Joanna Karniol

Gospodarczy wymiar przepływu danych osobowych

- 26 maja 2011 -

Karniol Małecki i Wspólnicy Sp.k.
ul. Świętojerska 5/7, 00-236 Warszawa
Te. +48 22 828 14 60,
e-mail: kancelaria@kmw-adwokaci.pl www.kmw-adwokaci.pl

Spis treści

I. Prawna ochrona danych osobowych

1. Prawa podstawowe

1.1 Konstytucja

Prawo do prywatności jest fundamentalną zasadą państwa demokratycznego, głęboko osadzoną w kulturze europejskiej. Ochrona danych osobowych wywodzi się z tej tradycyjnej wartości. Polska Konstytucja w swoim art. 47 stanowi, że każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.

Art. 51 ustanawia prawo osoby fizycznej do informacyjnego samookreślenia się, przyjmując następujące zasady:

1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.

2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.

3. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.

4. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.

5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.

1.2 Konwencje Międzynarodowe

Polska jest członkiem wszystkich europejskich konwencji międzynarodowych poświęconych ochronie życia prywatnego. Prawo do prywatności jest jedną z fundamentalnych zasad Europejskiej Konwencji Praw Człowieka. Międzynarodowe standardy ochrony danych osobowych określa Konwencja 108 Rady Europy z 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych. Jest to jeden z najstarszych instrumentów poświęconych ochronie danych osobowych.

1.3 Prawo Europejskie

Prawo europejskie poświęca wiele uwagi ochronie danych osobowych. Ustawodawstwo europejskie rozwinęło się na fundamentalnej zasadzie Traktatu Ustanawiającego Wspólnotę Europejską (TWE), tj. na ustanowieniu wspólnego rynku i wprowadzeniu czterech swobód dotyczących przepływu towarów, kapitału, osób i usług. Realizacja tych swobód nie byłaby możliwa bez wprowadzenia zasady swobodnego przepływu danych osobowych na rynku wewnętrznym i ujednolicenia prawa państw członkowskich w zakresie ochrony danych osobowych. Podstawowym instrumentem harmonizacji prawa ochrony danych osobowych państw członkowskich stała się dyrektywa 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (zwana dalej dyrektywą). Nadto, obowiązuje wiele innych aktów prawa wtórnego, w tym dyrektywa o prywatności i łączności elektronicznej, dyrektywa w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnodostępnych usług łączności telefonicznej, dyrektywa w sprawie zobowiązania przewoźników do przekazywania danych pasażerów, rozporządzenie 2001/45/WE o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych.

W odróżnieniu od TWE, Traktaty z Lizbony, Traktat o Unii Europejskiej i Traktat o funkcjonowaniu Unii Europejskiej odnoszą się wyraźnie do ochrony danych osobowych. Traktat o funkcjonowaniu Unii Europejskiej statuuje zasadę, że każda osoba ma prawo do ochrony danych osobowych jej dotyczących oraz kompetencje Parlamentu Europejskiego i Rady w sprawie przyjmowania aktów prawnych dotyczących ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez instytucje, organy, jednostki organizacyjne Unii oraz przez Państwa Członkowskie, a także swobodnego przepływu takich danych. Przestrzeganie tych zasad podlega kontroli niezależnych organów. Warto podkreślić, że zakres obowiązywania prawa europejskiego w dziedzinie ochrony danych osobowych rozszerzy się na współpracę policyjną i sądową.

Zgodnie z Traktatem o Unii Europejskiej zasady ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez Państwa Członkowskie oraz swobodnego przepływu tych danych w ramach wspólnej polityki zagranicznej i bezpieczeństwa będą ustanawiane przez Radę w drodze decyzji.

Ochrona danych osobowych jest też jedną z zasad zawartych w Karcie Praw Podstawowych, która nie będzie w najbliższym czasie obowiązywała na terytorium Rzeczypospolitej Polskiej.

Prawo do prywatności konfrontowane jest z innymi prawami podstawowymi, w tym z prawem do informacji oraz swobodą działalności gospodarczej. Stosowne ustawy i akty prawa europejskiego starają się łagodzić ten konflikt. Szczególną rolę w tym względzie odgrywa ustawa z 29 sierpnia 1997 o ochronie danych osobowych.

2. Ustawa o ochronie danych osobowych z 29 sierpnia 1997r.

Ustawa o ochronie danych osobowych (zwana dalej ustawą) jest pierwszym w Polsce aktem prawnym kompleksowo regulującym zagadnienia ochrony danych osobowych. W myśl Konstytucji ustawa określa zasady i tryb gromadzenia oraz udostępniania informacji. Równocześnie stanowi transpozycję dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.

Przetwarzanie danych osobowych jest też przedmiotem licznych regulacji szczegółowych odnoszących się do poszczególnych dziedzin życia społecznego.

2.1. Zakres stosowania ustawy

Przetwarzanie danych osób fizycznych jest dozwolone, w zasadzie tylko w przypadkach i na warunkach określonych w ustawie. Ustawa określa zasady przetwarzania danych osobowych oraz prawa tych osób fizycznych, których dane są lub mogą być przetwarzane w zbiorach. Ustawę stosuje się do przetwarzania danych osobowych w zbiorach manualnych oraz w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych.

Poza zakresem ustawy pozostają zbiory danych osobowych sporządzone doraźnie, które powstały wyłącznie:

- ze względów technicznych albo,
- ze względów szkoleniowych albo,
- w związku z dydaktyką w szkołach wyższych

Dane osobowe powinny być usunięte albo poddane anonimizacji niezwłocznie po ich wykorzystaniu. Do tych zbiorów stosuje się jednak przepisy rozdziału piątego ustawy dotyczące zabezpieczenia danych osobowych.

Ustawę stosuje się do podmiotów publicznych a do podmiotów niepublicznych, o ile wykonują zadania publiczne albo działalność zarobkową, zawodową lub realizują cele statutowe. Chodzi o podmioty, które mają siedzibę albo miejsce zamieszkania na terytorium Rzeczpospolitej Polskiej albo w państwie trzecim, o ile przetwarzają dane przy pomocy środków technicznych znajdujących się na terytorium Rzeczypospolitej Polskiej. Administratorzy danych osobowych z siedzibą albo miejscem zamieszkania w państwie trzecim mają obowiązek wyznaczyć swojego przedstawiciela w Rzeczpospolitej Polskiej.

Ustawy nie stosuje się do :

- osób fizycznych, które przetwarzają dane wyłącznie w celach osobistych,
- podmiotów z siedzibą lub miejscem zamieszkania w państwie trzecim wykorzystujących środki techniczne znajdujące się w Polsce wyłącznie do przekazywania danych,
- działalności prasowej w rozumieniu przepisów prawa prasowego, działalności literackiej lub artystycznej, chyba że wolność wyrażania swoich poglądów i rozpowszechniania informacji istotnie narusza prawa i wolności osoby, której dane dotyczą. Do tych działalności stosuje się jednak przepisy ustawy dotyczące kontroli Generalnego Inspektora Ochrony Danych Osobowych (GIODO) (art. 14 - 19) i zabezpieczenia danych (art. 36 ust.1).

2.2. Podstawowe pojęcia

Ustawa definiuje różnorodne pojęcia, które następnie pojawiają się w jej tekście, niektóre z nich mają charakter ściśle techniczny, inne pozwalają zrozumieć istotę systemu ochrony danych osobowych. Poniżej przedstawiamy parę podstawowych definicji.

2.2.1. Administrator danych

Administratorem danych jest każda osoba lub jednostka organizacyjna nie mająca osobowości prawnej, podmiot publiczny lub niepubliczny, która decyduje o celach i środkach

przetwarzania danych. Administratorem danych nie jest każdy ich dysponent a tylko ten, który decyduje o celach i środkach ich przetwarzania. Administrator może przekazać dane innej osobie w celu ich przetwarzania w jego imieniu i na jego rzecz. Osoba ta nie stanie się administratorem, o ile nie wykorzysta danych do własnych celów.

Administrator danych musi legitymować się jedną z przesłanek legalności przetwarzania danych. Ciążą na nim obowiązki poinformowania osób o przetwarzaniu ich danych, zabezpieczenia danych, zarejestrowania zbioru i inne.

2.2.2. Dane osobowe

Dane osobowe zostały zdefiniowane jako informacja dotycząca osoby fizycznej zidentyfikowanej lub możliwej do zidentyfikowania.

Chodzi o informacje z różnych dziedzin życia, o ile istnieje możliwość powiązania ich z oznaczoną osobą. Mogą to być informacje obiektywne, subiektywne, wymierne lub ocenne, np. numer PESEL, wykształcenie, poglądy polityczne, przynależność partyjna lub religijna, cechy fizyczne lub fizjologiczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

2.2.3 Przetwarzanie danych

Przetwarzanie danych oznacza jakiekolwiek operacje wykonane na danych osobowych, począwszy od ich pozyskania aż do usunięcia, w tym zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

2.2.4. Zbiór danych

Zbiorem danych osobowych jest każdy posiadający strukturę zestaw danych o charakterze osobowym dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie. W literaturze panuje pogląd, że w celu stosowania przepisów ustawy dotyczących przetwarzania danych w zbiorze wystarczy, by dane były dostępne według jednego kryterium, za wyjątkiem przepisów o odpowiedzialności karnej. W orzecznictwie reprezentowany jest pogląd, że do uznania zestawu danych przetwarzanych przez administratora za zbiór decydujące znaczenie ma wspólny cel przetwarzania danych a nie liczba zastosowanych do przetwarzania systemów

informatycznych. Zdaniem GIODO kryterium dostępu do danych nie musi mieć charakteru osobowego.

2.2.5 Państwo trzecie

Państwo trzecie jest państwem nie należącym do Europejskiego Obszaru Gospodarczego (państwa członkowskie plus Norwegia, Islandia i Lichtenstein).

Przekazywanie danych do państw trzecich podlega dodatkowym ograniczeniom przewidzianym w ustawie. Natomiast zgodnie z prawem europejskim przepływ danych osobowych pomiędzy państwami członkowskimi, nie jest w żaden sposób ograniczony. Przetwarzanie danych osobowych podlega prawu państwa członkowskiego, w którym administrator danych ma siedzibę lub miejsce zamieszkania. Systemy prawne państw członkowskich są w zasadzie zharmonizowane na podstawie dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.

2.3 Zasady przetwarzania danych osobowych – obowiązki administratora

Administrator danych jako podmiot, który decyduje o celach i środkach przetwarzania danych musi stosować się do zasad oraz spełnić wiele obowiązków wynikających z ustawy, które zostały usystematyzowane według następującego schematu:

1) zasada legalności przetwarzania danych (art.23 i art.27),
2) obowiązki informacyjne w stosunku do osób, których dane są przetwarzane (art.24 – 25 , 32-33),
3) zasada jakości danych (art.26),
4) zasada poufności danych – zabezpieczenie danych osobowych (art. 36 -39),
5) obowiązek rejestracji zbioru (art.40),
6) obowiązki przy przekazywaniu danych osobowych do państwa trzeciego (art.47-48).

Wymienione zasady i obowiązki zostaną pokrótce omówione w niniejszym rozdziale.

2.3.1 Zasada legalności przetwarzania danych osobowych

Administrator danych osobowych jest uprawniony do przetwarzania tych danych wyłącznie, na podstawie prawnej określonej w ustawie. W większości przypadków ma on też obowiązek zgłoszenia zbioru danych do rejestracji przed przystąpieniem do ich przetwarzania. Dane osobowe dzielą się na dane zwykłe oraz na dane wrażliwe. Ustawa dopuszcza przetwarzanie danych wrażliwych wyjątkowo po spełnieniu rygorystycznych wymogów, w tym po zarejestrowaniu zbioru.

2.3.1.1 Podstawy prawne przetwarzania danych zwykłych

Ustawa określa pięć równoprawnych przesłanek legalizujących przetwarzanie danych zwykłych, a mianowicie:

1) zgoda osoby, której dane dotyczą, chyba że chodzi o usunięcie tych danych,

2) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,

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 to niezbędne do wykonywania określonych prawem zadań realizowanych dla dobra publicznego,

5) jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Każda z wymienionych przesłanek ma charakter autonomiczny i niezależny, co oznacza, że spełnienie którejkolwiek z nich jest niezbędne do legalizacji przetwarzania danych. Nadto w większości przypadków konieczne jest zgłoszenie zbioru danych osobowych do rejestracji.

2.3.1.1.1 Zgoda osoby, której dane dotyczą

Zgoda na przetwarzanie danych udzielona przez osobę, której dane dotyczą nie wymaga zachowania określonej formy, nie może być jedynie domniemana, ani dorozumiana

z oświadczenia woli o innej treści. Zgoda nie może być ogólna, powinna określać zakres i cel przetwarzania danych. Zgoda może dotyczyć jednego lub wielu administratorów, którzy powinni być wyraźnie wskazani a cel przetwarzania przez nich danych powinien być tożsamy. Zgoda może obejmować przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania danych.

Jeżeli przetwarzanie danych jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą a uzyskanie jej zgody jest niemożliwe, można przetwarzać dane bez zgody tej osoby do czasu gdy uzyskanie zgody okaże się możliwe.

2.3.1.1.2 Uprawnienie lub obowiązek wynikający z przepisu prawa

Komentowana przesłanka legalizacyjna przewiduje:

1) istnienie określonego przepisu prawa, który przyznaje administratorowi danych uprawnienie lub nakłada na niego obowiązek, oraz

2) niezbędność przetwarzania danych dla zrealizowania tego uprawnienia lub spełnienia obowiązku wynikającego z tego przepisu.

Wymogi te powinny być spełnione łącznie.

Uprawnienie lub obowiązek może wynikać z różnych przepisów prawa, które często określają zakres i warunki przetwarzania danych osobowych (np. przepisy ustaw o Policji, Prawa bankowego, Prawa telekomunikacyjnego). Mogą to być również przepisy aktów prawnych niższego rzędu stanowiących zgodnie z art.87 Konstytucji źródła powszechnie obowiązującego prawa (np. przepisy rozporządzenia Ministra Pracy i Polityki Socjalnej dotyczące prowadzenia przez pracodawców dokumentacji związanej ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika).

Zgodnie ze stanowiskiem GIODO, jeżeli przepisy prawa w sposób wyczerpujący oznaczają dane osobowe, które administrator może przetwarzać, zakres ten nie może być wolą stron poszerzany ani zmieniany. Oznacza to, że zgoda osoby, której dane dotyczą, nie może rozszerzyć ani zmienić zakresu danych, które zgodnie z przepisem prawa mogą być przetwarzane. Pogląd ten jest dyskusyjny i nie potwierdzony orzecznictwem sądów administracyjnych.

2.3.1.1.3. Zawieranie i wykonywanie umowy

Zgodnie z tą przesłanką legalizacyjną przetwarzanie danych osobowych jest dozwolone w dwóch sytuacjach:

1) wówczas gdy jest to konieczne do wykonania umowy, której stroną jest osoba, której dane dotyczą, albo

2) wówczas gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą.

Dane osobowe mogą być przechowywane nie dłużej, niż to jest niezbędne do osiągnięcia celu przetwarzania, tj. w tym przypadku do czasu wygaśnięcia roszczeń z tytułu umowy.

Przetwarzanie danych w związku z koniecznymi działaniami podejmowanymi przed zawarciem umowy jest dopuszczalne wyłącznie na żądanie osoby, której dane dotyczą. Chodzi o osobę zainteresowaną zawarciem umowy. Inicjatywa zawarcia umowy nie pochodzi, więc w tym przypadku, od przedsiębiorcy tylko od konsumenta.

2.3.1.1.4 Wykonywanie określonych prawem zadań w interesie publicznym

Omawiana przesłanka odwołuje się do trzech następujących kryteriów jej stosowania, które powinny być spełnione łącznie:

1. Działania w interesie publicznym przy użyciu form niewładczych, np. świadczenie pomocy ofiarom klęsk żywiołowych, świadczenie pomocy społecznej. Do zadań publicznych nie zalicza się organizowania imprez sportowych ani akcji charytatywnych.

2. Zadania publiczne muszą być określone prawem, np. zadania z zakresu bezpieczeństwa publicznego, opieki zdrowotnej, udzielanie pomocy ofiarom klęsk żywiołowych.

3. Przetwarzanie danych musi być niezbędne do wykonywania zadań w interesie publicznym. Niedopuszczalne jest gromadzenie danych na zapas lub na wszelki wypadek w zakresie szerszym, niż jest to potrzebne (np. pobieranie odcisków palców bez potrzeby procesowej, gromadzenie w policyjnych systemach informacyjnych danych osób chorych na AIDS lub nosicieli wirusa HIV.

Osoba, której dane są przetwarzane ma prawo wnieść:

1) pisemne umotywowane żądanie zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację,

2) sprzeciw wobec przetwarzania jej danych, gdy administrator zamierza je przetwarzać w celach marketingowych lub wobec przekazania jej danych osobowych innemu administratorowi.

2.3.1.1.5 Klauzula usprawiedliwionego celu

Jest to przesłanka legislacyjna najczęściej stosowana przez administratorów danych, obok zgody osoby, której dane dotyczą.

Przewiduje, że dozwolone jest przetwarzanie danych, jeżeli jest ono niezbędne do wypełnienia prawnie usprawiedliwionych celów:

1) administratora danych,

2) odbiorcy danych, a nadto

3) przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą (wyważenie interesów osoby, której dane dotyczą i administratora danych lub odbiorcy danych).

Art.23 ust.4 przewiduje, że za prawnie usprawiedliwiony cel uważa się w szczególności:

1) marketing bezpośredni własnych produktów lub usług administratora danych,

2) dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej.

Naczelny Sąd Administracyjny uznał, że klauzula usprawiedliwionego celu w postaci dochodzenia roszczeń z tytułu prowadzonej działalności gospodarczej dopuszcza przetwarzanie danych w związku z cesją wierzytelności konsumenckiej (I OPS 2/05).

Przetwarzanie danych w interesie administratora lub odbiorcy danych musi być niezbędne. Przetwarzanie danych nie będzie więc dopuszczalne, jeżeli interes ten można zaspokoić w inny sposób. Zdaniem Sądu Apelacyjnego w Poznaniu, w sytuacji, gdy ten sam skutek może być osiągnięty przez złożenie oferty w drodze przesyłki bezadresowej, wykorzystanie

do tego celu nazwisk nie jest niezbędne dla osiągnięcia zamierzonego celu. Administrator nie może przetwarzać danych przydatnych, ale niekoniecznych dla realizacji celu, nie może także przechowywać danych dłużej, niż jest to niezbędne dla osiągnięcia celu przetwarzania.

Przetwarzanie danych nie powinno naruszać praw i wolności osoby, której dane dotyczą. Chodzi tutaj o wyważenie interesów administratora danych z jednej strony i osoby, której dane dotyczą.

Osoba, której dane są przetwarzane w zbiorze ma prawo wnieść:

1) pisemne umotywowane żądanie zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację,

2) sprzeciw wobec przetwarzania jej danych, gdy administrator zamierza je przetwarzać w celach marketingowych lub wobec przekazania jej danych osobowych innemu administratorowi.

2.3.1.2 Podstawy prawne przetwarzania danych wrażliwych

Zasadą jest zakaz przetwarzania danych wrażliwych, do których zgodnie z ustawą zalicza się dane dotyczące:

1) pochodzenia rasowego lub etnicznego,

2) poglądów politycznych,

3) przekonań religijnych lub filozoficznych,

4) przynależności wyznaniowej, partyjnej lub związkowej,

5) stanu zdrowia,

6) kodu genetycznego,

7) nałogów,

8) życia seksualnego,

9) skazań, orzeczeń o ukaraniu, mandatów karnych oraz innych orzeczeń.

Ustawa dopuszcza przetwarzanie danych wrażliwych na podstawie jednej z dziesięciu przesłanek wymienionych w art. 27 ust. 2 ustawy, w tym m.in.:

1) pisemna zgoda osoby, której dane dotyczą, chyba że chodzi o usuniecie jej danych,

2) jest to niezbędne do wykonania statutowych zadań kościołów i innych związków wyznaniowych, stowarzyszeń, fundacji lub innych niezarobkowych organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, pod warunkiem, że przetwarzanie danych dotyczy wyłącznie członków tych organizacji lub instytucji albo osób utrzymujących z nimi stałe kontakty w związku z ich działalnością i zapewnione są pełne gwarancje ochrony przetwarzania danych,

3) przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem,

4) przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie,

5) 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.

2.3.2 Obowiązek informacyjny i prawa osoby, której dane dotyczą

2.3.2.1 Obowiązek informacyjny administratora

Administrator danych ma obowiązek przekazać osobie, której dane gromadzi podstawowe informacje na ten temat, przy czym nie jest istotne, czy informacje te mają być włączone do zbioru, czy nie. Zakres informacji zależy od tego, czy gromadzone dane są pozyskiwane od osoby, której dane dotyczą, czy też są pozyskiwane z innych źródeł.

Administrator danych ma obowiązek poinformować osobę, której dane dotyczą o: :

1) swojej nazwie albo imieniu i nazwisku oraz adresie siedziby albo miejsca zamieszkania,

2) celu zbierania danych, a w szczególności znanych mu lub przewidywanych odbiorcach lub kategoriach odbiorów danych,

3) prawie dostępu do treści swoich danych oraz ich poprawienia.

W przypadku zbierania danych osobowych od osoby, której dane dotyczą, administrator musi ponadto poinformować ją o dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

W przypadku zbierania danych osobowych nie od osoby, której one dotyczą administrator danych musi ponadto poinformować osobę, której dane dotyczą o:

1) celu i zakresie gromadzonych danych,

2) źródle danych,

3) o prawie dostępu do treści swoich danych oraz ich poprawienia,

4) o uprawnieniach wynikających z art.32 ust.1 pkt.7 i 8.

Administrator jest zwolniony z informowania osoby, której dane dotyczą, jeżeli posiada ona informacje podlegające notyfikacji.

Ustawa o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych wyłącza stosowanie przepisów ustawy dotyczących obowiązku informacyjnego.

Administrator jest zwolniony z obowiązku informacyjnego wobec osoby, która podała mu swoje dane osobowe, jeżeli przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania.

Takim przepisem szczególnym jest art. 34 ustawy o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu.

W przypadku gromadzenia danych z innych źródeł administrator jest ponadto zwolniony od informowania osoby, której dane dotyczą, jeżeli:

1) przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych, bez wiedzy osoby, której dane dotyczą,

2) dane są niezbędne do badań naukowych, historycznych, dydaktycznych, statystycznych lub badania opinii publicznej, ich przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą, a spełnienie obowiązku informacyjnego wymagałoby nadmiernych nakładów albo zagrażałoby realizacji celu badania,

3) jeżeli dane są przetwarzane przez podmioty publiczne oraz podmioty niepubliczne realizujące zadania publiczne.

Przykładowo zakłady ubezpieczeń oraz detektywi są uprawnieni do pozyskiwania danych osobowych bez wiedzy osób, których dane dotyczą.

2.3.2.2 Prawa osoby, której dane dotyczą

Ustawa przyznała osobom, których dane dotyczą szerokie uprawnienia do kontrolowania swoich danych, jeżeli są one przetwarzane w zbiorze. Można wśród nich wyróżnić uprawnienia:

1) informacyjne (art. 32 ust.1 pkt. 1-5a, art.33),

2) korekcyjne (art. 32 ust. 1 pkt. 6 i 9, art.35),

3) zakazowe (art.32 ust.1 pkt. 7-8, art. 35).

2.3.2.2.1. Uprawnienia informacyjne

Najogólniej, każda osoba może żądać pełnej informacji na temat swoich danych przetwarzanych przez administratora w zbiorze, w tym m. in. informacji o celu, zakresie i sposobie przetwarzania danych, o źródle informacji na temat przedmiotowych danych, o odbiorcach lub kategoriach odbiorców danych.

Osoba zainteresowana może korzystać z prawa do informacji nie częściej niż raz na sześć miesięcy.

Jeżeli osoba zainteresowana zwróci się do Administratora danych o udzielenie jej informacji na piśmie, wówczas administrator powinien jej tych informacji udzielić w terminie 30 dni w formie pisemnej.

Administrator może odstąpić od informowania osób o przetwarzaniu ich danych dla celów naukowych, historycznych, dydaktycznych, statystycznych, lub archiwalnych, w przypadkach, gdy pociągałoby to za sobą nakłady niewspółmierne z zamierzonym celem.

Administrator danych odmówi udzielenia informacji osobom, jeżeli powodowałoby to :

1) ujawnienie informacji niejawnych, albo

2) zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego, albo

3) zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa, albo istotne naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.

2.3.2.2.2. Uprawnienia korekcyjne

Każda osoba, której dane są przetwarzane w zbiorze może żądać m.in. uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane.

Administrator ma obowiązek bez zbędnej zwłoki zastosować się do żądania osoby, której dane dotyczą. W przeciwnym razie osoba ta może zwrócić się do GIODO z wnioskiem o nakazanie administratorowi dopełnienia tego obowiązku. Niezastosowanie się do decyzji GIODO może prowadzić do odpowiedzialności dyscyplinarnej (art.17 ust. 2) a nawet do odpowiedzialności karnej (art. 49 i 50).

Administrator danych ma obowiązek poinformować, bez zbędnej zwłoki innych administratorów, którym udostępnił zbiór danych o dokonanym uaktualnieniu lub sprostowaniu danych.

Ustawy nie stosuje się, jeżeli do uzupełnienia, sprostowania, uaktualnienia danych określonego rodzaju mają zastosowanie przepisy odrębnych ustaw.

2.3.2.2.3. Uprawnienia zakazowe

Jeżeli administrator przetwarza dane osobowe w związku z wykonywaniem określonych zadań w interesie publicznym albo na podstawie klauzuli usprawiedliwionego celu, wówczas osoba, której dane dotyczą ma prawo wnieść:

1) pisemne umotywowane żądanie zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację,

2) sprzeciw wobec przetwarzania jej danych, gdy administrator zamierza je przetwarzać w celach marketingowych lub wobec przekazania jej danych osobowych innemu administratorowi.

W razie wniesienia sprzeciwu dalsze przetwarzanie danych jest niedopuszczalne. Administrator może pozostawić w zbiorze jedynie imiona i nazwisko, PESEL lub adres w celu uniknięcia ponownego wykorzystania danych tej osoby w celach objętych sprzeciwem.

2.3.3. Zasada jakości danych

Zasada jakości danych wyraża się w obowiązkach administratora danych, który winien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą a nadto stosować się ściśle do następujących wymogów:

1) legalności,

2) celowości,

3) merytorycznej poprawności,

4) adekwatności,

5) ograniczenia czasowego.

Z zasad tych wynika, że dane osobowe mogą być przetwarzane wyłącznie zgodnie z obowiązującym prawem, dla określonego celu i niepoddawane dalszemu przetwarzaniu niezgodnemu z tym celem, dane powinny być adekwatne do celu ich przetwarzania (relewantne) oraz poprawne merytorycznie. Dane nie powinny być przetwarzane dłużej, niż to jest niezbędne dla osiągnięcia celu dla jakiego zostały zgromadzone.

Co do zasady, każda osoba powinna być poinformowana o celu i zakresie przetwarzania jej danych przed ich pozyskaniem. Administrator nie jest uprawniony do wykorzystywania i zbierania danych zbędnych (na zapas) do osiągnięcia celu ich przetwarzania.

Zgodnie z orzecznictwem sądów administracyjnych zakres wykorzystywanych danych w związku z wykonywaniem umów może być bardzo różny w zależności od wagi umowy i stopnia ryzyka administratora danych, co do jej prawidłowego wykonania przez konsumenta. Sądy w zasadzie potwierdziły, że praktyka banków przetwarzania danych klientów w szerokim zakresie w związku z udzielonymi im kredytami jest zgodna z zasadą adekwatności, bowiem te umowy obarczone są wysokim ryzykiem administratora danych. NSA stwierdził, że „Generalny Inspektor ani sąd administracyjny nie mogą zastępować ustawodawcy przez ustalenie, jakie dane osobowe możliwe są wyłącznie do przetwarzania przy zawieraniu i wykonywaniu umów kredytowych".

W przypadku zakładów ubezpieczeniowych sądy często stwierdzają nieadekwatność zbieranych danych do celu ich przetwarzania, np. dane dotyczące wykształcenia i stanu cywilnego w związku z ubezpieczeniem OC pojazdów.

Ustawowy katalog danych osobowych (Prawo telekomunikacyjne), które mogą być przetwarzane eliminuje konieczność badania przez GIODO i sąd adekwatności tych danych. Zgodnie z częścią orzecznictwa zgoda osoby na przetwarzanie jej danych w szerszym zakresie, niż to wynika z katalogu ustawowego, upoważnia przedsiębiorcę do przetwarzania tych danych.

Zgoda na przetwarzanie niektórych kategorii danych eliminuje konieczność badania ich adekwatności. Osoba wyrażająca zgodę powinna być poinformowania o celu i zakresie przetwarzania jej danych.

Ustawa przewiduje wyjątek od zasady celowości, a mianowicie dopuszcza przetwarzanie danych w innym celu, niż ten, dla którego zostały zebrane, jeżeli nie narusza to 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.

2.3.4. Zasada rejestracji zbiorów danych osobowych

Administrator danych obowiązany jest zgłosić zbiór danych do rejestracji, oraz zawiadomić o zmianach informacji zawartych w zgłoszeniu (zgłoszenie aktualizacyjne). GIODO prowadzi jawny rejestr zbiorów danych osobowych.

Zgłoszenie zbioru danych zwykłych do rejestru uprawnia administratora do rozpoczęcia przetwarzania danych osobowych. W przypadku danych wrażliwych konieczne jest zarejestrowanie zbioru przed dokonaniem pierwszej czynności przetwarzania danych.

Zgłoszenie aktualizacyjne następuje w terminie 30 dni od dnia dokonania zmiany w zbiorze. Natomiast jeżeli zmiana informacji dotyczącej opisu kategorii osób, których dane dotyczą oraz zakres przetwarzanych danych odnosi się do rozszerzenia zakresu przetwarzanych danych o dane wrażliwe, administrator danych jest obowiązany do jej zgłoszenia przed dokonaniem zmiany w zbiorze..

Ustawa przewiduje długą listę zwolnień od wymogu zgłoszenia zbioru danych osobowych do rejestru, dotyczy to m.in.: zbioru danych osobowych kandydatów do pracy, pracowników i osób świadczących usługi administratorom danych na podstawie umów cywilnoprawnych oraz osób u nich zrzeszonych lub uczących się, zbioru danych przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej, zbioru osób korzystających z usług medycznych administratora, usług notarialnych, adwokackich, radcy prawnego, rzecznika patentowego, doradcy podatkowego lub biegłego rewidenta, zbioru danych powszechnie dostępnych oraz zbioru danych przetwarzanych w zakresie drobnych bieżących spraw życia codziennego.

Należy podkreślić, że zwolnienie z obowiązku zgłoszenia zbioru danych osobowych do rejestru nie oznacza zwolnienia administratora danych z innych obowiązków przewidzianych w ustawie.

GIODO ma następujące kompetencje związane z rejestracją zbiorów danych:

1) wydawanie decyzji administracyjnych w przedmiocie, odmowy rejestracji zbioru danych, odmowy wpisu aktualizacyjnego do rejestru, wykreślenia zbioru danych z rejestru,

2) czynności faktyczne związane z prowadzeniem rejestru, w tym dokonywanie wpisów w rejestrze,

3) wydawanie zaświadczeń o zarejestrowaniu.

W razie odmowy zarejestrowania zbioru danych osobowych, administrator może ponownie zgłosić ten zbiór do rejestracji, ale wówczas przetwarzanie danych będzie dozwolone dopiero po zarejestrowaniu zbioru.

2.3.5 Przekazywanie danych osobowych do państwa trzeciego

Przekazanie danych do państwa trzeciego jest dopuszczalne, jeżeli państwo docelowe daje gwarancję ochrony danych osobowych na swoim terytorium przynajmniej takie, jakie obowiązują na terytorium Rzeczypospolitej Polskiej.

Administrator musi sam ocenić, czy państwo docelowe zapewnia adekwatną ochronę danych osobowych. GIODO nie wydaje w tym względzie żadnych zaświadczeń, ani wiążących interpretacji. Domniemanie adekwatności ochrony danych osobowych stanowi ratyfikowanie konwencji 108 Rady Europy dotyczącej ochrony osób w związku z automatycznym przetwarzaniem danych osobowych.

Nadto, Komisja Europejska wydała decyzje o adekwatności ochrony danych osobowych w niektórych państwach, w tym w Kanadzie, Szwajcarii i Argentynie.

Komisja Europejska wydała też decyzję o adekwatności ochrony przewidzianej przez zasady ochrony prywatności zwane „Zasadami bezpiecznego portu prywatności" oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu USA. Wymienione zasady obowiązują jedynie te podmioty z siedzibą w USA, które dobrowolnie do nich przystąpią i złożą odpowiednie oświadczenie w tym zakresie w Departamencie Handlu USA.

Administrator danych osobowych może przekazać dane osobowe do państwa trzeciego, które nie zapewnia adekwatnej ochrony tych danych, jeżeli zostanie spełniony jeden z wymienionych poniżej warunków:

1) osoba, której dane dotyczą udzieliła na to zgody na piśmie,

2) przekazanie jest niezbędne do wykonania umowy między administratorem danych a osobą, której dane dotyczą, lub jest podejmowane na jej życzenie,

3) przekazanie jest niezbędne do wykonania zawartej umowy w interesie osoby, której dane dotyczą, pomiędzy administratorem danych a innym podmiotem,

4) przekazanie jest niezbędne ze względu na dobro publiczne lub do wykazania zasadności roszczeń prawnych,

5) przekazanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą,

6) dane są ogólnie dostępne.

Jeżeli żaden z wymienionych warunków nie zostanie spełniony przekazanie danych osobowych do państwa trzeciego, które nie zapewnia adekwatnej ochrony może nastąpić po uzyskaniu zgody GIODO pod warunkiem, że administrator danych zapewni odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą.

Administrator danych może zapewnić odpowiednie zabezpieczenia przez zawarcie z odbiorcą danych osobowych umowy, która zawiera klauzule odnoszące się do ochrony danych osobowych. Komisja Europejska wydała na podstawie dyrektywy decyzje, w których sformułowała standardowe klauzule umowne dotyczące przekazywania danych osobowych do państw trzecich, a mianowicie:

1) decyzja 2001/497/WE w sprawie wzorcowych klauzul umownych w związku z przekazywaniem danych osobowych do państw trzecich (...),

2) decyzja 2004/915/WE w zakresie alternatywnego zestawu standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich,

3) decyzja 2002/16/WE w sprawie wzorcowych klauzul umownych w związku z przekazywaniem danych osobowych przetwarzającym w krajach trzecich (...).

Administratorzy danych mogą więc skorzystać z zaproponowanych przez Komisję odpowiednich zestawów klauzul umownych, w zależności od tego, czy przekazują dane

innym administratorom w państwie trzecim, czy też powierzają ich przetwarzanie podmiotom mającym siedzibę w państwie trzecim.

Stosowanie wymienionych klauzul nie jest obowiązkowe, administratorzy mogą zaproponować własne rozwiązania umowne w zakresie ochrony prywatności osób, których dane mają być przekazane do państwa trzeciego.

Jeżeli przekazywanie danych osobowych ma następować w ramach jednej grupy spółek, jednego koncernu, administrator danych może zastosować wiążące reguły korporacyjne.

Grupa Robocza powołana na podstawie art. 29 dyrektywy przyjęła dokument WP 74 zatytułowany „Przekazywanie danych osobowych do krajów trzecich: zastosowanie art. 26 ust. 2 dyrektywy UE w sprawie ochrony danych do wiążących reguł korporacyjnych zobowiązujących przedsiębiorstwa do ich stosowania przy międzynarodowym przepływie danych".

Wiążące zasady korporacyjne są ustalane w ramach poszczególnych koncernów i powinny być możliwe do wyegzekwowania na drodze prawnej. Grupa Robocza w swoim dokumencie nr 108 sformułowała listę kontrolną ze wszystkimi niezbędnymi elementami, które powinny zawierać wiążące reguły korporacyjne.

Europejskie organy ochrony danych osobowych przyjęły procedurę współpracy dotyczącą wspólnego rozpatrywania wniosków o wyrażenie zgody na przekazywanie danych osobowych na podstawie wiążących reguł korporacyjnych (WP 107 przyjęty 14 kwietnia 2005).

Warto dodać, że zgodnie z art. 26 ust. 3 dyrektywy UE państwo członkowskie, które wyda zezwolenie na przekazywanie danych do kraju trzeciego powiadamia o tym komisję i inne państwa członkowskie, co ułatwia wszczęcie stosownej procedury w razie stwierdzenia, że zostało naruszone prawo europejskie.

2.4. Uprawnienia GIODO. Odpowiedzialność

Generalny Inspektor Ochrony Danych Osobowych jest organem nadzorczym w rozumieniu dyrektywy, uprawnionym m.in. do kontroli zgodności przetwarzania danych osobowych z obowiązującym prawem w tym zakresie.

GIODO ma szerokie kompetencje w zakresie stosowania przepisów ustawy, w tym do najważniejszych należą:

1) wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych,

2) prowadzenie jawnego rejestru zbiorów danych osobowych,

3) kontrola zgodności przetwarzania danych z przepisami o ochronie danych osobowych.

GIODO z urzędu lub na wniosek osoby zainteresowanej nakazuje w drodze decyzji administracyjnej przywrócenie stanu zgodnego z prawem, w tym:

1) udostępnienie lub nie danych osobowych,

2) sprostowanie lub uzupełnienie danych,

3) wstrzymanie przekazywania danych za granicę,

4) zastosowanie dodatkowych środków zabezpieczających dane osobowe,

5) usunięcie danych osobowych.

GIODO wydaje też zaświadczenia np. potwierdzające zarejestrowanie zbioru danych osobowych.

W zasadzie postępowanie w sprawach uregulowanych w ustawie prowadzi się według przepisów kodeksu postępowania administracyjnego. Oznacza to, że strona niezadowolona z decyzji GIODO może zwrócić się do tego organu o ponowne rozpatrzenie sprawy. Na decyzję GIODO w sprawie wniosku o ponowne rozpatrzenie sprawy, stronie niezadowolonej przysługuje skarga do sądu administracyjnego, tj. do Wojewódzkiego Sądu Administracyjnego i ewentualnie skarga kasacyjna do Naczelnego Sądu Administracyjnego.

W razie stwierdzenia, że doszło do naruszenia prawa przez osoby odpowiedzialne, reprezentujące administratora danych GIODO kieruje zawiadomienie o popełnieniu przestępstwa, dołączając dowody dokumentujące podejrzenie.

Nadto, inspektorzy działający w imieniu GIODO mogą, na podstawie ustaleń kontroli, żądać wszczęcia postępowania dyscyplinarnego lub innego przewidzianego prawem postępowania

przeciwko osobom winnym dopuszczenia do uchybień. Inspektorzy mogą też żądać poinformowania ich w określonym terminie o wynikach postępowania i o podjętych działaniach.

GIODO może nałożyć w celu przymuszenia grzywnę na podmioty, które nie wykonują jego decyzji administracyjnych.

Wysokość takiej grzywny w stosunku do osoby fizycznej wynosi maksymalnie 10.000 zł a w stosunku do osoby prawnej oraz jednostki organizacyjnej nieposiadającej osobowości prawnej 50 000 zł. W przypadku jednak wielokrotnego nakładania grzywien w jednym postępowaniu egzekucyjnym ich łączna kwota nie będzie mogła przekraczać: 50 000 zł w odniesieniu do osób fizycznych oraz 200 000 zł w odniesieniu do osób prawnych i jednostek organizacyjnych nieposiadających osobowości prawnej.

W odniesieniu do niektórych zbiorów danych kontrola GIODO została znacznie ograniczona. Chodzi o zbiory, w których dane:

1) zawierają informacje niejawne,

2) albo zostały uzyskane w wyniku czynności operacyjno - rozpoznawczych przez uprawnionych do tych czynności funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego oraz Centralnego Biura Antykorupcyjnego,

3) albo dotyczą osób należących do kościoła lub innego związku wyznaniowego, o uregulowanej sytuacji prawnej i są przetwarzane na potrzeby tego kościoła lub innego związku wyznaniowego.

W odniesieniu do takich zbiorów nie stosuje się przepisów art. 12 pkt. 2, 14 pkt. 1, 3-5 oraz art. 15-18.

NSA wielokrotnie zwracał uwagę, że GIODO nie jest uprawniony do merytorycznej oceny zagadnień cywilnoprawnych. Kwestia ta pojawiła się na tle przetwarzania danych osobowych w związku z przelewem wierzytelności konsumenckiej. Sąd nie podzielił stanowiska GIODO o niedopuszczalności przetwarzania danych osobowych konsumentów przez nabywców

wierzytelności w celu realizacji ich roszczeń wobec konsumentów. Sąd stwierdził, że GIODO nie może ingerować w sferę stosunków cywilnoprawnych, w tym przypadku dokonywać oceny ważności przelewu wierzytelności, do tego bowiem jest uprawniony wyłącznie sąd powszechny.

Ustawa nie przewiduje żadnych przepisów dotyczących odpowiedzialności cywilnej. Bezprawne przetwarzanie danych osobowych może rodzić odpowiedzialność cywilną na gruncie kodeksu cywilnego, z tytułu naruszenia dóbr osobistych albo z tytułu deliktu.

Ustawa przewiduje odpowiedzialność karną administratora będącego osobą fizyczną albo osoby reprezentującej administratora będącego osobą prawną lub jednostką organizacyjną nie mającą osobowości prawnej w zakresie ochrony danych osobowych za nieprzestrzeganie zasad ochrony danych osobowych, w tym za:

1) przetwarzanie danych osobowych, których przetwarzanie jest niedopuszczalne,

2) przetwarzanie zbioru danych osobowych przez osobę nieuprawnioną,

3) udostępnianie lub umożliwianie dostępu do danych osobom nieupoważnionym,

4) naruszenie obowiązku zabezpieczania danych osobowych przed zabraniem, uszkodzeniem lub zniszczeniem,

5) niezgłoszenie do rejestracji zbioru danych osobowych

6) niedopełnienie obowiązku poinformowania osoby, której dane dotyczą o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w ustawie.

II. Zagadnienia szczegółowe, istotne w obrocie gospodarczym

1. Dane pracownicze, dane o kandydatach do pracy

Pracodawca jest administratorem danych pracowników oraz kandydatów do pracy. W zasadzie powinien on unikać przetwarzania tych danych na podstawie ich zgody. Istniejący między pracownikiem a pracodawcą stosunek podporządkowania, skłania do podejrzeń, że pracownik nie odmówi zgody pracodawcy, co z kolei wyklucza w wielu przypadkach swobodę składania oświadczenia woli o wyrażeniu zgody.

NSA w wyroku z 13 lutego 2003 r. stwierdził, że wyrażenie zgody na badania za pomocą wykrywacza kłamstw prowadzone przez pracodawcę stawia pod znakiem zapytania swobodę tej zgody.

Właściwą podstawą do przetwarzania danych pracowników jest realizacja uprawnienia lub spełnienie obowiązku wynikającego z przepisów prawa. Kodeks pracy uprawnia pracodawców do żądania od osób ubiegających się o zatrudnienie oraz od pracowników podania imienia (imion) i nazwiska, imion rodziców, daty urodzenia, miejsca zamieszkania, adresu do korespondencji, wykształcenia oraz przebiegu dotychczasowego zatrudnienia. Nadto, pracodawca może domagać się od pracownika również innych danych osobowych, a także imion i nazwisk oraz dat urodzenia dzieci pracownika, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy. Pracodawca może żądać od pracownika podania numeru PESEL. Pracodawca może także żądać od pracownika podania jeszcze innych danych, jeżeli obowiązek ich podania wynika z odrębnych przepisów (np. z przepisów ustawy o systemie ubezpieczeń społecznych).

Pracodawca nie ma prawa żądać od pracowników innych danych, niż to wynika z kodeksu pracy, takie żądanie mogłoby zostać uznane za godzące w godność i inne dobra osobiste a nawet za praktykę dyskryminacyjną. Jeżeli pracownik lub kandydat do pracy poda spontanicznie dane, których pracodawca nie ma prawa żądać, nie będzie to oczywiście traktowane jako naruszenie prawa.

Podstawą do przetwarzania danych jest przede wszystkim, wynikający z kodeksu pracy, obowiązek pracodawcy prowadzenia dokumentacji w sprawach związanych ze stosunkiem pracy oraz akt osobowych pracowników. Niedopełnienie tego obowiązku skutkować może odpowiedzialnością w postaci grzywny (art. 94 pkt 9a kodeksu pracy). Zagadnienia dotyczące dokumentacji pracowniczej zostały szczegółowo uregulowane w rozporządzeniu Ministra Pracy i Polityki Socjalnej w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika. W kwestionariuszu osobowym stanowiącym załącznik do wymienionego rozporządzenia mieści się o wiele więcej danych niż w przepisach kodeksu pracy, np. numer NIP, obywatelstwo, zainteresowania, stosunek do służby wojskowej. Pracodawca może jednak żądać tych danych, bowiem wynika to z odrębnych przepisów.

Pracodawca może przetwarzać także dane osobowe pracowników nie wynikające z odpowiednich przepisów kodeksu pracy, nie może ich jednak żądać od pracownika. Podstawy do przetwarzania takich danych mogą wynikać z konieczności realizacji umowy o pracę albo z klauzuli uzasadnionego celu administratora danych.

Ustawa o ochronie danych osobowych dopuszcza przetwarzanie danych wrażliwych pracowników i kandydatów do pracy oraz innych osób zatrudnionych na podstawie umów cywilnoprawnych, pod następującymi warunkami, które muszą być spełnione łącznie:

1) jest to niezbędne do wykonywania zadań administratora danych odnoszących się do zatrudnienia, i

2) zakres przetwarzanych danych jest określony w ustawie.

Przykładem może być przetwarzanie danych dotyczących przynależności partyjnej, jeżeli jest to niezbędne ze względu na wymóg apolityczności na określonym stanowisku pracy. Prawo żądania od kandydata informacji o stanie zdrowia wynika z przepisów dotyczących urzędników państwowych i samorządowych. Ustawa o związkach zawodowych przewiduje możliwość przetwarzania danych o przynależności związkowej pracowników i innych zatrudnionych. Zgodnie z ustawą o Krajowym Rejestrze Karnym prawo uzyskania informacji o osobach notowanych w tym rejestrze przysługuje pracodawcom w zakresie niezbędnym dla zatrudnienia pracownika, co do którego z przepisów ustawy wynika wymóg niekaralności, korzystania z pełni praw publicznych, a także ustalenia uprawnienia do zajmowania określonego stanowiska, wykonywania określonego zawodu lub prowadzenia określonej działalności gospodarczej. Zdaniem GIODO przepisy kodeksu pracy wyłączają możliwość przetwarzania danych o karalności pracownika na podstawie jego pisemnej zgody.

Pracodawca jest zwolniony z obowiązku rejestrowania zbioru danych m.in. kandydatów do pracy, pracowników i innych osób zatrudnionych na podstawie umowy cywilnoprawnej. Musi on jednak stosować się do wszystkich pozostałych zasad przetwarzania danych osobowych przewidzianych ustawą.

2. Dane osobowe przedsiębiorców

Ochrona danych osobowych przedsiębiorców jest ograniczona zasadą jawności obrotu gospodarczego. Oznacza to, że dane osobowe dostępne w jawnych rejestrach (ewidencja

działalności gospodarczej, KRS) mogą być wykorzystane dla potrzeb obrotu gospodarczego. Przetwarzanie tych danych w innych celach poddane jest rygorom ustawy.

3. Dane osobowe klientów

Marketing bezpośredni własnych produktów lub usług stanowi prawnie usprawiedliwiony cel realizowany przez administratora danych. Ustawa dopuszcza więc przetwarzanie danych klientów bez ich zgody w tym celu. Administrator danych ma jednak obowiązek poinformować klienta o przetwarzaniu jego danych, a klient ma prawo wnieść sprzeciw wobec przetwarzania tych danych. W razie wniesienia sprzeciwu dalsze przetwarzanie kwestionowanych danych jest niedopuszczalne. Nadto, zgodnie z ustawą o świadczeniu usług drogą elektroniczną zakazane jest przesyłanie niezamówionej informacji handlowej skierowanej do oznaczonego odbiorcy za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej. Również ustawa o ochronie niektórych praw konsumenta zabrania posługiwania się telefonem, wizjofonem, telefaksem, pocztą elektroniczną, automatycznym urządzeniem wywołującym lub innym środkiem komunikacji elektronicznej w celu złożenia propozycji zawarcia umowy (w tym zaproszenia do składania ofert) bez uprzedniej zgody konsumenta. Zgoda klienta jest więc konieczna w celu przesyłania mu drogą elektroniczną informacji handlowej.

Wykorzystywanie adresów i numerów telefonów w celach marketingowych bez znajomości imienia i nazwiska nie będzie stanowiło naruszenia przepisów o ochronie danych osobowych, chociaż może naruszać prawo do prywatności. NSA w wyroku z 10 sierpnia 2005 stwierdził, że wysyłanie SMS-ów dotyczących referendum unijnego do wszystkich abonentów danego operatora nie jest przetwarzaniem danych osobowych.

Zgodnie z orzecznictwem zgoda na przetwarzanie danych osobowych musi być wyraźna. Nie spełnia tego wymagania podpisanie oświadczenia o wyrażeniu zgody na przetwarzanie danych, stanowiącego dodatkowy element innego zobowiązania nie zawierającego informacji o celach i zakresie przetwarzania danych.

Umieszczanie we wzorach umów oświadczenia o wyrażeniu zgody na przetwarzanie danych jest praktyką błędną. Wykorzystanie danych osobowych w celu wykonania umowy nie wymaga zgody osoby zainteresowanej, jest to odrębna przesłanka przetwarzania danych. Zgoda nie jest również wymagana w celu marketingu własnych produktów lub usług.

W sytuacjach, gdy zgoda osoby, której dane dotyczą jest wymagana (np. na obrót bazami danych osobowych), powinna być odrębnym oświadczeniem woli a nie częścią regulaminu lub wzorca umownego. Dodatkowo przetwarzanie danych w kilku celach powinno być przedmiotem odrębnych oświadczeń.

III. Wykaz aktów prawnych

1. Konstytucja Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 roku
2. Europejska Konwencja Praw Człowieka i podstawowych wolności z dnia 4 listopada 1950 roku
3. Konwencja 108 Rady Europy sporządzona w Strasburgu dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych
4. Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską podpisany w Lizbonie dnia 13 grudnia 2007 r. zamieszczony na stronie: http://eur-lex.europa.eu/pl/treaties/dat/12007L/htm/12007L.html
5. Traktat ustanawiający Wspólnotę Europejską z dnia 25 marca 1957 roku
6. Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych
7. Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych
8. Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)
9. Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE

10. Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 roku w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej

11. Dyrektywa Parlamentu i Rady WE z dnia 8 czerwca 2000 w sprawie niektórych aspektów prawnych usług w społeczeństwie informacyjnym, a w szczególności handlu elektronicznego w obrębie wolnego rynku (2000/31/WE)

12. Decyzja Komisji z dnia 15 czerwca 2001 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich, na mocy dyrektywy 95/46/WE (2001/497/WE)

13. Decyzja Komisji z dnia 27 grudnia 2001 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych przetwarzającym dane mającym siedzibę w państwach trzecich, na mocy dyrektywy 95/46/WE (2002/16/WE)

14. Decyzja Komisji z dnia 26 lipca 2000 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie właściwej ochrony danych osobowych w Szwajcarii (2000/518/WE)

15. Decyzja Komisji z dnia 26 lipca 2000 r. przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach "bezpiecznej przystani" oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu USA (2000/520/WE)

16. Decyzja Komisji z dnia 20 grudnia 2001 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie odpowiedniej ochrony danych osobowych zapewnionej w ustawie kanadyjskiej o ochronie informacji osobowych i dokumentów elektronicznych (2002/2/WE)

17. Decyzja Komisji z dnia 30 czerwca 2003 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie właściwej ochrony danych osobowych w Argentynie (2003/490/WE)

18. Dokument roboczy WP 74 pt.: "Przekazywanie danych osobowych do krajów trzecich: zastosowanie art. 26 ust. 2 dyrektywy UE w sprawie ochrony danych w odniesieniu do

wiążących reguł korporacyjnych zobowiązujących przedsiębiorstwa do ich stosowania przy międzynarodowym przepływie danych"; zamieszczony na stronie: http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2003_en.htm

19. Dokument roboczy WP 108 przyjęty w dniu 14 kwietnia 2005 roku oraz dokument roboczy WP 107 przyjęty w dniu 14 kwietnia 2005 roku zamieszczone na stronie: http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm

20. Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy

21. Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny

22. Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika

23. Ustawa z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną

24. Ustawa z dnia 16 lipca 2004 roku Prawo telekomunikacyjne

25. Ustawa z dnia z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji

26. Ustawa z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów

27. Ustawa z dnia 23 sierpnia 2007 roku o przeciwdziałaniu nieuczciwym praktykom rynkowym

28. Ustawa z dnia 2 marca 2000 roku o ochronie niektórych praw konsumentów oraz odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny.