SEJM
RZECZYPOSPOLITEJ POLSKIEJ
IV kadencja
Prezes Rady Ministrów
RM 10-158-03

Druk nr 2120

Warszawa, 16 października 2003 r.

Pan
Marek Borowski
Marszałek Sejmu
Rzeczypospolitej Polskiej

Na podstawie art. 118 ust. 1 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. przedstawiam Sejmowi Rzeczypospolitej Polskiej projekt ustawy

- o zmianie ustawy o ochronie danych osobowych wraz z projektem podstawowego aktu wykonawczego,

co do którego Rada Ministrów zadeklarowała, że ma na celu dostosowanie polskiego ustawodawstwa do prawa Unii Europejskiej.

Jednocześnie, zgodnie z wymogami art. 34 ust. 5 regulaminu Sejmu, przekazuję, przetłumaczone na język polski, teksty przepisów Unii Europejskiej, do których ma być dostosowane prawo polskie.

W załączeniu przedstawiam także opinię dotyczącą zgodności proponowanych regulacji z prawem Unii Europejskiej.

Ponadto uprzejmie informuję, że do reprezentowania stanowiska Rządu w tej sprawie w toku prac parlamentarnych został upoważniony Minister Spraw Wewnętrznych i Administracji.

Z wyrazami szacunku

(-) Leszek Miller

Projekt

U S T A W A

z dnia

o zmianie ustawy o ochronie danych osobowych

Art. 1. W ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 i Nr 153, poz. 1271) wprowadza się następujące zmiany:

1) w art. 2 ust. 2 otrzymuje brzmienie:

„2. Ustawę stosuje się do przetwarzania danych osobowych:

1) w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych,
2) w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych.”;

2) art. 3 otrzymuje brzmienie:

„Art. 3. 1. Ustawę stosuje się do:

1) organów państwowych oraz organów samorządu terytorialnego,
2) państwowych i komunalnych jednostek organizacyjnych,
3) podmiotów niepaństwowych realizujących zadania publiczne,
4) osób fizycznych i osób prawnych oraz jednostek organizacyjnych nie posiadających osobowości prawnej, jeżeli przetwarzają dane osobowe w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych

– które mają siedzibę albo miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej, albo w kraju trzecim, o ile przetwarzają dane osobowe przy

wykorzystaniu środków technicznych znajdujących się na terytorium Rzeczypospolitej Polskiej.

2. W przypadku przetwarzania danych osobowych przez podmioty mające siedzibę albo miejsce zamieszkania w kraju trzecim, administrator danych jest obowiązany wyznaczyć swojego przedstawiciela w Rzeczypospolitej Polskiej. Przedstawiciel administratora danych w Rzeczypospolitej Polskiej ponosi odpowiedzialność za przestrzeganie przepisów niniejszej ustawy jak administrator danych, niezależnie od odpowiedzialności administratora danych.";

3) po art. 3 dodaje się art. 3a w brzmieniu:

„Art. 3a. 1. Ustawy nie stosuje się do:

1) osób fizycznych, które przetwarzają dane wyłącznie w celach osobistych lub domowych,

2) podmiotów mających siedzibę albo miejsce zamieszkania w kraju trzecim, wykorzystujących środki techniczne służące wyłącznie do przekazywania danych.

2. Z wyjątkiem przepisów rozdziału 5 ustawy, nie stosuje się również do prasowej działalności dziennikarskiej w rozumieniu ustawy z dnia 26 stycznia 1984 r. – Prawo prasowe (Dz. U. Nr 5, poz. 24, z późn. zm.[1)]) oraz do działalności literackiej lub artystycznej, chyba że prawo do wolności wypowiedzi istotnie narusza prawa i wolności osoby, której dane dotyczą.";

4) w art. 7:

a) pkt 4 otrzymuje brzmienie:

„4) administratorze danych – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których

mowa w art. 3 ust. 1, decydujące o celach i środkach przetwarzania danych osobowych,”,

b) po pkt 5 dodaje się pkt 6 i 7 w brzmieniu:

„6) odbiorcy danych – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:

a) osoby, której dane dotyczą,

b) osoby zatrudnionej przy przetwarzaniu danych,

c) przedstawiciela, o którym mowa w art. 3 ust. 2,

d) podmiotu, o którym mowa w art. 31,

e) organów państwowych lub samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,

7) kraju trzecim – rozumie się przez to państwo nie należące do Europejskiego Obszaru Gospodarczego.”;

5) po art. 12 dodaje się art. 12a w brzmieniu:

„Art. 12a. 1. Na wniosek Generalnego Inspektora Marszałek Sejmu może powołać nie więcej niż dwóch zastępców Generalnego Inspektora. Odwołanie zastępców Generalnego Inspektora następuje w tym samym trybie.

2. Generalny Inspektor określa zakres zadań swoich zastępców.”;

6) w art. 13 ust. 2 otrzymuje brzmienie:

„2. Generalny Inspektor, zastępcy Generalnego Inspektora oraz pracownicy Biura, zwani dalej „inspektorami”, są obowiązani zapewnić ochronę wiadomościom stanowiącym tajemnicę państwową lub służbową, z którymi zetknęli się w toku kontroli przetwarzania danych.”;

7) w art. 14 pkt 3 otrzymuje brzmienie:

„3) żądać okazania dokumentów i wszelkich danych mających bezpośredni związek z przedmiotem kontroli, w tym sporządzania ich kopii,”;

8) w art. 18 ust. 1 otrzymuje brzmienie:

„Art. 18. 1. W przypadku naruszenia przepisów o ochronie danych osobowych, Generalny Inspektor z urzędu lub na wniosek osoby zainteresowanej, w drodze decyzji administracyjnej, nakazuje przywrócenie stanu zgodnego z prawem, a w szczególności:

1) usunięcie uchybień,
2) uzupełnienie, uaktualnienie, sprostowanie, udostępnienie lub nieudostępnienie danych osobowych,
3) zastosowanie dodatkowych środków zabezpieczających zgromadzone dane osobowe,
4) wstrzymanie przekazywania danych osobowych do kraju trzeciego,
5) zabezpieczenie danych lub przekazanie ich innym podmiotom,
6) usunięcie danych osobowych.”;

9) w art. 23 w ust. 1:

a) pkt 2 i 3 otrzymują brzmienie:

„2) jest to niezbędne dla zrealizowania uprawnienia lub 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 życzenie osoby, której dane dotyczą,”,

b) pkt 5 otrzymuje brzmienie:

„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.”;

10) w art. 24 w ust. 1 pkt 3 otrzymuje brzmienie:

„3) prawie dostępu do swoich danych oraz ich poprawiania,”;

11) w art. 25:

a) w ust. 1 pkt 4 otrzymuje brzmienie:

„4) prawie dostępu do swoich danych oraz ich poprawiania,”,

b) w ust. 2:

– uchyla się pkt 2 i 4,

– pkt 5 otrzymuje brzmienie:

„5) dane są przetwarzane przez administratora, o którym mowa w art. 3 ust. 1 pkt 1-3, na podstawie przepisów prawa,”;

12) w art. 29 ust. 1 otrzymuje brzmienie:

„1. W przypadku udostępniania danych osobowych w celach innych niż włączenie do zbioru, administrator danych udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.”;

13) w art. 30 pkt 2 otrzymuje brzmienie:

„2) zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego,”;

14) w art. 31:

a) ust. 3 otrzymuje brzmienie:

„3. Podmiot, o którym mowa w ust.1, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36-39, oraz spełnić wymagania określone w przepisach, o których mowa w art. 45 pkt. 1.”,

b) dodaje się ust. 5 w brzmieniu:

„5. Do kontroli zgodności przetwarzania danych przez podmiot, o którym mowa w ust. 1, z przepisami o ochronie danych osobowych stosuje się odpowiednio przepisy art. 14 – 19.”;

15) w art. 32 w ust. 1 po pkt 5 dodaje się pkt 5a w brzmieniu:

„5a) uzyskania informacji o przesłankach podjęcia rozstrzygnięcia, o którym mowa w art. 26a ust. 2,”;

16) art. 36-39 otrzymują brzmienie:

„Art. 36. 1. Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

2. Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1.

3. W przypadku przetwarzania danych w systemie informatycznym, dokumentacja, o której mowa w ust. 2, obejmuje ponadto:

1) opis systemów informatycznych,

2) opis polityki bezpieczeństwa danych.

4. Administrator danych wyznacza administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad bezpieczeństwa danych, chyba że sam wykonuje te czynności.

Art. 37. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie wydane przez administratora danych.

Art. 38. Administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez

kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

Art. 39. 1. Administrator danych prowadzi ewidencję osób zatrudnionych przy ich przetwarzaniu, która powinna zawierać:

1) imię i nazwisko,
2) datę nadania i ustania upoważnienia do dostępu do danych osobowych,
3) zakres upoważnienia,
4) identyfikator użytkownika, jeżeli dane są przetwarzane w systemie informatycznym.

2. Osoby, o których mowa w ust. 1, mające dostęp do danych osobowych, są obowiązane zachować je w tajemnicy. Obowiązek ten istnieje również po ustaniu zatrudnienia.”;

17) w art. 41:

a) w ust. 1:

– pkt 3 otrzymuje brzmienie:

„3) cel przetwarzania danych,”,

– po pkt 3 dodaje się pkt 3a w brzmieniu:

„3a) opis kategorii osób, których dane dotyczą, oraz zakres przetwarzanych danych,”,

– pkt 7 otrzymuje brzmienie:

„7) informację dotyczącą ewentualnego przekazywania danych do kraju trzeciego.”,

b) ust. 2 otrzymuje brzmienie:

„2. Administrator danych jest obowiązany zgłaszać Generalnemu Inspektorowi każdą zmianę informacji, o której mowa w ust. 1, w terminie 30 dni od dnia dokonania zmiany w zbiorze danych. Do zgłaszania zmian stosuje się odpowiednio przepisy o rejestracji zbiorów danych.”;

18) w art. 42:

a) ust. 1 otrzymuje brzmienie:

„1. Generalny Inspektor prowadzi ogólnokrajowy, jawny rejestr zbiorów danych osobowych. Rejestr powinien zawierać informacje, o których mowa w art. 41 ust. 1 pkt 1-4a i 7.”,

b) ust. 3 otrzymuje brzmienie:

„3. Na żądanie administratora danych może być wydane zaświadczenie o zarejestrowaniu zgłoszonego przez niego zbioru danych.”;

19) w art. 43:

a) w ust. 1 pkt 3 i 4 otrzymują brzmienie:

„3) związanych z przynależnością do kościoła lub innego związku wyznaniowego, o uregulowanej sytuacji prawnej, przetwarzanych na potrzeby tego kościoła lub związku wyznaniowego,

4) przetwarzanych w związku z zatrudnieniem u nich, świadczeniem im usług na podstawie umów cywilnoprawnych, a także dotyczących osób u nich zrzeszonych lub uczących się,”,

b) po ust. 1 dodaje się ust. 1a w brzmieniu:

„1a. Przepisów ust. 1 pkt 2, 2a, 4-11 nie stosuje się w przypadku przetwarzania danych, o których mowa w art. 27 ust. 1.”;

20) w art. 44 ust. 2 i 3 otrzymują brzmienie:

„2. Odmawiając rejestracji zbioru danych, Generalny Inspektor, w drodze decyzji administracyjnej, nakazuje:

1) ograniczenie przetwarzania wszystkich albo niektórych kategorii danych wyłącznie do ich przechowywania lub

2) zastosowanie innych środków, o których mowa w art. 18 ust. 1.

3. Decyzja administracyjna, o której mowa w ust. 2, podlega natychmiastowemu wykonaniu.”;

21) po art. 44 dodaje się art. 44a w brzmieniu:

„Art. 44a. 1. Wpis o wykreśleniu z rejestru, o którym mowa w art. 42 ust. 1, jest dokonywany, w drodze decyzji administracyjnej, jeżeli:

1) zaprzestano przetwarzania danych w zarejestrowanym zbiorze,
2) przetwarzanie danych narusza zasady określone w art. 23–30 lub art. 36–39,
3) urządzenia i systemy informatyczne służące do przetwarzania danych nie spełniają podstawowych warunków technicznych i organizacyjnych,
4) rejestracji dokonano z naruszeniem prawa.

2. Do wykreślenia zbioru danych osobowych z rejestru stosuje się odpowiednio przepisy art. 44 ust. 2 – 5.”;

22) art. 45 otrzymuje brzmienie:

„Art. 45. Minister właściwy do spraw administracji publicznej określi, w drodze rozporządzenia:

1) w porozumieniu z ministrem właściwym do spraw informatyzacji, sposób prowadzenia i zakres dokumentacji, o której mowa w art. 36 ust. 2, oraz podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych z uwzględnieniem wymagań w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzanych danych oraz standardów obowiązujących w tym zakresie w krajach Unii Europejskiej,

2) wzór zgłoszenia, o którym mowa w art. 41 ust. 1, z uwzględnieniem obowiązku zamieszczenia informacji niezbędnych do stwierdzenia zgodności przetwarzania danych z wymogami ustawy,
3) wzór upoważnienia i legitymacji służbowej, o których mowa w art. 14 pkt 1, z uwzględnieniem konieczności imiennego wskazania inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych.”;

23) tytuł rozdziału 7 otrzymuje brzmienie:
„Przekazywanie danych osobowych do kraju trzeciego.”;

24) w art. 47:
a) ust. 1 otrzymuje brzmienie:
„1. Przekazanie danych osobowych do kraju trzeciego może nastąpić, jeżeli kraj docelowy daje gwarancje ochrony danych osobowych na swoim terytorium przynajmniej takie, jakie obowiązują na terytorium Rzeczypospolitej Polskiej.”,
b) w ust. 3 wprowadzenie do wyliczenia otrzymuje brzmienie:
„3. Administrator danych może jednak przekazać dane osobowe do kraju trzeciego, jeżeli:”;

25) art. 48 otrzymuje brzmienie:
„Art. 48. W przypadkach innych niż wymienione w art. 47 ust. 2 i 3 przekazanie danych osobowych do kraju trzeciego, który nie daje gwarancji ochrony danych osobowych przynajmniej takich, jakie obowiązują na terytorium Rzeczypospolitej Polskiej, może nastąpić po uzyskaniu zgody Generalnego Inspektora, pod warunkiem, że administrator danych zapewni odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą.”.

Art. 2. W ustawie z dnia 31 lipca 1981 r. o wynagrodzeniu osób zajmujących kierownicze stanowiska państwowe (Dz. U. Nr 20, poz. 101, z 1982 r. Nr 31, poz. 214, z 1985 r. Nr 22, poz. 98 i Nr 50, poz. 262, z 1987 r. Nr 21, poz. 123, z 1989 r. Nr 34, poz. 178, z 1991 r. Nr 100, poz. 443, z 1993 r. Nr 1, poz. 1, z 1995 r. Nr 34, poz. 163 i Nr 142, poz. 701, z 1996 r. Nr 73, poz. 350, Nr 89, poz. 402, Nr 106, poz. 496 i Nr 139, poz. 647, z 1997 r. Nr 75, poz. 469 i Nr 133, poz. 883, z 1998 r. Nr 155, poz. 1016 i Nr 160, poz. 1065, z 1999 r. Nr 110, poz. 1255, z 2000 r. Nr 6, poz. 69 i Nr 48, poz. 552, z 2001 r. Nr 154, poz. 1784 i 1800, z 2002 r. Nr 214, poz. 1805 i Nr 240, poz. 2052 oraz z 2003 r. Nr 45, poz. 391 i Nr 65, poz. 595) w art. 2 pkt 4 otrzymuje brzmienie:

„4) Prezesa Polskiej Akademii Nauk, sekretarza stanu, członka Krajowej Rady Radiofonii i Telewizji, pierwszego zastępcy Prezesa Narodowego Banku Polskiego, podsekretarza stanu (wiceministra), wiceprezesa Narodowego Banku Polskiego, Sekretarza Komitetu Integracji Europejskiej, Zastępcy Rzecznika Praw Obywatelskich, Zastępcy Generalnego Inspektora Ochrony Danych Osobowych, Rzecznika Ubezpieczonych, kierownika urzędu centralnego, wiceprezesa Polskiej Akademii Nauk, wojewody, zastępcy kierownika urzędu centralnego, wicewojewody.”.

Art. 3. Administratorzy danych prowadzący w dniu wejścia w życie niniejszej ustawy zbiory danych osobowych, które na jej podstawie podlegają obowiązkowi zgłoszenia do rejestracji, wykonają ten obowiązek w terminie do 3 miesięcy od dnia jej wejścia w życie.

Art. 4. Do postępowań wszczętych i niezakończonych przed dniem wejścia w życie niniejszej ustawy stosuje się przepisy tej ustawy.

Art. 5. Dotychczasowe przepisy wykonawcze wydane na podstawie art. 45 ustawy, o której mowa w art. 1, zachowują moc do czasu wydania nowych przepisów wykonawczych na podstawie upoważnienia zmienionego niniejszą ustawą, nie dłużej jednak niż przez 6 miesięcy od dnia wejścia w życie ustawy.

Art. 6. Ustawa wchodzi w życie z dniem uzyskania przez Rzeczpospolitą Polską członkostwa w Unii Europejskiej, z wyjątkiem art. 1 pkt 5-7 i 21, które wchodzą w życie po upływie 30 dni od dnia ogłoszenia.

[1)] Zmiany ustawy zostały ogłoszone w Dz. U. z 1988 r. Nr 41, poz. 324, z 1989 r. Nr 34, poz. 187, z 1990 r. Nr 29, poz. 173, z 1991 r. Nr 100, poz. 442, z 1996 r. Nr 114, poz. 542, z 1997 r., Nr 88, poz. 554 i Nr 121, poz. 770, z 1999 r. Nr 90, poz. 999, z 2001 r. Nr 112, poz. 1198 oraz z 2002 r. Nr 153, poz. 1271.

U Z A S A D N I E N IE

Kilkuletni okres obowiązywania ustawy o ochronie danych osobowych pozwala na stwierdzenie, że ustawa ta wymaga zmian. Poprzednia, znacząca nowelizacja z 2001 r.[1)], która miała na celu przede wszystkim zmianę definicji danych osobowych oraz wprowadzenie do polskiego prawa zakazu podejmowania tzw. rozstrzygnięć automatycznych, nie doprowadziła do pełnego dostosowania ustawy do standardów Dyrektywy 95/46 WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych[2)]. Na brak pełnej zgodności ustawy ze standardami powołanej wyżej Dyrektywy zwracała uwagę Komisja Europejska – Dyrekcja Generalna ds. Rynku Wewnętrznego, stąd konieczność wprowadzenia dalszych zmian w ustawie.

Jednocześnie konieczność zmiany ustawy w zakresie „europejskim" stworzyła możliwość wprowadzenia w ustawie innych zmian, podyktowanych doświadczeniami wynikającymi ze stosowania ustawy.

Poniżej, przy każdym komentowanym przepisie, przedstawione zostaną przyczyny uzasadniające zmianę dotychczasowych regulacji.

Zmiana zaproponowana do art. 2 ust. 2 rozstrzyga w sposób nie budzący wątpliwości, że ustawę stosuje się do przetwarzania danych osobowych w zbiorach tradycyjnych (kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych), a bez względu na istnienie zbioru danych osobowych, w razie przetwarzania danych w systemach informatycznych.

Nowelizacja art. 2 ust. 2 wynika z zaleceń Komisji Europejskiej, która wskazywała na potrzebę precyzyjnego ustalenia zakresu przedmiotowego stosowania ustawy.

Zmiany wprowadzone w art. 3 i art. 3a mają na celu wyraźne rozgraniczenie przepisów określających do jakich podmiotów ustawa o ochronie danych ma zastosowanie (art. 3) oraz, które podmioty mimo tego, że przetwarzają dane

osobowe, nie są do jej stosowania obowiązane (art. 3a ust. 1), ewentualnie są obowiązane do jej stosowania w ograniczonym zakresie (art. 3a ust. 2).

Przepis art. 3, po zmianach, precyzyjnie będzie określał podmioty przetwarzające dane osobowe, które są obowiązane do stosowania przepisów ustawy o ochronie danych osobowych. Ustawę w aktualnym brzmieniu stosuje się m.in. do administratorów, którzy nie mają siedziby lub miejsca zamieszkania na terytorium Polski, ale przetwarzają dane przy wykorzystaniu środków znajdujących się w Polsce. Takie brzmienie przepisu prowadzi do sytuacji, gdy przetwarzanie danych przez administratora mającego swoją siedzibę w jednym z państw Europejskiego Obszaru Gospodarczego może podlegać regulacji dwóch ustaw – ustawy kraju pochodzenia administratora danych oraz ustawy polskiej. Częste były sytuacje, gdy np. podmiot zagraniczny mający siedzibę w Unii Europejskiej zgłaszał Generalnemu Inspektorowi do rejestracji zbiór danych osobowych, gdyż taki obowiązek narzuca literalnie interpretowana ustawa w aktualnym jej brzmieniu. Formalnie obowiązany jest on także do stosowania wszystkich innych przepisów ustawy. Taki stan jest jednak sprzeczny z ideą jednolitej ochrony danych w państwach członkowskich, przy czym chodzi o ochronę przez prawo kraju, w którym siedzibę lub miejsce zamieszkania ma administrator. Ideę tę ustanawia również Dyrektywa. W art. 4 zwalnia ona z obowiązku stosowania prawa krajowego wówczas, gdy administrator danych z jednego kraju członkowskiego przetwarza dane przy wykorzystaniu środków znajdujących się na terytorium innego kraju członkowskiego. Nie ma przy tym znaczenia, o jakie środki techniczne chodzi.

Inna zasada obowiązuje w przypadku kraju trzeciego – zwolnienie z wymogów ustawy jest dopuszczalne tylko wówczas, gdy zlokalizowane w kraju członkowskim środki, przy pomocy których przetwarzane są dane, służą wyłącznie do ich tranzytu. W tym zakresie Dyrektywa w art. 4 ust. 1c stanowi, że „każde państwo członkowskie stosuje w odniesieniu do przetwarzania danych osobowych postanowienia prawa krajowego /.../, gdy administrator danych nie prowadzi działalności na terytorium Wspólnoty, lecz dla celów przetwarzania danych osobowych wykorzystuje środki, zarówno zautomatyzowane jak i inne, znajdujące się na terytorium wymienionego

państwa członkowskiego, o ile środki te nie są wykorzystywane wyłącznie do celów tranzytu przez terytorium Wspólnoty".

Proponowana zmiana wynika przede wszystkim z zaleceń Komisji Europejskiej, która wskazała na niezgodność obecnej regulacji z przepisami Dyrektywy.

Nowy art. 3a ust. 2 ustawy określa ograniczenie stosowania przepisów ustawy, jeżeli przetwarzanie danych miałoby związek z prasową działalnością dziennikarską, literacką bądź artystyczną. Aktualny pozostałby jedynie obowiązek odpowiedniego zabezpieczenia zbiorów, przewidziany w rozdziale 5 ustawy. Proponowana zmiana wynika przede wszystkim z zaleceń Komisji, która zwracała uwagę stronie polskiej na brak w polskiej ustawie odpowiednika art. 9 Dyrektywy, statuującego zwolnienie (w odpowiednim zakresie) spod rygorów prawa ochrony danych działalność wykonywaną „...wyłącznie w celach dziennikarskich lub dla celów wypowiedzi artystycznej bądź literackiej...". Wzorem rozwiązania przyjętego w Dyrektywie - powyższe wyłączenie nie ma bezwzględnego charakteru. Nie dotyczy ono bowiem sytuacji, w których prawo do wolności wypowiedzi istotnie narusza prawa i wolności osoby, której dane dotyczą.

Do art. 7 wprowadza się dwie nowe definicje, które wynikają z zaleceń Komisji Europejskiej, wskazującej na konieczność zdefiniowania określonych pojęć w sposób tożsamy z Dyrektywą.

Zdefiniowanie odbiorcy danych (art. 7 pkt 6) ma na celu dostosowanie ustawy do art. 2g Dyrektywy.

Bardzo istotną zmianą, o znaczących konsekwencjach, jest zdefiniowanie pojęcia „kraju trzeciego" (art. 7 pkt 7), którym nie będzie żaden kraj należący do Europejskiego Obszaru Gospodarczego, w tym kraj członkowski Unii Europejskiej. Oznacza to, że przepływ danych do tych krajów będzie traktowany tak samo, jak transfer danych na terytorium Polski. Swobodny przepływ danych w ramach Unii Europejskiej jest koniecznym wymogiem naszego członkostwa w strukturach Unii. Poza tym, po przystąpieniu Polski do UE, przejmując unijny dorobek prawny, staniemy się członkiem Europejskiego Obszaru Gospodarczego (EEA). Niezbędne, i zgodne z istotą postanowień Dyrektywy,

jest zatem zapewnienie swobodnego przepływu danych również do krajów EEA nie będących członkami Unii (Norwegia, Islandia, Lichtenstein).

Uzasadniając dodanie nowego art. 12a do ustawy należy wyjaśnić, że doświadczenie Generalnego Inspektora wskazuje na potrzebę powołania jego zastępców. Przejęliby oni część obowiązków Generalnego Inspektora. Podkreślenia bowiem wymaga, że z jednej strony znacząco wzrasta ilość spraw załatwianych przez Generalnego Inspektora, z drugiej zaś – niezbędny jest udział przedstawiciela niezależnego organu ochrony danych osobowych odpowiednio wysokiej rangi w wielu przedsięwzięciach międzynarodowych. Jako przykład można wskazać cykliczne, kilkudniowe spotkania Grupy Roboczej Art. 29, w trakcie których rzecznicy ochrony danych państw członkowskich i kandydujących dyskutują na temat bieżących problemów dotyczących ochrony danych i wypracowują rozwiązania problemów praktycznych.
Proponowana zmiana wzorowana jest na regulacji przyjętej w ustawie o Rzeczniku Praw Obywatelskich.

W związku z wprowadzeniem przepisu umożliwiającego powołanie zastępców Generalnego Inspektora, w art. 13 ust. 2 konieczne stało się objęcie osób pełniących tę funkcję obowiązkiem zapewnienia ochrony wiadomościom stanowiącym tajemnicę państwową lub służbową, z którymi zetknęli się w toku kontroli przetwarzania danych.
Podobnie, stosownego uzupełnienia wymaga ustawa z dnia 31 lipca 1981 r. o wynagrodzeniu osób zajmujących kierownicze stanowiska państwowe (Dz. U. Nr 20, poz. 101, z późn. zm.), co znalazło odzwierciedlenie w art. 2 projektowanej ustawy. Zmiana ta pozwoli na stosowanie wymienionej ustawy o wynagrodzeniu osób (...) do zastępców Generalnego Inspektora Ochrony Danych Osobowych. Zastępcy GIODO, z uwagi na podobny charakter funkcji do sekretarza stanu i podsekretarza stanu w ministerstwie, zostali uwzględnieni w art. 2 pkt 4 tej ustawy.
Zmiana art. 14 pkt 3 jest konsekwencją praktycznych problemów, z którymi Generalny Inspektor spotykał się w swojej dotychczasowej działalności. Częste

były bowiem przypadki, gdy kontrolowani administratorzy danych odmawiali inspektorom upoważnionym do przeprowadzenia kontroli prawa sporządzania kopii dokumentów mających bezpośredni związek z przedmiotem kontroli. W praktyce oznaczało to konieczność sporządzania notatek z dokumentów, co znacznie wydłuża czas trwania czynności kontrolnych i de facto utrudnia jej sprawne przeprowadzenie.

Zmiana w art. 18 podyktowana jest doświadczeniami wynikającymi z praktyki stosowania ustawy o ochronie danych osobowych. W aktualnym stanie prawnym, na podstawie tego przepisu, Generalny Inspektor nie ma możliwości wydania decyzji nakazującej podmiotowi innemu niż administrator danych przywrócenia w procesie przetwarzania danych osobowych stanu zgodnego z prawem, w przypadku stwierdzenia naruszenia przez niego przepisów o ochronie danych. Dotyczy to w szczególności podmiotów, którym przetwarzanie danych zostało powierzone w oparciu o art. 31 ustawy o ochronie danych osobowych. Wykreślenie z art. 18 w jego aktualnym brzmieniu słów „administratorowi danych" umożliwi Generalnemu Inspektorowi wydawanie, na jego podstawie, decyzji administracyjnych wobec wszystkich podmiotów przetwarzających dane osobowe, a nie tylko wobec administratorów danych.

Zmiany w art. 23 ust. 1 wynikają głównie z zaleceń Komisji Europejskiej i dostosowują ustawę do brzmienia Dyrektywy.
Nowe brzmienie punktu 2 odpowiada w większym stopniu praktycznym potrzebom przetwarzania danych, zwykle bowiem uprawnienie lub obowiązek przetwarzania danych wynika z konieczności wypełnienia zobowiązania nałożonego przez przepis prawa. Ponadto w dokładny sposób odzwierciedla ono brzmienie przepisu art. 7c Dyrektywy, który legalizuje przetwarzanie danych osobowych w sytuacji, gdy „jest to konieczne dla zgodności z zobowiązaniem prawnym, któremu administrator danych podlega".
Również brzmienie znowelizowanego punktu 3 miało na celu pełniejsze dostosowanie jego treści do art. 7b Dyrektywy.
Istotną zmianę w punkcie 5 stanowi rezygnacja ze wskazania, że prawnie usprawiedliwiony cel administratora danych udostępniającego dane osobowe

dotyczyć może jedynie administratorów ze sfery prywatnej. Takie różnicowanie administratorów nie znajdowało uzasadnienia prawnego.

Uzasadniając zmiany do art. 24 pkt 3 i art. 25 pkt 4 ustawy należy podkreślić, że prawo do kontroli przetwarzania danych nie powinno być utożsamiane z prawem fizycznego wglądu do nośników (informatycznych lub manualnych) zawierających te dane. Nie istnieje więc prawo wglądu do danych w dosłownym znaczeniu tego słowa – z zasady prawo to należy sprowadzić do prawa dostępu do informacji o warunkach, zakresie, celu i podstawie prawnej przetwarzania danych osobowych. Stąd właśnie proponowana zamiana w art. 24 pkt 3 i art. 25 pkt 4 polegająca na usunięciu wyrazów „wglądu do" i zastąpieniu ich wyrazami „dostępu do". Takim właśnie sformułowaniem posługuje się bowiem nie tylko art. 51 ust. 3 Konstytucji RP („Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych."), ale również art. 10 pkt c, art. 11 pkt c i art. 12 Dyrektywy („the right of access to data", które powinno być tłumaczone jako „dostęp do danych"). Jednocześnie żaden z przepisów Dyrektywy nie uprawnia osoby, której dane dotyczą, do fizycznego wglądu w nośniki zawierające jej dane osobowe przetwarzane przez administratora. W pewnych sytuacjach realizacja prawa dostępu do danych może polegać na umożliwieniu fizycznego wglądu do danych, jednakże nałożenie na administratora danych obowiązku każdorazowego realizowania prawa dostępu przez umożliwienie osobie, której dane dotyczą, fizycznego wglądu w dokumenty, ewentualnie w system informatyczny, byłaby rozwiązaniem niemożliwym do wykonania.

Skreślenie pkt 2 i 4 w art. 25 ust. 2 ustawy wynika z zaleceń Komisji Europejskiej i zapewni zgodność polskiej ustawy z Dyrektywą. Dyrektywa nie przewiduje bowiem w żadnym przepisie możliwości zwolnienia z obowiązku informacyjnego administratora danych zbierającego dane nie od osoby, której dane dotyczą, nawet w sytuacji, gdy zebrano dane powszechnie dostępne (pkt 2), a także wtedy, gdy dane były wykorzystywane jednorazowo (pkt 4). Należy podkreślić, że dotychczasowe doświadczenia Generalnego Inspektora potwierdzają trafność przyjętych przez Dyrektywę rozwiązań. Przepisy

w dotychczasowym brzmieniu niejednokrotnie uniemożliwiały lub utrudniały osobom, których dane dotyczą, sprawowanie kontroli nad ich danymi osobowymi i korzystanie z uprawnień wynikających z przepisów ustawy, w szczególności osoby te nie miały wiedzy o tym, kto jest administratorem ich danych i w jakim celu je przetwarza, jeżeli administratorzy danych przetwarzali je z powołaniem się na wykorzystywanie danych jednorazowo lub z powołaniem się na źródło powszechnie dostępne. Duża liczba skarg kierowanych do Generalnego Inspektora wynikała z nadużywania przez sektor prywatny zwolnień z obowiązku informacyjnego. Wobec osób, których dane pozyskano np. z książki telefonicznej lub od innego administratora danych w celu jednokrotnego wykorzystania – nie był wykonywany obowiązek informacyjny, o którym mowa w art. 25 ust.1 ustawy o ochronie danych osobowych, a nawet – jeżeli otrzymywały imiennie adresowane materiały o charakterze marketingowym – na materiałach tych nie umieszczano informacji, o których mowa w art. 25 ust. 1 ustawy.

W art. 29 proponuje się wprowadzić zasadę, że przepis ten znajduje zastosowanie do udostępniania danych w celu innym niż włączenie do zbioru, przez każdego administratora, a nie, tak jak dotychczas, wyłącznie przez administratora ze sfery publicznej. Nie ma bowiem żadnych merytorycznych podstaw do różnicowania pozycji administratorów danych ze względu na ich status.

Zmiana w art. 30 pkt 2 polegająca na skreśleniu wyrazu „mienia” ma na celu zapewnienie pełnej zgodności brzmienia tego przepisu z art. 13 ust. 1 Dyrektywy.

Dalsze zmiany są podyktowane wątpliwościami co do obowiązków spoczywających na podmiocie, któremu administrator danych powierzył przetwarzanie danych, także np. w zakresie poddania się kontroli dokonywanej przez GIODO, czy stosowania przepisów wykonawczych do ustawy. Aby te wątpliwości rozstrzygnąć proponuje się wprowadzić ustęp 5 do art. 31, który wprost przyznaje GIODO uprawnienia kontrolne wobec tych podmiotów oraz

art. 31 ust. 3, w którym zostaje wprost nałożony obowiązek spełniania wymagań określonych w przepisie wykonawczym do ustawy, o którym mowa w art. 45 pkt. 1 ustawy.

W art. 32 proponuje się dodać pkt 5a, który rozszerzy uprawnienia osoby, której dane dotyczą do uzyskania określonych informacji o prawie do pozyskania informacji o przesłankach podejmowania rozstrzygnięć automatycznych. Zmiana ta jest związana z brzmieniem art. 12a Dyrektywy, który szczegółowo wymienia uprawnienia osoby, której dane dotyczą.

Istotą nowelizacji art. 36 - 39, zawartych w rozdziale 5 ustawy, określającym zasady zabezpieczenia zbiorów danych, jest rozwinięcie i sprecyzowanie obowiązków administratora danych. Dotychczas były one określone w przepisach wykonawczych do ustawy, co było kwestionowane z punktu widzenia zgodności z Konstytucją (obowiązki może wprowadzać tylko ustawa lub wydane w granicach upoważnienia rozporządzenie). Po nowelizacji, rozporządzenie wykonawcze do ustawy będzie określać jedynie warunki techniczne i organizacyjne przetwarzania danych w systemach informatycznych, mające na celu prawidłowe wykonanie obowiązku zabezpieczenia danych wynikającego z przepisów ustawy.

Zmiany wprowadzane w art. 41 - 44, znajdujących się w rozdziale dotyczącym rejestracji zbiorów danych osobowych, mają charakter porządkujący oraz uzupełniający obowiązujące przepisy w celu zapewnienia pełnej zgodności z Dyrektywą.

Proponuje się uzupełnić art. 41 ust. 1 o odrębny punkt precyzujący, że zgłoszenie zbioru danych do rejestracji powinno zawierać opis kategorii osób, których dane dotyczą, oraz zakres przetwarzanych danych (zmiana wskazana jako niezbędna przez Komisję Europejską, wynikająca z brzmienia art. 19 ust. 1 pkt c Dyrektywy). Przepis art. 41 ust. 1 pkt 3 ustawy w dotychczasowym brzmieniu również zobowiązywał administratora danych do podania zakresu danych w zgłoszeniu do rejestracji. Proponuje się zatem wyodrębnić w pkt 3

„cel przetwarzania danych” oraz dodać pkt 3a obejmujący opis kategorii osób i zakres przetwarzanych danych.
W art. 41 proponuje się także – w związku z tym, iż dotychczas procedura zgłaszania zmian nie była uregulowana w ustawie – dodanie w ust. 2 zdania wskazującego wprost, że do zgłaszania zmian stosuje się odpowiednio przepisy o rejestracji zbiorów danych.

Propozycja znowelizowania art. 42 ust. 1, przez ograniczenie zakresu informacji dostępnych w jawnym rejestrze zbiorów danych osobowych prowadzonym przez GIODO jest podyktowana koniecznością zabezpieczenia interesu administratora danych. W rejestrze nie powinny znajdować się informacje, które dotyczą zabezpieczeń organizacyjnych i technicznych zbioru, a zatem informacje, które są niezbędne Generalnemu Inspektorowi do oceny poziomu ochrony danych, przetwarzanych w zgłoszonym do rejestracji zbiorze. Informacje o szczegółowych rozwiązaniach w zakresie zabezpieczenia zbiorów danych – z uwagi na interes administratora danych i bezpieczeństwo danych przetwarzanych przez administratora – powinny być przekazywane do wyłącznej wiadomości Generalnego Inspektora. Należy jednocześnie podkreślić, że Dyrektywa nie wprowadza obowiązku zamieszczania w rejestrze opisu środków organizacyjnych i technicznych mających na celu zapewnienie ochrony przetwarzanych danych osobowych (art. 21 ust. 2 Dyrektywy).

Propozycja zmian w art. 42 ust. 3 polega na ograniczeniu kręgu podmiotów uprawnionych do otrzymania zaświadczenia wyłącznie do administratora i wyłącznie co do zbioru przez niego zgłoszonego. Zmiana ta wynika z dotychczasowych doświadczeń Generalnego Inspektora, które wskazują na konieczność zawężenia kręgu podmiotów uprawnionych do otrzymywania zaświadczeń na podstawie art. 42 ust. 3 ustawy o ochronie danych osobowych. Jak na razie administratorzy danych zgłosili do rejestracji ok. 80 tys. zbiorów. Dotychczasowe brzmienie art. 42 ust. 3 de facto uprawnia każdego do otrzymania zaświadczenia o wszystkich zarejestrowanych zbiorach. Przyjęcie proponowanej zmiany ograniczy krąg podmiotów uprawnionych do otrzymania zaświadczenia na podstawie art. 42 ust. 3 ustawy wyłącznie do administratorów

danych, którzy zgłosili swoje zbiory do rejestracji. Wydawanie zaświadczeń innym podmiotom (np. osobom, dla których posiadanie zaświadczenia byłoby niezbędne w celu dochodzenia praw przed sądem) odbywałoby się na zasadach określonych w Kodeksie postępowania administracyjnego, a zatem będzie uzależnione od wykazania przez wnioskodawcę interesu prawnego; w praktyce pozwoli to na odmowę uwzględnienia wniosku obywatela występującego o wydanie kilkudziesięciu tysięcy zaświadczeń o zarejestrowaniu zbiorów. Niezależnie od tego podkreślenia wymaga, że każdy (w tym także osoba, której odmówiono wydania zaświadczenia ze względu na brak interesu prawnego) ma prawo wglądu do jawnego rejestru zbiorów zgłoszonych do rejestracji.

Projekt zmiany art. 43 ust. 1 pkt 4 wynika z trudności interpretacyjnych dotychczasowego brzmienia przepisu, a zwłaszcza wątpliwości co do tego, czy zwolnienie obejmuje zbiory danych osób świadczących pracę na jakiejkolwiek podstawie, czy tylko na podstawie stosunków pracowniczych, oraz czy dotyczy osób zatrudnionych aktualnie, czy także w przeszłości. Wobec powyższego uzasadnione wydaje się usunięcie tych wątpliwości przez nowelizację tego przepisu w zaproponowanym brzmieniu. Jednocześnie doprecyzowano też pkt 3 w art. 43 ust. 1 ustawy.

Istotna zmiana jest związana z wprowadzeniem nowego art. 43 ust. 1a. Przepis ten oznaczałby, że pomimo zwolnienia z obowiązku zgłoszenia zbioru do rejestracji określonego w art. 43 ust. 1, obowiązek taki będzie istniał, jeżeli administrator przetwarza tzw. dane szczególnie chronione, wymienione w art. 27 ust. 1. Podkreślić należy, że jest to wymóg Komisji Europejskiej, która wskazywała na nie w pełni implementowanie przez polską ustawę Dyrektywy, nakładającej szczególne obowiązki w zakresie ochrony danych sensytywnych, w tym obowiązek tzw. wstępnej oceny prawidłowości przetwarzania danych. Komisja oceniała katalog zwolnień z obowiązku rejestracji jako zbyt szeroki i sprzeczny z Dyrektywą.

Wstępna ocena prawidłowości przetwarzania danych odbywa się na etapie zgłaszania zbiorów danych do zarejestrowania. Tymczasem – zgodnie z polską ustawą o ochronie danych osobowych w jej aktualnym brzmieniu –

przeważająca większość zbiorów zawierających dane szczególnie chronione została zwolniona z obowiązku rejestracji, czyli faktycznie, spod wstępnej kontroli prawidłowości przetwarzania danych. W praktyce oznacza to, że zakres wyłączeń spod obowiązku rejestracji musi być radykalnie ograniczony, jednakże, w związku z brzmieniem przepisu art. 43 ust. 2 ustawy, ograniczającego kompetencje Generalnego Inspektora w odniesieniu do zbiorów danych, o których mowa w art. 43 ust. 1 pkt 1,1a i 3 ustawy, nadal z obowiązku rejestracji – nawet przetwarzając dane szczególnie chronione – zwolnieni będą administratorzy danych:

1) objętych tajemnicą państwową ze względu na obronność lub bezpieczeństwo państwa, ochronę życia i zdrowia ludzi, mienia lub bezpieczeństwa i porządku publicznego,
2) które zostały uzyskane w wyniku czynności operacyjno-rozpoznawczych przez funkcjonariuszy organów uprawnionych do tych czynności,
3) dotyczących członków kościoła lub innego związku wyznaniowego, o uregulowanej sytuacji prawnej.

Należy jednocześnie podkreślić, że zwolnienie z obowiązku rejestracji zbioru nie jest tożsame ze zwolnieniem z obowiązku stosowania innych przepisów o ochronie danych osobowych.

Pozostałe zmiany w tym rozdziale, tzn. zmiany art. 44, 44a i 45 mają na celu doprecyzowanie zagadnień proceduralnych. Praktyka GIODO wskazuje, że w ustawie brakuje instytucji „wykreślenia” zbioru. Częste są sytuacje, gdy uprzednio zarejestrowany zbiór nie jest już prowadzony, bądź też, że administrator już nie istnieje. Zdarzyć się mogą także sytuacje, gdy zbiór zostanie zarejestrowany z naruszeniem prawa, np. przez niedopełnienie przez administratora wymagań prawnych przewidzianych w ustawie lub rozporządzeniu wykonawczym. W tych wszystkich przypadkach aktualnie nie istnieje możliwość prawnej reakcji GIODO. Z tych powodów zasadne jest wprowadzenie instytucji wykreślenia zbioru, określenia przesłanek jej stosowania oraz wskazania przepisów proceduralnych.

Projektowana nowelizacja art. 44 ust. 2 zawiera istotne propozycje zmian, podyktowanych doświadczeniami praktycznymi. W aktualnym stanie prawnym odmowa rejestracji zbioru danych jest związana z koniecznością wydania decyzji o odmowie rejestracji zbioru, nakazującej równocześnie usunięcie nie zarejestrowanego zbioru, lub zakazującej jego przetwarzania. Tymczasem w wielu przypadkach odmowa rejestracji nie powinna być związana z tak daleko idącymi konsekwencjami dla administratora danych, zwłaszcza wówczas, gdy uchybienia w procesie przetwarzania danych są niewielkie, bądź też gdy dotyczą części zbioru. Proponowana jest zatem taka zmiana przepisu, aby Generalny Inspektor odmawiając rejestracji zbioru, miał możliwość wyboru proporcjonalnych środków prawnych, w zależności od wagi naruszenia prawa.

W rozdziale 7 ustawy zastąpiono wyrazy „za granicę" wyrazami „kraj trzeci". Ideą tej zmiany jest zapewnienie swobodnego przepływu danych do krajów Unii Europejskiej i krajów EEA spoza Unii.
Ponadto w art. 48 ustawy, dotyczącym udzielania przez Generalnego Inspektora zgody na przekazywanie danych osobowych do kraju trzeciego, dodano - wzorem rozwiązania przyjętego w art. 26 ust. 2 Dyrektywy - warunek zapewnienia przez administratora danych odpowiednich zabezpieczeń w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą.

Uzasadniając treść art. 3 projektu ustawy o zmianie ustawy (termin zgłoszenia do rejestracji zbiorów, zawierających dane szczególnie chronione, które obecnie są zwolnione z obowiązku rejestracji) należy zauważyć, że zgłoszenie zbioru do rejestracji nie jest czynnością skomplikowaną, która wymagałaby szczególnego nakładu czasu i środków. W związku z powyższym, 3-miesięczny okres na dopełnienie tego obowiązku wydaje się optymalny.

Art. 4 projektu ustawy o zmianie ustawy o ochronie danych osobowych został wprowadzony z uwagi na konieczność ustalenia, według jakich przepisów toczyć się będą postępowania wszczęte i niezakończone przed dniem jej wejścia w życie.

Odnośnie do terminu wejścia w życie przepisów ustawy o zmianie ustawy o ochronie danych osobowych uznać należy, że z uwagi na charakter wprowadzanych zmian, mających na celu implementację Dyrektywy do polskiego porządku prawnego, ustawa - co do zasady - powinna wejść w życie z dniem uzyskania przez Rzeczpospolitą Polską członkostwa w Unii Europejskiej. Krótszy okres vacatio legis przewidziano dla przepisów dotyczących możliwości powołania zastępców Generalnego Inspektora Ochrony Danych Osobowych oraz w odniesieniu do art. 44a, przewidującego instytucję „wykreślenia zbioru danych osobowych z rejestru" prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych.

OCENA SKUTKÓW REGULACJI

1. Wpływ na sektor finansów publicznych.

   Ustawa nie spowoduje automatycznie wzrostu wydatków w budżecie państwa. Jednakże w przypadku powołania zastępców Generalnego Inspektora Ochrony Danych Osobowych, która to możliwość jest przewidziana w ustawie – skutki te w istocie nastąpią. Ich wielkość w skali roku będzie uzależniona od wynagrodzenia ustalonego dla zastępcy (-ów), i – jak należy się spodziewać – zbliżona do wynagrodzenia Generalnego Inspektora Ochrony Danych Osobowych.
2. Wpływ na rynek pracy.

   Brak wpływu.
3. Wpływ na konkurencyjność wewnętrzną i zewnętrzną gospodarki.

   Brak wpływu.
4. Wpływ na sytuację i rozwój regionalny.

   Brak wpływu.

[1)] Ustawa z dnia 25 sierpnia 2001 r. o zmianie ustawy o ochronie danych osobowych, (Dz. U. Nr 100, poz. 1087).

[2)] Ilekroć w niniejszym uzasadnieniu używane będzie pojęcie „Dyrektywa", oznacza ono Dyrektywę 95/46 WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego obiegu tych danych.

UZASADNIENIE DOSTOSOWAWCZEGO CHARAKTERU PROJEKTU USTAWY O ZMIANIE USTAWY O OCHRONIE DANYCH OSOBOWYCH

Projekt ustawy o zmianie ustawy o ochronie danych osobowych ma na celu pełne wdrożenie do polskiego porządku prawnego postanowień Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych. Projekt ustawy uwzględnia jednocześnie uwagi Komisji Europejskiej dotyczące poprawności transpozycji Dyrektywy 95/46/WE.

Zmiany o charakterze dostosowawczym (zmiana nr 1, 2 i 3) mają na celu dokładne określenie przedmiotowe oraz podmiotowe ustawy. Zostało wyraźnie uregulowane do jakiego rodzaju przetwarzania danych stosuje się ustawę oraz umożliwiono stosowanie jej na tych samych zasadach do krajów Europejskiego Obszaru Gospodarczego. Oznacza to, że przepływ danych do tych krajów będzie traktowany tak samo, jak transfer danych na terytorium Polski. Jednocześnie projekt ustawy w rozdziale VII (zmiana nr 24 i 25) umożliwia przekazywanie danych osobowych do krajów trzecich, znajdujących się poza obszarem Europejskiego Obszaru Gospodarczego oraz określa warunki pod jakimi Generalny Inspektor Ochrony danych Osobowych może udzielić zgodę na przekazywanie takich danych. Ponadto, projekt ustawy (zmiany nr 4, 9, 10, 11, 13, 15, 16 i 17) doprowadza do pełnej zgodności ustawy z postanowieniami odpowiednich artykułów dyrektywy 95/46/WE usuwając tym samym niezgodności ustawy przedstawione przez Komisję Europejską.

URZĄD
KOMITETU INTEGRACJI EUROPEJSKIEJ

MINISTER
Prof. dr hab. Danuta Hübner

Min. DH- 3246 /03/DPE-apl

Warszawa, 3 października 2003 r.

Pan
Aleksander Proksa
Sekretarz Rady Ministrów

Opinia o zgodności *projektu ustawy o zmianie ustawy o ochronie danych osobowych* z prawem Unii Europejskiej wyrażona na podstawie art. 2 ust. 1 pkt. 2 ustawy z dnia 8 sierpnia 1996 r. o Komitecie Integracji Europejskiej (DZ. U. Nr 106 poz. 49), przez Sekretarza Komitetu Integracji Europejskiej, Minister Danutę Hübner, działającą z upoważnienia Przewodniczącego Komitetu Integracji Europejskiej.

W związku z przedłożonym projektem ustawy (RM-10-158-03 – *tekst po RM*), pozwalam sobie wyrazić następującą opinię:

I. Projekt ustawy swoim zakresem obejmuje materię, która jest objęta zakresem prawa Unii Europejskiej (Dyrektywa 95/46/WE Parlamentu i Rady z 24 października 1995 r. o ochronie osób w związku z przetwarzaniem danych osobowych oraz o swobodnym obiegu tychże danych) oraz regulacje, które nie są przedmiotem harmonizacji prawa wspólnotowego.

Zakres projektu regulacji transponuje lub doprecyzowuje postanowienia Dyrektywy 95/46/WE w szczególności w następujących zmianach do ustawy o ochronie danych osobowych:

- zmiana nr 1, 2 i 3 – zakres przedmiotowy i podmiotowy ustawy (art. 2, 3, 4 i 9 Dyrektywy);
- zmiana nr 4 – dodanie nowych definicji (art. 2 Dyrektywy);
- zmiana nr 9 – doprecyzowanie transpozycji art. 7 b, c, f Dyrektywy;
- zmiana nr 10 – doprecyzowanie transpozycji art. 10 c Dyrektywy;
- zmiana nr 11 – doprecyzowanie transpozycji art. 11 ust. 1 c Dyrektywy;

- zmiana nr 13 – transpozycja art. 13 ust. 1 Dyrektywy;
- zmiana nr 15 – transpozycja art. 12 a Dyrektywy
- zmiana nr 16 – transpozycja art. 17 ust. 1 Dyrektywy
- zmiana nr 17 – doprecyzowanie transpozycji art. 19 ust. 1 c Dyrektywy;
- zmiana nr 24 i 25 – przekazywanie danych do kraju trzeciego – art. 25 i 26 Dyrektywy.

II. Analiza zgodności projektowanej regulacji z wymogami prawa Unii Europejskiej pozwala na stwierdzenie, iż przedłożony projekt ustawy stanowi prawidłową transpozycję Dyrektywy 95/46/WE.

W konkluzji pozwalam sobie stwierdzić, iż przedłożony projekt ustawy jest zgodny z prawem Unii Europejskiej

Z poważaniem,

Z up. Sekretarza Komitetu
Integracji Europejskiej
PODSEKRETARZ STANU
Jarosław Pietras

Do uprzejmej wiadomości:

Pan Tadeusz Matusiak
Podsekretarz Stanu, Ministerstwo Spraw Wewnętrznych i Administracji.

Pani Ewa Kulesza
Generalny Inspektor Ochrony Danych Osobowych

projekt

ROZPORZĄDZENIE

MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI

z dnia ....2003 r.

w sprawie podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych

Na podstawie art. 45 pkt 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z 2002 r. Nr 153, poz. 1271 oraz z 2003 r. Nr....., poz. .....) zarządza się, co następuje:

§ 1.

Ilekroć w rozporządzeniu jest mowa o:

1) ustawie – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych;
2) identyfikatorze użytkownika – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę uprawnioną do pracy w systemie informatycznym;
3) haśle – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znanych jedynie osobie uprawnionej do pracy w systemie informatycznym;
4) sieci telekomunikacyjnej – rozumie się przez to sieć telekomunikacyjną w rozumieniu ustawy z dnia 21 lipca 2000 r. Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z 2001 r. Nr 122, poz. 1321 i Nr 154, poz. 1800 i 1802, z 2002 r. Nr 25, poz. 253, Nr 74, poz. 676 i Nr 166, poz. 1360 oraz z 2003 r. Nr 50, poz. 424 i Nr 113, poz. 1070);
5) teletransmisji – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej.

§ 2.

1. W celu właściwego zarządzania zabezpieczeniami danych w systemie informatycznym administrator danych osobowych, zwany dalej "administratorem" jest obowiązany do:
   1) ochrony fizycznej obiektu, w którym znajdują się urządzenia i nośniki danych wchodzące w skład systemu informatycznego służącego do przetwarzania danych osobowych;

2) używania systemu informatycznego zapewniającego poufność, rozliczalność i integralność przetwarzanych danych.

2. W celu realizacji obowiązków, o których mowa w ust. 1, administrator jest obowiązany do:
   1) określenia celów przetwarzania danych osobowych, przeprowadzenia analizy ryzyka oraz opracowania na tej podstawie zasad bezpieczeństwa;
   2) oszacowanie środków technicznych i organizacyjnych niezbędnych dla realizacji celów określonych w polityce bezpieczeństwa;
   3) sporządzenia wykazu prowadzonych zbiorów danych osobowych wraz ze wskazaniem używanych do ich przetwarzania systemów informatycznych;
   4) opracowania instrukcji określających sposób zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych oraz sposób postępowania w sytuacji naruszenia ochrony danych osobowych.

§ 3.

1. Zasady bezpieczeństwa, o których mowa w § 2 ust. 2 pkt 1, powinny zostać opracowane w formie pisemnej i określać w szczególności:
   1) środki techniczne i organizacyjne stosowane w celu zabezpieczenia danych osobowych adekwatne do zagrożeń i ryzyka oraz ilości danych i ich zakresu;
   2) sposób monitorowania poprawności działania środków, o których mowa w pkt 1;
   3) zasady opracowywania i wdrażania programów szkoleń w zakresie zabezpieczeń systemów informatycznych;
   4) sposób wykrywania i właściwego reagowania na przypadki naruszenia bezpieczeństwa danych osobowych i systemów informatycznych, w których dane te są przetwarzane;
   5) obszar, w którym przetwarzana są dane osobowe oraz wydzieloną z niego specjalną strefę z urządzeniami i nośnikami danych, na których przechowywane są dane osobowe.
2. Zasady bezpieczeństwa powinny być aktualizowana i dostosowywana do zmieniających się technologicznych i organizacyjnych warunków przetwarzania danych osobowych oraz pojawiających się nowych zagrożeń.

§ 4.

1. Administrator określa obiekty, pomieszczenia lub części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem sprzętu komputerowego.
2. Z obszaru, o którym mowa w ust. 1, administrator wydziela specjalną strefę z urządzeniami i nośnikami danych, na których przechowywane są dane osobowe.
3. Przebywanie osób nieupoważnionych do przetwarzania danych osobowych w obszarze, o którym mowa w ust. 1, jest dopuszczalne tylko za zgodą administratora lub w obecności osoby upoważnionej do przetwarzania danych.
4. Przebywanie osób nieupoważnionych do przetwarzania danych osobowych w strefie, o której mowa w ust. 2, jest dopuszczalne tylko za zgodą administratora danych i w obecności osoby upoważnionej do przetwarzania danych, a dostęp do tej strefy podlega kontroli.
5. Budynki lub pomieszczenia, w których przetwarza się dane osobowe, powinny być zamykane na czas nieobecności osób zatrudnionych przy przetwarzaniu danych osobowych w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym.

§ 5.

1. Administrator jest obowiązany do opracowania i wdrożenia instrukcji, określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, z uwzględnieniem wymogów bezpieczeństwa systemu informatycznego.
2. Instrukcja, o której mowa w ust. 1, jest sporządzona na piśmie i zawiera w szczególności:
   1) nazwy i lokalizacje zbiorów danych oraz systemów informatycznych i programów użytych do ich przetwarzania;
   2) sposób przekazywania danych osobowych pomiędzy poszczególnymi zbiorami danych;
   3) sposób rejestrowania i wyrejestrowywania użytkowników oraz wskazanie osób odpowiedzialnej za te czynności;
   4) sposób uwierzytelniania użytkowników;
   5) określenie procedury rozpoczęcia, zawieszania i zakończenia pracy;
   6) metodę i częstotliwość tworzenia kopii awaryjnych danych osobowych oraz systemów informatycznych służących do ich przetwarzania;

7) sposób, miejsce i czas przechowywania elektronicznych nośników informacji zawierających dane osobowe, systemów używanych do ich przetwarzania oraz wydruków;
8) metodę sprawdzania obecności wirusów komputerowych oraz procedurę aktualizacji bazy antywirusowej;
9) sposób dokonywania przeglądów i konserwacji systemu, użytego do przetwarzania danych osobowych oraz elektronicznych nośników informacji używanych do ich przechowywania;
10) sposób zapewnienia bezpieczeństwa danych podczas ich teletransmisji;
11) sposób zabezpieczenia danych przed zagrożeniami z sieci zewnętrznej;
12) sposób zabezpieczania danych w przypadku ewakuacji.

§ 6.

1. Administrator jest obowiązany do opracowania i wdrożenia instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych, przeznaczonej dla osób zatrudnionych przy przetwarzaniu tych danych.

2. Instrukcja, o której mowa w ust. 1, jest sporządzona na piśmie i określa tryb postępowania w przypadku, gdy:
   1) stwierdzono naruszenie zabezpieczenia systemu informatycznego;
   2) stan systemu informatycznego, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej - mogą wskazywać na naruszenie zabezpieczeń danych osobowych;
   3) wystąpiło zagrożenie naruszenia bezpieczeństwa systemów informatycznych.
3. W przypadkach wystąpienia sytuacji, o których mowa w ust. 2, osoba przetwarzająca dane osobowe jest obowiązana niezwłocznie powiadomić o tym administratora lub inną upoważnioną przez niego osobę.

§ 7.

1. System informatyczny służący do przetwarzania danych osobowych jest wyposażony w mechanizmy uwierzytelnienia użytkownika oraz kontroli dostępu do tych danych.
2. Dla każdego użytkownika systemu informatycznego, w którym przetwarzane są dane osobowe, administrator lub upoważniona przez niego osoba ustala odrębny identyfikator użytkownika.

3. Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora użytkownika oraz dokonaniu uwierzytelnienia.
4. Identyfikator użytkownika, rejestruje się w systemie informatycznym.
5. Identyfikator użytkownika nie powinien być zmieniany bez uzasadnionej przyczyny, a po wyrejestrowaniu z systemu informatycznego nie może być przydzielany innej osobie.
6. Identyfikator użytkownika przypisany osobie, która utraciła uprawnienia do przetwarzania danych osobowych, należy niezwłocznie wyrejestrować z systemu informatycznego oraz podjąć działania zmierzające do zapobieżenia dalszego dostępu tej osoby do danych osobowych.
7. W przypadku, gdy proces uwierzytelnienia osób odpowiedzialnych za administrowanie systemu informatycznego odbywa się przy użyciu hasła, hasło to powinno być przechowywane w miejscu dostępnym jedynie dla upoważnionych osób, a jego udostępnienie i użycie powinno być rejestrowane.
8. W przypadku, gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana powinna następować nie rzadziej, niż co 30 dni. Hasło powinno się składać, co najmniej z 6 znaków.
9. Hasło użytkownika, umożliwiające dostęp do systemu informatycznego, utrzymuje się w tajemnicy, również po upływie jego ważności.

§ 8.

1. Kopie awaryjne, o których mowa w § 5 ust. 2 pkt 6, należy:
   1) sporządzać według określonych procedur;
   2) przechowywać w miejscach zabezpieczających je przed utratą danych;
   3) okresowo sprawdzać pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu;
   4) bezzwłocznie usuwać po ustaniu ich użyteczności.
2. Kopie awaryjne, nie mogą być przechowywane w tych samych pomieszczeniach, w których przechowywane są dane osobowe eksploatowane na bieżąco.

§ 9.

Nośniki informacji, w tym wydruki z danymi osobowymi, przechowuje się w warunkach uniemożliwiających dostęp do nich osobom nieupoważnionym.

§ 10.

Aktualizacja bazy antywirusowej, o której mowa w § 5 ust. 2 pkt 8 powinna być przeprowadzana na bieżąco, nie rzadziej jednak, niż co 30 dni.

§ 11.

1. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób trwały uniemożliwiający ich odczytanie.
2. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do ich przetwarzania, pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie.
3. Urządzenia, dyski lub inne elektroniczne nośniki informacji, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych w sposób uniemożliwiający ich odzyskanie, bądź też naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.
4. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w sposób uniemożliwiający ich odczytanie.

§ 12.

Urządzenia służące do teletransmisji danych osobowych powinny zapewniać ich poufność i integralność podczas teletransmisji.

§ 13.

Urządzenia i systemy informatyczne służące do przetwarzania danych osobowych powinny być zabezpieczone przed utratą tych danych spowodowaną awarią zasilania oraz zakłóceniami w sieci zasilającej.

§ 14.

Osoba użytkująca przenośny komputer zawierający dane osobowe, obowiązana jest zachować szczególną ostrożność podczas jego transportu i przechowywania w celu zapobieżenia dostępowi osób nieupoważnionych do znajdujących się na nim danych osobowych, a w szczególności jest obowiązana:

1) zabezpieczyć dostęp do komputera za pomocą środków zapewniających uwierzytelnienie;

2) nie zezwalać na używanie komputera osobom nieupoważnionym do przetwarzania danych osobowych;
3) zastosować wobec danych osobowych środki ochrony kryptograficznej.

§ 15.

1. Dla każdej osoby, której dane są przetwarzane w systemie informatycznym, w systemie tym odnotowuje się:
   1) datę pierwszego wprowadzenia danych tej osoby, identyfikator użytkownika wprowadzającego te dane oraz źródło ich pochodzenia, jeśli mogą one pochodzić z różnych źródeł,
   2) informacje, komu, kiedy i w jakim zakresie dane zostały udostępnione, chyba że dane te są powszechnie dostępne,
   3) żądania, o którym mowa w art. 32 ust. 1 pkt 7 ustawy, po jego uwzględnieniu oraz sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy,
   4) identyfikator użytkownika wprowadzającego zmiany, datę ich wprowadzenia, a także treść danych przed, jak i po dokonaniu zmian w przetwarzanych danych osobowych.
2. W przypadku, gdy udostępnianie danych osobowych, o których mowa w ust. 1 pkt 2 innemu podmiotowi wykonywane jest systematycznie na podstawie art. 23 ust. 1 pkt 2 lub 3 ustawy, wówczas dopuszczalne jest jednorazowe, zbiorcze ich odnotowanie w systemie informatycznym.

§ 16.

Dla każdej osoby, której dane są przetwarzane w systemie informatycznym, system ten powinien zapewniać możliwość sporządzenia wydruku treści wszystkich dotyczących jej danych przetwarzanych w systemie, wraz z informacjami, o których mowa w §15. Treść wydruku powinna być przedstawiona w powszechnie zrozumiałej formie.

§ 17.

1. W przypadku powierzenia przetwarzania danych osobowych innemu podmiotowi administrator jest obowiązany do sprawdzenia warunków technicznych i organizacyjnych jakie zapewnia podmiot któremu powierzono to przetwarzanie oraz sprawdzenia systemów informatycznych używanych do przetwarzania tych danych.

2. Sprawdzanie, o którym mowa w ust. 1 powinno być dokonywane co najmniej raz w roku i dokumentowane w formie protokołu.

§ 18.

Administrator przetwarzanych w dniu wejścia w życie niniejszego rozporządzenia danych obowiązany jest dostosować system informatyczny, służący do ich przetwarzania, do warunków określonych w niniejszym rozporządzeniu w terminie roku od dnia wejścia w życie rozporządzenia.

§ 19.

Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

Minister Spraw Wewnętrznych i Administracji

U Z A S A D N I E N I E

Projektowany akt ma zastąpić rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 80, poz. 521 z późn. zm.).

Od wejścia w życie ww. rozporządzenia upłynęło już ponad 5 lat. Okres ten w technologii i organizacji systemów informatycznych przyniósł wiele zmian. Nastąpiło upowszechnienie technologii internetowych, nastąpiły zmiany w organizacji pracy, powstały nowe metody uwierzytelniania użytkowników systemów informatycznych. Pojawiły się również nowe zagrożenia.

W okresie od 1998 r. opracowano wiele dokumentów o charakterze normatywnym w zakresie funkcjonalności i bezpieczeństwa systemów informatycznych. Wydano szereg norm w zakresie zarządzania bezpieczeństwem systemów informatycznych (w tym między innymi PN-I-13335-1 – *Wytyczne do zarządzania bezpieczeństwem systemów informatycznych- Pojęcia i modele bezpieczeństwa systemów informatycznych*, PN- ISO/IEC 17799 – *Praktyczne zasady zarządzania bezpieczeństwem informacji*).
W okresie od 1998 r. ustanowione zostały ustawy takie jak: ustawa o ochronie informacji niejawnych (Dz. U. 1999 Nr 11, poz. 95), ustawa o podpisie elektronicznym (Dz. U. 2001, Nr 130, poz. 1450), ustawa o świadczeniu usług drogą elektroniczną (Dz. U. 2002, Nr 144, poz. 1204), w których wprowadzono szereg pojęć oraz regulacji w zakresie wymaganych funkcjonalności oraz bezpieczeństwa systemów informatycznych
Konsekwencją powyższych zmian jest projektowana regulacja.

Szczegółowe omówienie proponowanych zmian:
1.W §1 projektu wprowadzono definicje pojęć używanych w dalszej części rozporządzenia.
2.Zmiana treści §2 ma na celu wskazanie w sposób ogólny obowiązków administratora danych przetwarzającego dane osobowe w systemach informatycznych oraz określenie zadań, których wykonanie w ramach wskazanych obowiązków jest niezbędne. Ponadto wprowadzono pojęcie "zasad bezpieczeństwa".
3.W §3 projektu rozporządzenia dookreślono wymagania odnoszące się do postaci i zawartości dokumentu określającego zasady bezpieczeństwa. Dodatkowo, w §3 ust. 2 projektu nałożono obowiązek dostosowywania zasad bezpieczeństwa do zmieniających się warunków przetwarzania danych. Przesłanką do sprecyzowania w treści rozporządzenia bardziej szczegółowych wymagań odnoszących się do zawartości dokumentu określającego zasady bezpieczeństwa jest mała świadomość wielu administratorów w zakresie treści, jakie dokument taki powinien zawierać. Zasady bezpieczeństwa powinny okreslać procedury wynikające z rzeczywistych, występujących w konkretnym środowisku potrzeb, uwarunkowanych istniejącymi w danych warunkach zagrożeniami i ryzykiem. Zagrożenia, ryzyko i podatność systemu na ich wystąpienia, nie są własnościami bezwzględnymi, lecz własnościami uzależnionymi od środowiska, w jakim dany system jest użytkowany oraz wiedzy i doświadczenia jego użytkowników. W treści projektu rozporządzenia usunięto zapis (§3 rozporządzenia) mówiący o obowiązku wyznaczenia przez administratora danych osoby odpowiedzialnej za bezpieczeństwo danych w systemie informatycznym. Zapis ten usunięto z uwagi na wprowadzenie go do treści ustawy (art. 36 ust. 4 projektu).

1. W §4 projektu zapisano obowiązek wyznaczenia obszaru, w którym przetwarzane są dane osobowe (dotychczas §7 rozporządzenia) oraz obowiązek wyznaczenia strefy specjalnej, w której zlokalizowane są urządzenia, na których przechowywane są dane osobowe. Podział obszaru przetwarzania na dwie kategorie wprowadzono z uwagi na różnice w zakresie potrzeb ich ochrony. Nie ulega wątpliwości, że ochrona urządzeń, na których znajdują się przetwarzane dane osobowe jest ważniejsza (i na czym innym polega) od ochrony urządzeń, które jedynie służą do przetwarzania danych osobowych. W projekcie rozporządzenia wprowadzono takie rozróżnienie i złagodzono warunki, na jakich w obszarze przetwarzania mogą przebywać osoby nieupoważnione do przetwarzania danych osobowych. Zgodnie z treścią §4 projektu, w obszarze przetwarzania danych osobowych, gdzie na urządzeniach używanych do ich przetwarzania nie są przechowywane dane osobowe, mogą przebywać osoby już na podstawie zgody administratora danych. Nie jest w tym celu wymagana obecność osób upoważnionych do przetwarzania danych. Oznacza to, że w pomieszczeniach, gdzie znajdują się komputery, ale nie ma na nich danych osobowych, osoby, które nie posiadają upoważnień do przetwarzania danych osobowych – np. osoby sprzątające, mogą wykonywać swoją pracę poza godzinami zatrudnienia osób upoważnionych do przetwarzania danych.
2. W §5 projektu rozporządzenia zapisano obowiązek administratora danych do opracowania i wdrożenia instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. W §5 ust. 1 projektu zapisano, że istnieje nie tylko obowiązek opracowania instrukcji zarządzania systemem informatycznym, ale również obowiązek jej wdrożenia. W §5 ust 2 projektu rozporządzenia poszerzono zakres zagadnień, jakie powinny być opisane w w/w instrukcji. Wprowadzone zmiany wynikają z potrzeb, jakie powstają w związku z budową coraz bardziej złożonych systemów informatycznych, gdzie dane osobowe mogą być zlokalizowane w różnych miejscach, na różnych urządzeniach (problem przepływu danych) oraz w związku z upowszechnianiem się nowych metod uwierzytelniania (karty mikroprocesorowe, biometria itp.).
3. W §6 projektu zapisano wymóg opracowania i wdrożenia instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych. W stosunku do aktualnej wersji (§6 rozporządzenia) wprowadzono zapis zobowiązujący administratora danych do wdrożenia opracowanej instrukcji. W ust. 2 w/w paragrafy określającej zawartość instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych nie wprowadzono istotnych zmian.
4. W §7 projektu rozporządzenia zapisano podstawowe warunki, jakie powinien spełniać system informatyczny służący do przetwarzania danych osobowych (w aktualnej wersji rozporządzenia warunki te zapisane są w §14). Wyliczone w §7 warunki, jakim powinien odpowiadać system informatyczny, w treści swojej podobne są do poprzednich zapisów zawartych w §14 rozporządzenia. Wprowadzone zmiany polegają głownie na uwzględnieniu nowych rozwiązań i istniejących obecnie standardów. Potrzeby wprowadzenia zmian w treści poprzednich zapisów spowodowana została również zmianami, jakie nastąpiły w technologii systemów informatycznych. Tak np. w ust 2 zapisano, że administrator danych lub upoważniona przez niego osoba ustala *odrębny identyfikator i sposób uwierzytelniania* zamiast dotychczasowego brzmienia „*odrębny identyfikator i hasło”*. Zaproponowana zmiana usuwa błąd w dotychczasowej treści §14 ust. 3 polegający na tym, że zapis o treści „*ustala odrębny identyfikator i hasło*” sugeruje, że środkiem służącym do uwierzytelniania powinno być hasło oraz, że administrator przydzielając hasło użytkownikowi powinien znać jego treść. Interpretacja powyższa jest niepoprawna. Aktualnie znanych jest wiele innych niż identyfikator i hasło metod uwierzytelniania. Standardem stają się metody uwierzytelnienie bazujące nie tylko na odwołaniu się do tego co się zna (np. hasło), ale na kombinacji różnych elementów, np. na tym co się zna i posiada (karta procesorowa z zapisanym identyfikatorem + numer PIN) lub na tym co się zna i kim się jest (hasło + biometryczny dowód tożsamości). W § 7 ust. 7 zapisano istotne z punktu widzenia zarządzania bezpieczeństwem danych,

zasady przechowywania środków służących uwierzytelnianiu osób odpowiedzialnych za eksploatację systemów informatycznych i nadzór nad użytkowanym środowiskiem informatycznym, w którym przetwarzane są dane. Zasady te w istotny sposób różnią się od tych, które odnoszą się do zwykłych użytkowników systemu. W §9 ust. 8 w zapisie dotyczącym częstotliwości zmiany hasła dodano zapis zobowiązujący do stosowania haseł spełniających, co najmniej minimalne wymagania bezpieczeństwa.

5. W §10 projektu zapisano wymóg aktualizowania bazy danych programów antywirusowych dostosowując kryteria zarządzania bezpieczeństwem do ogólnie przyjętych standardów w tym zakresie.
6. W §12 projektu wprowadzono zapis zezwalający na teletransmisje danych osobowych wyłącznie w przypadku, gdy dane te są powszechnie dostępne lub, gdy podczas teletransmisji zapewniona jest ich poufność i integralność. Wprowadzony w §12 zapis zastępuje zapis istniejący w §2 ust. 3 aktualnej wersji rozporządzenia, który był niejednoznaczny. Jego treść „*określić potrzeby w zakresie zabezpieczenia zbiorów danych osobowych i systemów informatycznych, z uwzględnieniem potrzeb kryptograficznej ochrony danych osobowych, w szczególności podczas ich przesyłania za pomocą teletransmisji danych*" był niejednoznaczny. Nie wskazywał on, kiedy zabezpieczenia kryptograficzne powinno się stosować. Użyte tam sformułowania „*uwzględnienia potrzeb kryptograficznej ochrony danych*" nie wnosiło praktycznie żadnych skutków.
7. W §14 projektu zmieniono zawarte aktualnie w §9 rozporządzenia wymagania odnoszące się do użytkowania komputerów przenośnych. Zamiast obowiązku zabezpieczenia komputera hasłem, zapisano bardziej ogólnie obowiązek zabezpieczenia dostępu za pomocą środków zapewniających uwierzytelnienie (nie koniecznie hasłem). Dodatkowo wprowadzono obowiązek stosowania środków ochrony kryptograficznej. Przesłanką do zaostrzenia wymagań w powyższym zakresie są zgłoszenia do GIODO kradzieży komputerów przenośnych z danymi osobowymi oraz postęp w dostępności środków ochrony kryptograficznej. Środki takie dostępne są obecnie coraz częściej w ramach standardowego oprogramowania systemowego komputerów.
8. W §15 projektu zawarto wymogi w zakresie odnotowywania w systemie informatycznym służącym do przetwarzania danych osobowych informacji o:
   - dacie pierwszego wprowadzania danych osobowych do systemu, identyfikatorze użytkownika, który je wprowadził oraz źródle ich pozyskania (§15 ust. 1 pkt 1 projektu),
   - udostępnieniach danych innym podmiotom w zakresie komu, kiedy i jakie informacje zostały udostępnione (§15 ust. 1 pkt 2 projektu),
   - żądaniach oraz sprzeciwach, o których mowa w art. 32 ust. 1 pkt 7 i 8 ustawy (§15 ust. 1 pkt 3 projektu), oraz
   - wprowadzanych zmianach w treści przetwarzanych danych poprzez odnotowanie identyfikatora użytkownika wprowadzającego zmiany, daty tych zmian, a także treści danych przed jak i po dokonaniu zmian (§15 pkt 4 projektu).

   Zaproponowany zapis §15 projektu, podobnie zresztą, jak zapis istniejący w §16 aktualnego rozporządzenia sugeruje, aby informacje o dacie wpisania danych, identyfikatorze osoby wpisującej oraz źródle pochodzenia danych wpisywać zbiorczo w odniesieniu do wszystkich (całej „paczki" danych – nazywanych w terminologii informatycznej rekordem), wpisywanych podczas rejestracji danych, a nie w odniesieniu do każdej danej oddzielnie. Celem tych zapisów jest zapewnienie możliwości sprawowania przez administratora danych, zadań, o których mowa w art. 38 ustawy t.j. *zapewnienia kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane, zwłaszcza, gdy przekazuje się je za pomocą urządzeń teletransmisji danych*. Z brzmienia powyższego zapisu ustawy nie wynika jednoznacznie, czy chodzi o:

1) odnotowanie w/w informacji jednorazowo przy wpisie całej „paczki" danych odnoszącej się do danej osoby, a następnie rejestrowanie poszczególnych zmian, czy też, o
2) odnotowanie w/w informacji przy każdej danej odnoszącej się do danej osoby.

Przy założeniu, że dane osoby składają się z „paczki" danych, na którą składają się:
- imię i nazwisko,
- data urodzenia,
- miejsca zamieszkania,
- miejsca pracy,
- nr telefonu domowego,
- nr telefonu komórkowego,

przy rozumieniu obowiązku odnotowania, jak w punkcie 1, wraz z wpisem powyższych danych należałoby odnotować datę, utworzenia wpisu, identyfikator osoby wpisującej oraz źródło pozyskania danych rozszerzając wpis np. w następujący sposób:
- imię i nazwisko,
- data urodzenia,
- miejsca zamieszkania,
- miejsca pracy,
- nr telefonu domowego,
- nr telefonu komórkowego,
- *data wpisu,*
- *identyfikator wpisującego,*
- *źródło pozyskania danych.*

Rzeczą naturalną jest jednak, że dane dotyczące danej osoby, mogą być wpisane w różnych częściach przez różne osoby. Inne też mogą być źródła poszczególnych informacji. Ponadto, dane te mogą być uzupełniane i modyfikowane w czasie. W związku z powyższym uzasadniona może być interpretacja art. 38 ustawy prowadząca do wniosku, że należy wprowadzać odnotowania w sensie, o którym mowa w punkcie 15 ppkt 2 przedmiotowego pisma. Spowoduje to jednak konieczność tworzenia wpisu w systemie informatycznym w postaci umożliwiającej odnotowywanie w/w informacji przy każdej danej, co zilustrowano poniżej:

imię i nazwisko	*data wpisu,*	*identyfikator wpisującego*	*źródło pozyskania danych*
data urodzenia,	*data wpisu,*	*identyfikator wpisującego*	*źródło pozyskania danych*
miejsce zamieszkania	*data wpisu,*	*identyfikator wpisującego*	*źródło pozyskania danych*
miejsca pracy	*data wpisu,*	*identyfikator wpisującego*	*źródło pozyskania danych*
nr tel. dom.	*data wpisu,*	*identyfikator wpisującego*	*źródło pozyskania danych*
nr tel. kom.	*data wpisu,*	*identyfikator wpisującego*	*źródło pozyskania danych*

Niezależnie od powyższego, w przypadku modyfikacji jakiejkolwiek danej dodatkowo powinny być tworzone wpisy typu:

Nazwa modyfikowanej danej	*aktualna wartość danej*	*nowa wartość danej*	*data modyfikacji*	*identyfikator modyfikujacego*	*źródło danych do modyfikacji*

Zaproponowany zapis § 15 projektu, stanowi pośrednie rozwiązanie powyższego problemu. W rozwiązaniu tym wprowadza się obowiązek odnotowania informacji o dacie wprowadzenia danych, identyfikatorze użytkownika wprowadzającego dane oraz źródle pozyskania danych, jeden raz w odniesieniu do całej „paczki" danych (§15 pkt 1 projektu). Informacje o zmianach danych, w tym również uzupełnianiu danych, których nie wprowadzono przy tworzeniu pierwszego wpisu, proponuje się odnotowywać w postaci prowadzenia tzw.

rejestru zmian (§15 pkt 4 projektu). Zaproponowane rozwiązanie w zakresie *„zapewnienia kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone”* są zgodne ze stosowaną w tym zakresie praktyką.

9. § 16 projektu zaproponowano nowe brzmienie warunku, który aktualnie stanowi § 17 rozporządzenia. Celem wprowadzonych zmian jest jednoznaczne wskazanie, że system służący do przetwarzania danych osobowych powinien posiadać funkcję umożliwiającą sporządzenie wydruku danych osobowych wskazanej osoby.
10. W § 18 przewidziano roczny termin dla administratorów na dostosowanie systemów informatycznych służących do przetwarzania danych do warunków określonych w projektowanym akcie.

Zestawienie przepisów prawa Unii Europejskiej, których wdrożenie jest celem projektu ustawy o zmianie ustawy o ochronie danych osobowych

Lp.	Nr i treść przepisu implementowanej Dyrektywy 95/46 Parlamentu Europejskiego oraz Rady z 24 października 1995 r. o ochronie osób fizycznych w związku z przetwarzaniem ich danych osobowych oraz o swobodnym obiegu tych danych	Nr i treść przepisu w brzmieniu nadawanym projektowaną ustawą o zmianie ustawy o ochronie danych osobowych wdrażającego odpowiedni przepis Dyrektywy
1.	**Artykuł 3 ust. 1:** Niniejsza Dyrektywa dotyczy przetwarzania danych osobowych w całości lub w części w sposób zautomatyzowany oraz innego przetwarzania danych osobowych, stanowiących część zbioru danych lub mających stanowić część zbioru danych.	**Art. 2 ust. 2 pkt 2:** Ustawę stosuje się do przetwarzania danych (...): 2) w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych.
2.	**Artykuł 4 ust. 1 lit.c:** Każde państwo członkowskie stosuje w odniesieniu do przetwarzania danych osobowych postanowienia prawa krajowego, jakie wprowadzi na podstawie niniejszej Dyrektywy wówczas, gdy (...) administrator danych nie prowadzi działalności na terytorium Wspólnoty lecz, dla celów przetwarzania danych osobowych, wykorzystuje środki, zarówno zautomatyzowane jak i inne, znajdujące się na terytorium wymienionego państwa członkowskiego (...).	**Art. 3 ust. 1:** Ustawę stosuje się do: 1) organów państwowych oraz organów samorządu terytorialnego, 2) państwowych i komunalnych jednostek organizacyjnych, 3) podmiotów niepaństwowych realizujących zadania publiczne, 4) osób fizycznych i osób prawnych oraz jednostek organizacyjnych nie posiadających osobowości prawnej, jeżeli przetwarzają dane osobowe w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych, - które mają siedzibę albo miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej, albo w kraju trzecim, o ile przetwarzają dane osobowe przy wykorzystaniu środków technicznych znajdujących się na terytorium Rzeczypospolitej Polskiej.

3.	**Artykuł 4 ust. 1 lit.c:** Każde państwo członkowskie stosuje w odniesieniu do przetwarzania danych osobowych postanowienia prawa krajowego, jakie wprowadzi na podstawie niniejszej Dyrektywy wówczas, gdy (...) administrator danych nie prowadzi działalności na terytorium Wspólnoty lecz, dla celów przetwarzania danych osobowych, wykorzystuje środki, zarówno zautomatyzowane jak i inne, znajdujące się na terytorium wymienionego państwa członkowskiego, o ile środki te nie są wykorzystywane wyłącznie do celów tranzytu przez terytorium Wspólnoty.	**Art. 3a ust. 1 pkt 2:** Ustawy nie stosuje się do (...): 2) podmiotów mających siedzibę albo miejsce zamieszkania w kraju trzecim, wykorzystujących środki techniczne służące wyłącznie do przekazywania danych.
4.	**Artykuł 4 ust. 2:** W okolicznościach, o których mowa w ust. 1 lit.c, administrator danych musi wyznaczyć swojego przedstawiciela na terytorium tego państwa członkowskiego, niezależnie od środków prawnych, jakie mogą być podjęte przeciwko samemu administratorowi danych.	**Art. 3 ust. 2:** W przypadku przetwarzania danych osobowych przez podmioty mające siedzibę albo miejsce zamieszkania w kraju trzecim, administrator danych jest obowiązany wyznaczyć swojego przedstawiciela w Rzeczypospolitej Polskiej. Przedstawiciel administratora danych w Rzeczypospolitej Polskiej ponosi odpowiedzialność za przestrzeganie przepisów niniejszej ustawy, jak administrator danych, niezależnie od odpowiedzialności administratora danych.
5.	**Artykuł 9:** Państwa członkowskie wprowadzą wyłączenia lub zwolnienia z postanowień niniejszego rozdziału, rozdziału IV i rozdziału VI, w przypadku przetwarzania danych osobowych wyłączenie w celach dziennikarskich lub dla celu artystycznej lub literackiej wypowiedzi jedynie wówczas, gdy jest to konieczne dla pogodzenia prawa do prywatności z normami dotyczącymi wolności wypowiedzi.	**Art. 3a ust. 2:** Z wyjątkiem przepisów rozdziału V ustawy nie stosuje się również do prasowej działalności dziennikarskiej w rozumieniu ustawy z dnia 26 stycznia 1984 r. Prawo prasowe (Dz.U. z 1984 r. Nr 5, poz. 24 z późn. zm.) oraz do działalności literackiej lub artystycznej chyba, że prawo do wolności wypowiedzi istotnie narusza prawa i wolności osoby, której dane dotyczą.
6.	**Artykuł 2 lit.g:** Dla potrzeb niniejszej Dyrektywy (...): g) „odbiorca” oznacza osobę fizyczną lub prawną, urząd publiczny, agendę lub inny organ, któremu ujawniane są dane, będący lub niebędący osobą trzecią;	**Art. 7 pkt 6:** Ilekroć w ustawie jest mowa o (...): 6) odbiorcy danych – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:

	jednakże władze, które mogą otrzymywać dane w ramach konkretnego dochodzenia nie są uważane za odbiorcę.	a) osoby, której dane dotyczą, b) osoby zatrudnionej przy przetwarzaniu danych, c) przedstawiciela, o którym mowa w art. 3 ust. 2, d) podmiotu, o którym mowa w art. 31, e) organów państwowych lub samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.
7.	**Artykuł 7 lit.c:** Państwa członkowskie zapewnią, aby dane osobowe mogły być przetwarzane tylko wówczas, gdy (...): c) przetwarzanie danych jest konieczne dla zgodności z zobowiązaniem prawnym, któremu administrator danych podlega.	**Art. 23 ust. 1 pkt 2:** Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy (...): 2) jest to niezbędne dla zrealizowania uprawnienia lub obowiązku wynikającego z przepisu prawa.
8.	**Artykuł 7 lit.b:** Państwa członkowskie zapewnią, aby dane osobowe mogły być przetwarzane tylko wówczas, gdy (...): 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.	**Art. 23 ust. 1 pkt 3:** Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy (...): 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 życzenie osoby, której dane dotyczą.
9.	**Artykuł 7 lit.f:** Państwa członkowskie zapewnią, aby dane osobowe mogły być przetwarzane tylko wówczas, gdy (...): f) przetwarzanie danych jest konieczne dla potrzeb wynikających z uzasadnionych interesów administratora danych lub osoby trzeciej, przed którą ujawnia się dane, z wyjątkiem sytuacji kiedy interesy takie podporządkowane są interesom związanym z podstawowymi prawami i wolnościami osoby, której dane dotyczą, i które wymagają ochrony na podstawie art. 1 ust. 1.	**Art. 23 ust. 1 pkt 5:** Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy (...): 5) jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych bądź odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.
10.	**Artykuł 10 lit.c tiret trzecie:** Państwa członkowskie zapewnią, że administrator danych lub jego przedstawiciel zobowiązany będzie przedstawić osobie, której dane dotyczą i od której gromadzone są dane co najmniej następujące informacje, z	**Art. 24 ust. 1 pkt 3:** W przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o (...):

	wyjątkiem przypadku, kiedy posiada już ona informacje dotyczące (...): - prawa dostępu do swoich danych oraz ich poprawienia.	3) prawie dostępu do swoich danych oraz ich poprawiania.
11.	**Artykuł 11 ust. 1 lit.c tiret trzecie:** W przypadku gdy dane nie zostały uzyskane od osoby, której dane dotyczą, państwa członkowskie zapewnią, aby administrator danych albo jego przedstawiciel był zobowiązany w chwili przystąpienia do rejestracji danych osobowych lub w przypadku planowania ujawnienia osobie trzeciej, ale nie później gdy dane te są ujawniane po raz pierwszy, dostarczyć osobie, której dane dotyczą, z wyjątkiem przypadku, gdy uzyskał je już wcześniej, co najmniej następujące informacje (...): - prawie wglądu do swoich danych oraz ich poprawienia.	**Art. 25 ust. 1 pkt 4:** W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o (...): 4) prawie dostępu do swoich danych oraz ich poprawiania.
12.	**Artykuł 13 ust. 1:** Państwo członkowskie może przyjąć środki ustawodawcze w celu ograniczenia zakresu praw i obowiązków, przewidzianych w art. 6 ust. 1, 10, 11 ust. 1, 12 oraz 21, kiedy ograniczenie takie stanowi środek konieczny dla zabezpieczenia: (a) bezpieczeństwa narodowego; (b) obronności; (c) bezpieczeństwa publicznego; (d) działań prewencyjnych, prowadzonych czynności dochodzeniowo-śledczych i prokuratorskich w sprawach kryminalnych lub sprawach o naruszenie zasad etyki w zawodach podlegających regulacjom; (e) ważnego interesu ekonomicznego lub finansowego państwa członkowskiego lub Unii Europejskiej, łącznie ze sprawami monetarnymi, budżetowymi i podatkowymi; (f) funkcji kontrolnych, inspekcyjnych i regulacyjnych związanych, nawet sporadycznie z wykonywaniem władzy publicznej w przypadkach wymienionych w lit. (c), (d) i (e); (g) ochrony osoby, której dane dotyczą oraz praw i wolności innych osób.	**Art. 30 pkt 2:** Administrator danych odmawia udostępnienia danych osobowych ze zbioru danych podmiotom i osobom innym niż wymienione w art. 29 ust. 1, jeżeli spowodowałoby to (...): 2) zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego.
13.	**Artykuł 12 lit.a tiret trzecie:**	**Art. 32 ust. 1 pkt 5a:**

	Państwa członkowskie zapewnią każdej osobie, której dane dotyczą, prawo do uzyskania od administratora danych bez ograniczeń, w odpowiednich odstępach czasu oraz bez nadmiernego opóźnienia lub kosztów (...) wiadomości na temat zasad automatycznego przetwarzania dotyczących jej danych przynajmniej w przypadku zautomatyzowanego procesu decyzyjnego, o którym w art. 15 ust. 1.	Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do (...): „5a) uzyskania informacji o przesłankach podjęcia rozstrzygnięcia, o którym mowa w art. 26a ust. 2,”.
14.	**Artykuł 17 ust. 1:** Państwa członkowskie zapewnią, aby administrator danych wprowadził odpowiednie środki techniczne i organizacyjne w celu ochrony danych osobowych przed przypadkowym lub nielegalnym zniszczeniem lub przypadkową utratą, zmianą, niedozwolonym ujawnieniem lub dostępem, szczególnie wówczas, gdy przetwarzanie danych obejmuje transmisje danych w sieci, jak również przed wszelkimi innymi nielegalnymi formami przetwarzania. Środki te zapewnią poziom bezpieczeństwa odpowiedni do zagrożeń wynikających z przetwarzania danych oraz charakteru danych objętych ochroną.	**Art. 36 ust. 1:** Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
15.	**Artykuł 19 ust. 1 lit.c:** Państwa członkowskie ustalą, jakie informacje zostaną podane w powiadomieniu. Będą one obejmować co najmniej (...): c) opis jednej lub kilku kategorii osób, których dane dotyczą oraz danych lub kategorii danych, które się do nich odnoszą.	**Art. 41 ust. 1 pkt 3a:** Zgłoszenie zbioru danych do rejestracji powinno zawierać (...): 3a) opis kategorii osób, których dane dotyczą oraz zakres przetwarzanych danych.
16.	**Artykuł 18 ust. 2 tiret pierwsze:** Państwa członkowskie mogą prowadzić uproszczenie procedury lub zwolnienie z obowiązku powiadomienia tylko w następujących sytuacjach oraz na następujących warunkach (...): - jeżeli, w przypadku kategorii operacji przetwarzania, co do których mało prawdopodobne jest, biorąc pod uwagę dane przeznaczone do przetworzenia, aby niekorzystnie wpłynęły na prawa i wolności osób, których dane dotyczą, określają cele przetwarzania danych, dane lub kategorie danych, przechodzących proces przetwarzania, kategorię lub kategorie osób, których dane dotyczą, odbiorców lub kategorie odbiorców, którym dane mają być ujawnione oraz długość okresu	**Art. 43 ust. 1a:** Przepisów ust. 1 pkt 2, 2a, 4-11 nie stosuje się w przypadku przetwarzania danych, o których mowa w art. 27 ust. 1.

	przechowywania danych (...). **Artykuł 20 ust. 1:** Państwa członkowskie zdefiniują operacje przetwarzania danych mogące stwarzać określone zagrożenia dla praw i wolności osób, których dane dotyczą oraz będą kontrolować, czy operacje te są badane przed ich rozpoczęciem (...).	
17.	**art. 25 ust. 1** Państwa członkowskie zapewnią, że przekazywanie do kraju trzeciego danych osobowych poddawanych przetwarzaniu lub przeznaczonych do przetwarzania po ich przekazaniu może nastąpić tylko wówczas, gdy - niezależnie od zgodności z krajowymi przepisami przyjętymi na podstawie innych postanowień niniejszej dyrektywy - dany kraj trzeci zapewni odpowiedni stopień ochrony.	**art. 47** Przekazanie danych osobowych do kraju trzeciego może nastąpić, jeżeli kraj docelowy daje gwarancje ochrony danych osobowych na swoim terytorium przynajmniej takie, jakie obowiązują na terytorium Rzeczypospolitej Polskiej.
18.	**Artykuł 26 ust. 2** (...) Niezależnie od postanowień ust. 1, państwo członkowskie może zezwolić na przekazanie lub przekazywanie danych osobowych do kraju trzeciego, który nie zapewnia odpowiedniego stopnia ochrony w znaczeniu art. 25 ust. 2, jeżeli administrator danych zapewni odpowiednie zabezpieczenia odnośnie ochrony prywatności oraz podstawowych praw i wolności osoby oraz odnośnie wykonywania związanych z nimi praw; zabezpieczenia takie mogą w szczególności wynikać z odpowiednich klauzul umownych.	**Art. 48:** W przypadkach innych niż wymienione w art. 47 ust. 2 i 3 przekazanie danych osobowych do kraju trzeciego, który nie daje gwarancji ochrony danych osobowych przynajmniej takich, jakie obowiązują na terytorium Rzeczypospolitej Polskiej, może nastąpić po uzyskaniu zgody Generalnego Inspektora, pod warunkiem, że administrator danych zapewni odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą.
19.	**Rozdział IV Dyrektywy 95/46/WE** Przekazywanie danych osobowych do **krajów trzecich**	**Art. 7 pkt 7:** Ilekroć w ustawie jest mowa o (...): 7) kraju trzecim - rozumienie się przez to kraj nie należący do Europejskiego Obszaru Gospodarczego.

DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY

z dnia 24 października 1995

w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych

95/46/WE

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ:

uwzględniając Traktat ustanawiający Wspólnotę Europejską, a w szczególności zaś jego art. 100a,

uwzględniając projekt Komisji[1],

uwzględniając opinię Komitetu Ekonomiczno - Społecznego[2],

oraz działając zgodnie z procedurą ustanowioną w art. 189b Traktatu[3],

a także mając na uwadze , że

(1) cele Wspólnoty, określone w Traktacie, wraz ze zmianami wprowadzonymi Traktatem o Unii Europejskiej, obejmują tworzenie coraz ściślejszej wspólnoty narodów Europy, kształtowanie bliższych stosunków między państwami należącymi do Wspólnoty, zapewnienie postępu ekonomiczno-społecznego poprzez wspólne działania na rzecz likwidacji barier dzielących Europę, pobudzanie ciągłej poprawy warunków życia jej narodów, ochronę i umacnianie pokoju i wolności oraz rozwój demokracji w oparciu o fundamentalne prawa uznane w konstytucjach i ustawodawstwach państw członkowskich oraz w Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności;

(2) systemy przetwarzania danych są tworzone po to, aby służyły człowiekowi; zważywszy, że muszą one, niezależnie od obywatelstwa czy miejsca stałego zamieszkania osób fizycznych, respektować ich podstawowe prawa i wolności, szczególnie prawo do prywatności, oraz przyczyniać się do postępu ekonomiczno-społecznego, rozwoju handlu oraz dobrobytu jednostek;

(3) utworzenie i funkcjonowanie rynku wewnętrznego, na którym zgodnie z art. 7a Traktatu, zapewniony jest swobodny przepływ towarów, osób, usług i kapitału wymaga nie tylko

---

Dz.U. WE nr C 277, 5. 11. 1990, str. 3 i Dz.U. WE nr C 311, 27. 11. 1992, str. 30.

[2] Dz.U. WE nr C 159, 17. 06. 1991, str. 38

[3] Opinia Parlamentu Europejskiego z 11. 03. 1992 (Dz.U. WE nr C 94, 13.04.1992, str. 198) zatwierdzona 2 grudnia 1993 (Dz.U. WE nr C 342, 20.12.1993, str. 30); Wspólna pozycja Rady z dnia 20 lutego 1995 (Dz.U. WE nr C 93, 13.04.1995, str. 1) i Decyzja Parlamentu Europejskiego z 15 czerwca 1995 (Dz.U. WE nr C 166, 3.07.1995).

zapewnienia swobodnego przepływu danych osobowych z jednego państwa członkowskiego do drugiego, lecz również ochrony podstawowych praw jednostek;

(4) coraz częściej we Wspólnocie korzysta się z przetwarzania danych osobowych w różnych sferach życia gospodarczego i społecznego, a postęp technologii w dziedzinie przetwarzania informacji sprawia, że przetwarzanie i wymiana danych stają się coraz łatwiejsze;

(5) integracja ekonomiczno-społeczna będąca wynikiem utworzenia i funkcjonowania rynku wewnętrznego w rozumieniu art. 7a Traktatu będzie prowadzić do znacznego zwiększenia przepływu danych osobowych przez granicę między wszystkimi podmiotami zaangażowanymi prywatnie lub publicznie w działalność ekonomiczną i społeczną w państwach członkowskich; wzrośnie wymiana danych osobowych między przedsiębiorstwami działającymi w różnych państwach członkowskich; władze państwowe poszczególnych państw członkowskich podejmują się na mocy prawa Wspólnoty do współpracy i wymiany danych osobowych w celu uzyskania zdolności wykonywania swoich obowiązków oraz realizacji zadań w imieniu władz innego państwa członkowskiego w kontekście obszaru bez granic wewnętrznych, ustanowionego przez rynek wewnętrzny;

(6) ponadto, zwiększenie współpracy naukowo-technicznej oraz proces skoordynowanego wprowadzania nowych sieci telekomunikacyjnych we Wspólnocie narzuca konieczność i ułatwia przepływ danych osobowych przez granicę;

(7) różnica w stopniu ochrony praw i swobód jednostek, szczególnie prawa do prywatności, w odniesieniu do przetwarzania danych osobowych, zapewnionego w poszczególnych państwach członkowskich może uniemożliwiać przesyłanie tych danych z terytorium jednego państwa członkowskiego do drugiego państwa członkowskiego; różnica ta może zatem stanowić przeszkodę w realizacji szeregu przedsięwzięć ekonomicznych na szczeblu Wspólnoty, zakłócać konkurencję i utrudniać władzom wykonywanie ich obowiązków wynikających z przepisów prawa Wspólnoty; wspomniana różnica w stopniu ochrony jest wynikiem istnienia wielkiej różnorodności krajowych ustaw, przepisów i postanowień o charakterze administracyjnym;

(8) w celu zniesienia przeszkód w przepływie danych osobowych, stopień ochrony praw i swobód jednostki w zakresie przetwarzania tych danych musi być równoważny we wszystkich państwach członkowskich; cel ten ma żywotne znaczenie dla rynku wewnętrznego, lecz nie może on być osiągnięty przez same państwa członkowskie, szczególnie mając na uwadze skalę rozbieżności, jakie obecnie występują między odpowiednim ustawodawstwem państw członkowskich oraz potrzebę dokonania koordynacji przepisów ustawodawczych państw członkowskich w celu zapewnienia jednolitej regulacji przepływu danych osobowych przez granicę, zgodnie z celem rynku wewnętrznego, o którym mowa w art. 7a Traktatu; konieczne są działania Wspólnoty na rzecz zbliżenia ustawodawstwa;

(9) biorąc pod uwagę ochronę równorzędną wynikającą ze zbliżania ustawodawstwa krajowego, państwa członkowskie nie będą już mogły utrudniać między sobą swobodnego przepływu danych osobowych na podstawie ochrony praw i wolności jednostek, a zwłaszcza prawa do prywatności; państwa członkowskie będą miały

pozostawiony margines swobody działania, z którego mogą również, w kontekście wdrażania dyrektywy. korzystać partnerzy handlowi i społeczni; państwa członkowskie będą zatem mogły określić w swoim ustawodawstwie ogólne warunki regulujące legalność procesu przetwarzania danych; podejmując te działania państwa członkowskie będą dokładać starań w celu poprawienia ochrony, gwarantowanej przez ich obecne ustawodawstwo; w granicach wspomnianego marginesu swobody działania oraz zgodnie z prawem Wspólnoty mogą wystąpić rozbieżności we wdrażaniu dyrektywy, co może mieć wpływ na przepływ danych w państwie członkowskim jak również we Wspólnocie;

(10) celem krajowego ustawodawstwa dotyczącego przetwarzania danych osobowych jest ochrona podstawowych praw i wolności, szczególnie prawa do prywatności, które zostało uznane zarówno w art. 8 Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności oraz w ogólnych zasadach prawa Wspólnoty; z tego powodu zbliżanie ustawodawstw nie powinno wpłynąć na zmniejszenie ochrony, jaką gwarantują, lecz przeciwnie, musi dążyć do zapewnienia jak najwyższego stopnia ochrony we Wspólnocie;

(11) zasady ochrony praw i swobód jednostek, szczególnie prawa do prywatności, które zawarte są w niniejszej dyrektywie, utrwalają i umacniają zasady wyrażone w Konwencji Rady Europy z dnia 28 stycznia 1981 w sprawie ochrony jednostek w zakresie automatycznego przetwarzania danych osobowych;

(12) zasady ochrony muszą odnosić się do całokształtu przetwarzania danych osobowych przez każdą osobę, której działania podlegają przepisom prawa Wspólnoty; należy wyłączyć przetwarzanie danych dokonywane przez osobę fizyczną w ramach działań o charakterze wyłącznie osobistym lub domowym, jak np. korespondencja i przechowywanie spisów adresów;

(13) działania, o których mowa w rozdziałach V i VI Traktatu o Unii Europejskiej odnoszących się do bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa w dziedzinie prawa karnego, bez wpływu na obowiązki nałożone na państwa członkowskie na mocy art. 56 ust. 2, art. 57 lub art. 100a Traktatu o utworzeniu Wspólnoty Europejskiej, nie wchodzi w zakres prawa wspólnotowego, przetwarzanie danych osobowych konieczne dla zapewnienia ochrony dobrego stanu gospodarczego państwa nie wchodzi w zakres niniejszej dyrektywy, o ile przetwarzanie danych dotyczy spraw bezpieczeństwa państwa;

(14) jeżeli w ramach społeczeństwa informacyjnego ma znaczenie rozwój technik gromadzenia, przekazywania, kompilowania, rejestrowania, przechowywania i przesyłania danych dźwiękowych i obrazowych osób fizycznych, niniejsza dyrektywa powinna mieć zastosowanie do przetwarzania takich danych;

(15) przetwarzanie tych danych jest objęte niniejszą dyrektywą tylko wówczas, gdy jest ono zautomatyzowane lub jeśli dane zawarte są lub przeznaczone do umieszczenia w zbiorze danych zorganizowanym według określonych kryteriów dotyczących osób fizycznych w celu zapewnienia łatwego dostępu do wspomnianych danych osobowych;

(16) przetwarzanie danych dźwiękowych i obrazowych, np. w przypadku nadzoru kamer wideo, nie wchodzi w zakres niniejszej dyrektywy, jeśli dokonywane jest dla potrzeb bezpieczeństwa publicznego, obronności, bezpieczeństwa narodowego lub też w trakcie

działań organów państwowych w dziedzinie prawa karnego lub innych działań nie wchodzących w zakres prawa Wspólnoty;

(17) jeśli chodzi o przetwarzanie danych dźwiękowych i obrazowych dla potrzeb dziennikarstwa, lub dla potrzeb literackich lub artystycznych, zwłaszcza w dziedzinie techniki audiowizualnej, zasady dyrektywy mają zastosowanie ograniczone, zgodnie z postanowieniami określonymi w art. 9;

(18) aby nie dopuścić do pozbawienia jednostek ochrony, do której mają prawo na mocy niniejszej dyrektywy, wszelkie przetwarzanie danych osobowych we Wspólnocie musi odbywać się zgodnie z przepisami prawa jednego z państw członkowskich, w związku z tym przetwarzanie danych, za które odpowiada administrator danych prowadzący działalność gospodarczą na terenie państwa członkowskiego, powinno być regulowane przez ustawodawstwo danego państwa;

(19) prowadzenie działalności gospodarczej na terytorium państwa członkowskiego zakłada efektywne i rzeczywiste prowadzenie działań poprzez stabilne postanowienia; forma prawna prowadzonej działalności gospodarczej, niezależnie czy to oddział lub filia z osobowością prawną, nie jest w tym względzie czynnikiem decydującym; w przypadku ustanowienia jednego administratora danych na terytorium kilku państw członkowskich, szczególnie w postaci filii, w celu uniknięcia obejścia przepisów krajowych, musi on zapewnić, że każda z prowadzonej działalności gospodarczej będzie spełniać obowiązki wynikające z krajowego ustawodawstwa;

(20) przetwarzanie danych przez osobę prowadzącą działalność w kraju trzecim nie powinno stać na przeszkodzie ochrony osób fizycznych przewidzianej w niniejszej dyrektywie; w tych przypadkach przetwarzanie danych powinno podlegać przepisom prawa państwa członkowskiego, w którym znajdują się wykorzystywane do tego celu środki oraz powinny istnieć gwarancje, zapewniające przestrzeganie w praktyce praw i obowiązków przewidzianych w niniejszej dyrektywie;

(21) niniejsza dyrektywa nie narusza zasad terytorialności, stosowanych w sprawach kryminalnych;

(22) państwa członkowskie sprecyzują w ogłaszanych ustawach lub przy wprowadzaniu w życie środków podjętych w niniejszej dyrektywie ogólne warunki, w których przetwarzanie danych jest zgodne z prawem; w szczególności art. 5 w połączeniu z art. 7 i 8, umożliwia państwom członkowskim, niezależnie od zasad ogólnych, zapewnienie specyficznych warunków przetwarzania danych dla konkretnych branż oraz dla różnych kategorii danych objętych art. 8;

(23) państwa członkowskie są upoważnione do zapewnienia ochrony osób fizycznych zarówno poprzez ogólne ustawodawstwo o ochronie jednostek w odniesieniu do przetwarzania danych osobowych oraz poprzez ustawodawstwo branżowe, jak np. odnoszące się do urzędów statystycznych;

(24) niniejsza dyrektywa nie dotyczy ustawodawstwa dotyczącego ochrony osób prawnych w odniesieniu do przetwarzania ich danych;

(25) zasady ochrony powinny znajdować odzwierciedlenie, z jednej strony w obowiązkach nałożonych na osoby, władze publiczne, przedsiębiorstwa, agencje i inne organy odpowiedzialne za przetwarzanie danych, zwłaszcza w zakresie jakości danych, bezpieczeństwa technicznego, zawiadamiania organu nadzoru oraz okoliczności, w których może odbywać się przetwarzanie danych, jak również, z drugiej strony, w prawie osób, których dane są przedmiotem przetwarzania, do uzyskania informacji, że takie przetwarzanie danych ma miejsce, do konsultowania danych, żądania poprawek lub nawet sprzeciwu wobec przetwarzania danych w niektórych przypadkach;

(26) zasady ochrony danych muszą odnosić się do wszelkich informacji dotyczących zidentyfikowanych lub możliwych do zidentyfikowania osób; w celu ustalenia, czy daną osobę można zidentyfikować, należy wziąć pod uwagę wszystkie sposoby, jakimi może posłużyć się administrator danych lub inna osoba w celu zidentyfikowania owej osoby; zasady ochrony danych nie dotyczą danych, którym nadano anonimowy charakter w taki sposób, że osoba, której dane dotyczą, nie będzie mogła być zidentyfikowana; zasady postępowania w rozumieniu art. 27 mogą być przydatnym instrumentem w udzielaniu wskazówek co do sposobów nadawania danym charakteru anonimowego oraz zachowania w formie, w której identyfikacja osoby, której dane dotyczą;

(27) ochrona jednostek musi odnosić się zarówno do automatycznego przetwarzania danych, jak i ręcznego przetwarzania; zważywszy, że zakres tej ochrony nie powinien w efekcie być zależny od zastosowanych technik, ponieważ w przeciwnym razie wystąpiłoby poważne ryzyko obchodzenia zasad; niemniej w przypadku ręcznego przetwarzania danych, niniejsza dyrektywa obejmuje jedynie zbiory danych, nie zaś niezorganizowane zbiory; w szczególności zawartość zbiorów musi być zorganizowana według określonych kryteriów dotyczących osób fizycznych, zapewniających łatwy dostęp do danych; zgodnie z definicją zawartą w art. 2 lit. c, poszczególne państwa członkowskie mogą określić różne kryteria określania części składowych zorganizowanego zestawu danych oraz różne kryteria dostępu do takiego zestawu; zbiory lub zestawy zbiorów oraz ich strony tytułowe, które nie są zorganizowane według określonych kryteriów nie powinny w żadnych okolicznościach wchodzić w zakres niniejszej dyrektywy;

(28) przetwarzanie danych osobowych musi być zgodne z prawem i rzetelne wobec zainteresowanych osób; w szczególności dane muszą być adekwatne, właściwe i nie wykraczać poza cele, dla których są przetwarzane; cele takie muszą być jednoznaczne i uzasadnione oraz określone w czasie gromadzenia danych; cele dalszego przetwarzania danych po ich zgromadzeniu nie mogą być niezgodne z pierwotnie określonymi celami;

(29) dalsze przetwarzanie danych osobowych dla celów historycznych, statystycznych i naukowych nie jest na ogół uważane za niezgodne z celami, dla których dane były pierwotnie gromadzone, pod warunkiem zapewnienia przez państwo członkowskie odpowiednich zabezpieczeń; zabezpieczenia te muszą w szczególności wykluczać wykorzystywanie danych na rzecz działań lub decyzji dotyczących konkretnej osoby;

(30) zgodność z prawem procesu przetwarzania danych osobowych wymaga ponadto, aby dokonywane było ono za zgodą osoby, której dane dotyczą lub było konieczne dla zawarcia lub realizacji umowy wiążącej w sprawie osoby, której dane dotyczą, bądź miało charakter wymogu prawnego, lub też służyło realizacji zadania wykonywanego w interesie publicznym lub wykonywaniu władzy publicznej, bądź też w uzasadnionym interesie osoby fizycznej lub prawnej, pod warunkiem, że interesy lub prawa i wolności

osoby, której dane dotyczą nie mają charakteru nadrzędnego; w celu utrzymania równowagi między wspomnianymi interesami a gwarantowaniem skutecznej konkurencji, państwa członkowskie mogą określić okoliczności, w których dane osobowe mogą być wykorzystane lub ujawnione osobie trzeciej w związku ze zgodną z prawem, zwykłą aktywnością gospodarczą przedsiębiorstw i innych ciał; państwa członkowskie mogą podobnie określić warunki, na których dane osobowe mogą być ujawniane osobom trzecim dla celów marketingu o charakterze komercyjnym, lub realizowanego przez organizację charytatywną, lub też przez inne stowarzyszenie lub fundację, np. o charakterze politycznym, z zastrzeżeniem postanowień dopuszczających prawo sprzeciwu przysługujące osobie, której te dane dotyczą wobec przetwarzania tych danych - bezpłatnie i bez konieczności podania uzasadnienia;

(31) przetwarzanie danych osobowych musi być również uznawane za zgodne z prawem, kiedy dokonywane jest w celu zapewnienia ochrony interesu, który jest niezbędny dla życia osoby, której dane dotyczą;

(32) ustawodawstwo krajowe powinno ustalić, czy administrator danych wykonujący zadanie realizowane w interesie publicznym powinien być organem administracji publicznej czy inną osobą fizyczną lub prawną podlegającą prawu publicznemu lub prawu prywatnemu, jak np. stowarzyszenie zawodowe.

(33) dane mogące ze względu na ich charakter powodować naruszenie podstawowych swobód lub prywatności nie powinny być przetwarzane, o ile osoba, której dotyczą nie udzieli wyraźnej zgody; należy jednak przewidzieć odstępstwa od tego zakazu dla szczególnych potrzeb, zwłaszcza w przypadkach, gdy przetwarzanie danych odbywa się w określonych celach zdrowotnych przez osoby podlegające prawnemu obowiązkowi zachowania tajemnicy zawodowej, lub też w trakcie legalnych działań niektórych stowarzyszeń lub fundacji, których celem jest umożliwienie realizacji podstawowych swobód;

(34) państwa członkowskie muszą być również uprawnione, w sytuacjach, kiedy jest to uzasadnione przez ważny interes publiczny do uchylania zakazu przetwarzania wrażliwych kategorii danych w takich dziedzinach, jak zdrowie publiczne i ochrona socjalna - szczególnie w celu zapewnienia odpowiedniej jakości i zasadności ekonomicznej procedur stosowanych do rozstrzygania roszczeń w sprawie świadczeń i usług w ramach systemu ubezpieczeń społecznych - badania naukowe i statystyka rządowa; obowiązkiem ich jest jednak stworzenie konkretnych i odpowiednich zabezpieczeń dla ochrony podstawowych praw i prywatności osób;

(35) ponadto, przetwarzanie danych osobowych przez władze publiczne dla osiągnięcia określonych w prawie konstytucyjnym lub międzynarodowym prawie publicznym celów oficjalnie uznanych związków religijnych jest dokonywane z ważnych względów wynikających z interesu publicznego;

(36) jeżeli w trakcie czynności wyborczych funkcjonowanie systemu demokratycznego w niektórych państwach członkowskich wymaga gromadzenia przez partie polityczne danych na temat opinii politycznych obywateli, przetwarzanie tych danych może być dozwolone ze względu na ważny interes publiczny, pod warunkiem stworzenia odpowiednich zabezpieczeń'

(37) przetwarzanie danych osobowych dla potrzeb dziennikarstwa lub wypowiedzi literackiej lub artystycznej, zwłaszcza w dziedzinie techniki audiowizualnej, powinno kwalifikować się do zwolnienia z wymagań niektórych postanowień niniejszej dyrektywy, o ile je to konieczne, aby pogodzić podstawowe prawa osób fizycznych z wolnością informacji, a zwłaszcza prawem do uzyskiwania i udzielania informacji, co gwarantuje w szczególności art. 10 Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności; państwa członkowskie powinny w związku z tym ustalić zwolnienia i odstępstwa konieczne dla zapewnienia równowagi pomiędzy podstawowymi prawami odnoszącymi się do ogólnych środków w sprawie legalności przetwarzania danych, środków w sprawie przesyłania danych do krajów trzecich i kompetencjami organów nadzoru; nie powinno to jednak powodować wprowadzenia przez państwa członkowskie uregulowań stanowiących odstępstwo od obowiązku zapewnienia bezpieczeństwa przetwarzania danych; przynajmniej organ nadzoru odpowiedzialny za tę dziedzinę powinien być również wyposażony w niektóre uprawnienia *ex post*, np. publikowania regularnych sprawozdań lub kierowania spraw do władz sądowniczych;

(38) 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 niego, musi otrzymać dokładne i pełne informacje, uwzględniające okoliczności pozyskiwania danych;

(39) niektóre czynności w zakresie przetwarzania danych obejmują dane, których administrator danych nie uzyskał bezpośrednio od osoby, które te dane dotyczą; ponadto, dane mogą być legalnie ujawnione osobie trzeciej, nawet jeżeli ich ujawnienie nie było przewidywane w czasie, kiedy uzyskiwano dane od osoby, której dotyczą; we wszystkich tych przypadkach osoba, której dane dotyczą powinna być informowana przy rejestracji danych lub też najpóźniej kiedy dane są po raz pierwszy ujawnione osobie trzeciej;

(40) nie jest jednak konieczne nakładanie takiego obowiązku, kiedy osoba, której dane dotyczą posiada już tę informację; ponadto obowiązek taki nie występuje wówczas, gdy rejestracja lub ujawnianie danych jest wyraźnie przewidziane przez prawo lub jeżeli dostarczanie informacji osobie, której dane dotyczą okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku, co może mieć miejsce w przypadku przetwarzania danych dla celów historycznych, statystycznych lub naukowych; pod tym względem można brać pod uwagę liczbę osób, których dane dotyczą, wiek danych oraz przyjęte środki wyrównawcze;

(41) każda osoba musi mieć możliwość skorzystania z prawa dostępu do dotyczących jej danych, które poddane są przetwarzaniu, w celu zweryfikowania zwłaszcza prawidłowości danych oraz legalności ich przetwarzania; z tych samych powodów każda osoba, której dane dotyczą musi również mieć prawo zapoznania się z zasadami automatycznego przetwarzania danych, które ją dotyczą, przynajmniej w przypadku zautomatyzowanego procesu decyzyjnego, o którym mowa w art. 15 ust. 1; prawo to nie powinno w niekorzystny sposób wpływać na stan tajemnicy handlowej lub własności intelektualnej, w szczególności na prawo autorskie chroniące oprogramowanie; względy te nie powinny jednak powodować odmowy udzielenia osobie, której dane dotyczą wszystkich informacji;

(42) państwa członkowskie mogą, w interesie osoby, której dane dotyczą lub w celu zapewnienia ochrony praw i swobód innych osób, ograniczać prawo dostępu do danych i

informacji; mogą one np. postanowić, że dostęp do danych medycznych może uzyskać tylko personel medyczny;

(43) ograniczenia prawa dostępu i informacji oraz niektórych obowiązków kontrolera mogą w podobny sposób być wprowadzane przez państwa członkowskie, o ile jest to konieczne dla zapewnienia np. ochrony bezpieczeństwa narodowego, obronności, bezpieczeństwa publicznego lub ważnych ekonomicznych lub finansowych interesów państwa członkowskiego lub Unii, jak również dochodzenia i ścigania naruszeń prawa karnego oraz naruszeń zasad etyki w zawodach podlegających określonym regulacjom; lista wyłączeń i ograniczeń powinna obejmować zadania w zakresie nadzoru, kontroli i regulacji koniecznych w trzech ostatnich dziedzinach, dotyczących bezpieczeństwa publicznego, interesów ekonomicznych lub finansowych oraz walki z przestępczością; sporządzenie listy zadań we wspomnianych trzech dziedzinach nie wpływa na zasadność wprowadzenia wyłączeń i ograniczeń ze względu na bezpieczeństwo lub obronność państwa;

(44) państwa członkowskie mogą również, na mocy postanowień prawa Wspólnoty, uchylić się od postanowień niniejszej dyrektywy odnośnie prawa dostępu, obowiązku informowania obywateli oraz jakości danych w celu zapewnienia realizacji niektórych celów, o których mowa powyżej;

(45) w przypadkach, gdy dane mogą być legalnie przetwarzane ze względu na interes publiczny, wykonywania władzy publicznej lub uzasadnione interesy osoby fizycznej lub prawnej, osoba, której dane te dotyczą powinna jednak mieć prawo, ze względu na uzasadnione i ważkie przyczyny związane z jej sytuacją, do sprzeciwienia się przetwarzaniu tych danych; państwa członkowskie mogą jednak ustalić krajowe przepisy o przeciwnej treści;

(46) ochrona praw i wolności osób, których dotyczą przetwarzane dane osobowe wymaga przyjęcia odpowiednich rozwiązań technicznych i organizacyjnych, zarówno przy opracowywaniu systemu przetwarzania danych, jak i podczas samego ich przetwarzania, szczególnie w celu utrzymania bezpieczeństwa i niedopuszczenia do niedozwolonego przetwarzania danych; na państwie członkowskim spoczywa obowiązek zapewnienia stosowania tych rozwiązań przez administratora danych; uregulowania te muszą zapewnić odpowiedni stopień bezpieczeństwa, uwzględniając stan wiedzy w tej dziedzinie oraz koszty ich realizacji w odniesieniu do ryzyka wynikającego z przetwarzania danych oraz charakteru danych podlegających ochronie;

(47) w przypadku przekazywania komunikatu zawierającego dane osobowe przy pomocy urządzeń telekomunikacyjnych lub poczty elektronicznej, których wyłącznym przeznaczeniem jest przekazywanie takich komunikatów, za administratora danych osobowych zawartych w takim komunikacie uważać się będzie osobę, od której komunikat wychodzi, nie zaś osobę wykonującą usługę w zakresie transmisji danych; podmioty wykonujące takie usługi są z reguły uważane za administratorów danych odniesieniu do przetwarzania dodatkowych danych osobowych potrzebnych do wykonywania usług;

(48) procedury dotyczące zawiadamiania organu nadzoru są skonstruowane w taki sposób, aby zapewnić ujawnienie celów i głównych cech operacji przetwarzania danych dla

ustalenia, czy operacja taka jest zgoda z krajowymi uregulowaniami przyjętymi na podstawie niniejszej dyrektywy;

(49) w celu uniknięcia zbędnych formalności państwa członkowskie mogą wprowadzić zwolnienia z obowiązku zawiadamiania oraz uproszczenia procedury zawiadamiania w przypadkach, gdy mało prawdopodobne jest, aby przetwarzanie danych mogło niekorzystnie wpłynąć na prawa i wolności osób, których dane dotyczą zapewniając, że jest to zgodne ze środkami podejmowanymi przez państwa członkowskie określającymi ich granice; zwolnienia lub uproszczenia mogą być równocześnie przewidziane przez państwa członkowskie, jeżeli osoba wskazana przez administratora danych zapewni, że jest mało prawdopodobne, aby przetwarzanie mogło niekorzystnie wpłynąć na prawa i wolności osoby, której dane dotyczą; urzędnik odpowiedzialny za ochronę danych będący lub nie będący pracownikiem administratora danych, musi mieć możliwość wykonywania swoich funkcji w sposób całkowicie niezależny;

(50) wspomniane zwolnienie lub uproszczenie procedury mogłoby być stosowane w przypadku operacji przetwarzania danych, których wyłącznym celem jest prowadzenie rejestru mającego służyć, zgodnie z prawem krajowym, za źródło informacji dla ogółu społeczeństwa, otwarte do publicznego wglądu i każdej osoby posiadającej uzasadniony interes w uzyskaniu informacji;

(51) jednak uproszczenie procedury lub zwolnienie z obowiązku zawiadamiania nie będzie zwalniać administratora danych z innych obowiązków wynikających z niniejszej dyrektywy;

(52) w tym kontekście kontrola ex-post przeprowadzana przez właściwe władze musi z reguły być uznawana za wystarczające rozwiązanie;

(53) jednak niektóre operacje przetwarzania danych mogą stwarzać określone zagrożenia dla praw i wolności osób, których dane dotyczą ze względu na ich charakter, ich zakres lub przeznaczenie, jak np. pozbawienie jednostki przysługującego jej prawa, korzyści lub kontraktu, lub ze względu na szczególne zastosowanie nowych technologii; do państw członkowskich należy, jeżeli tego sobie życzą, wskazanie na takie zagrożenia w ich ustawodawstwie;

(54) w stosunku do wszystkich operacji przetwarzania danych podejmowanych w społeczeństwie, liczba tych, które niosą ze sobą określone zagrożenia jest bardzo ograniczona; państwa członkowskie muszą zapewnić kontrolę przetwarzania danych przez organ nadzorczy lub urzędnika odpowiedzialnego za ochronę danych, współpracującego z tym organem przed ich przetworzeniem; po takiej wstępnej kontroli, organ nadzorczy może, zgodnie z prawem krajowym, wydać opinię lub zezwolenie na przetwarzanie danych; kontrola taka może również następować w trakcie opracowywania ustawodawczego środka parlamentu krajowego lub środka opartego na takim środku ustawodawstwa, które określa charakter przetwarzania danych oraz stwarza odpowiednie zabezpieczenia;

(55) na wypadek nieprzestrzegania przez administratora danych praw osób, których dane dotyczą, ustawodawstwo krajowe musi przewidywać odpowiednie środki prawne; szkody, jakie osoba może ponieść wskutek niezgodnego z prawem przetwarzania danych musi być wyrównana przez administratora danych, który może być zwolniony z

odpowiedzialności w przypadku udowodnienia, że szkoda nie powstała z jego winy, szczególnie wówczas, gdy stwierdzi wystąpienie winy po stronie osoby, której dane dotyczą lub w przypadku siły wyższej; należy nakładać sankcje na każdą osobę, podlegającą prawu prywatnemu lub publicznemu, która nie spełni wymagań wynikających z przyjętych krajowych środków wprowadzonych na podstawie niniejszej dyrektywy;

(56) przepływ danych osobowych przez granicę jest koniecznym warunkiem rozwoju handlu międzynarodowego; ochrona osób jaką niniejsza dyrektywa gwarantuje we Wspólnocie nie stanowi przeszkody dla przekazywania danych osobowych do krajów trzecich, które zapewniają odpowiedni stopień ochrony; prawidłowość stopnia ochrony danych zapewnianej przez kraj trzeci należy oceniać w świetle wszystkich okoliczności dotyczących operacji przekazywania danych lub zestawu takich operacji;

(57) z drugiej strony należy zakazać przekazywania danych osobowych do kraju trzeciego, który nie zapewnia odpowiedniego stopnia ochrony;

(58) należy przewidzieć zwolnienia z tego zakazu w określonych okolicznościach, jeżeli osoba, której dane dotyczą wyrazi na to zgodę, jeżeli przekazanie danych jest konieczne w związku z umową lub roszczeniem prawnym, jeżeli wymagać tego będzie ochrona ważnego interesu publicznego, jak np. przesyłanie danych za granicę przez władze podatkowe i celne lub przez służby odpowiedzialne za sprawy ubezpieczeń społecznych, lub w przypadku przekazania danych z rejestru utworzonego na mocy prawa i przeznaczonego do wglądu dla ogółu społeczeństwa lub osób posiadających uzasadniony interes w uzyskaniu informacji; w tym przypadku przekazanie danych nie powinno obejmować ich całości lub całych kategorii danych oraz, jeżeli rejestr jest przeznaczony do wglądu dla osób posiadających uzasadniony interes w uzyskaniu informacji, przekazanie danych powinno nastąpić jedynie na wniosek tych osób, lub wówczas, gdy osoby te mają być odbiorcami danych;

(59) podejmowane mogą być konkretne działania w celu zrekompensowania braku ochrony w kraju trzecim, jeżeli administrator danych oferuje odpowiednie zabezpieczenia; ponadto, należy przewidzieć procedury negocjacji między Wspólnotą a krajami trzecimi;

(60) w każdym przypadku przekazywanie danych do krajów trzecich może następować jedynie w pełnej zgodności z postanowieniami przyjętymi przez państwa członkowskie na podstawie niniejszej dyrektywy, a w szczególności art. 8.

(61) państwa członkowskie i Komisja muszą - w zakresie swoich kompetencji - zachęcać stowarzyszenia zawodowe oraz inne reprezentatywne organizacje do opracowania reguł postępowania w celu ułatwienia stosowania niniejszej dyrektywy, biorąc pod uwagę specyficzne cechy procesu przetwarzania danych w niektórych branżach, z poszanowaniem dla krajowych przepisów przyjętych w celu jej realizacji;

(62) utworzenie w państwach członkowskich organów nadzorczych, wykonujących swoje funkcje w sposób całkowicie niezależny jest zasadniczym elementem ochrony jednostek w zakresie przetwarzania danych osobowych;

(63) organy te muszą dysponować określonymi środkami do realizacji swoich obowiązków, włączając uprawnienia do przeprowadzania dochodzenia i interwencji, szczególnie w

przypadkach skarg od obywateli, jak również uprawnienia do uczestniczenia w postępowaniu sądowym; organy te muszą przyczyniać się do zapewnienia przejrzystości przetwarzania danych w państwach członkowskich, którym właściwości podlegają;

(64) władze różnych państw członkowskich muszą wspierać się wzajemnie w wykonywania swoich obowiązków w celu zapewnienia właściwego poszanowania zasad ochrony danych w całej Unii Europejskiej;

(65) na szczeblu Wspólnoty należy powołać zespół roboczy do spraw ochrony osób fizycznych w zakresie przetwarzania danych osobowych, który będzie całkowicie niezależny w realizacji swoich funkcji; ze względu na jego specyficzny charakter, musi on służyć radą Komisji oraz, w szczególności, przyczyniać się do jednolitego stosowania przepisów krajowych przyjętych na podstawie niniejszej dyrektywy;

(66) w odniesieniu do przekazywania danych do krajów trzecich, stosowanie niniejszej dyrektywy wymaga nadania Komisji uprawnień wykonawczych oraz ustanowienia procedury zgodnie z decyzją Rady 87/373/EWG[1];

(67) 20 grudnia 1994 zawarta została pomiędzy Parlamentem Europejskim, Radą i Komisją umowa w sprawie *modus vivendi* dotycząca sposobów wprowadzania w życie aktów przyjętych w trybie określonym w art. 189b Traktatu o WE;

(68) zasady określone w niniejszej dyrektywie odnośnie ochrony praw i wolności osób fizycznych, szczególnie ich prawa do prywatności w odniesieniu do przetwarzania danych osobowych mogą być uzupełniane lub wyjaśniane, zwłaszcza w przypadku niektórych branż, w formie szczegółowych przepisów opartych na wspomnianych zasadach;

(69) należy wyznaczyć państwom członkowskim okres nie dłuższy niż trzy lata od wejścia w życie krajowych uregulowań stanowiących transpozycję niniejszej dyrektywy, w którym będą one zobowiązane do progresywnego stosowania nowych przepisów krajowych w odniesieniu do wszystkich realizowanych już operacji przetwarzania danych; dla ułatwienia ich realizacji przy uzasadnionych ekonomicznie kosztach, wyznaczony zostanie państwom członkowskim kolejny okres 12 lat od daty uchwalenia niniejszej dyrektywy, w celu zapewnienia zgodności istniejących ręcznych zbiorów danych z niektórymi postanowieniami dyrektywy; jeżeli we wspomnianym przedłużonym okresie przejściowym dane zawarte w owych zbiorach będą przetwarzane ręcznie, konieczne będzie doprowadzenie do zgodności tych zbiorów ze wspomnianymi postanowieniami w czasie przetwarzania danych;

(70) nie jest konieczne aby osoba, której dane dotyczą udzieliła ponownej zgody, aby umożliwić administratorowi danych dalsze przetwarzanie, po wejściu w życie krajowych przepisów przyjętych na podstawie niniejszej dyrektywy, wszelkich wrażliwych danych koniecznych do realizacji umowy zawartej na warunkach dobrowolnej i świadomej zgody stron przed wejściem w życie wspomnianych przepisów;

(71) niniejsza dyrektywa nie stanowi przeszkody dla wprowadzania przez państwo członkowskie regulującej działalności marketingowej, skierowanej na konsumentów

[1] Dz.U. WE nr C 277, z 5. 11. 1990, str. 3 i Dz.U. WE nr C 311, z 27. 11. 1992, str. 30.

zamieszkałych na jego terytorium, o ile regulacja ta nie będzie dotyczyć ochrony osób fizycznych w zakresie przetwarzania danych osobowych;

(72) niniejsza dyrektywa zezwala na uwzględnianie zasady publicznego dostępu do oficjalnych dokumentów przy realizacji zasad określonych w niniejszej dyrektywie,

PRZYJMUJĄ NINIEJSZĄ DYREKTYWĘ:

ROZDZIAŁ I

POSTANOWIENIA OGÓLNE

Artykuł 1

Cel dyrektywy

1. Zgodnie z postanowieniami niniejszej dyrektywy, państwa członkowskie zobowiązują się chronić podstawowe prawa i wolności osób fizycznych, a w szczególności ich prawo do prywatności w odniesieniu do przetwarzania danych osobowych.

2. Państwa członkowskie nie będą ograniczać ani zakazywać swobodnego przepływu danych osobowych pomiędzy państwami członkowskimi ze względów związanych z ochroną przewidzianą w ust. 1.

Artykuł 2

Definicje

Dla potrzeb niniejszej dyrektywy :

(a) „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 specyficznych czynników określających jej fizyczną, fizjologiczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość;

(b) „przetwarzanie danych osobowych” („przetwarzanie”) oznacza każdą operację lub zestaw operacji dokonywanych na danych przy pomocy środków zautomatyzowanych lub innych, jak np. gromadzenie, rejestracja, porządkowanie, przechowywanie, adaptacja lub modyfikacja, odzyskiwanie, konsultowanie, wykorzystywanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, układanie lub kompilowanie, zestawianie, usuwanie lub niszczenie danych;

(c) „zbiór danych osobowych” („zbiór danych") oznacza każdy uporządkowany zestaw danych osobowych, dostępnych według określonych kryteriów, scentralizowanych. zdecentralizowanych lub rozproszonych funkcjonalnie lub geograficznie;

(d) „administrator danych” oznacza osobę fizyczną lub prawną, urząd publiczny, agendę 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 innych przepisach krajowych lub przepisach Wspólnoty, administrator danych może być powoływany lub kryteria jego powołania mogą być ustalane przez ustawodawstwo krajowe lub ustawodawstwo Wspólnoty;

(e) „przetwarzający” oznacza osobę fizyczną lub prawną, urząd publiczny, agendę lub inny organ przetwarzający dane osobowe w imieniu administratora danych;

(f) „osoba trzecia” oznacza osobę fizyczną lub prawną, urząd publiczny, agendę lub inny organ nie będący osobą, której dane dotyczą, ani administratorem danych, ani przetwarzającym lub jedną z osób, które pod bezpośrednim zwierzchnictwem administratora danych lub przetwarzającego upoważnione są do przetwarzania danych;

(g) „odbiorca" oznacza osobę fizyczną lub prawną, urząd publiczny, agendę lub inny organ, któremu ujawniane są dane, będący lub nie będący osobą trzecią; jednakże władze, które mogą otrzymywać dane w ramach konkretnego dochodzenia nie są uważane za odbiorcę;

(h) „zgoda osoby, której dane dotyczą" oznacza konkretne i świadome, dobrowolne wskazanie przez osobę, której dane dotyczą na to, że wyraża przyzwolenie na przetwarzanie jej danych osobowych.

Artykuł 3

Zakres działania

1. Niniejsza dyrektywa dotyczy przetwarzania danych osobowych w całości lub w części w sposób zautomatyzowany oraz innego przetwarzania danych osobowych, stanowiących część zbioru danych lub mających stanowić część zbioru danych.

2. Niniejsza dyrektywa nie dotyczy przetwarzania danych osobowych:

- w ramach działalności wykraczającej poza zakres prawa Wspólnoty takiej, o której mowa w rozdziałach V i VI Traktatu o Unii Europejskiej, oraz w każdym przypadku - przetwarzania związanego z bezpieczeństwem publicznym, obronnością, bezpieczeństwem państwa (łącznie ze stanem gospodarki państwa, kiedy przetwarzanie danych dotyczy bezpieczeństwa państwa) oraz z działalnością państwa w dziedzinach prawa karnego,

- przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze.

Artykuł 4

Stosowane prawo krajowe

1. Każde państwo członkowskie stosuje w odniesieniu do przetwarzania danych osobowych postanowienia prawa krajowego, jakie wprowadzi na podstawie niniejszej dyrektywy wówczas, gdy:

   (a) przetwarzanie danych odbywa się w zakresie prowadzenia przez administratora danych działalności na terytorium państwa członkowskiego; jeżeli ten sam administrator danych prowadzi działalność na terytorium kilku państw członkowskich, musi on podjąć niezbędne działania, aby zapewnić, że każda z tych agend wywiązuje się z obowiązków ustalonych przez stosowane prawo krajowe;

   (b) administrator danych nie prowadzi działalności na terytorium państwa członkowskiego, lecz w miejscu, gdzie jego prawo krajowe stosowane jest na mocy międzynarodowego prawa publicznego;

   (c) administrator danych nie prowadzi działalności na terytorium Wspólnoty lecz, dla celów przetwarzania danych osobowych wykorzystuje środki, zarówno zautomatyzowane jak i inne, znajdujące się na terytorium wymienionego państwa członkowskiego, o ile środki te nie są wykorzystywane wyłącznie do celów tranzytu przez terytorium Wspólnoty.

2. W okolicznościach, o których mowa w ust. 1 lit. (c), administrator danych musi wyznaczyć swojego przedstawiciela na terytorium tego państwa członkowskiego, niezależnie od środków prawnych, jakie mogą być podjęte przeciwko samemu administratorowi danych.

ROZDZIAŁ II

OGÓLNE ZASADY LEGALNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

Artykuł 5

Państwa członkowskie określą, w granicach postanowień zawartych w niniejszym rozdziale, bardziej szczegółowe warunki legalności przetwarzania danych osobowych.

CZĘŚĆ 1

ZASADY DOTYCZĄCE JAKOŚCI DANYCH

Artykuł 6

1. Państwa członkowskie zapewnią, aby dane osobowe były:

(a) przetwarzane rzetelnie i legalnie;

(b) gromadzone do określonych, wyraźnych i legalnych celów oraz nie będą poddawane dalszemu przetwarzaniu w sposób niezgodny z tym celem. Dalsze przetwarzanie danych w celach historycznych, statystycznych lub naukowych nie będzie uważane za niezgodne z przepisami pod warunkiem stworzenia przez państwa członkowskie odpowiednich zabezpieczeń;

(c) stosowne, istotne i nie wykraczające poza konieczne 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 dane 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.

2. Na administratorze danych spoczywa obowiązek zapewnienia przestrzegania postanowień ust. 1.

CZĘŚĆ II

KRYTERIA LEGALNOŚCI PRZETWARZANIA DANYCH

Artykuł 7

Państwa członkowskie zapewnią, aby dane osobowe mogły być przetwarzane tylko wówczas, gdy:

(a) osoba, której dane dotyczą jednoznacznie wyraziła na to 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 zgodności z zobowiązaniem prawnym, 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 się dane; lub

(f) przetwarzanie danych jest konieczne dla potrzeb wynikających z uzasadnionych interesów administratora danych lub osoby trzeciej, przed która ujawnia się dane, z wyjątkiem sytuacji, kiedy interesy takie podporządkowane są interesom związanym z podstawowymi prawami i wolnościami osoby, której dane dotyczą, które wymagają ochrony na podstawie art. 1 ust. 1.

CZĘŚĆ III

SZCZEGÓLNE KATEGORIE PRZETWARZANIA DANYCH

Artykuł 8

Przetwarzanie szczególnych kategorii danych

1. Państwa członkowskie zabronią przetwarzania danych osobowych ujawniającego pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych, jak również przetwarzanie danych dotyczących zdrowia i życia płciowego.

2. Ust. 1 nie będzie miał zastosowania, jeśli:

(a) osoba, której dane dotyczą danych udzieliła wyraźnej zgody na przetwarzanie tych danych, chyba że ustawodawstwo państwa członkowskiego przewiduje, że zakaz, o którym mowa w ust. 1 nie może być uchylony mimo udzielonej zgody przez osobę, której dane dotyczą; lub

(b) przetwarzanie danych jest konieczne do wypełniania obowiązków i szczególnych uprawnień administratora danych w dziedzinie prawa pracy, o ile jest to dozwolone przez prawo krajowe przewidujące odpowiednie zabezpieczenia; lub

(c) przetwarzanie danych jest konieczne dla ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby, w przypadku, gdy osoba, której dane dotyczą jest fizycznie lub prawnie niezdolna do udzielenia zgody; lub

(d) przetwarzanie danych jest dokonywane się w ramach legalnej działalności wspartej odpowiednimi gwarancjami przez fundację, stowarzyszenie lub inną nie komercyjną 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 oraz że dane nie zostaną ujawnione osobie trzeciej bez zgody osób, których dane dotyczą; lub

(e) przetwarzanie dotyczy danych, które są podawane do wiadomości publicznej przez osobę, której dane dotyczą, lub jest konieczne do ustalenia, wykonania lub obrony roszczeń prawnych.

3. Ust. 1 nie ma zastosowania w przypadku, gdy przetwarzanie danych wymagane jest dla celów medycyny prewencyjnej, 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, podlegający obowiązkowi zachowania tajemnicy zawodowej lub przez inną osobę również zobowiązaną do zachowania tajemnicy.

4. Pod warunkiem stworzenia odpowiednich zabezpieczeń, państwa członkowskie mogą, ze względu na istotny interes publiczny, ustalić dodatkowe zwolnienia, poza tymi, które zostały określone w ust. 2 na mocy prawa krajowego lub decyzją organu nadzorczego.

5. Przetwarzanie danych dotyczących przestępstw, wyroków skazujących lub środków bezpieczeństwa może być dokonywane jedynie pod kontrolą oficjalnych władz, lub też, jeżeli zgodnie z prawem krajowym stworzone zostały odpowiednie szczególne zabezpieczenia, z uwzględnieniem wyłączeń, które państwo członkowskie może wprowadzić zgodnie z obowiązującymi przepisami krajowymi, zapewniając odpowiednie szczególne zabezpieczenia. Jednak kompletny rejestr skazanych może być prowadzony tylko pod kontrolą oficjalnego organu władzy.
   Państwa członkowskie mogą przewidzieć, że dane dotyczące sankcji administracyjnych lub orzeczeń w sprawach cywilnych będą również przetwarzane pod kontrolą oficjalnych władz.

6. Wyłączenia stosowania ust. 1, o których mowa w ust. 4 i 5 będą notyfikowane Komisji.

7. Państwa członkowskie określą warunki, w których może następować przetwarzanie krajowego numeru identyfikacyjnego lub innego identyfikatora ogólnego stosowania.

Artykuł 9

Przetwarzanie danych osobowych i wolność wypowiedzi

Państwa członkowskie wprowadzą wyłączenia lub zwolnienia z postanowień niniejszego rozdziału, rozdziału IV i rozdziału VI w przypadku przetwarzania danych osobowych wyłącznie w celach dziennikarskich lub dla celu artystycznej lub literackiej wypowiedzi jedynie wówczas, gdy jest to konieczne dla pogodzenia prawa do prywatności z normami dotyczącymi wolności wypowiedzi.

CZĘŚĆ IV

PRZEKAZYWANIE INFORMACJI OSOBIE, KTÓREJ DANE DOTYCZĄ

Artykuł 10

Informacje w przypadku zbierania danych od osoby, której dane dotyczą

Państwa członkowskie zapewnią, że administrator danych lub jego przedstawiciel zobowiązany będzie przedstawić osobie, której dane dotyczą i, od której gromadzone są dane,

co najmniej następujące informacje, z wyjątkiem przypadku, kiedy posiada już ona informacje dotyczące:

(a) tożsamości administratora danych i ewentualnie jego przedstawiciela;

(b) celów przetwarzania danych, do których dane są przeznaczone;

(c) wszelkich dalszych informacji, jak np.:
- odbiorcy lub kategorie odbiorców danych,
- tego czy odpowiedzi na pytania są obowiązkowe czy dobrowolne oraz ewentualne konsekwencje nie udzielenia odpowiedzi,
- istnienie prawa dostępu do swoich danych oraz ich poprawienia,

o ile takie dalsze informacje będą potrzebne, biorąc od uwagę szczególne okoliczności, w których dane są gromadzone, w celu zagwarantowania rzetelnego przetwarzania danych w związku z osobą, której dane dotyczą.

Artykuł 11

Informacje w przypadku uzyskiwania danych z innych źródeł niż osoba, której dane dotyczą

1. W przypadku, gdy dane nie zostały uzyskane od osoby, której dane dotyczą, państwa członkowskie zapewnią, aby administrator danych lub jego przedstawiciel był zobowiązany, w chwili przystąpienia do rejestracji danych osobowych lub w przypadku planowania ujawnienia danych osobie trzeciej, ale nie później niż gdy dane te są ujawniane po raz pierwszy, dostarczyć osobie, której dane dotyczą, z wyjątkiem przypadku, gdy uzyskał je już wcześniej, co najmniej następujące informacje:

(a) tożsamości administratora danych i ewentualnie jego przedstawiciela;

(b) cele przetwarzania danych;

(c) wszelkich dalszych informacji, jak np.:
- kategorie potrzebnych danych,
- odbiorcy lub kategorie odbiorców danych,
- istnienie prawa wglądu do swoich danych oraz ich poprawienia,

o ile takie dalsze informacje będą potrzebne, biorąc od uwagę szczególne okoliczności, w których dane są przetwarzane, w celu zagwarantowania rzetelnego ich przetwarzania odnośnie osoby, której dane dotyczą.

2. Ust. 1 nie ma zastosowania wówczas - szczególnie w przypadku przetwarzania danych dla celów statystycznych, historycznych lub naukowych - gdy 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.

CZĘŚĆ V

PRAWO DOSTĘPU DO DANYCH OSOBY, KTÓREJ DANE DOTYCZĄ

Artykuł 12

Prawo dostępu do danych

Państwa członkowskie zapewnią każdej osobie, której dane dotyczą prawo 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 zrozumiałej formie o danych przechodzących przetwarzanie oraz dostępnych informacjach o ich źródłach,

- wiadomości na temat zasad automatycznego przetwarzania dotyczących jej danych przynajmniej w przypadku zautomatyzowanego procesu decyzyjnego, o którym mowa w art. 15 ust. 1;

(b odpowiednio możliwość poprawienia, usunięcia lub zablokowania danych, których przetwarzanie jest niezgodne z postanowieniami niniejszej dyrektywy, szczególnie ze względu na niekompletność lub niedokładność danych;

(c) zawiadomienia osób trzecich, którym dane zostały ujawnione, o każdym poprawieniu, usunięciu lub zablokowaniu danych zgodnie z lit. (b), o ile nie okaże się to niemożliwe lub nie będzie wymagało niewspółmiernie dużego wysiłku.

CZĘŚĆ VI

ZWOLNIENIA I OGRANICZENIA

Artykuł 13

Zwolnienia i ograniczenia

1. Państwo członkowskie może przyjąć środki ustawodawcze w celu ograniczenia zakresu praw i obowiązków, przewidzianych w art. 6 ust.1, 10, 11 ust. 1, 12 oraz 21, kiedy ograniczenie takie stanowi środek konieczny dla zabezpieczenia:

   (a) bezpieczeństwa narodowego;

   (b) obronności;

(c) bezpieczeństwa publicznego;

(d) działań prewencyjnych, prowadzonych czynności dochodzeniowo-śledczych i prokuratorskich w sprawach kryminalnych lub sprawach o naruszenie zasad etyki w zawodach podlegających regulacjom;

(e) ważnego interesu ekonomicznego lub finansowego państwa członkowskiego lub Unii Europejskiej, łącznie ze sprawami monetarnymi, budżetowymi i podatkowymi;

(f) funkcji kontrolnych, inspekcyjnych i regulacyjnych związanych, nawet sporadycznie z wykonywaniem władzy publicznej w przypadkach wymienionych w lit. (c), (d) i (e);

(g) ochrony osoby, której dane dotyczą oraz praw i wolności innych osób.

2. Z zastrzeżeniem obowiązku zapewnienia odpowiedniego stopnia zabezpieczeń prawnych, w szczególności, aby dane nie były wykorzystywane do podejmowania działań lub decyzji dotyczących konkretnych osób, państwa członkowskie mogą w przypadku, gdy wyraźnie nie występuje ryzyko naruszenia prywatności osoby, której dane dotyczą, ograniczyć przy pomocy środków legislacyjnych prawa przewidziane w art. 12, kiedy dane są przetwarzane wyłącznie do celów badań naukowych lub przechowywane są w formie osobistej przez okres nie przekraczający długości okresu potrzebnego wyłącznie w celu uzyskania wyników statystycznych.

CZĘŚĆ VII

PRAWO SPRZECIWU PRZYSŁUGUJĄCE OSOBIE, KTÓREJ DANE DOTYCZĄ

Artykuł 14

Prawo sprzeciwu przysługujące osobie, której dane dotyczą

Państwa członkowskie przyznają osobie, której dane dotyczą, prawo:

(a) przynajmniej w przypadkach wymienionych w art. 7 lit. e i f – sprzeciwu, w dowolnym czasie z ważkich i prawnie uzasadnionych przyczyn wynikających z jej konkretnej sytuacji, co do przetwarzania dotyczących jej danych, chyba że ustawodawstwo krajowe przewiduje inaczej. W przypadku uzasadnionego sprzeciwu przetwarzanie danych prowadzone przez administratora danych nie może już obejmować tych danych, których sprzeciw dotyczy;

(b) sprzeciwu, na wniosek i bez opłaty, wobec przetwarzania dotyczących jej danych osobowych, które administrator danych zamierza przetwarzać dla potrzeb marketingu bezpośredniego, lub uzyskania informacji przed ujawnieniem danych osobowych po raz pierwszy osobom trzecim lub wykorzystaniem tych danych w ich imieniu dla potrzeb marketingu bezpośredniego, jak również do wyraźnego powoływania się na prawo bezpłatnego sprzeciwu wobec ujawniania lub wykorzystywania danych.

Państwa członkowskie podejmą konieczne działania, aby osoby, których dane dotyczą były świadome istnienia praw wymienionych w pierwszej części litery (b).

Artykuł 15

Zautomatyzowane decyzje indywidualne

1. Państwa członkowskie przyznają każdej osobie prawo nie podlegania decyzji, która wywołuje skutki prawne, które dotyczą jej lub mają na nią istotny wpływ, oraz która oparta jest wyłącznie na zautomatyzowanym przetwarzaniu danych, którego celem jest dokonanie oceny niektórych dotyczących ją aspektów o charakterze osobistym, jak np. wyniki osiągane w pracy, wypłacalność, wiarygodność, sposób zachowania itp.

2. Z zastrzeżeniem postanowień innych artykułów niniejszej dyrektywy, państwa członkowskie spowodują, że każda osoba będzie mogła być poddana decyzji opisanej 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 mu przedstawienie swojego punktu widzenia; lub

(b) zostanie dozwolona przez prawo, które określa również sposoby zabezpieczenia uzasadnionych interesów osoby, której dane dotyczą.

CZĘŚĆ VIII

POUFNOŚĆ I BEZPIECZEŃSTWO PRZETWARZANIA DANYCH

Artykuł 16

Poufność przetwarzania danych

Żadnej osobie podlegającej władzy administratora danych lub przetwarzającego, włączając samego przetwarzającego, mającej dostęp do danych osobowych nie wolno ich przetwarzać w sposób odbiegający od wskazówek administratora danych, chyba, że wymaga tego prawo.

Artykuł 17

Bezpieczeństwo przetwarzania danych

1. Państwa członkowskie zapewnią, aby administrator danych wprowadził odpowiednie środki techniczne i organizacyjne w celu ochrony danych osobowych przed przypadkowym lub nielegalnym zniszczeniem lub przypadkową utratą, zmianą, niedozwolonym ujawnieniem

lub dostępem, szczególnie wówczas. gdy przetwarzanie danych obejmuje transmisję danych w sieci, jak również przed wszelkimi innymi nielegalnymi formami przetwarzania.

Uwzględniając stan wiedzy w tej dziedzinie oraz koszt realizacji, środki te zapewnią poziom bezpieczeństwa odpowiedni do zagrożeń wynikających z przetwarzania danych oraz charakteru danych objętych ochroną.

2. Państwa członkowskie zobowiążą administratora danych, w przypadku przetwarzania danych w jego imieniu, do wybrania przetwarzającego, o wystarczających gwarancjach odnośnie technicznych środków bezpieczeństwa oraz rozwiązań organizacyjnych, regulujących przetwarzanie danych, oraz do zapewnienia stosowania tych środków i rozwiązań.

3. Przetwarzanie danych przez przetwarzającego musi być regulowane przez umowę lub akt prawny, na mocy których przetwarzający podlega administratorowi danych i które w szczególności postanawiają, że:

- przetwarzający będzie działać wyłącznie na polecenie administratora danych,

- obowiązki ustalone w ust. 1, określone przez ustawodawstwo państwa członkowskiego, w którym przetwarzający prowadzi działalność gospodarczą, będą również dotyczyć przetwarzającego.

4. Dla celów dowodowych, części umowy lub aktu prawnego dotyczącego ochrony danych i wymagań dotyczących środków wymienionych w ust. 1 będą sporządzane na piśmie lub w innej równorzędnej formie.

CZĘŚĆ IX

POWIADOMIENIE

Artykuł 18
Obowiązek powiadomienia organu nadzorczego

1. Państwa członkowskie zobowiążą administratora danych lub jego ewentualnego przedstawiciela do powiadomienia organu nadzorczego, wymienionego w art. 28 przed przeprowadzeniem całościowej lub częściowej operacji automatycznego przetwarzania danych lub zestawu takich operacji mających służyć jednemu celowi lub wielu powiązanym ze sobą celom.

2. Państwa członkowskie mogą wprowadzić uproszczenie procedury lub zwolnienie z obowiązku powiadomienia tylko w następujących sytuacjach oraz na następujących warunkach:

- jeżeli, w przypadku kategorii operacji przetwarzania, co do których mało prawdopodobne jest, biorąc pod uwagę dane przeznaczone do przetworzenia, aby niekorzystnie wpłynęły na prawa i wolności osób, których dane dotyczą, określają cele przetwarzania danych, dane lub kategorie danych przechodzących proces przetwarzania, kategorię lub kategorie

osób, których dane dotyczą, odbiorców lub kategorie odbiorców, którym dane mają być ujawnione oraz długość okresu przechowywania danych i/lub

- jeżeli administrator danych, zgodnie z dotyczącymi go przepisami krajowymi, powoła urzędnika do spraw ochrony danych osobowych, odpowiedzialnego w szczególności:

  - za zapewnienie w niezależny sposób wewnętrznego stosowania krajowych przepisów przyjętych na podstawie niniejszej dyrektywy,

  - za prowadzenie rejestru operacji przetwarzania danych wykonywanych przez administratora danych i zawierających informacje, o których mowa w art. 21 ust. 2, zapewniając przy tym, że nie zostaną naruszone prawa i wolności osób, których dane dotyczą.

3. Państwa członkowskie mogą ustalić, że ust. 1 nie odnosi się do przetwarzania danych, którego wyłącznym celem jest prowadzenie rejestru, który zgodnie z obowiązującymi ustawami lub przepisami ma służyć za źródło informacji dla społeczeństwa oraz który będzie przeznaczony do wglądu dla ogółu społeczeństwa lub osób posiadających uzasadniony interes w uzyskaniu informacji;

4. Państwa członkowskie mogą wprowadzić zwolnienie z obowiązku powiadamiania lub uprościć procedurę powiadamiania w przypadku operacji przetwarzania danych, o których mowa w art. 8 ust. 2 lit. d).

5. Państwa członkowskie mogą postanowić, że niektóre lub wszystkie nie zautomatyzowane operacje przetwarzania danych osobowych będą zgłaszane lub ustalą dla takich operacji uproszczony tryb zawiadamiania.

Artykuł 19
Treść powiadomienia

1. Państwa członkowskie ustalą, jakie informacje zostaną podane w powiadomieniu. Będą one obejmować co najmniej:

(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.

2. Państwa członkowskie określą procedury, w myśl których wszelkie zmiany mające wpływ na wszystkie informacje, o których mowa w ust. 1 muszą być zgłaszane do organu nadzorczego.

Artykuł 20

Kontrola wstępna

1. Państwa członkowskie zdefiniują operacje przetwarzania danych mogące stwarzać określone zagrożenia dla praw i wolności osób, których dane dotyczą oraz będą kontrolować, czy operacje te są badane przed ich rozpoczęciem.

2. Kontrole wstępne będą przeprowadzane przez organ nadzorczy po przyjęciu powiadomienia od administratora danych lub urzędnika odpowiedzialnego za ochronę danych, który w razie wątpliwości winien konsultować się z organem nadzorczym.

3. Państwa członkowskie mogą również przeprowadzać takie kontrole w kontekście opracowywania odpowiedniego uregulowania w parlamencie krajowym lub uregulowania opartego na takim rozwiązaniu legislacyjnym, które określa charakter przetwarzania danych oraz stwarza odpowiednie zabezpieczenia.

Artykuł 21
Upublicznienie operacji przetwarzania danych

1. Państwa członkowskie podejmą odpowiednie środki, aby zapewnić upublicznienie operacji przetwarzania danych.

2. Państwa członkowskie zapewnią, że organ nadzorczy będzie prowadzić rejestr operacji przetwarzania danych zgłoszonych zgodnie z art.18.
Rejestr będzie zawierać co najmniej informacje, o których mowa w art. 19 ust. 1 lit. a) -e).
Każda osoba może mieć wgląd do rejestru.

3. Państwa członkowskie zapewnią, - w odniesieniu do operacji przetwarzania danych nie podlegających zgłaszaniu – aby administratorzy danych lub inne instytucje powołane przez państwa członkowskie będą udostępniać przynajmniej te informacje, o których mowa w art. 19 ust. 1 lit. a) - e) w odpowiedniej formie każdej osobie na żądanie.
Państwa członkowskie mogą ustalić, że postanowienie to nie będzie dotyczyć przetwarzania danych, którego wyłącznym celem jest prowadzenie rejestru, który zgodnie z ustawami i innymi przepisami ma służyć za źródło informacji dla społeczeństwa i jest udostępniony albo do publicznego wglądu albo do wglądu każdej osoby posiadającej uzasadniony interes w uzyskaniu informacji;

ROZDZIAŁ III

ŚRODKI OCHRONY PRAWNEJ, ODPOWIEDZIALNOŚĆ I SANKCJE

Artykuł 22

Środki ochrony prawnej

Niezależnie od postępowania administracyjnego, które może być wszczęte przed wkroczeniem na drogę sądową, w szczególności przez organ nadzorczy, o którym mowa w art. 28, państwa członkowskie zapewnią każdej osobie możliwość wniesienia skargi do sądu, w przypadku naruszenia praw gwarantowanych jej przez prawo krajowe dotyczące przetwarzania danych.

Artykuł 23
Odpowiedzialność

1. Państwa członkowskie zapewnią, że każdej osobie, która poniosła szkodę wskutek niezgodnej z prawem operacji przetwarzania danych lub innej czynności niezgodnej z przepisami krajowymi przyjętymi na podstawie niniejszej dyrektywy przysługuje od administratora danych odszkodowanie za poniesioną szkodę.

2. Administrator danych może być zwolniony z tej odpowiedzialności w całości lub w części, jeżeli udowodni, że nie jest odpowiedzialny za zdarzenie, które spowodowało szkodę.

Artykuł 24
Sankcje

Państwa członkowskie przyjmą odpowiednie środki w celu zapewnienia pełnej realizacji postanowień niniejszej dyrektywy oraz w szczególności określą sankcje, jakie należy nałożyć w przypadku naruszenia postanowień przyjętych na podstawie dyrektywy.

ROZDZIAŁ IV

PRZEKAZYWANIE DANYCH OSOBOWYCH DO KRAJÓW TRZECICH

Artykuł 25
Zasady

1. Państwa członkowskie zapewnią, że przekazywanie do kraju trzeciego danych osobowych poddawanych przetwarzaniu lub przeznaczonych do przetwarzania po ich przekazaniu może nastąpić tylko wówczas, gdy - niezależnie od zgodności z krajowymi przepisami przyjętymi na podstawie innych postanowień niniejszej dyrektywy - dany kraj trzeci zapewni odpowiedni stopień ochrony.

2. Odpowiedniość stopnia ochrony danych zapewnianej przez kraj trzeci należy oceniać w świetle wszystkich okoliczności dotyczących operacji przekazania danych lub zestawu takich operacji; szczególną uwagę zwracać się będzie na charakter danych, cel i czas trwania proponowanych operacji przetwarzania danych, kraj pochodzenia i kraj ostatecznego

przeznaczenia, normy prawne, zarówno ogólne jak i branżowe, obowiązujące w kraju trzecim oraz przepisy zawodowe i środki bezpieczeństwa stosowane w tym kraju.

3. Państwa członkowskie i Komisja będą informować się wzajemnie o przypadkach, kiedy uznają, że kraj trzeci nie zapewnia odpowiedniego stopnia ochrony w znaczeniu ust. 2.

4. Jeżeli Komisja stwierdzi, na podstawie procedury przewidzianej w art. 31 ust. 2, że kraj trzeci nie zapewnia odpowiedniego stopnia ochrony w znaczeniu ust. 2 niniejszego artykułu, państwa członkowskie podejmą konieczne środki, aby nie dopuścić do przekazania jakichkolwiek danych tego samego rodzaju do wspomnianego kraju trzeciego.

5. We właściwym czasie Komisja przystąpi do negocjacji w celu naprawienia rozpoznanej sytuacji, o której mowa w ust. 4.

6. Komisja może stwierdzić, zgodnie z procedurą, o której mowa w art. 31 ust. 2, że kraj trzeci zapewnia prawidłowy stopień ochrony w znaczeniu ust. 2 niniejszego artykułu, co wynika z jego prawa krajowego lub międzynarodowych zobowiązań, jakie kraj ten podjął, szczególnie po zakończeniu negocjacji, o których mowa w ust. 5, w zakresie ochrony życia prywatnego i podstawowych wolności i praw osób fizycznych.

Państwa członkowskie podejmą konieczne działania w celu wykonania decyzji Komisji.

Artykuł 26

Wyłączenia

1. W drodze odstępstwa od art. 25 oraz, o ile prawo krajowe dotyczące konkretnych przypadków nie stanowi inaczej, państwa członkowskie zapewnią, że przekazanie lub przekazywanie danych osobowych do kraju trzeciego, który nie zapewnia odpowiedniego stopnia ochrony w znaczeniu art. 25 ust. 2 może nastąpić pod warunkiem, że:

(a) osoba, której dane dotyczą jednoznacznie udzieli zgody na proponowane przekazanie danych; lub

(b) przekazanie danych jest konieczne dla realizacji umowy między osobą, której dane dotyczą i administratorem danych lub dla wprowadzenia w życie ustaleń poprzedzających zawarcie umowy na wniosek osoby, której dane dotyczą; lub

(c) przekazanie danych jest konieczne dla zawarcia lub wykonania umowy zawartej w interesie osoby, której dane dotyczą; między administratorem danych i osobą trzecią; lub

(d) przekazanie danych jest konieczne lub wymagane przez prawo z ważnych względów publicznych lub w celu ustanowienia, wykonania lub obrony tytułu prawnego; lub

(e) przekazanie danych jest konieczne dla zapewnienia ochrony żywotnych interesów osoby, której dane dotyczą; lub

(f) przekazanie danych następuje z rejestru, który zgodnie z obowiązującymi przepisami ma służyć za źródło informacji dla ogółu społeczeństwa i jest udostępniony albo do publicznego wglądu albo każdej osobie posiadającej uzasadniony interes w uzyskaniu informacji, o ile warunki określone przez prawo odnośnie wglądu do takiego rejestru zostały w danym przypadku spełnione.

2. Niezależnie od postanowień ust. 1, państwo członkowskie może zezwolić na przekazanie lub przekazywanie danych osobowych do kraju trzeciego, który nie zapewnia odpowiedniego stopnia ochrony w znaczeniu art. 25 ust. 2, jeżeli administrator danych zapewni odpowiednie zabezpieczenia odnośnie ochrony prywatności oraz podstawowych praw i wolności osoby oraz odnośnie wykonywania związanych z nimi praw; zabezpieczenia takie mogą w szczególności wynikać z odpowiednich klauzul umownych.

3. Państwo członkowskie będzie informować Komisję i inne państwa członkowskie o wydanych zezwoleniach na podstawie ust. 2.

Jeżeli państwo członkowskie lub Komisja będą zgłaszać sprzeciwy w oparciu o uzasadnione przyczyny związane z ochroną prywatności oraz podstawowych praw i wolności osób, Komisja podejmie odpowiednie działania zgodnie z procedurą określoną w art. 31 ust. 2.

Państwa członkowskie podejmą konieczne środki w celu zastosowania się do decyzji Komisji.

4. Jeżeli Komisja postanowi, zgodnie z procedurą, o której mowa w art. 31 ust. 2, że określone klauzule umowne zapewniają odpowiednie zabezpieczenia wymagane w ust. 2, państwa członkowskie podejmą konieczne środki w celu zastosowania się do decyzji Komisji.

ROZDZIAŁ V

REGUŁY POSTĘPOWANIA

Artykuł 27

1. Państwa członkowskie i Komisja będą zachęcać do opracowywania reguł postępowania, których celem będzie usprawnienie procesu prawidłowego wprowadzania krajowych przepisów przyjętych przez państwa członkowskie na podstawie niniejszej dyrektywy, uwzględniając specyficzne cechy różnych branż.

2. Państwa członkowskie zapewnią stowarzyszeniom zawodowym i innym instytucjom reprezentującym inne kategorie administratorów danych, które opracowały projekty krajowych reguł postępowania lub które zamierzają dokonać zmiany lub uzupełnienia istniejących krajowych reguł postępowania, przedstawienie ich do zaopiniowania organowi władz państwowych.

Państwa członkowskie zapewnią ustalenie przez wspomniany organ m.in., czy przedstawiony mu projekt jest zgodny z przepisami krajowymi przyjętymi na podstawie niniejszej dyrektywy. Jeżeli organ ów uzna to za stosowne, będzie starać się o opinie osób, których dane dotyczą lub ich przedstawicieli.

3. Projekty reguł wspólnotowych, jak również zmiany i uzupełnienia istniejących reguł wspólnotowych mogą być przedstawione zespołowi roboczemu, o którym mowa w art. 29. Zespól roboczy ustali m.in., czy przedstawione mu projekty zgodne są z przepisami krajowymi przyjętymi na podstawie niniejszej dyrektywy. Jeżeli organ uzna to za stosowne, będzie starać się o opinię osób, których dane dotyczą, lub ich przedstawicieli. Komisja może zapewnić odpowiednie rozpowszechnienie reguł zatwierdzonych przez zespól roboczy.

ROZDZIAŁ VI

ORGAN NADZORCZY I ZESPÓL ROBOCZY DO SPRAW OCHRONY OSÓB FIZYCZNYCH W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

Artykuł 28
Organ nadzorczy

1. Każde państwo członkowskie zapewnia, że jeden lub kilka organów publicznych, będzie odpowiedzialnych za kontrolę stosowania na jego terytorium postanowień przyjętych przez państwa członkowskie na podstawie niniejszej dyrektywy.

Organy te będą postępować w sposób całkowicie niezależny wykonując powierzone im funkcje.

2. Każde państwo członkowskie wprowadzi obowiązek konsultowania się z organami nadzorczymi przy opracowywaniu środków administracyjnych lub przepisów dotyczących ochrony praw i wolności osób w zakresie przetwarzania danych osobowych.

3. Każdy organ będzie wyposażony w szczególności w:

- uprawienia dochodzeniowe, takie jak prawo dostępu do danych stanowiących przedmiot operacji przetwarzania danych oraz prawo gromadzenia wszelkich informacji potrzebnych do wykonywania jego funkcji nadzorczych,

- skuteczne uprawnienia interwencyjne, takie jak np. do wyrażenia opinii przed przystąpieniem do operacji przetwarzania danych zgodnie z art. 20, oraz do zapewnienia odpowiedniej publikacji tych opinii, zarządzania blokady, usunięcia lub zniszczenia danych, nakładania czasowego lub ostatecznego zakazu przetwarzania danych, ostrzegania lub upominania administratora danych, lub też prawo kierowania sprawy do parlamentów krajowych lub innych instytucji politycznych;

- uprawnienia do udziału w postępowaniu sądowym w przypadku naruszenia krajowych przepisów przyjętych na podstawie niniejszej dyrektywy lub zwrócenia uwagi władz sądowniczych na takie naruszenia.

Od decyzji organu nadzorczego, co do których zgłaszane są zastrzeżenia, przysługuje odwołanie do właściwego sądu.

4. Każdy organ nadzorczy będzie rozpatrywać skargi zgłaszane przez każdą osobę lub przez stowarzyszenie ją reprezentujące, odnośnie ochrony jej praw i wolności w zakresie

przetwarzania danych osobowych. Zainteresowana osoba zostanie poinformowana o wyniku sprawy.

Każdy organ nadzorczy będzie w szczególności rozpatrywać skargi dotyczące kontroli legalności przetwarzania danych, zgłaszane przez dowolną osobę, kiedy będą mieć zastosowanie krajowe przepisy przyjęte na podstawie art. 13 niniejszej dyrektywy. Osoba ta zostanie w każdym przypadku poinformowana o przeprowadzeniu kontroli.

5. Każdy organ nadzorczy będzie regularnie sporządzać raport ze swojej działalności. Raport będzie podany do wiadomości publicznej.

6. Każdy organ nadzorczy jest władny, niezależnie od krajowych przepisów dotyczących danego przypadku przetwarzania danych, do wykonywania na terytorium państwa członkowskiego kompetencji powierzonych mu zgodnie z ust. 3. Każdy organ może być poproszony o skorzystanie ze swoich uprawnień przez odpowiedni organ innego państwa członkowskiego.

Organy nadzorcze będą ze sobą współpracować w zakresie koniecznym do wykonywania ich obowiązków, zwłaszcza poprzez wymianę wszelkich przydatnych informacji.

7. Państwa członkowskie zapewnią, że członkowie kierownictwa i personel organu nadzorczego będą podlegać obowiązkowi zachowania tajemnicy zawodowej również po rozwiązaniu stosunku pracy, w odniesieniu do poufnych informacji, do których mają dostęp.

Artykuł 29

Zespół roboczy do spraw ochrony osób fizycznych w zakresie przetwarzania danych osobowych

1. Niniejszym powołuje się zespół roboczy do spraw ochrony osób fizycznych w zakresie przetwarzania danych osobowych, dalej zwany „zespołem roboczym".

Zespół będzie miał charakter doradczy i będzie działać w sposób niezależny.

2. W skład zespołu roboczego będą wchodzić przedstawiciel organu lub organów nadzorczych, powołanych przez każde państwo członkowskie oraz przedstawiciel organu lub organów ustanowionych dla instytucji i organów Wspólnoty, oraz przedstawiciel Komisji.

Każdy członek zespołu roboczego będzie powoływany przez instytucję, organ lub organy, które reprezentuje. Jeżeli państwo członkowskie powoła więcej niż jeden organ nadzorczy, organy te mianują wspólnego przedstawiciela. Ta sama zasada dotyczy organów utworzonych przez instytucje i organy Wspólnoty.

3. Zespól roboczy będzie podejmować decyzje zwykłą większością głosów przedstawicieli organów nadzorczych.

4. Zespół roboczy powoła swojego przewodniczącego. Kadencja przewodniczącego trwa dwa lata. Jego mandat będzie odnowiony.

5. Sekretariat zespołu roboczego będzie zapewniony przez Komisję

6. Zespół roboczy ustali własny regulamin.

7. Zespół roboczy będzie rozważać pozycje zamieszczone w porządku dziennym przez przewodniczącego, bądź to z jego inicjatywy, bądź na wniosek przedstawiciela organu nadzorczego lub na wniosek Komisji.

Artykuł 30

1. Zespół roboczy będzie:

(a) badać każdą kwestię dotyczącą stosowania krajowych środków przyjętych na podstawie niniejszej dyrektywy, aby przyczynić się w ten sposób do jednolitego stosowania tych środków;

(b) przekazywać Komisji opinie na temat stopnia ochrony we Wspólnocie i w krajach trzecich;

(c) doradzać Komisji w sprawie wszelkich proponowanych zmian niniejszej dyrektywy, dodatkowych lub szczegółowych środków mających na celu zabezpieczenie praw i wolności osób fizycznych w zakresie przetwarzania danych osobowych oraz innych proponowanych przez środków wspólnotowych wpływających na prawa i wolności;

(d) wydawać opinie na temat reguł postępowania opracowywanych na szczeblu Wspólnoty.

2. Jeżeli zespół roboczy stwierdzi występowanie rozbieżności między przepisami i praktyką w poszczególnych państwach członkowskich, mogących wpływać na równorzędność ochrony osób fizycznych w zakresie przetwarzania danych osobowych we Wspólnocie, zespół poinformuje o tym Komisję.

3. Zespół roboczy może, z własnej inicjatywy przedstawiać zalecenia we wszystkich sprawach związanych z ochroną osób fizycznych w zakresie przetwarzania danych osobowych we Wspólnocie.

4. Opinie i zalecenia zespołu roboczego będą przekazywane do Komisji oraz do komitetu, o którym mowa w art. 31.

5. Komisja będzie informować zespół roboczy o podejmowanych działaniach w odpowiedzi na jego opinie i zalecenia. Będzie to czynić w formie raportu, który przekazywany będzie również do Parlamentu Europejskiego i do Rady. Raport będzie udostępniony opinii publicznej.

6. Zespół roboczy będzie sporządzać roczny raport na temat sytuacji dotyczącej ochrony osób fizycznych w zakresie przetwarzania danych osobowych we Wspólnocie orz w krajach trzecich, które będzie przekazywać Komisji, Parlamentowi Europejskiemu i Radzie. Raport będzie udostępniony opinii publicznej.

ROZDZIAŁ VII

ŚRODKI WYKONAWCZE PODEJMOWANE PRZEZ WSPÓLNOTĘ

Artykuł 31
Komitet

1. Komisja będzie korzystać z pomocy komitetu, w którego skład wchodzić będą przedstawiciele państw członkowskich i któremu będzie przewodniczyć przedstawiciel Komisji.

2. Przedstawiciel Komisji przedstawi komitetowi projekt środków, jakie należy podjąć. Komitet wyda opinię o projekcie w terminie wyznaczonym przez przewodniczącego zależnie od stopnia pilności sprawy.

Opinia zostanie przyjęta większością głosów określoną w art. 148 ust. 2 Traktatu. Głosy przedstawicieli państw członkowskich w komitecie będą ważone w sposób określony w tym artykule. Przewodniczący nie bierze udziału w głosowaniu.

Komisja przyjmie środki, które będą stosowane bezpośrednio. Jeżeli jednak środki te nie będą zgodne z opinią komitetu, Komisja niezwłocznie powiadomi o tym Radę. W takim przypadku:

- Komisja odroczy wprowadzenie przyjętych środków na okres trzech miesięcy od daty powiadomienia,

- Rada może podjąć inną decyzję kwalifikowaną większością głosów w terminie określonym w powyższym akapicie.

POSTANOWIENIA KOŃCOWE

Artykuł 32

1. Państwa członkowskie wprowadzą w życie ustawy, rozporządzenia i przepisy administracyjne konieczne do wdrożenia niniejszej dyrektywy nie później niż trzy lata od daty jej przyjęcia.

Środki te powinny zawierać odniesienie do niniejszej dyrektywy lub odniesienie to powinno towarzyszyć ich urzędowej publikacji. Metody dokonywania takiego odniesienia określają państwa członkowskie.

2. Państwa członkowskie zapewnią, że przetwarzanie danych będące już w toku w dniu przyjęcia przepisów krajowych na podstawie niniejszej dyrektywy, zostanie dostosowane tych przepisów w terminie trzech lat od wspomnianej daty.

Odstępując od poprzedniego akapitu, ustala się, że państwa członkowskie mogą wprowadzić wymóg, aby przetwarzanie danych, które są już przechowywane w ręcznych systemach ewidencji w dniu wejścia w życie krajowych przepisów przyjętych na podstawie niniejszej dyrektywy zostały dostosowane do wymogów art. 6 - 8 dyrektywy w ciągu 12 lat od daty ich

przyjęcia. Państwa członkowskie przyznają osobie, której dane dotyczą prawo uzyskania, na jej wniosek, a szczególnie w czasie wykonywania przysługującego mu prawa dostępu, poprawy, usunięcia lub zablokowania danych, które są niekompletne, nieprawidłowe lub przechowywane w sposób niezgodny z uzasadnionymi celami realizowanymi przez administratora danych.

3. Odstępując od ust. 2, państwa członkowskie mogą ustalić - z zastrzeżeniem odpowiednich zabezpieczeń - że dane przechowywane wyłącznie dla potrzeb badań historycznych nie muszą być dostosowywane do wymogów art. 6 - 8 niniejszej dyrektywy.

4. Państwa członkowskie przekażą Komisji teksty podstawowych przepisów prawa krajowego, przyjętych na podstawie niniejszej dyrektywy.

Artykuł 33

Komisja będzie składać Radzie i Parlamentowi Europejskiemu regularne raporty, począwszy nie później niż trzy lata od daty wskazanej w art. 32 ust. 1, na temat wprowadzania w życie niniejszej dyrektywy, załączając do raportu, w razie potrzeby, odpowiednie propozycje zmian. Raport będzie podany do publicznej wiadomości.

Komisja zbada w szczególności stosowanie niniejszej dyrektywy w odniesieniu do przetwarzania danych dźwiękowych i obrazowych dotyczących osób fizycznych oraz przedstawi odpowiednie propozycje, które okażą się konieczne, biorąc pod uwagę zmiany techniki informacyjnej oraz stan postępu zachodzącego w społeczeństwie informacyjnym.

Artykuł 34

Niniejsza dyrektywa skierowana jest do państw członkowskich.

Sporządzono w Luksemburgu, dnia 24 października 1995 r.

W imieniu Parlamentu Europejskiego

Przewodniczący

K. HÄNSCH

W imieniu Rady

Przewodniczący

L. ATIENZA SERNA

LISTA PRZEKAZANYCH DOKUMENTÓW
DO
PROJEKTU USTAWY
O
ZMIANIE USTAWY
O OCHRONIE DANYCH OSOBOWYCH

przyjętego przez Radę Ministrów
w dniu 23 września 2003 r.

Obszar Negocjacyjny: „Swoboda świadczenia usług"
Narodowy Program Przygotowania do Członkostwa Polski w Unii Europejskiej:
Rozdział 3.

1.	Deklaracja dotycząca dostosowawczego charakteru projektu ustawy wraz z uzasadnieniem jego dostosowawczego charakteru
2.	Projekt ustawy wraz z uzasadnieniem oraz projektem podstawowego aktu wykonawczego
3.	Zestawienie przepisów dostosowujących projektowanej ustawy z odpowiednimi przepisami Unii Europejskiej (tabela zgodności)
4.	Opinia Urzędu Komitetu Integracji Europejskiej o zgodności projektu z prawem Unii Europejskiej wydana dnia 3 października 2003 r.
5.	Tłumaczenie na język polski Dyrektywy 95/46/WE Parlamentu europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych