjną – manualnie, czy też dane przetwarzane są w systemie informatycznym),
- czy zbiór już istnieje, czy dopiero powstanie na podstawie gromadzonych danych.

Artykuł 24 ust. 1 ustawy stanowi, iż w przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o:

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

Informacje te należy przekazać osobie, której dane dotyczą. Poinformowanie powinno mieć charakter indywidualny w tym znaczeniu, iż nie może być zastąpione, np. ogłoszeniem czy też adnotacją umieszczoną w regulaminie, jeśli osoba nie ma możliwości bezpośrednio zapoznania się z jego treścią. Obowiązek ten powinien być wykonany w zasadzie przed rozpoczęciem zbierania danych. Ustawa nie zawiera bowiem w tym zakresie żadnych wskazówek, podobnie jak nie przesądza, w jakiej formie obowiązek informacyjny powinien być spełniony. Skoro zaś ustawodawca nie narzuca żadnej formy, należy uznać, iż jest ona w zasadzie dowolna (informacje mogą być udzielone np. ustnie).

Uwaga! Z punktu widzenia dowodowego wskazane jest jednak posłużenie się formą pisemną. Bowiem w razie ewentualnego sporu co do dopełnienia obowiązku informacyjnego, ciężar udowodnienia, że w rzeczywistości został on wykonany, spoczywał będzie na administratorze danych. Ważne jest także, aby przekazana osobie zainteresowanej informacja była pełna i zawierała wszystkie elementy wskazane w cytowanym art. 24 ustawy. Konieczne jest też, aby była ona w dostateczny sposób wyodrębniona spośród innych informacji przekazywanych oso-

bie zainteresowanej przez administratora danych, a także, aby była wyrażona w formie zrozumiałej dla adresata.

Dopełnienie obowiązku informacyjnego, o którym mowa w art. 24 ust. 1, powinno nastąpić z inicjatywy administratora danych. Nie jest tu potrzebna prośba czy też wniosek ze strony zainteresowanego.

Przepisu zawartego w art. 24 ust. 1 ustawy nie stosuje się, jeżeli:

- 1) przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania,
- 2) osoba, której dane dotyczą, posiada informacje, o których mowa w ust. 1 (art. 24 ust. 2).

W tym drugim przypadku (art. 24 ust. 2) wyłączenia obowiązku informacyjnego nie można oprzeć na subiektywnym odczuciu administratora, że osoba zainteresowana jest świadoma wszystkich okoliczności związanych ze zbieraniem jej danych osobowych. Musi być to okoliczność stwierdzona w sposób obiektywny i sprawdzona, czy rzeczywiście podmiotowi danych wszystkie informacje wymienione w art. 24 ust. 1 są znane.

Przykładowa klauzula informacyjna

Zgodnie z art. 24 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz.U. z 2002 r. nr 101, poz. 926 ze zm.) informuję, iż:

- 1) administratorem Pani/Pana danych osobowych jest XYZ Sp. z o.o. z siedzibą w Warszawie (00-111), ul Kwiatowa 1, zwana dalej Spółką,
- 2) Pani/Pana dane osobowe przetwarzane będą w celu marketingu produktów i usług Spółki i nie będą udostępniane innym odbiorcom,
- 3) posiada Pani/Pan prawo dostępu do treści swoich danych oraz ich poprawiania,
- 4) podanie Spółce danych osobowych jest dobrowolne.

Odrębnie (art. 25 ustawy) uregulowany został obowiązek informacyjny spoczywający na administratorze danych w sytuacji, gdy gromadzi on informacje o określonych osobach z innych źródeł niż one same.

W przypadku zbierania danych osobowych nie od osoby, której dane 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 (chodzi o prawo do złożenia sprzeciwu wobec przetwarzania danych w celach marketingowych lub przekazywania ich innym podmiotom oraz żądania zaprzestania przetwarzania danych ze względu na szczególną sytuację osoby, której one dotyczą).*

Porównując ten obowiązek z powinnościami administratora wynikającymi z art. 24 ustawy, wskazać można na trzy zasadnicze różnice dotyczące:

- 1) czasu, w którym administrator ma przekazać informacje,
- 2) zakresu informacji, jakie mają być przez administratora udzielone,
- 3) zakresu okoliczności zwalniających administratora z obowiązku dostarczenia informacji.

Ad. 1) O ile w przypadku obowiązku informacyjnego, o którym mowa w art. 24, informacje określone tym przepisem powinny być przekazane osobie, której dane dotyczą, przed pozyskaniem danych, o tyle w przypadku obowiązku informacyjnego, o którym mowa w art. 25, powinien być on wykonany – co wynika wprost z brzmienia ust. 1 – bezpośrednio po utrwaleniu zebranych danych. Chodzi przy tym o utrwalenie danych tej osoby, której informacje mają być przekazane, a nie utrwalenie wszystkich danych, które administrator zbiera w określonym celu.

Utrwalenie danych polega na zapisaniu ich na jakimkolwiek nośniku (papierowym, elektronicznym lub innym). Zastrzeżenie, że udzielenie informacji nastąpić ma „bezpośrednio po” utrwaleniu danych wskazuje, że między tymi dwoma zdarzeniami, tj. utrwaleniem danych i poinformowaniem, nie może występować odstęp czasowy większy niż z obiektywnych powodów konieczny (J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Lex a Wolters Kluwer business, Kraków 2007, str. 493–494). W wyroku z dnia 13 lipca 2004 r. (sygn. akt OSK 507/2004) Naczelny Sąd Administracyjny

orzekł, że w sytuacji, gdy jeden podmiot kupił dane osobowe od innego, musi o tym niezwłocznie poinformować osoby, których dotyczy transakcja. Nie wolno wysłać jednocześnie ofert marketingowych, gdyż dalsze korzystanie z takich danych zależy od zainteresowanych, którzy mogą zgłosić sprzeciw lub skorzystać z innych form kontroli. W innym wyroku (II SA 2665/2002) Sąd ten stwierdził zaś, że „Firma, która nabyła zbiór danych osobowych od innego administratora danych, powinna powiadomić klientów, że posiada ich dane, oraz dać im czas, aby mieli szansę wnieść sprzeciw na ich przetwarzanie w celach marketingowych. Niedotrzymanie tych warunków łamie przepisy o ochronie danych osobowych”.

Ad. 2) Informacje, o których mowa w art. 25 ust. 1 są w znacznej części tożsame z zawartymi w art. 24 ust. 1. Różnica polega na tym, że art. 25 ust. 1 dodatkowo zobowiązuje administratora do poinformowania o źródle, z którego pozyskał dane, oraz o służących zainteresowanemu uprawnieniach kontrolnych wynikających z art. 32 ust. 1 pkt 7 i 8.

Ad. 3) Art. 25 ust. 2 zawiera poszerzony – w porównaniu z art. 24 ust. 2 – katalog przypadków pozwalających administratorowi danych odstąpić od przekazania informacji.

Może on to uczynić, gdy:

- 1) *przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą,*
- 2) *dane te 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 ust. 1 wymagałoby nadmiernych nakładów lub zagrażałoby realizacji celu badania,*
- 3) *dane są przetwarzane przez administratora, o którym mowa w art. 3 ust. 1 i ust. 2 pkt 1, na podstawie przepisów prawa,*
- 4) *osoba, której dane dotyczą, posiada informacje, o których mowa w ust. 1.*

Przykładowa klauzula informacyjna

Zgodnie z art. 25 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz.U. z 2002 r. nr 101, poz. 926 ze zm.) informuję, iż:

- 1) administratorem Pani/Pana danych osobowych jest XYZ Sp. z o.o. z siedzibą w Warszawie (00-111), ul. Kwiatowa 1, zwana dalej Spółką,
- 2) Pani/Pana dane osobowe przetwarzane będą w celu marketingu produktów i usług Spółki i nie będą udostępniane innym odbiorcom,
- 3) Spółka pozyskała Pani/Pana dane osobowe od IJK Sp. z o.o. z siedzibą w Krakowie (10-001), ul. Zielna 100,
- 4) posiada Pani/Pan prawo dostępu do treści swoich danych oraz ich poprawiania,
- 5) na podstawie art. 32 ust. 1 pkt 7 ustawy o ochronie danych osobowych przysługuje Pani/Panu prawo wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania Pani/Pana danych ze względu na Pani/Pana szczególną sytuację, jak również – na podstawie art. 32 ust. 1 pkt 8 ustawy o ochronie danych osobowych ma Pani/Pan prawo wniesienia sprzeciwu wobec przetwarzania Pani/Pana danych w celach marketingowych lub wobec przekazywania ich innemu administratorowi danych.

Ustawodawca nałożył na administratora danych jeszcze jeden obowiązek, realizowany tym razem na wniosek zainteresowanego. Art. 33 ust. 1 ustawy stanowi, iż *na wniosek osoby, której dane dotyczą, administrator danych jest obowiązany, 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 zebrano dane,*
- 3) *w jakim celu i zakresie dane są przetwarzane,*
- 4) *w jakim zakresie oraz komu dane zostały udostępnione.*

Również na wniosek osoby zainteresowanej wymienionych informacji udziela się na piśmie.

Należy podkreślić, że realizacji uprawnień kontrolnych można odmówić osobie, której dane dotyczą, gdy udostępnienie informacji spowodowałoby:

- 1) *ujawnienie wiadomości stanowiących tajemnicę państwową,*
- 2) *zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego,*
- 3) *zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa,*

- 4) *istotne naruszenie dóbr osobistych osób, których dane dotyczą, lub innych osób (art. 30 ustawy).*

Wywiązywanie się przez administratora danych z obowiązków informacyjnych może być przedmiotem badania przez Generalnego Inspektora w ramach postępowania administracyjnego wszczętego z urzędu lub zainicjowanego skargą osoby, wobec której obowiązek ten nie został zrealizowany.

W kontekście realizacji obowiązków informacyjnych należy również zwrócić uwagę na art. 54 ustawy, który przewiduje sankcje karne w postaci grzywny, ograniczenia wolności albo pozbawienia wolności do roku wobec osoby administrującej zbiorem danych, która nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o jej prawach (zawartych w ustawie) i możliwościach korzystania z nich.

V. REALIZACJA OBOWIĄZKÓW ADMINISTRATORA DANYCH I PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ – PYTANIA I ODPOWIEDZI

Czy administratorem danych w spółce prawa handlowego jest ta spółka, czy też są to jej organy, osoby zasiadające w organach tej spółki, czy też osoby pełniące funkcje kierownicze w spółce?

Pojęcie administratora danych zdefiniowane zostało w art. 7 pkt 4 ustawy o ochronie danych osobowych. Zgodnie z tym przepisem jest to organ, jednostka organizacyjna, podmiot lub osoba, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych.

Administratorem danych osobowych wykorzystywanych w zakresie działalności prowadzonej przez przedsiębiorcę jest, co do zasady, przedsiębiorca, a w szczególności spółka z ograniczoną odpowiedzialnością, spółka akcyjna, spółka jawna oraz spółka komandytowa. Tak więc administratorem danych jest sama spółka prawa handlowego, nie zaś jej organy, osoby zasiadające w organach tej spółki lub pełniące w niej funkcje kierownicze.

W przypadku osoby prowadzącej działalność gospodarczą jest ona administratorem danych także wtedy, gdy wyznaczy pracownika odpowiedzialnego za przetwarzanie danych osobowych.

Czym są dane osobowe, jak interpretować art. 6 ust. 3 ustawy o ochronie danych osobowych?

Zgodnie z art. 6 ust. 1 ustawy *za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej*. Z kolei art. 6 ust. 2 stanowi, że *osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne*. W myśl ust. 3, *informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu i działań*. Danymi osobowymi będą zatem zarówno takie dane, które pozwalają na określenie tożsamości konkretnej osoby, jak i takie, które nie pozwalają na jej natychmiastową identyfikację, ale są, przy pewnym nakładzie kosztów, czasu i działań, wystarczające do jej ustalenia. Do danych osobowych należeć będzie taka informacja, która pozwala na ustalenie tożsamości danej osoby, bez nadzwyczajnego wysiłku i nakładów, zwłaszcza przy wykorzystaniu łatwo osiągalnych i powszechnie dostępnych źródeł. Poza zakresem przedmiotowej definicji znajdzie się zatem taka informacja, której uzyskanie wymagać będzie nieracjonalnych, nieproporcjonalnie dużych nakładów kosztów, czasu lub działań.

W świetle powyższej definicji należy przyjąć, że danymi osobowymi nie będą pojedyncze informacje o dużym stopniu ogólności, np. nazwa ulicy i numer domu czy wysokość wynagrodzenia. Jednak będą one danymi osobowymi wówczas, gdy zostaną zestawione z innymi dodatkowymi informacjami, które można odnieść do konkretnej osoby. Przykładem takiej pojedynczej informacji jest natomiast numer PESEL, który – zgodnie z art. 31a ust. 1 ustawy z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych (Dz.U. z 2001 r. nr 87, poz. 960 ze 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 służącą do komputerowej kontroli poprawności nadanego numeru ewidencyjnego. Można więc stwierdzić, że numer PESEL *ex definitione* należy do da-

nych osobowych, których przetwarzanie podlega wszelkim rygorom przewidzianym w ustawie o ochronie danych osobowych.

Ustawodawca, formułując art. 6 ustawy, posłużył się klauzulą generalną. Tym samym nie określił zamkniętego katalogu informacji stanowiących dane osobowe. Dlatego też przy rozstrzyganiu, czy określona informacja lub informacje stanowią dane osobowe, nieuniknione jest, w większości przypadków, dokonanie zindywidualizowanej oceny, przy uwzględnieniu konkretnych okoliczności oraz rodzaju środków czy metod potrzebnych w określonej sytuacji do identyfikacji osoby.

W jakich okolicznościach adres poczty elektronicznej należy zaliczyć do danych osobowych, w rozumieniu przepisów ustawy o ochronie danych osobowych?

Zgodnie z art. 6 ust. 1 ustawy *za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej*. Jednocześnie ust. 2 precyzuje, że *osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne*. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań (art. 6 ust. 3 ustawy).

W myśl art. 6 ust. 1 ustawy za dane osobowe uznaje się zarówno takie informacje, które pozwalają bezpośrednio na określenie tożsamości konkretnej osoby, jak również takie, które nie pozwalają na jej natychmiastową identyfikację, są jednakże przy pewnym nakładzie kosztów, czasu lub działań wystarczające do jej ustalenia. Nie stanowią natomiast danych osobowych takie informacje, na podstawie których nie jest możliwe zidentyfikowanie osoby oraz takie, na podstawie których wprawdzie można byłoby ją zidentyfikować, lecz wiązałyby się to z nadmiernymi kosztami, czasem lub działaniami.

W świetle przywołanego wyżej art. 6 ustawy adres poczty elektronicznej bez żadnych dodatkowych informacji umożliwiających ustalenie tożsamości osoby, co do zasady, nie zalicza się do danych osobowych. Wyjątkiem jest sytuacja, gdy jego elementy pozwalają bez nad-

miernych kosztów, czasu lub działań na ustalenie na ich podstawie tożsamości danej osoby.

Czy dane osób zmarłych podlegają ochronie przewidzianej w ustawie o ochronie danych osobowych?

Ustawa określa zasady postępowania przy przetwarzaniu danych osobowych oraz prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych (art. 2 ust. 1). Stosuje się ją zatem tylko do danych osobowych osób fizycznych. Zgodnie z powszechnie obowiązującą wykładnią osobą fizyczną jest człowiek uczestniczący w stosunkach prawnych. Zdolność prawna człowieka, a tym samym zdolność do bycia podmiotem praw i obowiązków ustaje z chwilą jego śmierci.

Sama ustawa, wśród przesłanek dopuszczalności przetwarzania danych, wymienia zgodę osoby, której dane dotyczą, a także mówi m.in. o sprostowaniu, dostępie do danych czy możliwości sprzeciwu wobec przetwarzania swoich danych. Skorzystać z tego rodzaju uprawnień może jedynie osoba żyjąca.

W związku z powyższym ustawa ma zastosowanie tylko do przetwarzania danych osobowych osób żyjących, a odmowę udzielania informacji na temat osób zmarłych z powołaniem się na ustawę należy uznać za nieuzasadnioną.

W przypadku wykorzystania danych osób zmarłych (np. przesyłania ulotek reklamowych adresowanych do nieżyjącej osoby), osobom bliskim, których dobra osobiste (np. kult pamięci o osobie zmarłej) zostały naruszone, przysługuje prawo wystąpienia z powództwem cywilnym do sądu powszechnego.

Czy informacje o podmiotach prowadzących działalność gospodarczą podlegają ochronie wynikającej z przepisów ustawy o ochronie danych osobowych?

Zgodnie z art. 6 ust. 1 ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Zakresem przedmiotowym ustawy objęte są więc wyłącznie dane dotyczące osób fizycznych. Jej przepisów nie stosuje się natomiast do przetwarzania informacji o innych podmiotach, w szcze-

gólności o osobach prawnych, jednostkach organizacyjnych nieposiadających osobowości prawnej oraz podmiotach prowadzących działalność gospodarczą w oparciu o przepisy ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz.U. nr 173, poz. 1807, ze zm.) w takim zakresie, w jakim dane te identyfikują podmiot w obrocie gospodarczym i ściśle wiążą się z prowadzoną przez niego działalnością gospodarczą.

Powyższe stanowisko prezentowane przez Generalnego Inspektora podzielił również Naczelny Sąd Administracyjny, który w uzasadnieniu wyroku z dnia 28 listopada 2002 r. (sygn. akt II SA 3389/01) stwierdził, że ochrona danych osobowych nie odnosi się do danych indywidualnych, dających się powiązać z podmiotem gospodarczym albo inną osobą prawną lub jednostką organizacyjną niemającą osobowości prawnej, mimo że dane te tworzą wspólnie z danymi osobowymi jedną kategorię danych jednostkowych.

Jednak kluczowe znaczenie dla rozwiązania przedstawionego problemu miała nowelizacja ustawy – Prawo działalności gospodarczej z dnia 19 listopada 1999 r. (Dz.U. nr 101, poz. 1178, ze zm.), na mocy której dodano art. 7a, wyłączający spod ochrony, wynikającej z ustawy o ochronie danych osobowych, dane zawarte w ewidencji działalności gospodarczej. Przepis ten wyraźnie rozstrzygnął kwestię budzącą wcześniej wątpliwości.

W dniu 21 sierpnia 2004 r. weszły w życie przepisy ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz.U. nr 173, poz. 1807), które nie zawierają uregulowania analogicznego do art. 7a ust. 2 ustawy – Prawo działalności gospodarczej.

Należy podkreślić jednak, że zgodnie z art. 66 pkt 2 ustawy z dnia 2 lipca 2004 r. – Przepisy wprowadzające ustawę o swobodzie działalności gospodarczej (Dz.U. nr 173, poz. 1808), art. 7 a ust. 2 ustawy – Prawo działalności gospodarczej zachował moc obowiązującą do dnia 31 grudnia 2006 r. Z kolei art. 1 pkt 2 ustawy z dnia 16 listopada 2006 r. o zmianie ustawy – Przepisy wprowadzające ustawę o swobodzie działalności gospodarczej (Dz.U. nr 225, poz. 1636) przedłużył ten termin do 30 września 2008 r.

Trzeba także podkreślić, że – w myśl art. 24 ust. 1 i 2 ustawy o swobodzie działalności gospodarczej – ewidencja działalności gospodarczej

jest jawna i każdy ma prawo dostępu zarówno do zgromadzonych w niej danych, jak też do przeglądania akt ewidencyjnych przedsiębiorcy.

Jak rozumieć pojęcie „doraźności” użyte w art. 2 ust. 3 ustawy o ochronie danych osobowych?

Artykuł 2 ust. 3 ustawy stanowi, że w odniesieniu do zbiorów danych osobowych sporządzanych doraźnie, wyłącznie ze względów technicznych, szkoleniowych lub w związku z dydaktyką w szkołach wyższych, a po ich wykorzystaniu niezwłocznie usuwanych albo poddawanych anonimizacji, mają zastosowanie jedynie przepisy rozdziału 5 (dotyczące zabezpieczenia zbiorów danych osobowych).

Pojęcie „doraźności” użyte w powyższym artykule jest ocenne, nie-dookreślone – ustawa nie definiuje go. W tej sytuacji konieczne jest odwołanie się do konkretnych okoliczności faktycznych towarzyszących przetwarzaniu przez administratora danych dla określonych, precyzyjnie wskazanych celów. Wykładni art. 2 ust. 3 nie można bowiem dokonywać w sposób abstrakcyjny, nie znając szczegółowo okoliczności przetwarzania danych w konkretnym przypadku. Nie ulega jednak wątpliwości, że istotną rolę w praktycznym rozumieniu tego przepisu odgrywa czynnik czasu, w ciągu którego dane osobowe są przetwarzane. Poza tym konieczne jest rozważenie celu (zadań), któremu służyć ma przetwarzanie danych w określonej strukturze. O ile pierwszy z tych czynników (czas) nie jest z oczywistych powodów ściśle, ustawowo określony (tzn. trudno o wskazanie ścisłych, czasowych granic zbioru doraźnego), o tyle pojęcie doraźności musi być uzależnione od celu przetwarzania danych w zbiorze. Jeżeli dane tworzące określoną strukturę służą realizacji zasadniczego, głównego celu przetwarzania, to trudno uznać tę strukturę za zbiór doraźny. Nie zmienia tego okoliczność, że okres jej przetwarzania jest relatywnie krótki.

Czy jako zbiór danych można zakwalifikować zestaw danych, składający się z aplikacji składanych przez przyszłych pracowników do celów rekrutacji (aplikacje są przechowywane w systemie informacyjnym, przy czym kryterium dostępu do tych informacji jest numer referencyjny bądź nazwa stanowiska, na które dana osoba aplikację złożyła)?

Przez zbiór danych, zgodnie z definicją zawartą w art. 7 pkt 1 ustawy, rozumie się *każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie*. Cechą wyróżniającą zbiór danych od innego ich zestawienia jest jego uporządkowany charakter, co zapewnia możliwość wyszukania konkretnych danych za pomocą określonego kryterium. Aby określony zestaw danych zaklasyfikować jako zbiór w rozumieniu przepisów ustawy, wystarczające jest istnienie jednego kryterium wyszukiwawczego w zestawieniu danych. Z powyższego wynika przysługująca administratorowi danych dowolność w wyborze rodzaju kryterium dostępu, którym, w omawianym przypadku, może być również numer referencyjny. Możliwość wyszukania według powyższego kryterium bądź nazwy stanowiska, na które dana osoba aplikuje, dokumentu zawierającego dane osobowe, przesądza o uporządkowanym charakterze zestawienia danych i tym samym stanowi o zakwalifikowaniu tegoż zestawienia jako zbioru danych w rozumieniu art. 7 pkt 1 ustawy.

Jeżeli osoba przychodzi do Urzędu Miasta, w celu załatwienia swojej sprawy (dotyczącej np. wydania dowodu osobistego, wydania decyzji o warunkach zabudowy, przyznania dodatku mieszkaniowego), to czy urzędnik może uznać, że posiada ona informacje, o których mowa w art. 24 ustawy o ochronie danych osobowych, czy też należy spełnić wobec niej obowiązek informacyjny? Czy podanie danych jest w takim przypadku dobrowolne, czy jest obowiązkiem tej osoby?

Stosownie do art. 24 ust. 1 ustawy w przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o:

1. adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku,
2. celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
3. prawie dostępu do treści swoich danych oraz ich poprawiania,

4. *dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.*

Zgodnie zaś z ust. 2 tego art. ust. 1 nie stosuje się, jeżeli:

1. *przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania,*
2. *osoba, której dane dotyczą, posiada informacje, o których mowa w ust. 1.*

Na mocy art. 24 ust. 2 pkt 2 ustawy administrator danych jest zwolniony z obowiązku wynikającego z art. 24 ust. 1 jedynie wtedy, gdy osoba, której dane dotyczą, posiada wszystkie informacje zawarte w cytowanym ust. 1, a administrator danych ma co do tego pewność. Świadomość ta powinna ponadto mieć charakter obiektywny, a nie jedynie opierający się na subiektywnych odczuciach administratora. Przykładowo można wskazać, że sytuacja taka występuje w szczególności wtedy, gdy zainteresowany „zna administratora danych, orientuje się co do celu zbierania danych, wie, czy jest zobowiązany przepisami prawa do udzielenia informacji” (J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona Danych Osobowych. Komentarz*, Zakamycze 2004). Zakresem zastosowania art. 24 ust. 2 pkt 2 objęte są również te sytuacje, w których administrator danych pozostaje w stałych kontaktach z osobą, której dane dotyczą (A. Drozd, *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy*, Wydawnictwo Prawnicze Lexis Nexis, Warszawa 2004).

Z uwagi na powyższe wskazać należy, iż o zwolnieniu z obowiązku informacyjnego na podstawie omawianego art. 24 ust. 2 pkt 2 ustawy można mówić jedynie wówczas, gdy administrator ma pewność, że osoba, której dane dotyczą, posiada wszystkie informacje wymienione w art. 24 ust. 1.

Należy zaznaczyć, że gdy dochodzi do ponownego zbierania danych (przez tego samego administratora, do tych samych celów), zwłaszcza w niedużym odstępnie czasowym bądź już po raz kolejny, można powołać się na udzielone już wcześniej informacje. Pierwotne zaś poinformowanie powinno nastąpić przed rozpoczęciem zbierania danych, w niezbyt dużym odstępnie czasowym. Istotne jest bowiem, aby informacje były już i jeszcze w świadomości osoby zainteresowanej, w czasie przekazywania danych osobowych.

Trzeba podkreślić, że w sytuacji, gdy obowiązujące przepisy prawa obligują podmiot danych do udostępnienia określonych informacji na swój temat, nie można mówić o dobrowolności ich podania.

Czy niepubliczny zakład opieki zdrowotnej może pozyskać od innych niepublicznych zakładów opieki zdrowotnej – na potrzeby realizacji programu profilaktyki raka piersi – dane osobowe kobiet, bez ich wiedzy, w celu wysłania zaproszeń na bezpłatne badania profilaktyczne?

W pytaniu mowa jest o sytuacji, gdy niepubliczny zakład opieki zdrowotnej przetwarza dane osobowe kobiet, niebędących jego pacjentkami, w celu wysyłania im zaproszeń na bezpłatne badania, np. mammograficzne. Dane te są pozyskiwane w związku z realizacją programu profilaktyki raka piersi od innych niepublicznych zakładów opieki zdrowotnej, z których usług korzystają zapraszane na badania osoby. Jednocześnie zakład opieki zdrowotnej pozyskujący dane nie informuje pacjentek o otrzymaniu ich danych osobowych z innych placówek. Tym samym nie dopełnia obowiązku informacyjnego wynikającego z art. 25 ustawy o ochronie danych osobowych.

Zgodnie z treścią przywołanego przepisu w przypadku, gdy dane osobowe zbierane są nie od osoby, której dane dotyczą, administrator jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych (czyli zapisaniu ich na dowolnym nośniku, np. papierowym, informatycznym, magnetycznym) – m.in. o celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych, jak i źródle pozyskania danych oraz prawach przysługujących osobom, których dane zostały zgromadzone, wynikających z art. 32 ust. 1 pkt 7 i 8 ustawy.

W praktyce Generalnego Inspektora zdarzył się przypadek, że w takiej sytuacji, jak opisana powyżej, zakład opieki zdrowotnej, prowadzący badania profilaktyczne, spełnił obowiązek informacyjny, wynikający z art. 25 ustawy, ale dopiero po przesłaniu zaproszeń na badania profilaktyczne. Spowodowało to u kobiet, które takie zaproszenia otrzymały wątpliwości co do legalności działań tego zakładu. Tymczasem, zgodnie z art. 23 ust. 1 pkt 4 ustawy przetwarzanie danych jest dopuszczalne, gdy jest to niezbędne do wykonania określonych prawem zadań re-

alizowanych dla dobra publicznego. Przepis ten stanowi zatem podstawę prawną przetwarzania danych przez zakład opieki zdrowotnej i jego działanie w tym zakresie jest legalne. Jednak opóźnienie w spełnieniu tego obowiązku powoduje, że osoby, których dane dotyczą, jeszcze przed wykorzystaniem danych nie mają świadomości, że mogą skorzystać ze swoich praw, np. do wniesienia sprzeciwu wobec przetwarzania danych lub żądania zaprzestania ich przetwarzania.

Jakie warunki musi spełnić klauzula zgody, jaką firma zamierza zamieścić w treści umów zawieranych z klientami?

Zgodnie z art. 7 pkt 5 ustawy, przez zgodę *osoby, której dane dotyczą, rozumie się oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.*

Z definicji tej nie wynikają szczegółowe zasady formułowania zgody, jednakże podkreśla się, że z treści 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. Stanowisko takie wyraził także Naczelny Sąd Administracyjny w wyroku z dnia 4 kwietnia 2003 r. (sygn. akt II SA 2135/2002), w którego sentencji zawarł stwierdzenie, iż „Zgoda na przekazywanie danych musi mieć charakter wyraźny, a jej wszystkie aspekty muszą być jasne dla podpisującego w momencie jej wyrażania. Czynności takiej nie konwaliduje późniejsze poinformowanie o treści regulaminu, ani możliwość zgłoszenia zastrzeżeń wobec pewnych form przetwarzania danych”.

Czy prawidłową praktyką jest zamieszczanie w treści umowy zawieranej z klientem klauzuli zgody na przetwarzanie danych osobowych tak, by osoba zgadzająca się na zaproponowane warunki umowy, zgadzała się jednocześnie na przetwarzanie danych w celu wykonania tej umowy lub w innych celach wskazanych przez administratora?

Do Generalnego Inspektora zwracają się osoby, które czują się zmuszane do wyrażania zgody na przetwarzanie ich danych osobowych. Do

takich sytuacji dochodzi najczęściej przy okazji zawierania różnego rodzaju umów. Sprzedawcy lub świadczeniodawcy usług sporządzają kwestionariusze, formularze zawierające w ich treści klauzulę zgody na przetwarzanie danych osobowych. Takie klauzule obejmują zgodę na przetwarzanie danych w celu wykonania zawieranej umowy, a dodatkowo zgodę na przeprowadzanie innych operacji na danych osobowych, np. na ich udostępnianie innym podmiotom, przekazywanie za granicę lub wykorzystywanie w celach marketingowych.

Z takiej konstrukcji klauzuli zgody wynika, że jeśli klient nie zgodzi się na wykorzystywanie jego danych osobowych w sposób określony przez firmę w treści klauzuli, to tym samym nie zgodzi się na ich wykorzystywanie w celu wykonania umowy. Formularze zawierające takie klauzule zgody są przedkładane do podpisu klientom, którzy tym samym, przy okazji wypełniania przygotowanych przez różne firmy formularzy czy druków, są niejako zmuszani do wyrażania zgody na wykorzystywanie ich danych osobowych do określonych w klauzuli zgody celów, pozostając w przekonaniu, że bez jej wyrażenia nie będą mogli skorzystać z produktów lub usług świadczonych przez firmę, czyli nie będą mogli zrealizować umowy.

Tymczasem, zgodnie z ustawą, na wykorzystywanie danych w celu zawarcia lub wykonania umowy zgoda w ogóle nie jest potrzebna. Jednym z podstawowych warunków zgodnego z prawem przetwarzania danych osobowych jest bowiem spełnienie tylko jednego z pięciu warunków określonych w art. 23 ust. 1 ustawy. Zatem, jeśli zgodnie z pkt 3 tego artykułu, wykorzystywanie danych uzasadnia konieczność realizacji umowy, gdy osoba, której dane dotyczą jest jej stroną lub gdy jest to konieczne do podjęcia niezbędnych działań przed zawarciem takiej umowy, to dodatkowe żądanie zgody na przetwarzanie danych w celu realizacji umowy, jest zbędne. Jeśli firma gromadzi dane swojego przyszłego klienta i ma zamiar wykorzystywać je jedynie do celu realizacji umowy, którą z nim zawiera, nie powinna zwracać się o zgodę na przetwarzanie danych. Natomiast, gdyby firma zamierzała wykorzystać dane swoich klientów w innym celu niż do realizacji lub wykonania umowy zawartej z klientem, nie spełniając przy tym żadnego z warunków określonych w art. 23 ust. 1 pkt 2–5 ustawy, o taką zgodę powinna się zwrócić.

Zgodnie z art. 23 ust. 1 pkt 1 ustawy administrator danych jest uprawniony do wykorzystywania danych osobowych, jeśli osoba, której dane dotyczą, wyrazi na to zgodę. Ustawa precyzuje pojęcie zgody. Zgodą (art. 7 pkt 5 ustawy) jest oświadczenie woli pochodzące od osoby, której dane dotyczą, *którego treścią jest zgoda na przetwarzanie danych tego, kto składa to oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.*

Z definicji tej nie wynikają szczegółowe zasady formułowania klauzuli zgody, ale warto podkreślić, że, zgodnie z tą definicją, z treści zgody na przetwarzanie danych osobowych powinno w sposób nie budzący 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. Jednocześnie podkreślenia wymaga czynnik woli osoby wyrażającej zgodę. Oświadczenie o wyrażeniu zgody musi być zgodne z zamiarem osoby. Nie może ona czuć się zmuszona do złożenia oświadczenia o wyrażeniu zgody.

Z powyższego wynika, że podmiot, który przy okazji zawierania umowy zamierza również pozyskać zgodę na przetwarzanie danych osobowych kontrahenta, zobligowany jest do wyodrębnienia stosownego oświadczenia od oświadczenia wyrażającego chęć związania się postanowieniami umowy. Nie można bowiem utożsamiać woli zawarcia umowy ze złożeniem oświadczenia woli, na podstawie którego osoba, której dane dotyczą, zgadza się na wykorzystywanie jej danych osobowych do innych celów.

Powyższe stanowisko Generalnego Inspektora znajduje potwierdzenie zarówno w orzecznictwie sądów administracyjnych, jak i doktrynie. Zgodnie z ugruntowanym w literaturze przedmiotu poglądem: jeżeli osoba zbierająca czy w inny sposób przetwarzająca dane osobowe zwraca się o zgodę, to musi to zostać sformułowane w sposób jednoznaczny i wyróżniać się spośród innych pochodzących od tej osoby informacji i oświadczeń (J. Barta, R. Markiewicz, *Ochrona danych osobowych – komentarz*, Zakamycze 2001, s. 311). Zgodnie z treścią wyroku Naczelnego Sądu Administracyjnego z dnia 19 listopada 2001 r. (sygn. akt II SA 2748/00) „nie ulega wątpliwości, iż celem osoby zawierającej umowę jest chęć nabycia oferowanego produktu za ustaloną opłatą, a nie chęć pozbycia się swojego prawa do ochrony danych osobowych określonego w art. 1 ust. 1 ustawy. Tym samym uznać należy,

że działania osób dokonujących zamówienia jednego z oferowanych przez Spółkę produktów zmierzają do zawarcia stosownej umowy a nie wyrażenia zgody na przetwarzanie dotyczących ich danych osobowych”. W tym samym wyroku NSA stwierdził również, że udostępnienie danych osobowych podmiotom trzecim powinno być odrębnym oświadczeniem woli, nie musi bowiem dana osoba godzić się na udostępnienie swoich danych osobom trzecim. W literaturze przedmiotu prezentowany jest pogląd, że jeśli oświadczenie woli o wyrażaniu zgody na przetwarzanie danych nie obejmowało możliwości udostępnienia danych innemu administratorowi, działanie takie jest niedopuszczalne, bowiem dla udostępnienia danych innym podmiotom konieczna jest dodatkowa zgoda osoby, której dane dotyczą (J. Barta, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Zakamycze 2002, s. 388; S. Grynhoffi, P. Woźny, *Ochrona Danych Osobowych w praktyce*, pkt 2/2, s. 7–11).

Czy mogę zastrzec swoje dane osobowe, jeśli nie chcę, aby jakaś firma przysyłała mi ulotki, reklamujące swoje produkty lub przekazywała moje dane osobowe innym firmom?

Przepisy ustawy nie przewidują możliwości „zastrzeżenia danych osobowych”. Trzeba jednak podkreślić, że w art. 32 ust. 1 pkt 8 każdej osobie, której dane są przetwarzane w zbiorach danych, przyznaje się prawo do kontroli ich przetwarzania. Można je zrealizować poprzez wniesienie sprzeciwu wobec przetwarzania danych osobowych, gdy administrator jako przesłankę legalizującą przetwarzanie danych wskazuje art. 23 ust. 1 pkt 4 i 5 ustawy, gdy zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.

W razie wniesienia sprzeciwu [...] dalsze przetwarzanie kwestionowanych danych jest niedopuszczalne. Administrator danych może jednak pozostawić w zbiorze imię lub imiona i nazwisko osoby oraz numer PESEL lub adres wyłącznie w celu uniknięcia ponownego wykorzystania danych tej osoby w celach objętych sprzeciwem (art. 32 ust. 3 ustawy). W sytuacji nieuwzględnienia przedmiotowego sprzeciwu przez te podmioty, osobie, która z nim wystąpiła, przysługuje prawo wystąpienia do Generalnego Inspektora ze stosowną skargą.

Uprawnienie wynikające z przywołanego art. 32 ust. 1 pkt 8 przysługuje osobie, której dane dotyczą, jedynie względem administratora. Za administratora uważa się – zgodnie z art. 7 pkt 4 ustawy – *organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych*. Skierowanie takiego sprzeciwu skutkuje brakiem możliwości przetwarzania danych osobowych dotyczących osoby z nim występującej wyłącznie przez administratora danych będącego odbiorcą tego sprzeciwu. Nie oznacza to natomiast zakazu przetwarzania danych tej osoby przez innych administratorów posiadających już w prowadzonych przez siebie zbiorach dane osoby wnoszącej sprzeciw. Innymi słowy, sprzeciw skierowany do konkretnego administratora danych nie ma charakteru generalnego i w żaden sposób nie wpływa na przetwarzanie danych przez pozostałych administratorów.

Podkreślenia wymaga to, że wniesienie przedmiotowego sprzeciwu nie jest tożsame z instytucją „zastrzeżenia danych osobowych”. Prawo do wniesienia sprzeciwu nie przysługuje, gdy osoba wyraziła zgodę na przetwarzanie danych przez danego administratora oraz wtedy, gdy możliwość przetwarzania danych wynika z przepisów prawa.

Jakaś firma przysłała mi imiennie adresowane ulotki reklamowe. Nigdy nie byłem klientem tej firmy i nie wyrażałem na to zgody. Nie wiem, do jakich jeszcze celów firma ta wykorzystuje informacje o mnie oraz jakie dane poza moim imieniem, nazwiskiem i adresem posiada. Gdzie mogę się dowiedzieć, w jaki sposób moje dane osobowe trafiły do tej firmy i do czego są wykorzystywane?

Ustawa (art. 32) gwarantuje każdej osobie prawo uzyskania wyczerpującej informacji na temat jej danych osobowych przetwarzanych w zbiorach. Prawo to można zrealizować poprzez zażądanie od podmiotu (ich administratora) wykorzystującego dane osobowe, np. firmy, która nadsyła ulotki reklamowe, informacji odnośnie do ich przetwarzania. Podmiot do którego osoba zwraca się z takim żądaniem, powinien poinformować ją m.in. o źródle informacji, celach, do których je wykorzystuje, zakresie i treści posiadanych danych. Aby taką informację uzyskać, należy wystąpić do firmy nadsyłającej ulotki ze stosownym wnioskiem, którego forma nie jest w ustawie określona.

Obowiązek udzielenia tej informacji przez administratora określony został w art. 33 ustawy. Na jego podstawie powinien on wyjaśnić zainteresowanej osobie jej prawa oraz odpowiedzieć:

- czy zbiór istnieje,
- kto jest jego administratorem (poprzez określenie jego pełnej nazwy i adresu, a gdy jest to osoba fizyczna – jej imienia i nazwiska oraz miejsca zamieszkania),
- od kiedy dane są przetwarzane,
- jakie jest źródło pozyskania danych (chyba że w tym zakresie administrator musi zachować tajemnicę państwową, służbową lub zawodową),
- w jaki sposób dane są udostępniane (w szczególności administrator jest zobowiązany do poinformowania o odbiorcach lub kategoriach odbiorców danych),
- jakie przesłanki przesądziły o podjęciu rozstrzygnięcia wyłącznie w wyniku operacji na danych osobowych prowadzonych w systemie informatycznym,
- w powszechnie zrozumiałej formie, jaka jest treść przetwarzanych danych (należy pamiętać, że nie oznacza to prawa wglądu do dokumentów, a jedynie prawo do informacji o treści danych osobowych).

W szczególności administrator jest obowiązany (art. 33 ust. 1 ustawy) do wskazania w formie zrozumiałej, w terminie 30 dni, a także – jeżeli wnosi o to zainteresowana osoba – na piśmie:

1. *jakie dane osobowe zawiera zbiór,*
2. *w jaki sposób zebrano dane,*
3. *w jakim celu i zakresie dane są przetwarzane,*
4. *w jakim zakresie oraz komu dane zostały udostępnione.*

Udzielenia takiej informacji administrator może odmówić jedynie wtedy (art. 30 ustawy), gdy spowodowałoby to:

1. *ujawnienie wiadomości stanowiących tajemnicę państwową,*
2. *zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego,*
3. *zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa,*
4. *istotne naruszenie dóbr osobistych, osób których dane dotyczą, lub innych osób.*

Aby dowiedzieć się, skąd firma reklamująca swoje produkty pozyskała dane osobowe, jakie dane posiada i do czego je wykorzystuje, należy, realizując swoje prawo do informacji, wystąpić do tej firmy z wnioskiem o wyjaśnienie.

Gdyby pozyskanie tych informacji z jakichś względów stało się utrudnione lub oczekiwana odpowiedź nie zostałaby udzielona, to fakt ten można, w formie skargi, zgłosić do Generalnego Inspektora, który w takich sprawach prowadzi postępowania administracyjne i może nakazać udzielenie żądanych informacji.

Należy pamiętać również (w szczególności dotyczy to podmiotów, do których o informację się zwrócono), że art. 54 ustawy przewiduje odpowiedzialność karną (grzywnę, ograniczenie lub pozbawienie wolności) za niedopełnienie *obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub nieprzekazanie tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w ustawie*. W celu dochodzenia odpowiedzialności karnej konieczne jest skierowanie sprawy na drogę postępowania karnego, czyli do organów ścigania: policji bądź prokuratury.

Chcę pozyskać dane niedotyczące mojej osoby. Czy występując do ich administratora muszę posłużyć się jakimś specjalnym formularzem, czy też dane osobowe powinny zostać mi udostępnione, jeśli zwrócę się o nie zwykłym pismem?

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia wzoru wniosku o udostępnienie danych osobowych, zgłoszenia zbioru danych do rejestracji oraz imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz.U. nr 80, poz. 522, ze zm.) określało wzór wniosku o udostępnienie danych osobowych. Obecnie rozporządzenie to nie obowiązuje, tym samym aktualność utracił formularz wniosku o udostępnienie danych osobowych.

Nowe rozporządzenia wykonawcze do ustawy, które weszły w życie w dniu 1 maja 2004 r., nie określiły wzoru wniosku o udostępnienie danych osobowych, nie ma zatem konieczności stosowania specjalnego formularza. Nie oznacza to jednak, że w przypadku żądania od administratora udostępnienia danych z powołaniem na cel inny niż włączenie

do zbioru, nie zachodzi konieczność złożenia pisemnego wniosku. Obowiązek jego złożenia wynika bowiem z art. 29 ust. 3 ustawy, który stanowi, że *dane osobowe udostępnia się na pisemny umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie*.

W obecnym stanie prawnym nie jest natomiast wymagane, aby wnioskodawca korzystał z konkretnego formularza czy urzędowego druku. Wystarczy, aby wniosek o udostępnienie danych osobowych, składany do administratora, spełniał wymienione powyżej wymagania. Każda pisemna forma jest dopuszczalna, zatem może to być np. list skierowany do administratora danych. Możliwe jest też skorzystanie z nieobowiązującego już formularza wniosku o udostępnienie danych osobowych, zawiera on bowiem wszystkie elementy wymagane w obecnym stanie prawnym. Zniesienie obowiązku stosowania tego formularza miało na celu ułatwienie pozyskania danych tym osobom, które miały trudności z dotarciem do niego.