Dorota Fleszer

Zakres przetwarzania danych osobowych w działalności gospodarczej

ABC
a Wolters Kluwer business

Dorota Fleszer

Zakres przetwarzania danych osobowych w działalności gospodarczej

ABC
a Wolters Kluwer business

Warszawa 2008

Stan prawny na 1 kwietnia 2008 r.

Wydawca
Izabella Małecka

Redaktor prowadzący
Joanna Fitt

Skład i łamanie
Rafał Rudziński, Faktoria Wyrazu Sp. o.o.

ISBN: 978-83-7601-206-3

ISBN PDF-a: 978-83-264-5392-2

Wydane przez:
Wolters Kluwer Polska Sp. z o.o.

Redakcja Książek

01-231 Warszawa, ul. Płocka 5a
tel. (022) 535 80 00

31-156 Kraków, ul. Zacisze 7
tel. (012) 630 46 00

e-mail: ksiazki@wolterskluwer.pl

www.wolterskluwer.pl
księgarnia internetowa www.profinfo.pl

SPIS TREŚCI

WYKAZ SKRÓTÓW

I. Źródła prawa

k.c.	–	ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz. U. Nr 16, poz. 93 z późn. zm.)
Konstytucja RP	–	Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483 z późn. zm.)
k.p.a.	–	ustawa z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (tekst jedn. Dz. U. z 2000 r. Nr 98, poz. 1071 z późn. zm.).
p.d.g.	–	ustawa z dnia 19 listopada 1999 r. – Prawo działalności gospodarczej (Dz. U. Nr 101, poz. 1178 z późn. zm.); uchylona, obowiązuje art. 7–7i do 30 września 2008 r.
pr. bank.	–	ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (tekst jedn. Dz. U. z 2002 r. Nr 72, poz. 665 z późn. zm.)
u.d.i.p.	–	ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. Nr 112, poz. 1198 z późn. zm.)
u.e.l.d.o.	–	ustawa z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych (tekst jedn. Dz. U. z 2006 r. Nr 139, poz. 993 z późn. zm.)
u.KRS	–	ustawa z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym (tekst jedn. Dz. U. z 2007 r. Nr 168, poz. 1186 z późn. zm.)
u.o.d.o.	–	ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.)
u.s.d.g.	–	ustawa z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (tekst jedn. Dz. U. z 2007 r. Nr 155, poz. 1095 z późn. zm.)
u.ś.u.d.e.	–	ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. Nr 144, poz. 1204 z późn. zm.)

II. Organy i instytucje

GIODO	–	Generalny Inspektor Ochrony Danych Osobowych
NSA	–	Naczelny Sąd Administracyjny

SA – Sąd Apelacyjny
SKO – Samorządowe Kolegium Odwoławcze
SN – Sąd Najwyższy
TK – Trybunał Konstytucyjny
WSA – Wojewódzki Sąd Administracyjny

III. Periodyki

Dz. U. – Dziennik Ustaw
Dz. Urz. – Dziennik Urzędowy
Dz. Urz. UE L – Dziennik Urzędowy Unii Europejskiej, seria L
GP – Gazeta Prawna
M. Pod. – Monitor Podatkowy
M. Praw. – Monitor Prawniczy
ODO – Ochrona Danych Osobowych. Biuletyn Administratorów Bezpieczeństwa Informacji
OI – Ochrona Informacji
ONSA – Orzecznictwo Naczelnego Sądu Administracyjnego
OSA – Orzecznictwo Sądów Apelacyjnych
OSNC – Orzecznictwo Sądu Najwyższego Izby Cywilnej
OSNKW – Orzecznictwo Sądu Najwyższego. Izba Karna i Wojskowa
OSNP – Orzecznictwo Sądu Najwyższego. Izba Pracy, Ubezpieczeń Społecznych i Spraw Publicznych
OSP – Orzecznictwo Sądów Polskich
OSS – Orzecznictwo w Sprawach Samorządowych
OTK – Orzecznictwo Trybunału Konstytucyjnego
OTK-A – Orzecznictwo Trybunału Konstytucyjnego; zbiór urzędowy, Seria A
ONSA – Orzecznictwo Naczelnego Sądu Administracyjnego
Pal. – Palestra
PiP – Państwo i Prawo
PPH – Przegląd Prawa Handlowego
Pr. Bank. – Prawo Bankowe
Pr. Spółek – Prawo Spółek
PUG – Przegląd Ustawodawstwa Gospodarczego
Rzeczposp. – Rzeczpospolita
Sam. Teryt. – Samorząd Terytorialny
Wok. – Wokanda

WSTĘP

Problematyka ochrony danych osobowych jest stosunkowo nową dziedziną prawa. Jej powstanie wiąże się z coraz większym i powszechniejszym wykorzystywaniem systemów informatycznych praktycznie w każdej dziedzinie życia. Najwięcej obaw rodził fakt stosunkowo łatwego gromadzenia w nich ogromnych ilości danych, informacji i następnie ich dowolnego zestawiania.

W Polsce do czasu wejścia w życie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych nie było aktu prawnego, który w sposób kompletny regulowałby kwestie związane z ochroną danych osobowych osoby fizycznej. Wobec tego zastosowane w niej rozwiązania prawne nie mogły mieć oparcia w polskich doświadczeniach i powstałym w tym zakresie orzecznictwie. Wpływ na treść ustawy miały więc przede wszystkim odpowiednie regulacje międzynarodowe, a zwłaszcza Konwencja Nr 108 Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (Dz. U. z 2003 r. Nr 3, poz. 25) oraz Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady Unii Europejskiej z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (Dz. Urz. UE L Nr 281 z dnia 23 listopada 1995 r.).

W ustawie zostały zdefiniowane nie tylko prawa osób, których dane są przetwarzane, ale także szczegółowo określone zasady postępowania przy przetwarzaniu danych osobowych.

Niezależnie od tego został powołany organ państwowy do spraw ochrony danych osobowych – Generalny Inspektor Ochrony Danych Osobowych. Do jego zadań należy m.in. kontrola zgodności przetwarzania danych z przepisami ustawy o ochronie danych osobowych oraz inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych.

Ustawodawca dostrzegł konieczność wyraźnego określenia obowiązków administratorów danych związanych z prowadzonym przez nich

procesem przetwarzania danych. Wyznaczył tym samym zasady postępowania z danymi osobowymi, które zawsze muszą być przez administratora danych przestrzegane. Obejmują one nie tylko samo przetwarzanie danych, ale także dbałość o ich jakość i przekazanie osobie, której dane podlegają przetwarzaniu, odpowiednich informacji z nim związanych. Tym samym, opierając się na stosownych regulacjach ustawowych, można określić obiektywnie model postępowania administratora danych z danymi osobowymi. Podejmowanie działań z nim sprzecznych oznacza naruszenie przepisów ustawy o ochronie danych osobowych. Przedmiot obowiązków administratorów danych ani sposób ich realizacji nie zostały zróżnicowane ze względu na kategorię podmiotu będącego administratorem danych. W równym stopniu zobowiązanymi do ich wykonania są podmioty publiczne, jak i prywatne.

Dla dokonania wyczerpującej analizy problematyki zakresu przetwarzania danych osobowych w działalności gospodarczej konieczne jest wcześniejsze wyjaśnienie głównych założeń publicznoprawnej ochrony danych osobowych w obowiązującym stanie prawnym. Omówione zostaną podstawowe założenia ustawy, jej terminologia oraz zasady szczególnej staranności, którymi kierować się ma administrator danych, wyznaczając zakres przetwarzanych danych osobowych i wykonując operacje na nich. Wpływ na treść i zakres przetwarzanych danych ma również osoba, której dane dotyczą, dzięki realizacji przyznanych jej praw do kontroli przetwarzania danych.

W sferze działalności gospodarczej informacje o charakterze osobowym mają coraz większe znaczenie. Przedsiębiorcy zainteresowani są nimi z dwóch powodów. Po pierwsze, postępująca globalizacja i konieczność zdobywania nowych rynków zbytu oraz ciągła walka o uzyskanie i podtrzymanie pozycji na rynku czyni wręcz niezbędnym posiadanie jak największej ilości i kategorii danych osobowych potencjalnych klientów celem poznania ich preferencji i dostosowania do nich oferty. Takie wykorzystywanie danych jest powszechnie utożsamiane z prowadzeniem marketingu bezpośredniego czy też z obrotem zbiorami danych, co budzi negatywne skojarzenia. Znajomość danych osobowych konsumentów jest niezbędna także choćby dla przewidzianej prawem realizacji nawiązanych zobowiązań umownych czy też wyegzekwowania roszczeń z tytułu prowadzenia działalności gospodarczej. Po drugie, odgrywa ona zasadniczą rolę w uzyskaniu przewagi na rynku i tym samym przyczynia się do powstania sukcesu gospodarczego; znajomość danych dotyczących

innych przedsiębiorców działających na rynku jako potencjalnych konkurentów ułatwia poznanie ich słabych i mocnych stron. Niezależnie od powyższego przedsiębiorca to także kontrahent, od którego oczekujemy sprawnego i szybkiego zrealizowania transakcji gospodarczej i który powinien dawać rękojmię uczciwości i pewności. Wobec tego niezwykle istotną sprawą staje się możliwość uzyskania o nim określonych informacji w tym zakresie.

Problemem związanym z ustaleniem zakresu przetwarzania danych osobowych przedsiębiorcy jest stały wzrost liczby informacji, które w myśl stosownych przepisów szczególnych są danymi jawnymi, powszechnie dostępnymi. Nie oznacza to jednak, że wszystkie dane osobowe przedsiębiorcy będącego osobą fizyczną są dostępne i wyłączona jest możliwość zachowania prywatności w takim zakresie, w jakim związana jest ona z prowadzeniem działalności gospodarczej. Jawność danych osobowych przedsiębiorcy wyłączona została ze względu na tajemnicę bankową, tajemnicę przedsiębiorcy, tajemnicę skarbową i tajemnicę postępowania administracyjnego.

Zagadnienie zakresu przetwarzania danych osobowych konsumenta wiąże się z kolei z koniecznością zachowania proporcjonalności pomiędzy koniecznością skutecznego zrealizowania transakcji gospodarczej a nadmiernym i zbędnym ingerowaniem w prywatność. Wyznaczanie zakresu przetwarzania danych konsumenta jest ściśle związane z okolicznością przetwarzania danych osobowych, na podstawie której następuje legalizowanie operacji przetwarzania danych osobowych.

Zakres przetwarzanych danych osobowych podlega stałemu rozszerzaniu. Dotyczy to zarówno podmiotów działających w sferze publicznej, jak i prywatnej. Brak jednocześnie jasno określonych unormowań mających wpływ na ograniczanie tego negatywnego zjawiska. Również przepisy ustawy o ochronie danych osobowych nie zawierają norm, które w sposób kompletny i wyczerpujący odnosiłyby się do zasad ustalania zakresu przetwarzania danych osobowych w działalności gospodarczej. W powstałym do tej pory dorobku doktryny i orzecznictwa fragmentarycznie analizowano poszczególne elementy mające wpływ na ustalenie zakresu przetwarzania danych osobowych w działalności gospodarczej. Brak natomiast całościowego opracowania, w którym zostałyby omówione wszystkie aspekty wpływające na ustalenie kategorii danych osobowych, które powinny być przetwarzane w działalności gospodarczej, i reguł ich wyznaczania. Ze względu na szeroki zakres zagadnienia oraz

różnorodność jego aspektów podstawowym problemem badawczym będzie usystematyzowanie pod względem przedmiotowym powstałego orzecznictwa sądów i Generalnego Inspektora Ochrony Danych Osobowych.

Podstawowa metoda badawcza zastosowana w pracy to metoda dogmatyczna. Podsumowaniem pracy są wnioski *de lege lata* i *de lege ferenda*, w których wskazano na konieczność dalszej modyfikacji systemu prawnego dotyczącego zakresu przetwarzania danych osobowych w działalności gospodarczej.

Rozdział I

PODSTAWY PRAWNE OCHRONY DANYCH OSOBOWYCH

1. Ochrona danych osobowych w Unii Europejskiej

1.1. Konwencja Nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych

Państwa zachodniej części Europy po latach podziałów rozpoczęły budowę wspólnoty. Proces ten zainicjowano stworzeniem wspólnego rynku gospodarczego, na którym miał mieć miejsce swobodny przepływ towarów usług, osób i kapitału. Szybko jednak zorientowano się, że tak określony cel nie może być realizowany tylko przez wykorzystanie środków gospodarczych i ekonomicznych bez ingerencji w sferę praw i wolności osób, zwłaszcza w ich życie prywatne. Tendencja do integracji ekonomiczno-społecznej krajów Unii Europejskiej, a w konsekwencji globalizacja informacji (w tym również danych osobowych), wymiana danych pomiędzy państwami członkowskimi, duża szybkość przepływu danych i ich praktycznie powszechna dostępność ujawniły nowe problemy w zakresie ochrony danych osobowych, co z kolei spowodowało dyskusję na temat potrzeby wprowadzenia odpowiednich uregulowań prawnych i pogodzenia prawa do prywatności ze stale rozwijającym się rynkiem wewnętrznym Unii Europejskiej.

Najważniejszym aktem prawnym w zakresie danych osobowych w skali międzynarodowej jest Konwencja Nr 108 Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych. Konwencja jest aktem prawnym wiążącym państwa będące jej stronami. Weszła w życie z dniem 1 października 1985 r., po tym jak ratyfikowało ją 5 państw (Francja, RFN, Norwegia, Hiszpania i Szwecja). Polska ratyfikowała Konwencję 24 kwietnia 2002 r.

Konwencja oddziałuje jedynie w sferze publicznoprawnej, nie wywołuje natomiast żadnych skutków prawnych bezpośrednio po stronie obywateli krajów, które ją ratyfikowały. Niemniej tworzy ona pewien konsensus w zakresie ochrony danych, z którym zmierzyć się muszą uregulowania przyjmowane w krajach europejskich, aczkolwiek chodzi tu o minimalny poziom ochrony. Zachęca ona kraje nieposiadające regulacji na tym polu do wydawania odpowiednich przepisów, ukierunkowując prace legislacyjne w tym zakresie i pozostawiając pewien margines swobody w kształtowaniu rozstrzygnięć odpowiadających danemu systemowi prawa. Konwencja bierze pod uwagę istniejące już w niektórych państwach rozstrzygnięcia prawne i stara się wprowadzić pewien wspólny poziom ochrony oraz nie tworzyć bariery dla wykorzystania nowoczesnej techniki informacyjnej i komunikacyjnej; okoliczności te są szczególnie istotne, jeśli zważy się fakt, iż Konwencja zajmuje się także kwestią przekazywania danych pomiędzy krajami[1]. Brak w Konwencji m.in. regulacji dotyczących sposobu wykonywania operacji na danych, takich jak np. ich pozyskiwanie, udostępnianie, przechowywanie i niszczenie. Kwestie te pozostawiono do uregulowania przez odpowiednie przepisy krajowe.

Konwencja, zawierając „minimum konwencyjne", wyznacza w ogólnym zarysie standardy ochrony danych. Każde z państw członkowskich w swym prawie krajowym zobowiązane jest wprowadzić stosowne środki prawne niezbędne do ich urzeczywistnienia. Środki takie mają być podjęte najpóźniej w dniu wejścia w życie Konwencji w stosunku do danego państwa. Poszczególne państwa członkowskie mogą, zgodnie z art. 11 Konwencji, ustanowić dalej idące środki ochrony[2].

Zgodnie z art. 1 Konwencji jej celem jest zapewnienie każdej osobie fizycznej, bez wzg lędu na narodowość lub miejsce zamieszkania, poszanowania jej prawa do prywatności w związku z automatycznym przetwarzaniem dotyczących jej danych osobowych („ochrona danych").

Według definicji zawartej w art. 2 lit. a) Konwencji termin „dane osobowe" oznacza każdą informację dotyczącą osoby fizycznej o określonej tożsamości lub dającej się zidentyfikować („osoba, której dane dotyczą"). Zatem, jak zauważa A. Mednis, cechą odróżniającą omawiane

[1] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Zakamycze, Kraków 2004, s. 70–71.

[2] A. Mednis, *Prawna ochrona danych osobowych*, Scholar, Warszawa 1995, s. 22.

dane od innych informacji dotyczących osób jest brak anonimowości. Innymi słowy, informacja ma charakter osobowy, dopóki jest możliwe ustalenie tożsamości osoby, której ona dotyczy[3].

Przez „automatyczne przetwarzanie" stosownie do art. 2 lit. c Konwencji należy rozumieć następujące operacje wykonane w całości lub części przy pomocy metod zautomatyzowanych: gromadzenie danych, stosowanie do nich operacji logicznych i/lub arytmetycznych, ich modyfikowanie, usuwanie, wybieranie lub rozpowszechnianie. Natomiast w myśl art. 2 lit. b Konwencji „zbiór zautomatyzowany" oznacza każdy zbiór danych będących przedmiotem automatycznego przetwarzania. Tym samym ochroną objęte są dane osobowe niezależnie od sposobu i struktury ich uporządkowania pod warunkiem jednak, że operacje na nich dokonywane są za pomocą procedur zautomatyzowanych. Należy zauważyć, że dla powstania zbioru danych nie jest niezbędne jego uporządkowanie. Wobec powyższego rację należy przyznać A. Mednisowi wskazującemu, że Konwencja może mieć zastosowanie w przypadku każdej informacji osobowej przetwarzanej automatycznie niezależnie od tego, czy występuje ona pojedynczo czy w zbiorze, oraz do danych osobowych przetwarzanych ręcznie, jeśli występują w zbiorze i o ile dane państwo rozciągnęło ochronę na zbiory ręczne[4].

Zobowiązanym do stosowania postanowień Konwencji zgodnie z jej art. 2 lit. d jest „administrator zbioru danych". Jest nim osoba fizyczna lub prawna, władza publiczna, agencja lub każdy inny organ właściwy na podstawie przepisów prawa wewnętrznego do określania celu, któremu ma służyć zautomatyzowany zbiór danych osobowych, kategorii gromadzonych danych osobowych oraz sposobu przetwarzania, jakiemu będą poddawane.

Konwencja daje państwom ją podpisującym, stosownie do regulacji art. 3, możliwość ograniczenia lub poszerzenia jej stosowania przez złożenie Sekretarzowi Generalnemu Rady Europy stosownego oświadczenia. Jego treścią może być:

1) wyłączenie stosowania Konwencji do niektórych kategorii zautomatyzowanych kartotek danych osobowych, zgodnie z załączoną listą. Nie można na niej umieścić zautomatyzowanych kartotek danych

[3] A. Mednis, *Ochrona danych osobowych w Konwencji Rady Europy i Dyrektywie Unii Europejskiej*, PiP 1996, z. 6, s. 34.

[4] A. Mednis, *Ochrona danych osobowych w Konwencji Rady Europy i Dyrektywie Unii Europejskiej*, cz. I, ODO 2000, nr 1, s. 11.

osobowych, które w myśl prawa wewnętrznego podlegają przepisom o ochronie danych osobowych;
2) deklaracja stosowania przepisów Konwencji wobec informacji dotyczących ugrupowań, stowarzyszeń, fundacji, spółek handlowych, korporacji i wszelkich innych podmiotów, w których skład wchodzą bezpośrednio lub pośrednio osoby fizyczne, niezależnie od posiadania osobowości prawnej;
3) stosowanie Konwencji również do zbiorów danych osobowych, które nie są przetwarzane automatycznie.

W myśl art. 5 Konwencji: „Dane osobowe będące przedmiotem automatycznego przetwarzania powinny być:
a) pozyskiwane oraz przetwarzane rzetelnie i zgodnie z prawem;
b) gromadzone dla określonych i usprawiedliwionych celów i nie mogą być wykorzystywane w sposób niezgodny z tymi celami;
c) odpowiednie, rzeczowe, niewykraczające poza potrzeby wynikające z celów, dla których są gromadzone;
d) dokładne i w razie potrzeby uaktualniane;
e) przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez okres nie dłuższy niż jest to wymagane ze względu na cel, dla którego dane zgromadzono.

Konwencja w art. 6 formułuje tryb postępowania ze szczególnymi kategoriami danych: „Dane osobowe ujawniające pochodzenie rasowe, poglądy polityczne, przekonania religijne lub inne, jak również dane osobowe dotyczące stanu zdrowia lub życia seksualnego nie mogą być przetwarzane automatycznie, chyba że prawo wewnętrzne zawiera odpowiednie gwarancje ochrony. To samo stosuje się do danych dotyczących skazujących wyroków karnych."

Regulacja art. 8 Konwencji przewiduje dodatkowe prawa osób, których dane są przetwarzane. Zgodnie z jej brzmieniem każda osoba powinna mieć zapewnione prawo do:
a) ustalenia, czy istnieje zautomatyzowany zbiór danych osobowych, zawierający dane jej dotyczące, poznania podstawowych celów jego utworzenia, a także tożsamości, miejsca zamieszkania lub siedziby administratora tego zbioru;
b) otrzymania, w rozsądnych odstępach czasu i bez nadmiernej zwłoki oraz nadmiernych kosztów, potwierdzenia obecności danych jej do-

tyczących w zautomatyzowanym zbiorze oraz do uzyskania, w czytelnej formie, wglądu do tych danych;

c) uzyskania możliwości sprostowania lub usunięcia danych jej dotyczących, jeżeli zostały one przetworzone z naruszeniem przepisów prawa wewnętrznego zapewniających przestrzeganie zasad ustanowionych w art. 5 i 6 Konwencji;

d) złożenia skargi w przypadku odmowy odpowiedzi na żądanie potwierdzenia obecności w zbiorze lub odmowy wglądu do danych jej dotyczących, sprostowania lub usunięcia tych danych, w myśl zasad określonych w punktach b i c.

Artykuł 7 Konwencji zobowiązuje do podjęcia odpowiednich środków bezpieczeństwa w odniesieniu do danych osobowych zgromadzonych w zbiorach zautomatyzowanych, aby zapobiec przypadkowemu zniszczeniu lub zniszczeniu bez zezwolenia albo przypadkowemu zagubieniu, jak również aby zapobiec niepowołanemu dostępowi do danych oraz ich zmienianiu lub rozpowszechnianiu bez upoważnienia.

1.2. Dyrektywa 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych

Ustawodawstwo wewnętrzne poszczególnych państw dotyczące ochrony danych osobowych, powstałe w dużej części po przyjęciu Konwencji Nr 108, okazało się bardzo zróżnicowane. Stało się to problemem utrudniającym utworzenie wspólnego rynku wewnętrznego, w którym miałby odbywać się swobodny przepływ towarów, osób, usług, kapitału – także danych osobowych pomiędzy państwami przy zapewnionej ochronie prywatności.

Dyrektywy to akty prawne, niemające odpowiednika w prawie polskim, skierowane do państw członkowskich, wskazujące cel, który muszą osiągnąć za pomocą dostępnych sobie środków[5].

Według M.T. Tinnefeld dyrektywy zobowiązują podmioty odpowiedzialne za przetwarzanie danych dla celów publicznych i gospodarczych do orientowania się na prawa podstawowe osoby, której dane dotyczą,

[5] D. Bogucka, *Co będzie nas obowiązywało,* GP z dnia 29 stycznia 2003 r. Organy państw członkowskich nie mogą wymagać od swoich obywateli postępowania zgodnego z dyrektywą. Dopiero przepisy krajowe wydane na podstawie dyrektyw stanowią źródło praw i obowiązków dla osób fizycznych i prawnych.

oraz do zastosowania wszystkich wymaganych zabezpieczeń, aby chronić dane także w obrocie międzynarodowym. Mają one na celu ułatwienie obrotu danymi osobowymi na terenie Wspólnoty przez harmonizację regulacji prawnych w ramach wspólnego rynku. Na zewnątrz służą stabilizacji tego obrotu i równocześnie chronią przed naruszeniem sformułowanych we Wspólnocie zasad[6].

Dyrektywy kierowane są wyłącznie do państw członkowskich. Nie wynikają z nich żadne prawa ani obowiązki dla osób prawnych i fizycznych. Państwo jest zobowiązane w swoim prawie wewnętrznym zrealizować wymagania dyrektywy, przy czym z reguły obojętna jest forma ich realizacji. Dyrektywa nie należy więc do *self-executing law*. Może ona być stosowana bezpośrednio jedynie w wypadku, gdy upłynął termin jej realizacji, a państwo nie dokonało jej implementacji lub dokonana implementacja jest wadliwa[7].

Ze względu na przedmiot regulacji należy wymienić następujące dyrektywy:

1) Dyrektywę 95/46/WE Parlamentu Europejskiego i Rady Unii Europejskiej z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (Dz. Urz. L Nr 281 z 23 listopada 1995 r. str. 31);
2) Dyrektywę 97/66/WE Parlamentu Europejskiego i Rady Unii Europejskiej z dnia 15 grudnia 1997 r. w sprawie przetwarzania danych osobowych i ochrony prywatności w sektorze telekomunikacyjnym (Dz. Urz. L. Nr 24 z 30 stycznia 1998 r. s. 1);
3) Dyrektywę 2000/31/WE Parlamentu i Rady Unii Europejskiej z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług w społeczeństwie informacyjnym, a w szczególności handlu elektronicznego w obrębie wolnego rynku (Dz. Urz. UE L Nr 178 z dnia 17 lipca 2000 r.);
4) Dyrektywę 2002/58/WE Parlamentu Europejskiego i Rady Unii Europejskiej z dnia 12 lipca 2002 r. w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej (Dz. Urz. UE L Nr 201 z dnia 31 lipca 2002 r.).

---

[6] M.T. Tinnefeld, *Ochrona danych – kamień węgielny budowy Europy* (w:) *Ochrona danych osobowych*, red. M. Wyrzykowski, Instytut Spraw Publicznych, Warszawa 1999, s. 43–44.

[7] http://www.giodo.gov.pl/234/j/pl/

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady Unii Europejskiej z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych wyznacza zasady ochrony podstawowych praw i wolności osób fizycznych, a w szczególności ich prawa do prywatności w odniesieniu do przetwarzania danych osobowych.

Regulacje Dyrektywy mają za cel:

1) zabezpieczenie jednolitego minimalnego poziomu ochrony prywatności osób fizycznych w związku z przetwarzaniem danych osobowych zawartych w zbiorach danych;
2) zapewnienie możliwości swobodnego przepływu danych osobowych pomiędzy krajami członkowskimi[8].

Według terminologii zawartej w art. 2 lit. a Dyrektywy „dane osobowe" oznaczają wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej („osoby, której dane dotyczą"); osoba możliwa do zidentyfikowania to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, szczególnie przez powołanie się na numer identyfikacyjny lub jeden bądź kilka szczególnych czynników określających jej fizyczną, fizjologiczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość. Zatem, jak stwierdza A. Mednis, na gruncie Dyrektywy informacją o charakterze osobowym może być każda informacja dotycząca konkretnej osoby, którą można zidentyfikować. Innymi słowy, informacja ma charakter osobowy dopóty, dopóki jest możliwe ustalenie tożsamości osoby[9]. Jeżeli w ramach społeczeństwa informacyjnego ma znaczenie rozwój technik gromadzenia, przekazywania, kompilowania, rejestrowania, przechowywania i przesyłania danych dźwiękowych i obrazowych osób fizycznych, Dyrektywa powinna mieć zastosowanie do przetwarzania takich danych (pkt 14 preambuły Dyrektywy). Przedmiotem ochrony przewidzianej w Dyrektywie nie są dane osób prawnych.

Zakres przedmiotowy Dyrektywy wyznaczony został regulacją art. 3 i dotyczy przetwarzania danych osobowych w całości lub w części w sposób zautomatyzowany oraz innego przetwarzania danych osobowych, stanowiących część zbioru lub mających stanowić część zbioru. Z kolei „przetwarzanie danych osobowych" w rozumieniu art. 2 lit. b Dyrektywy oznacza każdą operację lub zestaw operacji dokonywanych na da-

[8] J. Barta i in., *Ochrona danych osobowych*..., s. 90.

[9] A. Mednis, *U nas i gdzie indziej*, Rzeczposp. z dnia 21 stycznia 1995 r.

nych osobowych za pomocą środków zautomatyzowanych lub innych, jak np. gromadzenie, rejestracja, porządkowanie, przechowywanie, adaptacja lub modyfikacja, odzyskiwanie, konsultowanie, wykorzystywanie, ujawnianie przez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, układanie lub kompilowanie, blokowanie, usuwanie lub niszczenie danych. Regulacje Dyrektywy wymieniają etap samego gromadzenia (zbierania) danych jako element ich przetwarzania. Konsekwencją takiego ujęcia jest to, że objęcie ochroną następuje już w chwili ich gromadzenia, o ile dane te mają figurować w zbiorze lub mają być przetwarzane automatycznie[10].

W porównaniu do odpowiednich postanowień Konwencji, Dyrektywa w art. 2 lit. c precyzyjniej formułuje pojęcie „zbioru danych". Jest to „każdy uporządkowany zestaw danych osobowych, dostępnych według określonych kryteriów, scentralizowanych, zdecentralizowanych lub rozproszonych funkcjonalnie lub geograficznie".

Podmiotem obowiązków przewidzianych w Dyrektywie jest administrator danych. Stosownie do art. 2 lit. d Dyrektywy jest nim osoba fizyczna lub prawna, władza publiczna, agencja lub inny organ, który samodzielnie lub wspólnie z innymi podmiotami określa cele i sposoby przetwarzania danych; jeżeli cele i sposoby przetwarzania danych są określane w ustawach i przepisach wykonawczych krajowych lub przepisach Wspólnoty, administrator danych może być powoływany lub kryteria jego powołania mogą być ustanawiane przez ustawodawstwo krajowe lub ustawodawstwo Wspólnoty.

Na zasady legalnego przetwarzania składają się zasady dotyczące jakości danych i kryteria legalności przetwarzania danych.

Zasady dotyczące jakości danych określa art. 6 Dyrektywy, przewidujący obowiązek zapewnienia, aby dane osobowe były:

a) przetwarzane rzetelnie i zgodnie z prawem;
b) gromadzone do określonych, jednoznacznych i legalnych celów oraz nie były poddawane dalszemu przetwarzaniu w sposób niezgodny z tym celem. Dalsze przetwarzanie danych dla celów historycznych, statystycznych i naukowych nie będzie uważane za niezgodne z przepisami pod warunkiem stworzenia przez państwa członkowskie odpowiednich zabezpieczeń. Jak wynika z pkt 28 preambuły

[10] A. Mednis, *Ochrona danych osobowych w Konwencji Rady Europy i Dyrektywie Unii Europejskiej (cz. I)*, ODO 2000, nr 1, s. 12.

Dyrektywy, „(...) cele takie muszą być jednoznaczne i uzasadnione oraz określone w czasie gromadzenia danych; potrzeby dalszego przetwarzania danych dla potrzeb ich gromadzenia nie mogą być niezgodne z pierwotnie określonymi celami";

c) prawidłowe, stosowne oraz nienadmierne ilościowo w stosunku do celów, dla których zostały zgromadzone i/lub dalej przetworzone;
d) prawidłowe oraz w razie konieczności aktualizowane; należy podjąć wszelkie uzasadnione działania, aby zapewnić usunięcie lub poprawienie nieprawidłowych lub niekompletnych danych, biorąc pod uwagę cele, dla których zostały zgromadzone lub dla których są dalej przetwarzane;
e) przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez czas nie dłuższy niż jest to konieczne dla celów, dla których zostały zgromadzone lub dla których są dalej przetwarzane. Państwa członkowskie stworzą odpowiednie zabezpieczenia dla danych przechowywanych przez dłuższe okresy dla potrzeb historycznych, statystycznych i naukowych.

Obowiązek realizacji zasad dotyczących jakości danych zgodnie z art. 6 ust. 2 Dyrektywy ciąży na administratorze danych.

Kryteria legalności przetwarzania danych sformułowane zostały w art. 7 Dyrektywy. Muszą one zostać spełnione, aby miało miejsce przetwarzanie danych. Stosownie zatem do tego przepisu przetwarzanie danych jest dopuszczalne tylko wówczas, gdy:

a) osoba, której dane dotyczą, jednoznacznie wyraziła zgodę lub
b) przetwarzanie danych jest konieczne dla realizacji umowy, której stroną jest osoba, której dane dotyczą lub w celu podjęcia działań na życzenie osoby, której dane dotyczą przed zawarciem umowy lub
c) przetwarzanie danych jest konieczne dla wykonania zobowiązania prawnego, któremu administrator danych podlega lub
d) przetwarzanie danych jest konieczne dla ochrony żywotnych interesów osoby, której dane dotyczą lub
e) przetwarzanie danych jest konieczne dla realizacji zadania wykonywanego w interesie publicznym lub dla sprawowania władzy publicznej, przekazanej administratorowi danych lub osobie trzeciej, przed którą ujawnia dane lub
f) przetwarzanie danych jest konieczne dla potrzeb wynikających z uzasadnionych interesów administratora danych lub osoby trze-

ciej, przed którą ujawnia się dane, z wyjątkiem sytuacji, kiedy interesy takie podporządkowane są interesom związanym z podstawowymi prawami i wolnościami osoby, której dane dotyczą, a które gwarantują ochronę na podstawie art. 1 ust. 1 dyrektywy.

Większe wymagania Dyrektywa stawia w art. 8 wobec legalnego przetwarzania szczególnych kategorii danych, tj. ujawniających pochodzenie rasowe lub etniczne, opinie polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych, danych dotyczących zdrowia i życia płciowego. Wymienione kategorie danych obejmują szczególne informacje dotyczące sfery intymnej człowieka. Generalnie ich przetwarzanie jest zakazane, z wyjątkiem sytuacji, gdy:

a) osoba, której dane dotyczą, udzieliła wyraźnej zgody na przetwarzanie tych danych, chyba że ustawodawstwo państwa członkowskiego przewiduje, że zakaz nie może być uchylony mimo zgody udzielonej przez osobę, której dane dotyczą;
b) przetwarzanie danych jest konieczne do wypełnienia obowiązków i szczególnych uprawnień administratora danych w dziedzinie prawa pracy, o ile jest to dozwolone przez prawo krajowe przewidujące odpowiednie zabezpieczenia;
c) przetwarzanie danych jest konieczne dla ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby w przypadku, gdy osoba, której dane dotyczą, jest osobą fizycznie lub prawnie niezdolną do udzielenia zgody;
d) przetwarzanie danych dokonywane jest w ramach legalnej działalności wspartej odpowiednimi gwarancjami przez fundację, stowarzyszenie lub inną niekomercyjną instytucję, której cele mają charakter polityczny, filozoficzny, religijny lub związkowy, pod warunkiem że przetwarzanie danych odnosi się wyłącznie do członków tej instytucji lub osób mających z nią regularny kontakt, w związku z jej celami i dane nie zostaną ujawnione osobie trzeciej bez zgody osób, których dane dotyczą;
e) przetwarzanie dotyczy danych, które są podawane do wiadomości publicznej przez osobę, której dane dotyczą, lub jest konieczne do ustalenia, wykonania lub ochrony roszczeń prawnych.

Stosownie do art. 8 ust. 3 Dyrektywy można przetwarzać szczególne kategorie danych, jeśli jest to wymagane dla celów medycyny prewen-

cyjnej, diagnostyki medycznej, świadczenia opieki lub leczenia lub też zarządzania opieką zdrowotną, jak również w przypadkach, gdy dane są przetwarzane przez podmiot służby zdrowia zgodnie z przepisami prawa krajowego lub zasadami określonymi przez właściwe krajowe instytucje podlegające obowiązkowi zachowania tajemnicy zawodowej lub przez inną osobę, również zobowiązaną do zachowania tajemnicy. Zgodnie z art. 8 ust. 5 Dyrektywy przetwarzanie danych dotyczących przestępstw, wyroków skazujących lub środków bezpieczeństwa może być dokonywane jedynie pod kontrolą władz publicznych lub też jeżeli zgodnie z prawem krajowym ustanowiono odpowiednie środki zabezpieczające, z zachowaniem odstępstw, które państwo członkowskie może udzielić zgodnie z obowiązującymi przepisami krajowymi, zapewniając zachowanie odpowiednich zabezpieczeń. Jednak kompletny rejestr przestępstw kryminalnych, jak stanowi art. 8 ust. 5 Dyrektywy, może być prowadzony tylko pod kontrolą władzy publicznej.

W art. 10 Dyrektywy na administratora danych został nałożony obowiązek informacyjny. Jego wykonanie ma zapewnić osobie zainteresowanej wiedzę, przez kogo, jakie i w jakim celu jej dane są przetwarzane, z wyjątkiem przypadku, kiedy posiada już ona takie informacje, dotyczące:

a) tożsamości administratora danych i ewentualnie jego przedstawiciela;
b) celów przetwarzania danych, do których dane są przeznaczone;
c) wszelkich dalszych informacji, jak odbiorcy lub kategorie odbiorców danych; tego, czy odpowiedzi na pytania są obowiązkowe czy dobrowolne oraz jakie są ewentualnie konsekwencje nieudzielenia odpowiedzi; istnienie prawa wglądu do swoich danych oraz ich sprostowania.

Jak bowiem wynika z pkt 38 preambuły Dyrektywy: „Jeżeli przetwarzanie danych ma być rzetelne, osoba, której dane dotyczą, musi mieć możliwość dotarcia do informacji o wystąpieniu czynności przetwarzania danych oraz, jeżeli dane są uzyskiwane od niej, musi otrzymać dokładne i pełne informacje, uwzględniające okoliczności pozyskiwania danych".

Z kolei art. 11 ust. 1 Dyrektywy stanowi, że w przypadku, gdy dane są uzyskiwane z innych źródeł niż osoba, której dane dotyczą, państwa członkowskie zapewnią, aby administrator danych lub jego przedstawiciel był zobowiązany od początku gromadzenia danych osobowych lub w przypadku ujawnienia danych osobie trzeciej nie później niż do momentu, gdy dane są ujawniane po raz pierwszy, dostarczyć osobie,

której dane dotyczą, co najmniej następujące informacje, z wyjątkiem przypadku, kiedy posiada już ona takie informacje: a) tożsamość administratora danych i ewentualnie jego przedstawiciela; b) cele przetwarzania danych; c) wszelkie dalsze informacje, jak np. kategorie potrzebnych danych; odbiorcy lub kategorie odbiorców danych; istnienie prawa wglądu do swoich danych oraz ich sprostowania, o ile dalsze informacje są konieczne, biorąc pod uwagę szczególne okoliczności, w których dane są gromadzone, w celu zagwarantowania rzetelnego przetwarzania danych w stosunku do osoby, której dane dotyczą. Obowiązek przekazania wymienionych informacji nie powstaje, zgodnie z art. 11 ust. 2 Dyrektywy, gdy, szczególnie w przypadku przetwarzania danych dla celów statystycznych, historycznych lub naukowych, dostarczenie takich informacji wymagałoby niewspółmiernie dużego wysiłku lub jeżeli gromadzenie lub ujawnianie informacji jest wyraźnie przewidziane przez prawo. W takich przypadkach państwa członkowskie zapewnią odpowiednie zabezpieczenia.

Dyrektywa w art. 12 gwarantuje każdej osobie prawo dostępu do swoich danych. Polega ono na prawie do uzyskania od administratora danych:

a) bez ograniczeń, w odpowiednich odstępach czasu oraz bez nadmiernego opóźnienia lub kosztów:
   - potwierdzenia, czy dotyczące jej dane są przetwarzane oraz co najmniej informacji o celach przetwarzania danych; kategoriach danych oraz odbiorcach lub kategoriach odbiorców, którym dane te są ujawniane;
   - zawiadomienia w zrozumiałe formie o danych przechodzących przetwarzanie oraz posiadanych informacjach o ich źródłach;
   - wiadomości na temat zasad automatycznego przetwarzania dotyczących jej danych przynajmniej w przypadku zautomatyzowanego procesu decyzyjnego;
b) odpowiednio, możliwości sprostowania, usunięcia lub zablokowania danych, których przetwarzanie jest niezgodne z postanowieniami Dyrektywy, szczególnie ze względu na niekompletność lub niedokładność danych;
c) zawiadomienia osób trzecich, którym dane zostały ujawnione, o ewentualnym sprostowaniu, usunięciu lub zablokowaniu danych zgodnie z lit. b, o ile nie okaże się to niemożliwe lub nie będzie wymagało niewspółmiernie dużego wysiłku.

Prawo dostępu osoby do swoich danych nie jest prawem bezwzględnym. Przepis art. 13 Dyrektywy daje możliwość ograniczenia jego realizacji, jeśli jest to konieczne dla zabezpieczenia ważnego celu publicznego, takiego jak zabezpieczenie bezpieczeństwa narodowego, obronności, bezpieczeństwa publicznego, działań prewencyjnych, prowadzonych czynności dochodzeniowo-śledczych i prokuratorskich w sprawach karnych lub w sprawach o naruszenie zasad etyki w zawodach podlegających regulacjom, ważnego interesu ekonomicznego lub finansowego państwa członkowskiego lub Unii Europejskiej, łącznie ze sprawami monetarnymi, budżetowymi i podatkowymi, funkcji kontrolnych, inspekcyjnych i regulacyjnych związanych nawet sporadycznie z wykonywaniem władzy publicznej w przypadkach wymienionych w lit. c-e tego artykułu, ochrony osoby, której dane dotyczą, oraz praw i wolności innych osób.

Nawet w sytuacji, gdy dane przetwarzane są legalnie ze względu na interes publiczny, wykonywanie władzy publicznej lub uzasadnione interesy osoby fizycznej lub prawnej, osoba może w dowolnym czasie z ważkich i uzasadnionych przyczyn wynikających z jej konkretnej sytuacji wnieść w trybie art. 14 lit. a Dyrektywy sprzeciw wobec przetwarzania jej danych. Jeżeli jest on uzasadniony, administrator danych nie może przetwarzać kategorii danych objętych sprzeciwem. Osoba może również, stosownie do art. 14 lit. b Dyrektywy, wnieść sprzeciw wobec przetwarzania danych, które administrator danych zamierza przetwarzać dla potrzeb bezpośredniego obrotu, lub uzyskać informacje przed ujawnieniem danych osobowych po raz pierwszy osobom trzecim lub wykorzystaniem w ich imieniu dla potrzeb bezpośredniego obrotu, jak również ma prawo wyraźnego powoływania się na prawo sprzeciwu, bez opłat, wobec ujawniania lub wykorzystywania danych.

Dyrektywa narzuca w przepisie art. 15 ust. 1 obowiązek uwzględnienia w przepisach krajowych regulacji chroniących osobę przed podleganiem decyzji, która wywołuje skutki prawne jej dotyczące lub mające na nią istotny wpływ, jeśli decyzja ta oparta jest wyłącznie na zautomatyzowanym przetwarzaniu danych, w wyniku którego dokonywana jest ocena niektórych dotyczących osoby aspektów o charakterze osobistym, np. wyników osiąganych w pracy, wypłacalności, wiarygodności, sposobu zachowania itp. Zgodnie z art. 15 ust. 2 Dyrektywy „(...) Państwa członkowskie zapewniają, że każda osoba będzie mogła być wyłączona z zakresu objętego decyzją określoną w ust. 1, jeżeli decyzja taka a) zostanie podjęta w trakcie zawierania lub realizacji umowy, pod warunkiem, że

wniosek w sprawie zawarcia lub realizacji umowy wniesiony przez osobę, której dane dotyczą, zostanie przyjęty lub że istnieją odpowiednie sposoby zabezpieczenia jej uzasadnionych interesów, jak np. uregulowania umożliwiające jej przedstawienie swojego punktu widzenia; lub b) decyzja taka zostanie dozwolona przez prawo, które określa również sposoby zabezpieczenia uzasadnionych interesów osoby, której dane dotyczą".

Należy wspomnieć o jeszcze jednym ważnym obowiązku administratora danych. Jest nim zawarty w art. 17 ust. 1 Dyrektywy obowiązek zabezpieczenia będących w jego władaniu danych przed przypadkowym lub nielegalnym zniszczeniem, przypadkową utratą, zmianą, niedozwolonym ujawnieniem lub dostępem. Dyrektywa formułuje dodatkowo zasadę proporcjonalności, zgodnie z którą środki służące zabezpieczeniu danych osobowych powinny być odpowiednie do zagrożeń wynikających z przetwarzania danych oraz charakteru danych[11].

Skuteczne zastosowanie przedstawionych przepisów Dyrektywy wymaga utworzenia instytucji kontroli i nadzoru. Instytucja taka musi być niezależna w zakresie wykonywania swoich obowiązków, zwłaszcza w odniesieniu do agencji publicznych podlegających jej kontroli[12].

Celem ujednolicenia stosowanej w różnych państwach praktyki wprowadzono w art. 18 ust. 1 Dyrektywy zasadę zawiadamiania organu nadzorczego o przeprowadzaniu całościowej lub częściowej operacji automatycznego przetwarzania danych. Zawiadomienia należy dokonać przed rozpoczęciem przetwarzania danych i jego treść powinna zawierać, według art. 19 Dyrektywy, informacje obejmujące:

a) nazwę i adres administratora danych i ewentualnie jego przedstawiciela;
b) cel lub cele przetwarzania danych;
c) opis jednej lub kilku kategorii osób, których dane dotyczą, oraz danych lub kategorii danych, które się do nich odnoszą;
d) odbiorcę lub kategorie odbiorców, którym dane mogą być ujawnione;
e) propozycje przekazania danych do krajów trzecich;
f) ogólny opis umożliwiający dokonanie wstępnej oceny prawidłowości środków przyjętych w związku z art. 17 w celu zapewnienia bezpieczeństwa przetwarzania danych.

---

[11] A. Mednis, *Ochrona danych osobowych w Konwencji Rady Europy i Dyrektywie Unii Europejskiej*, cz. II, ODO 2000, nr 2, s. 6.

[12] *Biała księga – przygotowanie krajów stowarzyszeniowych Europy Środkowej i Wschodniej do integracji z Rynkiem wewnętrznym Unii Europejskiej*, s. 290–291.

W art. 20 Dyrektywy zostały wskazane zasady przeprowadzania kontroli przetwarzania danych. Państwa członkowskie zdefiniują operacje przetwarzania danych, mogące stwarzać określone zagrożenia dla praw i wolności osób, których dane dotyczą, oraz będą kontrolować, czy dane te są badane przed ich rozpoczęciem. Kontrole wstępne będzie przeprowadzać organ nadzorczy po przyjęciu powiadomienia od administratora danych lub urzędnika odpowiedzialnego za ochronę danych, który w razie wątpliwości winien konsultować się z organem nadzorczym. Państwa członkowskie mogą również, jak stanowi art. 20 ust. 3 Dyrektywy, przeprowadzać takie kontrole w kontekście opracowywania odpowiedniego środka w parlamencie narodowym lub środka opartego na takim rozwiązaniu legislacyjnym, które określa charakter przetwarzania danych oraz stwarza odpowiednie zabezpieczenia. Oprócz tego organ nadzoru będzie m.in. odpowiedzialny za kontrolę stosowania na jego terytorium postanowień przyjętych przez państwa członkowskie na podstawie Dyrektywy (art. 28 ust. 1 Dyrektywy) prowadzenia publicznego rejestru zbiorów danych osobowych (art. 21 Dyrektywy); będzie posiadał uprawnienia kontrolne wobec podmiotów przetwarzających dane osobowe (art. 28 ust. 3 Dyrektywy) oraz rozpatrywał skargi w zakresie ochrony praw i wolności związanych z przetwarzaniem danych (art. 28 ust. 4 Dyrektywy).

1.3. Rekomendacje i rezolucje

Zalecane standardy europejskie w zakresie ochrony danych osobowych, sformułowane w trybie rezolucji i rekomendacji Komitetu Ministrów RE lub Zgromadzenia Parlamentarnego RE, odnoszą się do różnych dziedzin życia. Akty te rozwijają ogólne zapisy Konwencji Nr 108, precyzują jej wymagania oraz wprowadzają dodatkowe warunki przetwarzania danych osobowych w nich określonych[13].

Na szczególną uwagę zasługuje Rekomendacja R(99)5 z dnia 23 lutego 1999 r. dotycząca prywatności w internecie; Rekomendacja R(87)18 z dnia 30 września 1997 r. dotycząca ochrony danych osobowych gromadzonych i przetwarzanych dla celów statystycznych; Rekomendacja R(97)5 z dnia 13 lutego 1997 r. dotycząca ochrony danych medycznych; Rekomendacja R(5)11 z dnia 11 września 1995 r. w sprawie zbierania, przedstawiania i archiwizacji orzeczeń sądów w skomputeryzowanych sy-

[13] http://www.giodo.gov.pl/230/j/pl/

stemach dokumentacji sądowej; Rekomendacja R(95)4 z dnia 7 lutego 1995 r. dotycząca danych osobowych w telekomunikacji ze szczególnym uwzględnieniem usług telefonicznych; Rekomendacja R(92)3 z dnia 10 lutego 1992 r. w sprawie genetycznych badań diagnostycznych i przesiewowych wykonywanych dla celów opieki zdrowotnej; Rekomendacja R(91)10 z dnia 9 września 1991 r. dotycząca ochrony danych osobowych przekazywanych osobom trzecim przez instytucje publiczne; Rekomendacja R(90)19 z dnia 13 września 1990 r. dotycząca ochrony danych osobowych wykorzystywanych dla potrzeb płatności oraz innych analogicznych operacji; Rekomendacja R(89)2 z dnia 18 stycznia 1989 r. w sprawie ochrony danych osobowych wykorzystywanych dla potrzeb zatrudnienia; Rekomendacja R(87)15 z dnia 17 września 1987 r. dotycząca ochrony danych osobowych wykorzystywanych w sektorze policji; Rekomendacja R(85)20 z dnia 25 października 1985 r. dotycząca ochrony danych osobowych wykorzystywanych dla potrzeb marketingu bezpośredniego

Ze względu na przedmiot uregulowania warto omówić Rekomendację R(85)20 z dnia 25 października 1985 r. dotyczącą ochrony danych osobowych wykorzystywanych dla potrzeb marketingu bezpośredniego. Zaleca ona Rządom Państw Członkowskich uwzględnienie w ich prawie i w praktyce krajowej związanej z wykorzystywaniem danych o charakterze osobistym dla potrzeb marketingu bezpośredniego wytycznych zawartych w Rekomendacji oraz zapewnienie szerokiego jej upowszechnienia oraz popierania wiedzy i informacji o ochronie danych osobowych. Według terminologii stosowanej w Rekomendacji mianem „marketingu bezpośredniego" objęto ogół działań, jak również wszelkich usług pomocniczych umożliwiających oferowanie produktów i usług bądź przekazywanie oświadczeń kierowanych do ludności za pośrednictwem kurierów, telefonów lub innych bezpośrednich środków w celach informacyjnych bądź w celu wywołania reakcji ze strony osoby zainteresowanej.

Na gruncie Rekomendacji regulacji zostały poddane kwestie związane z gromadzeniem danych dla potrzeb marketingu bezpośredniego, udostępnianiem list osobom trzecim, prawami osoby zainteresowanej, prezentacją oświadczeń i materiałów marketingowych, zabezpieczeniem danych osobowych.

Zasady gromadzenia danych dla potrzeb marketingu bezpośredniego określono w rozdziale II Rekomendacji. Każda osoba przy okazji two-