



SEJM

RZECZYPOSPOLITEJ POLSKIEJ

III kadencja

Prezes Rady Ministrów

RM 10-85-01

Druk nr 3171

Warszawa, 6 lipca 2001 r.

Pan

Maciej Płażyński

Marszałek Sejmu

Rzeczypospolitej Polskiej

Szanowny Panie Marszałku.

Na podstawie art. 118 ust. 1 i art. 123 ust. 1 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. przedstawiam Sejmowi Rzeczypospolitej Polskiej projekt ustawy

- o zmianie ustawy o ochronie danych osobowych,

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

Jednocześnie, zgodnie z wymogami art. 31 ust. 3b Regulaminu Sejmu, przekazuję, przetłumaczony na język polski, tekst przepisu Unii Europejskiej, do którego ma być dostosowane prawo polskie.

W załączeniu przedstawiam także uzasadnienie trybu pilnego.

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

Z poważaniem

(-) Jerzy Buzek

Uzasadnienie trybu pilnego

Szybka nowelizacja ustawy o ochronie danych osobowych jest niezbędna z uwagi na konieczność, wymaganego przez Komisję Europejską, dostosowania polskiej ustawy o ochronie danych osobowych do wymogów Dyrektywy 95/46/WE Parlamentu Europejskiego oraz Rady z dnia 24 października 1995 r. o ochronie osób w związku z przetwarzaniem danych osobowych oraz swobodnym przepływie tych danych. Stanowi także potwierdzenie zaangażowania Polski w harmonizowanie prawa polskiego ze wspólnotowym porządkiem prawnym.

Pod adresem polskiej ustawy, w trakcie różnego rodzaju rozmów z Komisją Europejską, często podnoszono zarzuty. W efekcie, w Raporcie Okresowym Komisji Europejskiej z dnia 8 listopada 2000 r. zapisano, iż potrzebne jest dalsze dostosowanie prawa, zwłaszcza jeśli chodzi o ochronę danych osobowych. Stwierdzono również, iż uwagi podniesione w poprzednim Raporcie Okresowym, dotyczące funkcjonowania ustawy o ochronie danych, pozostają aktualne.

Z tego też względu, w czasie posiedzenia Podkomitetu ds. Rynku Wewnętrznego, które odbyło się w dniach 22-23 marca 2001 r. w Brukseli, zaprezentowano projekt nowelizacji ustawy oraz złożono zobowiązanie, że jeszcze w tym roku polska ustawa zostanie znowelizowana.

Z uwagi na kończącą się kadencję Parlamentu, jedynie zastosowanie szybkiej ścieżki legislacyjnej zagwarantuje wywiązanie się strony polskiej z przyjętego zobowiązania.

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. Nr 133, poz. 883, z 2000 r. Nr 12, poz. 136, Nr 50, poz. 580 i Nr 116, poz. 1216 oraz z 2001 r. Nr 42, poz. 474) wprowadza się następujące zmiany:

1) art. 6 otrzymuje brzmienie:

„Art. 6. 1. W rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

2. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

3. Informacji nie uważa się za umożliwiającą określenie tożsamości, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.”;

2) w art. 7 po pkt 2 dodaje się pkt 2a i 2b w brzmieniu:

„2a) systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,

2b) zabezpieczeniu danych w systemie informatycznym - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,”;

3) w art. 14 w pkt 1 po wyrazach „w których zlokalizowany jest” skreśla się wyraz „zarejestrowany”;

4) w art. 15:

a) dotychczasową treść oznacza się jako ust. 1,

b) po ust. 1 dodaje się ust. 2 w brzmieniu:

„2. W toku kontroli zbiorów, o których mowa w art. 43 ust. 1 pkt 1a, inspektor przeprowadzający kontrolę ma prawo wglądu do zbioru zawierającego dane osobowe jedynie za pośrednictwem upoważnionego przedstawiciela kontrolowanej jednostki organizacyjnej.”;

5) w art. 18 po ust. 2 dodaje się ust. 2a w brzmieniu:

„2a. Decyzje Generalnego Inspektora, o których mowa w ust.1, w odniesieniu do zbiorów określonych w art. 43 ust. 1 pkt 1a, nie mogą nakazywać usunięcia danych osobowych zebranych w toku czynności operacyjno-rozpoznawczych prowadzonych na podstawie przepisów prawa.”;

6) w art. 23 w ust. 1 pkt 5 otrzymuje brzmienie:

„5) jest niezbędne do wypełnienia prawnie usprawiedliwionych celów administratorów danych, o których mowa w art. 3 ust. 2, lub osób trzecich, którym są przekazywane te dane - a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą.”;

7) w art. 25 w ust. 2 po pkt 4 dodaje się pkt 5 i 6 w brzmieniu:

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

6) osoba, której dane dotyczą, posiada informacje, o których mowa w ust.1.”;

8) po art. 26 dodaje się art. 26a w brzmieniu:

„Art. 26a. 1. Niedopuszczalne jest ostateczne rozstrzygnięcie indywidualnej sprawy osoby, której dane dotyczą, jeżeli jego treść jest wyłącznie wynikiem operacji na danych osobowych, prowadzonych w systemie informatycznym.

2. Przepisu ust. 1 nie stosuje się, jeżeli rozstrzygnięcie zostało podjęte

podczas zawierania lub wykonywania umowy i uwzględnia wniosek osoby, której dane dotyczą.”;

9) w art. 27:

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

„1a. Zabrania się przetwarzania danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.”,

b) w ust. 2:

- po wyrazach „ust. 1” dodaje się wyrazy „oraz ust. 1a”,

- po pkt 8 dodaje się pkt 9 w brzmieniu:

„9) jest to niezbędne do prowadzenia badań naukowych, w tym przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego; publikowanie wyników badań naukowych nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone.”;

10) w art. 28 skreśla się ust. 1;

11) w art. 32:

a) w ust. 1 po pkt 8 dodaje się pkt 9 w brzmieniu:

„9) wniesienia do administratora danych żądania ponownego, indywidualnego rozpatrzenia spra-

wy rozstrzygniętej z naruszeniem art. 26a ust.1.",

b) w ust. 2 wyraz „podejmuje” zastępuje się wyrazem „wydaje”,

c) po ust. 3 dodaje się ust.3a w brzmieniu:

„3a. W razie wniesienia żądania, o którym mowa w art. 32 ust.1 pkt 9, administrator danych bez zbędnej zwłoki rozpatruje sprawę albo przekazuje ją wraz z uzasadnieniem swojego stanowiska Generalnemu Inspektorowi, który wydaje stosowną decyzję.”;

12) w art. 35 po ust. 2 dodaje się ust. 3 w brzmieniu:

„3. Administrator danych jest obowiązany poinformować bez zbędnej zwłoki innych administratorów, którym dane osobowe zostały udostępnione, o dokonanych uzupełnieniu, uaktualnieniu lub sprostowaniu danych.”;

13) w art. 36 po wyrazach „zabranie przez osobę nieuprawnioną,” dodaje się wyrazy „przetwarzaniem z naruszeniem ustawy, zmianą, utratą,”;

14) w art. 41 w ust. 1:

a) po pkt 4 dodaje się pkt 4a w brzmieniu:

„4a) informację o odbiorcach lub kategoriach odbiorców, którym dane mogą być przekazywane,”,

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

„7) informację dotyczącą ewentualnego przekazywania danych za granicę.”;

15) w art. 43:

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

„1a) które zostały uzyskane w wyniku czynności operacyjno-rozpoznawczych przez funkcjonariuszy organów uprawnionych do tych czynności,”

b) w ust. 2 po wyrazach „o których mowa w ust. 1 pkt 1 i 3,” dodaje się wyrazy „oraz zbiorów, o których mowa w ust. 1 pkt 1a, przetwarzanych przez służby ochrony państwa w rozumieniu ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz.U. Nr 11, poz. 95, z 2000 r. Nr 12, poz. 136 i Nr 39, poz. 462 oraz z 2001 r. Nr 22, poz. 247 i Nr 27, poz. 298),”.

Art. 2.

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

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

Wprowadzenie do ustawy o ochronie danych osobowych proponowanych przepisów wynika z konieczności dostosowania unormowań przyjętych w polskim porządku prawnym do postanowień Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych oraz swobodnego przepływu tych danych, zwanej dalej „Dyrektywą”.

Art. 2a Dyrektywy definiuje dane osobowe, jako „wszelkie informacje dotyczące zidentyfikowanej lub dającej się zidentyfikować osoby fizycznej (podmiotu danych); osoba dająca się zidentyfikować jest osobą, której tożsamość można określić bezpośrednio lub pośrednio, szczególnie przez odniesienie się do numeru identyfikacyjnego lub innych wskaźników charakterystycznych dla jej fizycznej, fizjologicznej, umysłowej, gospodarczej, kulturowej lub społecznej tożsamości”.

W celu dostosowania polskich przepisów o ochronie danych osobowych do Dyrektywy, ochroną wynikającą z przepisów ustawy należy objąć nie tylko „każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby” (art. 6 ustawy w dotychczasowym brzmieniu), ale również wszelkie informacje dotyczące osoby fizycznej lub pozwalające

na identyfikację jej tożsamości bezpośrednio lub pośrednio, w szczególności przez odniesienie się do numeru identyfikacyjnego lub innych cech charakterystycznych dla jej fizycznej, fizjologicznej, umysłowej, gospodarczej, kulturowej lub społecznej tożsamości. Dotychczasowe brzmienie art. 6 ustawy zawężało zakres ochrony wyłącznie do informacji pozwalających na określenie tożsamości osoby fizycznej. Konsekwencją przyjęcia proponowanej zmiany będzie rozszerzenie zakresu ochrony wynikającej z ustawy na wszelkie informacje dotyczące osoby fizycznej lub pozwalające na identyfikację jej tożsamości bezpośrednio lub pośrednio.

Art. 7 rozszerzono przez zdefiniowanie systemu informatycznego oraz zabezpieczenia danych w systemie informatycznym.

Rozszerzenie art. 15 o ust. 2 pozwoli na kontrolowanie zbiorów przez inspektorów Generalnego Inspektora Ochrony Danych Osobowych, prowadzonych przez organy, np. Policji czy Straży Granicznej, z dodatkowym zagwarantowaniem tajemnicy danych przetwarzanych w zbiorach tych organów.

W art. 18 w ust. 2a wprowadzono zastrzeżenie ograniczające wprawdzie uprawnienia w zakresie podejmowania rozstrzygnięć przez Generalnego Inspektora Danych Osobowych, jednakże dotyczy ono tylko zbiorów tworzonych w wyniku czynności operacyjno-rozpoznawczych, których ostateczna weryfikacja jest dokonywana w toku postępowań prowadzonych przez prokuraturę lub sąd.

Art. 23 ust. 1 pkt 5 jest wzorowany na art. 7f Dyrektywy. Art. 7f Dyrektywy przyjmuje zasadę, że przetwarzanie danych w formie ich udostępnienia jest możliwe także wtedy, gdy to odbiorca danych legitymuje się prawnie usprawiedliwionym interesem w ich otrzymaniu. W aktualnym brzmieniu polskiej ustawy brakuje takiej przesłanki udostępnienia danych. W obecnej regulacji usprawiedliwiony cel ma dotyczyć jedynie administratora udostępniającego dane. Jeśli nie ma on interesu w ich udostępnieniu, to nie może ich udostępnić, pomimo, że taki interes posiada podmiot występujący o te dane. Z tego też powodu, z uwagi na praktyczne implikacje tej luki prawnej oraz w celu zharmonizowania naszego prawa z wymaganiami stawianymi przez Unię, proponuje się wzbogacić ten przepis o przedmiotową przesłankę. Należy podkreślić, że użyty łącznik „lub” (nie „oraz”) powoduje, iż wystarczające jest istnienie usprawiedliwionego interesu tylko po jednej stronie wymiany danych. Ponadto „usprawiedliwione cele” określono jako „prawnie usprawiedliwione cele” - zgodnie z Dyrektywą.

W art. 25 w ust. 2 dodano pkt 5 i 6. Obecnie przyjęte rozwiązanie, nakazujące wszystkim podmiotom dopełnianie obowiązku informacyjnego, nawet jeśli osoba, której dane dotyczą posiada informacje wymienione w art. 25 ust. 1 oraz podmiotom działającym w ramach obowiązujących przepisów prawa, jest zbyt rygorystyczne w stosunku do postanowień Dyrektywy i nakłada zbędne, z punktu widzenia zabezpieczenia interesów podmiotów danych, obowiązki. Dyrektywa zezwala na odstępnie od wykonania obowiązku infor-

macyjnego w sytuacji, gdy podmiot danych ma już pełną świadomość faktu i okoliczności przetwarzania oraz gdy przetwarzanie jest przewidziane prawem (pkt 40 i 49 wstępu do Dyrektywy oraz art. 11 ust. 2 Dyrektywy).

Dotychczasowa praktyka w zakresie przetwarzania danych objętych art. 28 powodowała liczne trudności, w szczególności dla osób, których dane dotyczyły, w związku z pozbawieniem ich prawa do decydowania o wykorzystaniu dotyczących ich rozstrzygnięć. Art. 28 w dotychczasowym brzmieniu wymaga wyłącznie podstawy ustawowej dla przetwarzania danych, nawet w przypadku orzeczeń wydanych w postępowaniu sądowym lub administracyjnym, których wykorzystanie w żaden sposób nie łączy się z ryzykiem poniżenia osób wskazanych w tych rozstrzygnięciach w opinii innych osób (np. orzeczenia sądowe dotyczące nabycia spadku w postaci nieruchomości nie mogą być w obecnym stanie prawnym włączone, jako dokument potwierdzający prawo własności nieruchomości, do akt klientów sprzedających nieruchomości za pośrednictwem biura pośrednictwa sprzedaży nieruchomości, ponieważ żadna ustawa nie zezwala biurom pośrednictwa do gromadzenia takich dokumentów). Rozwiązanie przyjęte w polskiej ustawie wykracza poza wymagania stawiane przez Dyrektywę 95/46 z dnia 24 października 1995 r. o ochronie osób w związku z przetwarzaniem danych (...). Art. 8 ust. 5 Dyrektywy kładzie nacisk na to, aby przetwarzanie danych dotyczących przestępstw, osób skazanych lub środków bezpieczeństwa mogło mieć miejsce jedynie pod kontrolą kompetentnych władz lub pod warunkiem podjęcia odpowiedzialnych środków zabezpieczających na mocy prawa

państwowego. Przepis ten dopuszcza również możliwość wprowadzenia przepisów nakazujących przetwarzanie danych dotyczących „sankcji administracyjnych lub orzeczeń w sprawach cywilnych” również pod kontrolą odpowiednich władz.

W świetle powyższych warunków stawianych przez Dyrektywę, właściwe zabezpieczenia danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym zapewni art. 27 ust. 2 dopuszczający przetwarzanie danych szczególnie chronionych wyłącznie po spełnieniu jednej z wymienionych enumeratywnie przesłanek.

Ponieważ ustawa w obecnym brzmieniu uniemożliwia uzyskanie dostępu do danych osobowych niezbędnych do prowadzenia badań naukowych, w tym przygotowania rozprawy niezbędnej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego (np. niemożliwe jest prowadzenie badań nt. błędu w sztuce lekarskiej czy powrotności do przestępstwa), niezbędne stało się stworzenie odrębnej przesłanki uprawniającej do przetwarzania danych osobowych - także szczególnie chronionych - na potrzeby badań naukowych, jednakże z zastrzeżeniem, że publikacja wyników badań naukowych nie może prowadzić do identyfikacji osób, których dane zostały wykorzystane w toku badań (art. 27 ust. 2 pkt 9).

Nałożono również na administratora obowiązek zawiadamiania osoby trzeciej, którym te dane będą udostępniane, o zaistniałych w nich zmianach.

Proponowana nowelizacja wprowadza też do ustawy nowy przepis regulujący problematykę rozstrzygnięć wydawanych wyłącznie na podstawie automatycznego przetwarzania danych osobowych.

Zgodnie z postanowieniami art. 15 Dyrektywy, państwa członkowskie mają obowiązek zagwarantowania każdej osobie prawa „niepodlegania decyzji mającej skutki prawne lub poważnie wpływającej na jej sytuację, która jest oparta wyłącznie na automatycznym przetwarzaniu danych mających na celu określenie pewnych aspektów personalnych odnoszących się do tej osoby, jej pracy, zdolności kredytowej, odpowiedzialności, reputacji itd.". Wyjątek od tej zasady stanowić mogą takie decyzje, które „powzięte zostały podczas zawierania lub wypełniania postanowień umowy; jeśli spełniono wnioski podmiotu danych w sprawie zawarcia lub wykonania postanowień umowy lub istnieją odpowiednie środki ochrony jego interesów, takie jak ustalenia pozwalające mu na wyrażenie swojej opinii”.

Przesłanką wprowadzenia w Dyrektywie powyższego rozwiązania był rozwój informatyki, a w szczególności jego konsekwencje, w postaci zagrożenia praw jednostki w procesie podejmowania rozstrzygnięć w sprawach indywidualnych wyłącznie na podstawie automatycznego przetwarzania danych osobowych.

Polska ustawa o ochronie danych osobowych nie zawiera podobnego rozwiązania, z tego względu należy stworzyć ustawowe gwarancje ochrony praw osób, wobec których zostało podjęte rozstrzygnięcie wyłącznie na podstawie automatycznego przetwarzania ich danych osobowych.

Według proponowanej nowelizacji przepis ustawy miałyby generalnie statuować niedopuszczalność rozstrzygnięć wydanych wyłącznie w wyniku automatycznego przetwarzania danych. Dopuszczalność takich rozstrzygnięć miałyby miejsce jedynie wówczas, gdyby były one podejmowane w toku zawierania lub wykonywania umowy i uwzględniały wniosek strony (art. 26 ust. 3).

Ponadto każda osoba, której dane przetworzone w sposób automatyczny stanowiłyby jedyną podstawę rozstrzygnięcia jej sprawy, powinna dysponować prawnymi środkami skutecznej obrony swoich interesów, przez możliwość żądania ponownego, indywidualnego rozpatrzenia jej sprawy. Zadość tym wymaganiom czyni dodany do art. 32 ust. 1 pkt 9, który stwarza materialną podstawę żądania ponownego, indywidualnego rozpatrzenia sprawy oraz dodany do art. 32 - ust. 3a, który nakłada na administratora danych obowiązek rozpatrzenia wniesionego żądania bez zbędnej zwłoki albo przekazania sprawy wraz z uzasadnieniem swojego stanowiska Generalnemu Inspektorowi Danych Osobowych.

Dodane do art. 32 przepisy tworzą prawną podstawę żądania indywidualnego rozstrzygnięcia sprawy oraz - w przypadku sporu między administratorem danych, który podjął rozstrzygnięcia a osobą, której sprawa była rozstrzygana co do zasadności żądania - możliwość kontroli i rozstrzygnięcia sprawy w formie decyzji przez niezależny organ.

Zmiana art. 36 ma zapewniać (przy zastosowaniu środków technicznych i organizacyjnych) odpowiedni do cha-

rakteru danych i zagrożeń związanych z przetwarzaniem danych poziom ochrony.

W art. 41 ust. 1 przyjęto, że zgłoszenie zbioru danych do rejestru powinno zawierać również informację o odbiorcach, którym dane mogą być przekazywane, oraz informację dotyczącą ewentualnego przekazywania danych osobowych za granicę.

Projektowana nowelizacja nie pociąga za sobą skutków finansowych.



SEKRETARZ
KOMITETU INTEGRACJI EUROPEJSKIEJ
Jacek Saryusz-Wolski

Sekr. Min. JSW/*JSW*/2001/DLE/AW

Warszawa, *26* czerwca 2001 r.

Pani
Jolanta Rusiniak
p.o. Sekretarza 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. 494) przez Sekretarza Komitetu Integracji Europejskiej, Jacka Saryusz-Wolskiego, działającego z upoważnienia Przewodniczącego Komitetu Integracji Europejskiej

W związku z przedłożonym projektem ustawy o zmianie ustawy o ochronie danych osobowych pozwalam sobie wyrazić następującą opinię.

- I. Projektowana zmiana ma na celu dostosowanie przepisów ustawy o ochronie danych osobowych do regulacji prawa Unii Europejskiej, głównie w zakresie zmiany definicji danych osobowych oraz automatycznego przetwarzania danych osobowych.
- II. Proponowana nowelizacja odnosi się do przepisów Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych oraz swobodnego przepływu tych danych.

III. Zgodnie z proponowaną nowelizacją, jak również zgodnie z definicjami przyjętymi w Dyrektywie 95/46/WE, zmianie uległ zakres pojęcia dane osobowe. Za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Określenie tożsamości osoby fizycznej może nastąpić zarówno bezpośrednio jak i pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej fizyczną, fizjologiczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość. Wszystkie powyższe przepisy są zgodne z art. 2 Dyrektywy 95/46/WE.

Na podstawie opiniowanej nowelizacji został dodany artykuł 26 a, który reguluje kwestie związane z automatycznym przetwarzaniem danych osobowych (w polskiej ustawie używa się terminologii „operacje prowadzone w systemie informatycznym”). Nowelizacja stanowi, że niedopuszczalne jest ostateczne rozstrzygnięcie indywidualnej sprawy osoby, której dane dotyczą, jeżeli jego treść jest wyłącznie wynikiem operacji na danych osobowych prowadzonych w systemie informatycznym. Wyjątek od powyższej zasady stanowi sytuacja, gdy rozstrzygnięcie zostało podjęte podczas zawierania lub wykonywania umowy i uwzględniania wniosek osoby, której dane dotyczą. Proponowany artykuł jest zgodny z art. 15 Dyrektywy 95/46/WE.

Proponowana zmiana ustawy do katalogu danych, których przetwarzanie jest dopuszczalne (art. 27 ust 2 ustawy) dodaje punkt o danych, których przetwarzanie jest niezbędne dla prowadzenia badań naukowych, w tym przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego. Publikowanie wyników badań naukowych nie może zaś następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone.

W art. 35 ustawy o ochronie danych osobowych dodaje się ustęp dotyczący obowiązku informowania przez administratora danych innych administratorów, którym dane osobowe zostały udostępnione, o dokonanym uzupełnieniu, uaktualnieniu lub sprostowaniu danych.

Zgodnie z Dyrektywą 95/46/WE nastąpiło uzupełnienie katalogu informacji, które powinny być zawarte w zgłoszeniu zbioru danych do rejestracji (art. 41 ust. 1 ustawy). Chodzi tu o informację o odbiorcach lub kategoriach odbiorców, którym dane mogą być przekazywane oraz informację dotyczącą ewentualnego przekazywania danych za granicę.

IV. W konkluzji należy stwierdzić, że projekt ustawy o zmianie ustawy z o ochronie danych osobowych jest zgodny z prawem Unii Europejskiej.

Z poważaniem,

SEKRETARZ
Komisji ds.
z up. Jacek Saryusz-Wolski
Sekretarz Stanu

Do uprzejmej wiadomości:

Pan Piotr Stachańczyk

Podsekretarz Stanu

Ministerstwo Spraw Wewnętrznych i Administracji



URZĄD
KOMITETU INTEGRACJI EUROPEJSKIEJ
Cezary Banasiński
Podsekretarz Stanu

Sekr. Min. CB./ 385 /2001/

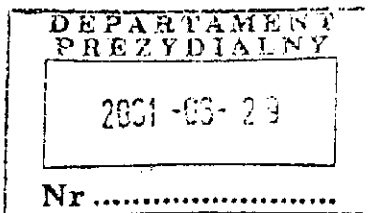
Warszawa, 29 czerwca 2001 r.

Pani
Jolanta Rusiniak
p.o. Sekretarza Rady Ministrów
Kancelaria Prezesa Rady Ministrów

Szanowna Pani Minister

Z upoważnienia Sekretarza Komitetu Integracji Europejskiej, przekazuję uzasadnienie dostosowawczego charakteru projektu ustawy o zmianie ustawy o ochronie danych osobowych.

Z poważaniem
PODSEKRETARZ STANU
Cezary Banasiński
Cezary Banasiński



21

Uzasadnienie dostosowawczego charakteru projektu ustawy o zmianie ustawy o ochronie danych osobowych

Głównym celem przedstawionego projektu jest dostosowanie polskich rozwiązań prawnych odnoszących się do ochrony przetwarzania danych osobowych do wymagań Unii Europejskiej.

Proponowana nowelizacja odnosi się do przepisów Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych oraz swobodnego przepływu tych danych.

Obowiązująca ustawa o ochronie danych osobowych w dużej mierze odpowiada wymaganiom zawartym w Dyrektywie 95/46/WE. Obecnie proponowane zmiany przyczynią się do uzyskania pełnej zgodności ustawy o ochronie danych osobowych z prawem Unii Europejskiej.

Zgodnie z proponowaną nowelizacją, jak również zgodnie z definicjami przyjętymi w Dyrektywie 95/46/WE, zmianie uległ zakres pojęcia dane osobowe. Za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Określenie tożsamości osoby fizycznej może nastąpić zarówno bezpośrednio jak i pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej fizyczną, fizjologiczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość. Powyższy przepis stanowi implementację art. 2 Dyrektywy 95/46/WE.

Opiniowana nowelizacja dodaje artykuł 26a, który reguluje kwestie związane z automatycznym przetwarzaniem danych osobowych (w polskiej ustawie używa się terminologii „operacje prowadzone w systemie informatycznym”). Nowelizacja stanowi, że niedopuszczalne jest ostateczne rozstrzygnięcie indywidualnej sprawy osoby, której dane dotyczą, jeżeli jego treść jest wyłącznie wynikiem operacji na danych osobowych prowadzonych w systemie informatycznym. Wyjątek od powyższej zasady stanowi sytuacja, gdy rozstrzygnięcie zostało podjęte podczas zawierania lub wykonywania umowy i uwzględniania wniosek osoby, której dane dotyczą. Proponowany artykuł implementuje do polskiego porządku prawnego art. 15 Dyrektywy 95/46/WE.

Kolejne zmiany dotyczą katalogu danych, których przetwarzanie jest dopuszczalne (art. 27 ust 2 ustawy). Dodany zostaje punkt regulujący dane, których przetwarzanie jest niezbędne dla prowadzenia badań naukowych, w tym przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego. Publikowanie wyników badań naukowych nie może zaś następować w sposób umożliwiający identyfikację osób, których dane

zostały przetworzone. Uregulowania te implementują odpowiednie przepisy Dyrektywy 95/46/WE.

W art. 35 ustawy o ochronie danych osobowych dodaje się ustęp dotyczący obowiązku informowania przez administratora danych innych administratorów, którym dane osobowe zostały udostępnione, o dokonanych uzupełnieniu, uaktualnieniu lub sprostowaniu danych.

Zgodnie z Dyrektywą 95/46/WE nastąpiło uzupełnienie katalogu informacji, które powinny być zawarte w zgłoszeniu zbioru danych do rejestracji (art. 41 ust. 1 ustawy). Chodzi tu o informacje o odbiorcach lub kategoriach odbiorców, którym dane mogą być przekazywane oraz informację dotyczącą ewentualnego przekazywania danych za granicę.

Reasumując, projekt ustawy o zmianie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych należy potraktować jako ustawę o charakterze dostosowującym polskie prawo do prawa Unii Europejskiej.

**Zestawienie przepisów dostosowujących projektowanej ustawy
z odpowiednimi przepisami Unii Europejskiej
(tabela zgodności)**

L.p.	UE	JUE	JPL	Treść zmiany	Intertemporalne	Uwagi
1.	95/46 WE	Art. 2a	Art. 6	Dotyczy zmiany definicji danych osobowych	Z dniem wejścia w życie ustawy	
2.	95/46 WE	Art. 28	Art. 14 pkt 1	Dotyczy uprawnień kontrolnych inspektorów GODO	Z dniem wejścia w życie ustawy	
3.	95/46 WE	Art. 28 w zw. z art. 13	Art. 15 ust. 2	Dotyczy uprawnień kontrolnych inspektorów GODO	Z dniem wejścia w życie ustawy	
4.	95/46 WE	Art. 28 w zw. z art. 13	Art. 18 ust. 2	Dotyczy uprawnień kontrolnych inspektorów GODO	Z dniem wejścia w życie ustawy	
5.	95/46 WE	Art. 7f	Art. 23 ust 1 p 5	Dotyczy podstaw legalizujących przetwarzanie, w tym udostępniania danych osobowych	Z dniem wejścia w życie ustawy	
6.	95/46 WE	Art. 11 ust. 2	Art. 25 ust 2 p 5 i 6	Dotyczy zwolnień z obowiązku informacyjnego	Z dniem wejścia w życie ustawy	
7.	95/46 WE	Art. 15	Art. 26a	Dotyczy zakazu automatyzacji indywidualnych rozstrzygnięć	Z dniem wejścia w życie ustawy	
8.	95/46 WE	Art. 8 Ust. 5	Art. 27 ust. 1a	Dotyczy podstaw legalizujących przetwarzanie danych wrażliwych	Z dniem wejścia w życie ustawy	
9.	95/46 WE	Art. 8 ust. 4 Art. 11 ust. 2	Art. 27 art. 1 p 9	Dotyczy podstaw legalizujących przetwarzanie danych wrażliwych	Z dniem wejścia w życie ustawy	
10.	95/46 WE	Art. 15	Art. 32 ust. 1 p 9	Dotyczy wzbogacenia kata - logu praw podmiotu danych	Z dniem wejścia w życie ustawy	
11.	95/46 WE	Art. 15	Art. 32 ust 3a	Dotyczy skutków niezastosowania się do zakazu automatyzacji rozstrzygnięć	Z dniem wejścia w życie ustawy	
12.	95/46 WE	Art. 12c	Art. 35 ust 3	Dotyczy obowiązku informowania osób trzecich o zmianach w zakresie jakości danych lub ich przetwarzania	Z dniem wejścia w życie ustawy	
13.	95/46 WE	Art. 19 ust. 1c	Art. 41 ust. 1 p 4a	Dotyczy obowiązku zgłoszenia do rejestracji informacji o odbiorcach lub kategorii odbiorców danych	Z dniem wejścia w życie ustawy	

14.	95/46 WE	Art. 19 ust. 1 e	Art. 41 ust. 1 p 7	Dotyczy obowiązku zgłoszenia do rejestracji faktu przesyłania danych do krajów trzecich	Z dniem wejścia w życie ustawy	
15.	95/46 WE	Art. 15	Art. 7 p 2a, 2b	Dotyczy definicji pojęć występujących w ustawie	Z dniem wejścia w życie ustawy	W ramach dopuszczalnych odrębności w regulacji krajowej, proponujemy zdefiniować te pojęcia w samej ustawie
16.	95/46 WE	Art. 13 ust. 1 pkt d	Art. 43 ust. 1 p 1a	Dotyczy uprawnień kontrolnych inspektorów GIODO	Z dniem wejścia w życie ustawy	W ramach dopuszczalnych odrębności w regulacji krajowej uprawnienia kontrolne władz nadzorczych mogą być ograniczone

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

uwzględniając wniosek Komisji¹,

uwzględniając opinię Komitetu Ekonomiczno - Społecznego²,

oraz działając zgodnie z procedurą ustanowioną w art. 189b Traktatu³,

- (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 konstytucji i ustawodawstwa 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, ludzi, usług i kapitału wymaga nie tylko zapewnienia swobodnego przepływu danych osobowych z jednego państwa członkowskiego do drugiego, lecz również ochrony podstawowych praw osób fizycznych;

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).

- (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, ustanowionym 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 jednakowy 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 zbliżenia 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 ustawodawstwa 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 kryminalnego, bez wpływu na obowiązki nałożone na państwa członkowskie na mocy art. 56 ust. 2, art. 57 lub art. 100a Traktatu o utworzeniu Wspólnoty Europejskiej; 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 zamkniętym układzie zbiorów 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 kryminalnego 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 ochronie 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 dokładniej 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, zapewnienia 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 przetwarzaniu 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 podmiot danych, nie będzie mógł być zidentyfikowany; 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 wykroczać poza cele, dla których są przetwarzane; cele takie muszą być jednoznaczne i uzasadnione oraz określone w czasie gromadzenia danych; potrzeby dalszego przetwarzania danych dla potrzeb ich gromadzenia nie mogą być niezgodne z pierwotnie określonymi celami;
- (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 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 angażują dane, których administrator danych nie uzyskał bezpośrednio od osoby, której 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 dane 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 dochodzenie i prowadzenie spraw kryminalnych oraz działań w związku z naruszeniem zasad etyki w zawodach podlegających

- określonym regulacjom; lista wyłączeń i ograniczeń powinna obejmować zadania w zakresie nadzoru, kontroli i regulacji koniecznych w trzech wymienionych ostatnio dziedzinach, dotyczące 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, oficjalne uprawnienia lub uzasadnione prawo osoby fizycznej lub prawnej, osoba, której dane te dotyczą powinna jednak mieć prawo, ze względu na uzasadnione i ważne 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 nie dopuszczenie 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 w 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 zgodna 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; 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 dla obywateli 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 podmiotu danych 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 dla niektórych okoliczności zwolnienie z tego zakazu, 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 uwzględnić 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 zainteresowane kręgi przemysłowe do opracowania kodeksów 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 angażowania się w postępowanie sądowe; 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 wykonywaniu 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/EWG¹;

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.

- (67) 20 grudnia 1994 zawarta została pomiędzy Parlamentem Europejskim, Radą i Komisją umowa w sprawie *modus vivendi* dotycząca sposobów wprowadzania w życie ustaw 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 systemów ewidencji danych z niektórymi postanowieniami dyrektywy; jeżeli we wspomnianym przedłużonym okresie przejściowym dane zawarte w owych systemach będą przetwarzane ręcznie, konieczne będzie doprowadzenie do zgodności tych systemów 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 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 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 przyjmuje się następujące definicje:

- (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” („zbiór”) oznacza każdy uporządkowany zestaw danych, 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, agencję lub inny organ przetwarzający dane osobowe w imieniu administratora danych;
- (f) „osoba trzecia” oznacza osobę fizyczną lub prawną, urząd publiczny, agencję 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, agencję 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 systemu ewidencji lub mających stanowić część zbioru danych.
2. Niniejsza dyrektywa nie dotyczy przetwarzania danych osobowych:
 - w ramach działalności wykraczającej poza zakres prawa Wspólnoty, jak np. dane, o których mowa w rozdziałach V i VI Traktatu o Unii Europejskiej, oraz w każdym przypadku - przetwarzania danych dotyczących bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (łącznie ze stanem gospodarki państwa, kiedy przetwarzanie danych dotyczy bezpieczeństwa państwa) oraz działalności państwa w dziedzinie prawa kryminalnego,
 - przez osobę fizyczną w trakcie czynności o czysto osobistym lub domowym charakterze.

Artykuł 4

Stosowane prawo krajowe

1. Każde państwo członkowskie będzie stosować w odniesieniu do przetwarzania danych osobowych postanowienia prawa krajowego, jakie wprowadzi na podstawie niniejszej dyrektywy wówczas, gdy:
 - (a) przetwarzanie danych będzie odbywać się w kontekście prowadzenia przez administratora danych działalności gospodarczej na terytorium państwa członkowskiego; jeżeli ten sam administrator danych prowadzi działalność gospodarczą na terytorium kilku państw członkowskich, musi on podjąć niezbędne

działania, aby zapewnić, że każda z tych firm wywiązuje się z obowiązków ustalonych przez stosowane prawo krajowe;

- (b) administrator danych nie będzie prowadzić działalności gospodarczej na terytorium państwa członkowskiego, lecz w miejscu, gdzie jego prawo krajowe obowiązuje na mocy międzynarodowego prawa publicznego;
 - (c) administrator danych nie będzie prowadził działalności gospodarczej na terytorium Wspólnoty oraz, dla celów przetwarzania danych osobowych będzie wykorzystywać środki, zarówno zautomatyzowane jak i inne, znajdujące się na terytorium wymienionego państwa członkowskiego, o ile środki te nie będą 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, bez wpływu na postępowania sądowego, jakie mogłyby być podjęte przeciwko samemu administratorowi danych.

ROZDZIAŁ II

OGÓLNE ZASADY LEGALNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

Artykuł 5

Państwa członkowskie określają, w granicach postanowień zawartych w niniejszym rozdziale, bardziej szczegółowe warunki ustalania 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) prawidłowe, stosowne oraz nie nadmierne ilościowo w stosunku do celów, dla których zostały zgromadzone i/lub dalej przetworzone;
- (d) prawidłowe oraz, w razie konieczności, aktualizowane; należy podjąć wszelkie uzasadnione działania, aby zapewnić usunięcie lub poprawienie nieprawidłowych lub

niekompletnych danych, biorąc pod uwagę cele, dla których zostały zgromadzone lub dla których są dalej przetwarzane;

- (e) przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą przez czas 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 osób, których 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 którą ujawnia się dane, z wyjątkiem sytuacji, kiedy interesy takie podporządkowane są interesom związanym z podstawowymi prawami i wolnością osoby, której dane dotyczą, które gwarantują ochronę 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, opinie 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 pracownika służby zdrowia zgodnie z przepisami prawa krajowego lub zasadami określonymi przez właściwe krajowe instytucje, podlegającemu 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 określone zabezpieczenia, z zachowaniem derogacji, które państwo członkowskie może udzielić zgodnie z obowiązującymi przepisami krajowymi, zapewniając zachowanie odpowiednich zabezpieczeń. Jednak kompletny rejestr przestępstw kryminalnych może być prowadzony tylko pod kontrolą oficjalnego organu władzy.
6. Uchylenia ust. 1, o których mowa w ust. 4 i 5 będą zgłoszone 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 słowa

Państwa członkowskie wprowadzą możliwość uchylenia lub zwolnienia z postanowień niniejszego rozdziału, rozdziału IV i rozdziału VI w przypadku przetwarzania danych osobowych wyłącznie w celach dziennikarskich lub w celu uzyskania wyrazu artystycznego lub literackiego jedynie wówczas, gdy jest to konieczne dla pogodzenia prawa prywatności z przepisami dotyczącymi wolności słowa.

CZEŚĆ 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 wglądu 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 uzyskiwane są z innych źródeł niż osoba, której dane dotyczą, państwa członkowskie zapewnią, aby administrator danych lub jego przedstawiciel był zobowiązany od początku gromadzenia danych osobowych lub w przypadku ujawnienia danych osobie trzeciej, nie później niż gdy dane są ujawniane po raz pierwszy - dostarczyć osobie, której dane dotyczą co najmniej następujące informacje, dane, z wyjątkiem przypadku, kiedy posiada już ona informacje dotyczące:

- (a) tożsamości kontrolera 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 gromadzone, w celu zagwarantowania rzetelnego przetwarzania danych w związku z osobą, 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.

CZEŚĆ V

PRAWO UZYSKANIA PRZEZ OSOBĘ, KTÓREJ DANE DOTYCZĄ DOSTĘPU DO DANYCH

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 go dane są przetwarzane oraz co najmniej informacji o celach przetwarzania danych, kategoriach danych oraz odbiorcach lub kategoriach odbiorców, którym dane te są ujawniane,
 - wyrażonej w zrozumiałej formie informacji o danych przechodzących przetwarzanie oraz posiadanych informacji o ich źródłach,
 - wiadomości na temat zasad automatycznego przetwarzania dotyczących go danych przynajmniej w przypadku zautomatyzowanego procesu decyzyjnego, o którym mowa w art. 15 ust. 1;
- (b) odpowiednio do przypadku, poprawa, 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 ewentualnej poprawie, usunięciu lub zablokowaniu danych zgodnie z lit. (b), o ile nie okaże się to niemożliwe lub nie będzie wymagało niewspółmiernie dużego wysiłku.

CZEŚĆ VI

ZWOLNIENIA I OGRANICZENIA

Artykuł 13

Zwolnienia i ograniczenia

1. Państwo członkowskie może przyjąć środki ustawodawcze w celu ograniczenia zakresu praw i obowiązków, przewidzianego 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 przypadkowo z wykonywaniem władzy publicznej w przypadkach wymienionych w lit. (c), (d) i (e);

(g)ochrony osoby, której dane dotyczą 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 uzasadnionych przyczyn wynikających z jego konkretnej sytuacji sprzeciwu co do przetwarzania dotyczących go danych, chyba że ustawodawstwo krajowe przewiduje inaczej. W przypadku uzasadnionego sprzeciwu przetwarzanie danych przez administratora danych nie może już obejmować tych danych;
- (b) sprzeciwu, na wniosek i bez opłaty, wobec przetwarzania dotyczących go danych osobowych, dla potrzeb bezpośredniego marketingu, lub prawa uzyskania informacji przed ujawnieniem danych osobowych po raz pierwszy osobom trzecim lub wykorzystaniem w ich imieniu dla potrzeb bezpośredniego marketingu, jak również wyraźnego powoływania się na prawo sprzeciwu, bez opłat, wobec ujawniania lub wykorzystywaniu 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 osiągnięte 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 podmiot umowy, zostanie przyjęty, lub że istnieją odpowiednie sposoby zabezpieczenia jego 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.

CZEŚĆ VIII

POUFNOŚĆ I BEZPIECZEŃSTWO PRZETWARZANIA DANYCH

Artykuł 16

Poufność przetwarzania danych

Żadna osoba podlegająca władzy administratora danych lub przetwarzającego, włączając samego przetwarzającego, który ma dostęp do danych osobowych nie może przetwarzać ich bez polecenia 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, przyjęte zostaną takie uregulowania, które zapewnią poziom bezpieczeństwa odpowiedni do zagrożeń wynikających w 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 zapewnił stosowanie 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 zachowania dowodów, 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.

CZEŚĆ 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 powiązanim ze sobą celów.

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).
6. Państwa członkowskie mogą postanowić, że niektóre lub wszystkie nie zautomatyzowane operacje przetwarzania danych osobowych będą zgłaszane lub ustalać 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 kategorii osoby, której dane dotyczą oraz danych lub kategorii danych, które się do niego 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 uregulowań 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 dane te są badane przed ich rozpoczęciem.
2. Kontrole wstępne będą przeprowadzane przez organ nadzorczy po przyjęciu przez od administratora danych lub urzędnika odpowiedzialnego za ochronę danych powiadomienia, 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

Publikowanie operacji przetwarzania danych

1. Państwa członkowskie podejmą odpowiednie środki, aby zapewnić publikację operacji przetwarzania danych.
2. Państwa członkowskie zapewnią, że organ nadzorczy będzie prowadzić rejestr operacji przetwarzania danych zgłoszony zgodnie z art.18.

Rejestr będzie zawierać co najmniej informacje, o których mowa w art. 19 ust. 1 lit. a) -e).

Rejestr może być sprawdzany przez dowolną osobę.

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 mającego służyć za źródło informacji dla ogółu społeczeństwa, otwarte dla obywateli i każdej osoby posiadającej uzasadniony interes w uzyskaniu informacji;

ROZDZIAŁ III

ŚRODKI PRAWNE, ODPOWIEDZIALOŚĆ I SANKCJE

Artykuł 22

Środki prawne

Niezależnie od wszystkich odwoławczych środków administracyjnych, które przed wkroczeniem na drogę prawną mogą być wprowadzone przez organ nadzorczy, o którym mowa w art. 28, państwa członkowskie zapewnią prawo każdej osoby do korzystania ze środków prawnych w związku z naruszeniem praw zagwarantowanych mu przez prawo krajowe dotyczące przetwarzania danych.

Artykuł 23

Odpowiedzialność

1. Państwa członkowskie zapewnią, że każda osoba, 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. Prawidłowość 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, przepisy prawa, 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 Odstępstwa

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, udostępniony do konsultacji obywateli i każdej osoby 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 zaleci odpowiednie zabezpieczenia odnośnie ochrony prywatności oraz podstawowych praw i wolności osoby oraz odnośnie stosowania odpowiednich praw; zabezpieczenia takie mogą w szczególności wynikać z odpowiednich klauzul umownych.

3. Państwo członkowskie będzie informować Wspólnotę 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

KODEKSY POSTĘPOWANIA

Artykuł 27

1. Państwa członkowskie i Komisja będą zachęcać do opracowywania kodeksów 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 umożliwią stowarzyszeniom zawodowym i innym instytucjom reprezentującym inne kategorie administratorów danych, które opracowały projekty krajowych kodeksów postępowania lub które zamierzają dokonać zmiany lub uzupełnienia istniejących krajowych kodeksów postępowania, przedstawienie ich do zaopiniowania organowi władz państwowych.

Państwa członkowskie spowodują 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 kodeksów Wspólnoty, jak również zmiany i uzupełnienia istniejących kodeksów Wspólnoty mogą być przedstawione zespołowi roboczemu, o którym mowa w art. 29. Zespół roboczy ustali m.in., czy przedstawione mu projekty zgodne są z przepisami krajowymi przyjętymi na podstawie niniejszej dyrektywy. Komisja może zapewnić odpowiednie rozpowszechnienie kodeksów zatwierdzonych przez zespół roboczy.

ROZDZIAŁ VI

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

Artykuł 28 Organ nadzorczy

1. Każde państwo członkowskie powoła jeden lub kilka urzędów publicznych, które będą odpowiedzialne za kontrolę stosowania na jego terytorium postanowień przyjętych przez państwa członkowskie na podstawie niniejszej dyrektywy.

Organ ten będzie postępować w sposób całkowicie niezależny wykonując powierzone mu 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 szczególnie wyposażony w:

- uprawnienia dochodzeniowe, jak np. prawo dostępu do danych stanowiących przedmiot operacji przetwarzania danych oraz prawo gromadzenia wszelkich informacji potrzebnych do wykonywania jego funkcji nadzorczych,
- skuteczne uprawnienia interwencyjne, jak np. prawo do wyrażania opinii przed przystąpieniem do operacji przetwarzania danych zgodnie z art. 20, oraz zapewnienia odpowiedniej publikacji swoich 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;
- prawo angażowania się w postępowanie sądowe w przypadku naruszenia krajowych przepisów przyjętych na podstawie niniejszej dyrektywy lub zwrócenie 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 dowolną 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 kompetentny, niezależnie od krajowych przepisów dotyczących danego przypadku przetwarzania danych, do pełnienia na terytorium państwa członkowskiego władzy nadanej mu zgodnie z ust. 3. Każdy organ może być proszony 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 przedstawiciele organu lub organów nadzorczych, powołanych przez każde państwo członkowskie oraz przedstawiciela organu lub organów ustanowionych dla instytucji i organów Wspólnoty, oraz z przedstawiciela Wspólnoty.

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. Zespół 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 uregulowań mających na celu zabezpieczenie praw i swobód osób fizycznych w zakresie przetwarzania danych osobowych oraz innych proponowanych przez Wspólnotę środków dotyczących praw i wolności;
- (d) wydawać opinie na temat kodeksów postępowania opracowywanych na szczeblu Wspólnoty.

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

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 oraz w krajach trzecich, które będzie przekazywać Komisji, Parlamentowi Europejskiemu i Radzie. Raport będzie udostępniony opinii publicznej.

ROZDZIAŁ VII

ŚRODKI 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 wazone w sposób określony w tym artykule. Przewodniczący nie bierze udziału w głosowaniu.

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

- Komisja odroczy wprowadzenie środków postanowionych na okres trzech miesięcy od daty przekazania,
- 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 uchwalenia.

Wspomniane środki powinny zawierać odniesienie lub odniesienie to powinno towarzyszyć ich urzędowej publikacji. Metody dokonywania takiego odniesienia określone są przez 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 prześlą 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.

Europejskiego

W imieniu Parlamentu

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 27 czerwca 2001 r.

1.	Deklaracja dotycząca dostosowawczego charakteru projektu ustawy wraz z uzasadnieniem jego dostosowawczego charakteru
2.	Projekt ustawy wraz z uzasadnieniem
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 26 czerwca 2001 r.
5.	Tłumaczenia zweryfikowane następujących aktów prawa Unii Europejskiej, w wersji papierowej i elektronicznej: Dyrektywa Parlamentu Europejskiego i Rady 95/46/WE z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych
6.	Uzasadnienie trybu pilnego