

DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY

z dnia 24 października 1995

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

95/46/WE

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ:

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

uwzględniając projekt Komisji¹,

uwzględniając opinię Komitetu Ekonomiczno - Społecznego²,

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

a także mając na uwadze , że

- (1) cele Wspólnoty, określone w Traktacie, wraz ze zmianami wprowadzonymi Traktatem o Unii Europejskiej, obejmują tworzenie coraz ściślejszej wspólnoty narodów Europy, kształtowanie bliższych stosunków między państwami należącymi do Wspólnoty, zapewnienie postępu ekonomiczno-społecznego poprzez wspólne działania na rzecz likwidacji barier dzielących Europę, pobudzanie ciągłej poprawy warunków życia jej narodów, ochronę i umacnianie pokoju i wolności oraz rozwój demokracji w oparciu o fundamentalne prawa uznane w konstytucjach i ustawodawstwach państw członkowskich oraz w Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności;
- (2) systemy przetwarzania danych są tworzone po to, aby służyły człowiekowi; zważywszy, że muszą one, niezależnie od obywatelstwa czy miejsca stałego zamieszkania osób fizycznych, respektować ich podstawowe prawa i wolności, szczególnie prawo do prywatności, oraz przyczyniać się do postępu ekonomiczno-społecznego, rozwoju handlu oraz dobrobytu jednostek;
- (3) utworzenie i funkcjonowanie rynku wewnętrznego, na którym zgodnie z art. 7a Traktatu, zapewniony jest swobodny przepływ towarów, osób, usług i kapitału wymaga nie tylko

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

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

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

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

- (4) coraz częściej we Wspólnocie korzysta się z przetwarzania danych osobowych w różnych sferach życia gospodarczego i społecznego, a postęp technologii w dziedzinie przetwarzania informacji sprawia, że przetwarzanie i wymiana danych stają się coraz łatwiejsze;
- (5) integracja ekonomiczno-społeczna będąca wynikiem utworzenia i funkcjonowania rynku wewnętrznego w rozumieniu art. 7a Traktatu będzie prowadzić do znacznego zwiększenia przepływu danych osobowych przez granicę między wszystkimi podmiotami zaangażowanymi prywatnie lub publicznie w działalność ekonomiczną i społeczną w państwach członkowskich; wzrośnie wymiana danych osobowych między przedsiębiorstwami działającymi w różnych państwach członkowskich; władze państwowe poszczególnych państw członkowskich podejmują się na mocy prawa Wspólnoty do współpracy i wymiany danych osobowych w celu uzyskania zdolności wykonywania swoich obowiązków oraz realizacji zadań w imieniu władz innego państwa członkowskiego w kontekście obszaru bez granic wewnętrznych, ustanowionego przez rynek wewnętrzny;
- (6) ponadto, zwiększenie współpracy naukowo-technicznej oraz proces skoordynowanego wprowadzania nowych sieci telekomunikacyjnych we Wspólnocie narzuca konieczność i ułatwia przepływ danych osobowych przez granicę;
- (7) różnica w stopniu ochrony praw i swobód jednostek, szczególnie prawa do prywatności, w odniesieniu do przetwarzania danych osobowych, zapewnionego w poszczególnych państwach członkowskich może uniemożliwiać przesyłanie tych danych z terytorium jednego państwa członkowskiego do drugiego państwa członkowskiego; różnica ta może zatem stanowić przeszkodę w realizacji szeregu przedsięwzięć ekonomicznych na szczeblu Wspólnoty, zakłócać konkurencję i utrudniać władzom wykonywanie ich obowiązków wynikających z przepisów prawa Wspólnoty; wspomniana różnica w stopniu ochrony jest wynikiem istnienia wielkiej różnorodności krajowych ustaw, przepisów i postanowień o charakterze administracyjnym;
- (8) w celu zniesienia przeszkód w przepływie danych osobowych, stopień ochrony praw i swobód jednostki w zakresie przetwarzania tych danych musi być równoważny we wszystkich państwach członkowskich; cel ten ma żywotne znaczenie dla rynku wewnętrznego, lecz nie może on być osiągnięty przez same państwa członkowskie, szczególnie mając na uwadze skalę rozbieżności, jakie obecnie występują między odpowiednim ustawodawstwem państw członkowskich oraz potrzebę dokonania koordynacji przepisów ustawodawczych państw członkowskich w celu zapewnienia jednolitej regulacji przepływu danych osobowych przez granicę, zgodnie z celem rynku wewnętrznego, o którym mowa w art. 7a Traktatu; konieczne są działania Wspólnoty na rzecz zbliżenia ustawodawstwa;
- (9) biorąc pod uwagę ochronę równorzędną wynikającą ze zbliżania ustawodawstwa krajowego, państwa członkowskie nie będą już mogły utrudniać między sobą swobodnego przepływu danych osobowych na podstawie ochrony praw i wolności jednostek, a zwłaszcza prawa do prywatności; państwa członkowskie będą miały pozostawiony margines swobody działania, z którego mogą również, w kontekście

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

- (10) celem krajowego ustawodawstwa dotyczącego przetwarzania danych osobowych jest ochrona podstawowych praw i wolności, szczególnie prawa do prywatności, które zostało uznane zarówno w art. 8 Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności oraz w ogólnych zasadach prawa Wspólnoty; z tego powodu zbliżanie ustawodawstw nie powinno wpłynąć na zmniejszenie ochrony, jaką gwarantują, lecz przeciwnie, musi dążyć do zapewnienia jak najwyższego stopnia ochrony we Wspólnocie;
- (11) zasady ochrony praw i swobód jednostek, szczególnie prawa do prywatności, które zawarte są w niniejszej dyrektywie, utrwalają i umacniają zasady wyrażone w Konwencji Rady Europy z dnia 28 stycznia 1981 w sprawie ochrony jednostek w zakresie automatycznego przetwarzania danych osobowych;
- (12) zasady ochrony muszą odnosić się do całokształtu przetwarzania danych osobowych przez każdą osobę, której działania podlegają przepisom prawa Wspólnoty; należy wyłączyć przetwarzanie danych dokonywane przez osobę fizyczną w ramach działań o charakterze wyłącznie osobistym lub domowym, jak np. korespondencja i przechowywanie spisów adresów;
- (13) działania, o których mowa w rozdziałach V i VI Traktatu o Unii Europejskiej odnoszących się do bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa w dziedzinie prawa karnego, bez wpływu na obowiązki nałożone na państwa członkowskie na mocy art. 56 ust. 2, art. 57 lub art. 100a Traktatu o utworzeniu Wspólnoty Europejskiej, nie wchodzi w zakres prawa wspólnotowego, przetwarzanie danych osobowych konieczne dla zapewnienia ochrony dobrego stanu gospodarczego państwa nie wchodzi w zakres niniejszej dyrektywy, o ile przetwarzanie danych dotyczy spraw bezpieczeństwa państwa;
- (14) jeżeli w ramach społeczeństwa informacyjnego ma znaczenie rozwój technik gromadzenia, przekazywania, kompilowania, rejestrowania, przechowywania i przesyłania danych dźwiękowych i obrazowych osób fizycznych, niniejsza dyrektywa powinna mieć zastosowanie do przetwarzania takich danych;
- (15) przetwarzanie tych danych jest objęte niniejszą dyrektywą tylko wówczas, gdy jest ono zautomatyzowane lub jeśli dane zawarte są lub przeznaczone do umieszczenia w zbiorze danych zorganizowanym według określonych kryteriów dotyczących osób fizycznych w celu zapewnienia łatwego dostępu do wspomnianych danych osobowych;
- (16) przetwarzanie danych dźwiękowych i obrazowych, np. w przypadku nadzoru kamer wideo, nie wchodzi w zakres niniejszej dyrektywy, jeśli dokonywane jest dla potrzeb bezpieczeństwa publicznego, obronności, bezpieczeństwa narodowego lub też w trakcie działań organów państwowych w dziedzinie prawa karnego lub innych działań nie wchodzących w zakres prawa Wspólnoty;

- (17) jeśli chodzi o przetwarzanie danych dźwiękowych i obrazowych dla potrzeb dziennikarstwa, lub dla potrzeb literackich lub artystycznych, zwłaszcza w dziedzinie techniki audiowizualnej, zasady dyrektywy mają zastosowanie ograniczone, zgodnie z postanowieniami określonymi w art. 9;
- (18) aby nie dopuścić do pozbawienia jednostek ochrony, do której mają prawo na mocy niniejszej dyrektywy, wszelkie przetwarzanie danych osobowych we Wspólnocie musi odbywać się zgodnie z przepisami prawa jednego z państw członkowskich, w związku z tym przetwarzanie danych, za które odpowiada administrator danych prowadzący działalność gospodarczą na terenie państwa członkowskiego, powinno być regulowane przez ustawodawstwo danego państwa;
- (19) prowadzenie działalności gospodarczej na terytorium państwa członkowskiego zakłada efektywne i rzeczywiste prowadzenie działań poprzez stabilne postanowienia; forma prawna prowadzonej działalności gospodarczej, niezależnie czy to oddział lub filia z osobowością prawną, nie jest w tym względzie czynnikiem decydującym; w przypadku ustanowienia jednego administratora danych na terytorium kilku państw członkowskich, szczególnie w postaci filii, w celu uniknięcia obejścia przepisów krajowych, musi on zapewnić, że każda z prowadzonej działalności gospodarczej będzie spełniać obowiązki wynikające z krajowego ustawodawstwa;
- (20) przetwarzanie danych przez osobę prowadzącą działalność w kraju trzecim nie powinno stać na przeszkodzie 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 precyzują w ogłaszanych ustawach lub przy wprowadzaniu w życie środków podjętych w niniejszej dyrektywie ogólne warunki, w których przetwarzanie danych jest zgodne z prawem; w szczególności art. 5 w połączeniu z art. 7 i 8, umożliwia państwom członkowskim, niezależnie od zasad ogólnych, zapewnienie specyficznych warunków przetwarzania danych dla konkretnych branż oraz dla różnych kategorii danych objętych art. 8;
- (23) państwa członkowskie są upoważnione do zapewnienia ochrony osób fizycznych zarówno poprzez ogólne ustawodawstwo o ochronie jednostek w odniesieniu do przetwarzania danych osobowych oraz poprzez ustawodawstwo branżowe, jak np. odnoszące się do urzędów statystycznych;
- (24) niniejsza dyrektywa nie dotyczy ustawodawstwa dotyczącego ochrony osób prawnych w odniesieniu do przetwarzania ich danych;
- (25) zasady ochrony powinny znajdować odzwierciedlenie, z jednej strony w obowiązkach nałożonych na osoby, władze publiczne, przedsiębiorstwa, agencje i inne organy odpowiedzialne za przetwarzanie danych, zwłaszcza w zakresie jakości danych, bezpieczeństwa technicznego, zawiadamiania organu nadzoru oraz okoliczności,

w których może odbywać się przetwarzanie danych, jak również, z drugiej strony, w prawie osób, których dane są przedmiotem przetwarzania, do uzyskania informacji, że takie przetwarzanie danych ma miejsce, do konsultowania danych, żądania poprawek lub nawet sprzeciwu wobec przetwarzania danych w niektórych przypadkach;

- (26) zasady ochrony danych muszą odnosić się do wszelkich informacji dotyczących zidentyfikowanych lub możliwych do zidentyfikowania osób; w celu ustalenia, czy daną osobę można zidentyfikować, należy wziąć pod uwagę wszystkie sposoby, jakimi może posłużyć się administrator danych lub inna osoba w celu zidentyfikowania owej osoby; zasady ochrony danych nie dotyczą danych, którym nadano anonimowy charakter w taki sposób, że osoba, której dane dotyczą, nie będzie mogła być zidentyfikowana; zasady postępowania w rozumieniu art. 27 mogą być przydatnym instrumentem w udzielaniu wskazówek co do sposobów nadawania danym charakteru anonimowego oraz zachowania w formie, w której identyfikacja osoby, której dane dotyczą;
- (27) ochrona jednostek musi odnosić się zarówno do automatycznego przetwarzania danych, jak i ręcznego przetwarzania; zważywszy, że zakres tej ochrony nie powinien w efekcie być zależny od zastosowanych technik, ponieważ w przeciwnym razie wystąpiłoby poważne ryzyko obchodzenia zasad; niemniej w przypadku ręcznego przetwarzania danych, niniejsza dyrektywa obejmuje jedynie zbiory danych, nie zaś niezorganizowane zbiory; w szczególności zawartość zbiorów musi być zorganizowana według określonych kryteriów dotyczących osób fizycznych, zapewniających łatwy dostęp do danych; zgodnie z definicją zawartą w art. 2 lit. c, poszczególne państwa członkowskie mogą określić różne kryteria określania części składowych zorganizowanego zestawu danych oraz różne kryteria dostępu do takiego zestawu; zbiory lub zestawy zbiorów oraz ich strony tytułowe, które nie są zorganizowane według określonych kryteriów nie powinny w żadnych okolicznościach wchodzić w zakres niniejszej dyrektywy;
- (28) przetwarzanie danych osobowych musi być zgodne z prawem i rzetelne wobec zainteresowanych osób; w szczególności dane muszą być adekwatne, właściwe i nie wykroczać poza cele, dla których są przetwarzane; cele takie muszą być jednoznaczne i uzasadnione oraz określone w czasie gromadzenia danych; cele dalszego przetwarzania danych po ich zgromadzeniu nie mogą być niezgodne z pierwotnie określonymi celami;
- (29) dalsze przetwarzanie danych osobowych dla celów historycznych, statystycznych i naukowych nie jest na ogół uważane za niezgodne z celami, dla których dane były pierwotnie gromadzone, pod warunkiem zapewnienia przez państwo członkowskie odpowiednich zabezpieczeń; zabezpieczenia te muszą w szczególności wykluczać wykorzystywanie danych na rzecz działań lub decyzji dotyczących konkretnej osoby;
- (30) zgodność z prawem procesu przetwarzania danych osobowych wymaga ponadto, aby dokonywane było ono za zgodą osoby, której dane dotyczą lub było konieczne dla zawarcia lub realizacji umowy wiążącej w sprawie osoby, której dane dotyczą, bądź miało charakter wymogu prawnego, lub też służyło realizacji zadania wykonywanego w interesie publicznym lub wykonywaniu władzy publicznej, bądź też w uzasadnionym interesie osoby fizycznej lub prawnej, pod warunkiem, że interesy lub prawa i wolności osoby, której dane dotyczą nie mają charakteru nadrzędnego; w celu utrzymania równowagi między wspomnianymi interesami a gwarantowaniem skutecznej konkurencji, państwa członkowskie mogą określić okoliczności, w których dane osobowe mogą być wykorzystane lub ujawnione osobie trzeciej w związku ze zgodną z prawem, zwykłą aktywnością gospodarczą przedsiębiorstw i innych ciał; państwa członkowskie

mogą podobnie określić warunki, na których dane osobowe mogą być ujawniane osobom trzecim dla celów marketingu o charakterze komercyjnym, lub realizowanego przez organizację charytatywną, lub też przez inne stowarzyszenie lub fundację, np. o charakterze politycznym, z zastrzeżeniem postanowień dopuszczających prawo sprzeciwu przysługujące osobie, której te dane dotyczą wobec przetwarzania tych danych - bezpłatnie i bez konieczności podania uzasadnienia;

- (31) przetwarzanie danych osobowych musi być również uznawane za zgodne z prawem, kiedy dokonywane jest w celu zapewnienia ochrony interesu, który jest niezbędny dla życia osoby, której dane dotyczą;
- (32) ustawodawstwo krajowe powinno ustalić, czy administrator danych wykonujący zadanie realizowane w interesie publicznym powinien być organem administracji publicznej czy inną osobą fizyczną lub prawną podlegającą prawu publicznemu lub prawu prywatnemu, jak np. stowarzyszenie zawodowe.
- (33) dane mogące ze względu na ich charakter powodować naruszenie podstawowych swobód lub prywatności nie powinny być przetwarzane, o ile osoba, której dotyczą nie udzieli wyraźnej zgody; należy jednak przewidzieć odstępstwa od tego zakazu dla szczególnych potrzeb, zwłaszcza w przypadkach, gdy przetwarzanie danych odbywa się w określonych celach zdrowotnych przez osoby podlegające prawnemu obowiązkowi zachowania tajemnicy zawodowej, lub też w trakcie legalnych działań niektórych stowarzyszeń lub fundacji, których celem jest umożliwienie realizacji podstawowych swobód;
- (34) państwa członkowskie muszą być również uprawnione, w sytuacjach, kiedy jest to uzasadnione przez ważny interes publiczny do uchylania zakazu przetwarzania wrażliwych kategorii danych w takich dziedzinach, jak zdrowie publiczne i ochrona socjalna - szczególnie w celu zapewnienia odpowiedniej jakości i zasadności ekonomicznej procedur stosowanych do rozstrzygania roszczeń w sprawie świadczeń i usług w ramach systemu ubezpieczeń społecznych - badania naukowe i statystyka rządowa; obowiązkiem ich jest jednak stworzenie konkretnych i odpowiednich zabezpieczeń dla ochrony podstawowych praw i prywatności osób;
- (35) ponadto, przetwarzanie danych osobowych przez władze publiczne dla osiągnięcia określonych w prawie konstytucyjnym lub międzynarodowym prawie publicznym celów oficjalnie uznanych związków religijnych jest dokonywane z ważnych względów wynikających z interesu publicznego;
- (36) jeżeli w trakcie czynności wyborczych funkcjonowanie systemu demokratycznego w niektórych państwach członkowskich wymaga gromadzenia przez partie polityczne danych na temat opinii politycznych obywateli, przetwarzanie tych danych może być dozwolone ze względu na ważny interes publiczny, pod warunkiem stworzenia odpowiednich zabezpieczeń'
- (37) przetwarzanie danych osobowych dla potrzeb dziennikarstwa lub wypowiedzi literackiej lub artystycznej, zwłaszcza w dziedzinie techniki audiowizualnej, powinno kwalifikować się do zwolnienia z wymagań niektórych postanowień niniejszej dyrektywy, o ile je to konieczne, aby pogodzić podstawowe prawa osób fizycznych z wolnością informacji, a zwłaszcza prawem do uzyskiwania i udzielania informacji, co gwarantuje w szczególności art. 10 Europejskiej Konwencji o Ochronie Praw Człowieka

i Podstawowych Wolności; państwa członkowskie powinny w związku z tym ustalić zwolnienia i odstępstwa konieczne dla zapewnienia równowagi pomiędzy podstawowymi prawami odnoszącymi się do ogólnych środków w sprawie legalności przetwarzania danych, środków w sprawie przesyłania danych do krajów trzecich i kompetencjami organów nadzoru; nie powinno to jednak powodować wprowadzenia przez państwa członkowskie uregulowań stanowiących odstępstwo od obowiązku zapewnienia bezpieczeństwa przetwarzania danych; przynajmniej organ nadzoru odpowiedzialny za tę dziedzinę powinien być również wyposażony w niektóre uprawnienia *ex post*, np. publikowania regularnych sprawozdań lub kierowania spraw do władz sądowniczych;

- (38) jeżeli przetwarzanie danych ma być rzetelne, osoba, której dane dotyczą musi mieć możliwość dotarcia do informacji o wystąpieniu czynności przetwarzania danych oraz, jeżeli dane są uzyskiwane od niego, musi otrzymać dokładne i pełne informacje, uwzględniające okoliczności pozyskiwania danych;
- (39) niektóre czynności w zakresie przetwarzania danych obejmują dane, których administrator danych nie uzyskał bezpośrednio od osoby, które te dane dotyczą; ponadto, dane mogą być legalnie ujawnione osobie trzeciej, nawet jeżeli ich ujawnienie nie było przewidywane w czasie, kiedy uzyskiwano dane od osoby, której dotyczą; we wszystkich tych przypadkach osoba, której dane dotyczą powinna być informowana przy rejestracji danych lub też najpóźniej kiedy dane są po raz pierwszy ujawnione osobie trzeciej;
- (40) nie jest jednak konieczne nakładanie takiego obowiązku, kiedy osoba, której dane dotyczą posiada już tę informację; ponadto obowiązek taki nie występuje wówczas, gdy rejestracja lub ujawnianie danych jest wyraźnie przewidziane przez prawo lub jeżeli dostarczanie informacji osobie, której dane dotyczą okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku, co może mieć miejsce w przypadku przetwarzania danych dla celów historycznych, statystycznych lub naukowych; pod tym względem można brać pod uwagę liczbę osób, których dane dotyczą, wiek danych oraz przyjęte środki wyrównawcze;
- (41) każda osoba musi mieć możliwość skorzystania z prawa dostępu do dotyczących jej danych, które poddane są przetwarzaniu, w celu zweryfikowania zwłaszcza prawidłowości danych oraz legalności ich przetwarzania; z tych samych powodów każda osoba, której dane dotyczą musi również mieć prawo zapoznania się z zasadami automatycznego przetwarzania danych, które ją dotyczą, przynajmniej w przypadku zautomatyzowanego procesu decyzyjnego, o którym mowa w art. 15 ust. 1; prawo to nie powinno w niekorzystny sposób wpływać na stan tajemnicy handlowej lub własności intelektualnej, w szczególności na prawo autorskie chroniące oprogramowanie; względy te nie powinny jednak powodować odmowy udzielenia osobie, której dane dotyczą wszystkich informacji;
- (42) państwa członkowskie mogą, w interesie osoby, której dane dotyczą lub w celu zapewnienia ochrony praw i swobód innych osób, ograniczać prawo dostępu do danych i informacji; mogą one np. postanowić, że dostęp do danych medycznych może uzyskać tylko personel medyczny;
- (43) ograniczenia prawa dostępu i informacji oraz niektórych obowiązków kontrolera mogą w podobny sposób być wprowadzane przez państwa członkowskie, o ile jest to konieczne dla zapewnienia np. ochrony bezpieczeństwa narodowego, obronności, bezpieczeństwa publicznego lub ważnych ekonomicznych lub finansowych interesów państwa

członkowskiego lub Unii, jak również dochodzenia i ścigania naruszeń prawa karnego oraz naruszeń zasad etyki w zawodach podlegających określonym regulacjom; lista wyłączeń i ograniczeń powinna obejmować zadania w zakresie nadzoru, kontroli i regulacji koniecznych w trzech ostatnich dziedzinach, dotyczących bezpieczeństwa publicznego, interesów ekonomicznych lub finansowych oraz walki z przestępczością; sporządzenie listy zadań we wspomnianych trzech dziedzinach nie wpływa na zasadność wprowadzenia wyłączeń i ograniczeń ze względu na bezpieczeństwo lub obronność państwa;

- (44) państwa członkowskie mogą również, na mocy postanowień prawa Wspólnoty, uchylić się od postanowień niniejszej dyrektywy odnośnie prawa dostępu, obowiązku informowania obywateli oraz jakości danych w celu zapewnienia realizacji niektórych celów, o których mowa powyżej;
- (45) w przypadkach, gdy dane mogą być legalnie przetwarzane ze względu na interes publiczny, wykonywania władzy publicznej lub uzasadnione interesy osoby fizycznej lub prawnej, osoba, której dane te dotyczą powinna jednak mieć prawo, ze względu na uzasadnione i 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 niedopuszczenia do niedozwolonego przetwarzania danych; na państwie członkowskim spoczywa obowiązek zapewnienia stosowania tych rozwiązań przez administratora danych; uregulowania te muszą zapewnić odpowiedni stopień bezpieczeństwa, uwzględniając stan wiedzy w tej dziedzinie oraz koszty ich realizacji w odniesieniu do ryzyka wynikającego z przetwarzania danych oraz charakteru danych podlegających ochronie;
- (47) w przypadku przekazywania komunikatu zawierającego dane osobowe przy pomocy urządzeń telekomunikacyjnych lub poczty elektronicznej, których wyłącznym przeznaczeniem jest przekazywanie takich komunikatów, za administratora danych osobowych zawartych w takim komunikacie uważać się będzie osobę, od której komunikat wychodzi, nie zaś osobę wykonującą usługę w zakresie transmisji danych; podmioty wykonujące takie usługi są z reguły uważane za administratorów danych odniesieniu do przetwarzania dodatkowych danych osobowych potrzebnych do wykonywania usług;
- (48) procedury dotyczące zawiadamiania organu nadzoru są skonstruowane w taki sposób, aby zapewnić ujawnienie celów i głównych cech operacji przetwarzania danych dla ustalenia, czy operacja taka jest 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 zapewniając, że jest to zgodne ze środkami podejmowanymi przez państwa członkowskie określającymi ich granice; zwolnienia lub uproszczenia mogą być równocześnie

przewidziane przez państwa członkowskie, jeżeli osoba wskazana przez administratora danych zapewni, że jest mało prawdopodobne, aby przetwarzanie mogło niekorzystnie wpłynąć na prawa i wolności osoby, której dane dotyczą; urzędnik odpowiedzialny za ochronę danych będący lub nie będący pracownikiem administratora danych, musi mieć możliwość wykonywania swoich funkcji w sposób całkowicie niezależny;

- (50) wspomniane zwolnienie lub uproszczenie procedury mogłoby być stosowane w przypadku operacji przetwarzania danych, których wyłącznym celem jest prowadzenie rejestru mającego służyć, zgodnie z prawem krajowym, za źródło informacji dla ogółu społeczeństwa, otwarte do publicznego wglądu i każdej osoby posiadającej uzasadniony interes w uzyskaniu informacji;
- (51) jednak uproszczenie procedury lub zwolnienie z obowiązku zawiadamiania nie będzie zwalniać administratora danych z innych obowiązków wynikających z niniejszej dyrektywy;
- (52) w tym kontekście kontrola ex-post przeprowadzana przez właściwe władze musi z reguły być uznawana za wystarczające rozwiązanie;
- (53) jednak niektóre operacje przetwarzania danych mogą stwarzać określone zagrożenia dla praw i wolności osób, których dane dotyczą ze względu na ich charakter, ich zakres lub przeznaczenie, jak np. pozbawienie jednostki przysługującego jej prawa, korzyści lub kontraktu, lub ze względu na szczególne zastosowanie nowych technologii; do państw członkowskich należy, jeżeli tego sobie życzą, wskazanie na takie zagrożenia w ich ustawodawstwie;
- (54) w stosunku do wszystkich operacji przetwarzania danych podejmowanych w społeczeństwie, liczba tych, które niosą ze sobą określone zagrożenia jest bardzo ograniczona; państwa członkowskie muszą zapewnić kontrolę przetwarzania danych przez organ nadzorczy lub urzędnika odpowiedzialnego za ochronę danych, współpracującego z tym organem przed ich przetworzeniem; po takiej wstępnej kontroli, organ nadzorczy może, zgodnie z prawem krajowym, wydać opinię lub zezwolenie na przetwarzanie danych; kontrola taka może również następować w trakcie opracowywania ustawodawczego środka parlamentu krajowego lub środka opartego na takim środku ustawodawstwa, które określa charakter przetwarzania danych oraz stwarza odpowiednie zabezpieczenia;
- (55) na wypadek nieprzestrzegania przez administratora danych praw osób, których dane dotyczą, ustawodawstwo krajowe musi przewidywać odpowiednie środki prawne; szkody, jakie osoba może ponieść wskutek niezgodnego z prawem przetwarzania danych musi być wyrównana przez administratora danych, który może być zwolniony z odpowiedzialności w przypadku udowodnienia, że szkoda nie powstała z jego winy, szczególnie wówczas, gdy stwierdzi wystąpienie winy po stronie osoby, której dane dotyczą lub w przypadku siły wyższej; należy nakładać sankcje na każdą osobę, podlegającą prawu prywatnemu lub publicznemu, która nie spełni wymagań wynikających z przyjętych krajowych środków wprowadzonych na podstawie niniejszej dyrektywy;
- (56) przepływ danych osobowych przez granicę jest koniecznym warunkiem rozwoju handlu międzynarodowego; ochrona osób jaką niniejsza dyrektywa gwarantuje we Wspólnocie nie stanowi przeszkody dla przekazywania danych osobowych do krajów trzecich, które

zapewniają odpowiedni stopień ochrony; prawidłowość stopnia ochrony danych zapewnianej przez kraj trzeci należy oceniać w świetle wszystkich okoliczności dotyczących operacji przekazywania danych lub zestawu takich operacji;

- (57) z drugiej strony należy zakazać przekazywania danych osobowych do kraju trzeciego, który nie zapewnia odpowiedniego stopnia ochrony;
- (58) należy przewidzieć zwolnienia z tego zakazu w określonych okolicznościach, jeżeli osoba, której dane dotyczą wyrazi na to zgodę, jeżeli przekazanie danych jest konieczne w związku z umową lub roszczeniem prawnym, jeżeli wymagać tego będzie ochrona ważnego interesu publicznego, jak np. przesyłanie danych za granicę przez władze podatkowe i celne lub przez służby odpowiedzialne za sprawy ubezpieczeń społecznych, lub w przypadku przekazania danych z rejestru utworzonego na mocy prawa i przeznaczonego do wglądu dla ogółu społeczeństwa lub osób posiadających uzasadniony interes w uzyskaniu informacji; w tym przypadku przekazanie danych nie powinno obejmować ich całości lub całych kategorii danych oraz, jeżeli rejestr jest przeznaczony do wglądu dla osób posiadających uzasadniony interes w uzyskaniu informacji, przekazanie danych powinno nastąpić jedynie na wniosek tych osób, lub wówczas, gdy osoby te mają być odbiorcami danych;
- (59) podejmowane mogą być konkretne działania w celu zrekompensowania braku ochrony w kraju trzecim, jeżeli administrator danych oferuje odpowiednie zabezpieczenia; ponadto, należy przewidzieć procedury negocjacji między Wspólnotą a krajami trzecimi;
- (60) w każdym przypadku przekazywanie danych do krajów trzecich może następować jedynie w pełnej zgodności z postanowieniami przyjętymi przez państwa członkowskie na podstawie niniejszej dyrektywy, a w szczególności art. 8.
- (61) państwa członkowskie i Komisja muszą - w zakresie swoich kompetencji - zachęcać stowarzyszenia zawodowe oraz inne reprezentatywne organizacje do opracowania reguł postępowania w celu ułatwienia stosowania niniejszej dyrektywy, biorąc pod uwagę specyficzne cechy procesu przetwarzania danych w niektórych branżach, z poszanowaniem dla krajowych przepisów przyjętych w celu jej realizacji;
- (62) utworzenie w państwach członkowskich organów nadzorczych, wykonujących swoje funkcje w sposób całkowicie niezależny jest zasadniczym elementem ochrony jednostek w zakresie przetwarzania danych osobowych;
- (63) organy te muszą dysponować określonymi środkami do realizacji swoich obowiązków, włączając uprawnienia do przeprowadzania dochodzenia i interwencji, szczególnie w przypadkach skarg od obywateli, jak również uprawnienia do uczestniczenia w postępowaniu sądowym; organy te muszą przyczynić 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, przyczynić 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;
- (67) 20 grudnia 1994 zawarta została pomiędzy Parlamentem Europejskim, Radą i Komisją umowa w sprawie *modus vivendi* dotycząca sposobów wprowadzania w życie aktów przyjętych w trybie określonym w art. 189b Traktatu o WE;
- (68) zasady określone w niniejszej dyrektywie odnośnie ochrony praw i wolności osób fizycznych, szczególnie ich prawa do prywatności w odniesieniu do przetwarzania danych osobowych mogą być uzupełniane lub wyjaśniane, zwłaszcza w przypadku niektórych branż, w formie szczegółowych przepisów opartych na wspomnianych zasadach;
- (69) należy wyznaczyć państwom członkowskim okres nie dłuższy niż trzy lata od wejścia w życie krajowych uregulowań stanowiących transpozycję niniejszej dyrektywy, w którym będą one zobowiązane do progresywnego stosowania nowych przepisów krajowych w odniesieniu do wszystkich realizowanych już operacji przetwarzania danych; dla ułatwienia ich realizacji przy uzasadnionych ekonomicznie kosztach, wyznaczony zostanie państwom członkowskim kolejny okres 12 lat od daty uchwalenia niniejszej dyrektywy, w celu zapewnienia zgodności istniejących ręcznych zbiorów danych z niektórymi postanowieniami dyrektywy; jeżeli we wspomnianym przedłużonym okresie przejściowym dane zawarte w owych zbiorach będą przetwarzane ręcznie, konieczne będzie doprowadzenie do zgodności tych zbiorów ze wspomnianymi postanowieniami w czasie przetwarzania danych;
- (70) nie jest konieczne aby osoba, której dane dotyczą udzieliła ponownej zgody, aby umożliwić administratorowi danych dalsze przetwarzanie, po wejściu w życie krajowych przepisów przyjętych na podstawie niniejszej dyrektywy, wszelkich wrażliwych danych koniecznych do realizacji umowy zawartej na warunkach dobrowolnej i świadomej zgody stron przed wejściem w życie wspomnianych przepisów;
- (71) niniejsza dyrektywa nie stanowi przeszkody dla wprowadzania przez państwo członkowskie regulującej działalności marketingowej, skierowanej na konsumentów 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:

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.

ROZDZIAŁ I

POSTANOWIENIA OGÓLNE

Artykuł 1

Cel dyrektywy

1. Zgodnie z postanowieniami niniejszej dyrektywy, państwa członkowskie zobowiązują się chronić podstawowe prawa i wolności osób fizycznych, a w szczególności ich prawo do prywatności w odniesieniu do przetwarzania danych osobowych.
2. Państwa członkowskie nie będą ograniczać ani zakazywać swobodnego przepływu danych osobowych pomiędzy państwami członkowskimi ze względów związanych z ochroną przewidzianą w ust. 1.

Artykuł 2

Definicje

Dla potrzeb niniejszej dyrektywy :

- (a) „dane osobowe” oznaczają wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej („osoby, której dane dotyczą”); osoba możliwa do zidentyfikowania, to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, szczególnie przez powołanie się na numer identyfikacyjny lub jeden bądź kilka specyficznych czynników określających jej fizyczną, fizjologiczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość;
- (b) „przetwarzanie danych osobowych” („przetwarzanie”) oznacza każdą operację lub zestaw operacji dokonywanych na danych przy pomocy środków zautomatyzowanych lub innych, jak np. gromadzenie, rejestracja, porządkowanie, przechowywanie, adaptacja lub modyfikacja, odzyskiwanie, konsultowanie, wykorzystywanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, układanie lub kompilowanie, zestawianie, usuwanie lub niszczenie danych;
- (c) „zbiór danych osobowych” („zbiór danych”) oznacza każdy uporządkowany zestaw danych osobowych, dostępnych według określonych kryteriów, scentralizowanych, zdecentralizowanych lub rozproszonych funkcjonalnie lub geograficznie;
- (d) „administrator danych” oznacza osobę fizyczną lub prawną, urząd publiczny, agendę lub inny organ, który samodzielnie lub wspólnie z innymi podmiotami określa cele i sposoby przetwarzania danych; jeżeli cele i sposoby przetwarzania danych są określone w ustawach i innych przepisach krajowych lub przepisach Wspólnoty, administrator danych może być powoływany lub kryteria jego powołania mogą być ustalane przez ustawodawstwo krajowe lub ustawodawstwo Wspólnoty;

- (e) „przetwarzający” oznacza osobę fizyczną lub prawną, urząd publiczny, agendę lub inny organ przetwarzający dane osobowe w imieniu administratora danych;
- (f) „osoba trzecia” oznacza osobę fizyczną lub prawną, urząd publiczny, agendę lub inny organ nie będący osobą, której dane dotyczą, ani administratorem danych, ani przetwarzającym lub jedną z osób, które pod bezpośrednim zwierzchnictwem administratora danych lub przetwarzającego upoważnione są do przetwarzania danych;
- (g) „odbiorca” oznacza osobę fizyczną lub prawną, urząd publiczny, agendę lub inny organ, któremu ujawniane są dane, będący lub nie będący osobą trzecią; jednakże władze, które mogą otrzymywać dane w ramach konkretnego dochodzenia nie są uważane za odbiorcę;
- (h) „zgoda osoby, której dane dotyczą” oznacza konkretne i świadome, dobrowolne wskazanie przez osobę, której dane dotyczą na to, że wyraża przyzwolenie na przetwarzanie jej danych osobowych.

Artykuł 3

Zakres działania

1. Niniejsza dyrektywa dotyczy przetwarzania danych osobowych w całości lub w części w sposób zautomatyzowany oraz innego przetwarzania danych osobowych, stanowiących część zbioru danych lub mających stanowić część zbioru danych.
2. Niniejsza dyrektywa nie dotyczy przetwarzania danych osobowych:
 - w ramach działalności wykraczającej poza zakres prawa Wspólnoty takiej, o której mowa w rozdziałach V i VI Traktatu o Unii Europejskiej, oraz w każdym przypadku - przetwarzania związanego z bezpieczeństwem publicznym, obronnością, bezpieczeństwem państwa (łącznie ze stanem gospodarki państwa, kiedy przetwarzanie danych dotyczy bezpieczeństwa państwa) oraz z działalnością państwa w dziedzinach prawa karnego,
 - przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze.

Artykuł 4

Stosowane prawo krajowe

1. Każde państwo członkowskie stosuje w odniesieniu do przetwarzania danych osobowych postanowienia prawa krajowego, jakie wprowadzi na podstawie niniejszej dyrektywy wówczas, gdy:
 - (a) przetwarzanie danych odbywa się w zakresie prowadzenia przez administratora danych działalności na terytorium państwa członkowskiego; jeżeli ten sam administrator danych prowadzi działalność na terytorium kilku państw członkowskich,

musi on podjąć niezbędne działania, aby zapewnić, że każda z tych agend wywiązuje się z obowiązków ustalonych przez stosowane prawo krajowe;

- (b) administrator danych nie prowadzi działalności na terytorium państwa członkowskiego, lecz w miejscu, gdzie jego prawo krajowe stosowane jest na mocy międzynarodowego prawa publicznego;
 - (c) administrator danych nie prowadzi działalności na terytorium Wspólnoty lecz, dla celów przetwarzania danych osobowych wykorzystuje środki, zarówno zautomatyzowane jak i inne, znajdujące się na terytorium wymienionego państwa członkowskiego, o ile środki te nie są wykorzystywane wyłącznie do celów tranzytu przez terytorium Wspólnoty.
2. W okolicznościach, o których mowa w ust. 1 lit. (c), administrator danych musi wyznaczyć swojego przedstawiciela na terytorium tego państwa członkowskiego, niezależnie od środków prawnych, jakie mogą być podjęte przeciwko samemu administratorowi danych.

ROZDZIAŁ II

OGÓLNE ZASADY LEGALNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

Artykuł 5

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

CZĘŚĆ 1

ZASADY DOTYCZĄCE JAKOŚCI DANYCH

Artykuł 6

1. Państwa członkowskie zapewnią, aby dane osobowe były:
- (a) przetwarzane rzetelnie i legalnie;
 - (b) gromadzone do określonych, wyraźnych i legalnych celów oraz nie będą poddawane dalszemu przetwarzaniu w sposób niezgodny z tym celem. Dalsze przetwarzanie danych w celach historycznych, statystycznych lub naukowych nie będzie uważane za niezgodne z przepisami pod warunkiem stworzenia przez państwa członkowskie odpowiednich zabezpieczeń;
 - (c) stosowne, istotne i nie wykraczające poza konieczne w stosunku do celów, dla których zostały zgromadzone i/lub dalej przetworzone;
 - (d) prawidłowe oraz, w razie konieczności, aktualizowane; należy podjąć wszelkie uzasadnione działania, aby zapewnić usunięcie lub poprawienie nieprawidłowych

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

- (e) przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą przez czas nie dłuższy niż jest to konieczne dla celów, dla których dane zostały zgromadzone lub dla których są dalej przetwarzane. Państwa członkowskie stworzą odpowiednie zabezpieczenia dla danych przechowywanych przez dłuższe okresy dla potrzeb historycznych, statystycznych i naukowych.
2. Na administratorze danych spoczywa obowiązek zapewnienia przestrzegania postanowień ust. 1.

CZĘŚĆ II

KRYTERIA LEGALNOŚCI PRZETWARZANIA DANYCH

Artykuł 7

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

- (a) osoba, której dane dotyczą jednoznacznie wyraziła na to zgodę; lub
- (b) przetwarzanie danych jest konieczne dla realizacji umowy, której stroną jest osoba, której dane dotyczą lub w celu podjęcia działań na życzenie osoby, której dane dotyczą przed zawarciem umowy; lub
- (c) przetwarzanie danych jest konieczne dla zgodności z zobowiązaniem prawnym, któremu administrator danych podlega; lub
- (d) przetwarzanie danych jest konieczne dla ochrony żywotnych interesów osoby, której dane dotyczą; lub
- (e) przetwarzanie danych jest konieczne dla realizacji zadania wykonywanego w interesie publicznym lub dla sprawowania władzy publicznej przekazanej administratorowi danych lub osobie trzeciej, przed którą ujawnia się dane; lub
- (f) przetwarzanie danych jest konieczne dla potrzeb wynikających z uzasadnionych interesów administratora danych lub osoby trzeciej, przed którą ujawnia się dane, z wyjątkiem sytuacji, kiedy interesy takie podporządkowane są interesom związanym z podstawowymi prawami i wolnościami osoby, której dane dotyczą, które wymagają ochrony na podstawie art. 1 ust. 1.

CZĘŚĆ III

SZCZEGÓLNE KATEGORIE PRZETWARZANIA DANYCH

Artykuł 8

Przetwarzanie szczególnych kategorii danych

1. Państwa członkowskie zabronią przetwarzania danych osobowych ujawniającego pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych, jak również przetwarzanie danych dotyczących zdrowia i życia płciowego.
2. Ust. 1 nie będzie miał zastosowania, jeśli:
 - (a) osoba, której dane dotyczą danych udzieliła wyraźnej zgody na przetwarzanie tych danych, chyba że ustawodawstwo państwa członkowskiego przewiduje, że zakaz, o którym mowa w ust. 1 nie może być uchylony mimo udzielonej zgody przez osobę, której dane dotyczą; lub
 - (b) przetwarzanie danych jest konieczne do wypełniania obowiązków i szczególnych uprawnień administratora danych w dziedzinie prawa pracy, o ile jest to dozwolone przez prawo krajowe przewidujące odpowiednie zabezpieczenia; lub
 - (c) przetwarzanie danych jest konieczne dla ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby, w przypadku, gdy osoba, której dane dotyczą jest fizycznie lub prawnie niezdolna do udzielenia zgody; lub
 - (d) przetwarzanie danych jest dokonywane się w ramach legalnej działalności wspartej odpowiednimi gwarancjami przez fundację, stowarzyszenie lub inną nie komercyjną instytucję, której cele mają charakter polityczny, filozoficzny, religijny lub związkowy, pod warunkiem, że przetwarzanie danych odnosi się wyłącznie do członków tej instytucji lub osób mających z nią regularny kontakt w związku z jej celami oraz że dane nie zostaną ujawnione osobie trzeciej bez zgody osób, których dane dotyczą; lub
 - (e) przetwarzanie dotyczy danych, które są podawane do wiadomości publicznej przez osobę, której dane dotyczą, lub jest konieczne do ustalenia, wykonania lub obrony roszczeń prawnych.
3. Ust. 1 nie ma zastosowania w przypadku, gdy przetwarzanie danych wymagane jest dla celów medycyny prewencyjnej, diagnostyki medycznej, świadczenia opieki lub leczenia, lub też zarządzania opieką zdrowotną, jak również w przypadkach, gdy dane są przetwarzane przez podmiot służby zdrowia zgodnie z przepisami prawa krajowego lub zasadami określonymi przez właściwe krajowe instytucje, podlegający obowiązkowi zachowania tajemnicy zawodowej lub przez inną osobę również zobowiązaną do zachowania tajemnicy.
4. Pod warunkiem stworzenia odpowiednich zabezpieczeń, państwa członkowskie mogą, ze względu na istotny interes publiczny, ustalić dodatkowe zwolnienia, poza tymi, które zostały określone w ust. 2 na mocy prawa krajowego lub decyzją organu nadzorczego.
5. Przetwarzanie danych dotyczących przestępstw, wyroków skazujących lub środków bezpieczeństwa może być dokonywane jedynie pod kontrolą oficjalnych władz,

lub też, jeżeli zgodnie z prawem krajowym stworzone zostały odpowiednie szczególne zabezpieczenia, z uwzględnieniem wyłączeń, które państwo członkowskie może wprowadzić zgodnie z obowiązującymi przepisami krajowymi, zapewniając odpowiednie szczególne zabezpieczenia. Jednak kompletny rejestr skazanych może być prowadzony tylko pod kontrolą oficjalnego organu władzy.

Państwa członkowskie mogą przewidzieć, że dane dotyczące sankcji administracyjnych lub orzeczeń w sprawach cywilnych będą również przetwarzane pod kontrolą oficjalnych władz.

6. Wyłączenia stosowania ust. 1, o których mowa w ust. 4 i 5 będą notyfikowane Komisji.
7. Państwa członkowskie określą warunki, w których może następować przetwarzanie krajowego numeru identyfikacyjnego lub innego identyfikatora ogólnego stosowania.

Artykuł 9

Przetwarzanie danych osobowych i wolność wypowiedzi

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

CZĘŚĆ IV

PRZEKAZYWANIE INFORMACJI OSOBIE, KTÓREJ DANE DOTYCZĄ

Artykuł 10

Informacje w przypadku zbierania danych od osoby, której dane dotyczą

Państwa członkowskie zapewnią, że administrator danych lub jego przedstawiciel zobowiązany będzie przedstawić osobie, której dane dotyczą i, od której gromadzone są dane, co najmniej następujące informacje, z wyjątkiem przypadku, kiedy posiada już ona informacje dotyczące:

- (a) tożsamości administratora danych i ewentualnie jego przedstawiciela;
- (b) celów przetwarzania danych, do których dane są przeznaczone;
- (c) wszelkich dalszych informacji, jak np.:
 - odbiorcy lub kategorie odbiorców danych,
 - tego czy odpowiedzi na pytania są obowiązkowe czy dobrowolne oraz ewentualne konsekwencje nie udzielenia odpowiedzi,
 - istnienie prawa dostępu do swoich danych oraz ich poprawienia,

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

Artykuł 11

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

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

- (a) tożsamości administratora danych i ewentualnie jego przedstawiciela;
- (b) cele przetwarzania danych;
- (c) wszelkich dalszych informacji, jak np.:
 - kategorie potrzebnych danych,
 - odbiorcy lub kategorie odbiorców danych,
 - istnienie prawa dostępu do swoich danych oraz ich poprawienia,

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

2. Ust. 1 nie ma zastosowania wówczas - szczególnie w przypadku przetwarzania danych dla celów statystycznych, historycznych lub naukowych - gdy dostarczenie takich informacji wymagałoby niewspółmiernie dużego wysiłku, lub jeżeli gromadzenie lub ujawnianie informacji jest wyraźnie przewidziane przez prawo. W takich przypadkach państwa członkowskie zapewnią odpowiednie zabezpieczenia.

CZĘŚĆ V

PRAWO DOSTĘPU DO DANYCH OSOBY, KTÓREJ DANE DOTYCZĄ

Artykuł 12

Prawo dostępu do danych

Państwa członkowskie zapewnią każdej osobie, której dane dotyczą prawo do uzyskania od administratora danych:

- (a) bez ograniczeń, w odpowiednich odstępach czasu oraz bez nadmiernego opóźnienia lub kosztów:

- potwierdzenia, czy dotyczące jej dane są przetwarzane oraz co najmniej informacji o celach przetwarzania danych, kategoriach danych oraz odbiorcach lub kategoriach odbiorców, którym dane te są ujawniane,
 - zawiadomienia w zrozumiałej formie o danych przechodzących przetwarzanie oraz dostępnych informacjach o ich źródłach,
 - wiadomości na temat zasad automatycznego przetwarzania dotyczących jej danych przynajmniej w przypadku zautomatyzowanego procesu decyzyjnego, o którym mowa w art. 15 ust. 1;
- (b) odpowiednio możliwość poprawienia, usunięcia lub zablokowania danych, których przetwarzanie jest niezgodne z postanowieniami niniejszej dyrektywy, szczególnie ze względu na niekompletność lub niedokładność danych;
- (c) zawiadomienia osób trzecich, którym dane zostały ujawnione, o każdym poprawieniu, usunięciu lub zablokowaniu danych zgodnie z lit. (b), o ile nie okaże się to niemożliwe lub nie będzie wymagało niewspółmiernie dużego wysiłku.

CZEŚĆ VI

ZWOLNIENIA I OGRANICZENIA

Artykuł 13

Zwolnienia i ograniczenia

1. Państwo członkowskie może przyjąć środki ustawodawcze w celu ograniczenia zakresu praw i obowiązków, przewidzianych w art. 6 ust.1, 10, 11 ust. 1, 12 oraz 21, kiedy ograniczenie takie stanowi środek konieczny dla zabezpieczenia:
 - (a) bezpieczeństwa narodowego;
 - (b) obronności;
 - (c) bezpieczeństwa publicznego;
 - (d) działań prewencyjnych, prowadzonych czynności dochodzeniowo-śledczych i prokuratorskich w sprawach kryminalnych lub sprawach o naruszenie zasad etyki w zawodach podlegających regulacjom;
 - (e) ważnego interesu ekonomicznego lub finansowego państwa członkowskiego lub Unii Europejskiej, łącznie ze sprawami monetarnymi, budżetowymi i podatkowymi;
 - (f) funkcji kontrolnych, inspekcyjnych i regulacyjnych związanych, nawet sporadycznie z wykonywaniem władzy publicznej w przypadkach wymienionych w lit. (c), (d) i (e);
 - (g) ochrony osoby, której dane dotyczą oraz praw i wolności innych osób.

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

CZEŚĆ VII

PRAWO SPRZECIWU PRZYSŁUGUJĄCE OSOBIE, KTÓREJ DANE DOTYCZĄ

Artykuł 14

Prawo sprzeciwu przysługujące osobie, której dane dotyczą

Państwa członkowskie przyznają osobie, której dane dotyczą, prawo:

- (a) przynajmniej w przypadkach wymienionych w art. 7 lit. e i f – sprzeciwu, w dowolnym czasie z ważkich i prawnie uzasadnionych przyczyn wynikających z jej konkretnej sytuacji, co do przetwarzania dotyczących jej danych, chyba że ustawodawstwo krajowe przewiduje inaczej. W przypadku uzasadnionego sprzeciwu przetwarzanie danych prowadzone przez administratora danych nie może już obejmować tych danych, których sprzeciw dotyczy;
- (b) sprzeciwu, na wniosek i bez opłaty, wobec przetwarzania dotyczących jej danych osobowych, które administrator danych zamierza przetwarzać dla potrzeb marketingu bezpośredniego, lub uzyskania informacji przed ujawnieniem danych osobowych po raz pierwszy osobom trzecim lub wykorzystaniem tych danych w ich imieniu dla potrzeb marketingu bezpośredniego, jak również do wyraźnego powoływania się na prawo bezpłatnego sprzeciwu wobec ujawniania lub wykorzystywania danych.

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

Artykuł 15

Zautomatyzowane decyzje indywidualne

1. Państwa członkowskie przyznają każdej osobie prawo nie podlegania decyzji, która wywołuje skutki prawne, które dotyczą jej lub mają na nią istotny wpływ, oraz która oparta jest wyłącznie na zautomatyzowanym przetwarzaniu danych, którego celem jest dokonanie oceny niektórych dotyczących ją aspektów o charakterze osobistym, jak np. wyniki 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 osobę, której dane dotyczą, zostanie przyjęty, lub że istnieją odpowiednie sposoby zabezpieczenia jej uzasadnionych interesów, jak np. uregulowania umożliwiające mu przedstawienie swojego punktu widzenia; lub
 - (b) zostanie dozwolona przez prawo, które określa również sposoby zabezpieczenia uzasadnionych interesów osoby, której dane dotyczą.

CZEŚĆ VIII

POUFNOŚĆ I BEZPIECZEŃSTWO PRZETWARZANIA DANYCH

Artykuł 16

Poufność przetwarzania danych

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

Artykuł 17

Bezpieczeństwo przetwarzania danych

1. Państwa członkowskie zapewnią, aby administrator danych wprowadził odpowiednie środki techniczne i organizacyjne w celu ochrony danych osobowych przed przypadkowym lub nielegalnym zniszczeniem lub przypadkową utratą, zmianą, niedozwolonym ujawnieniem lub dostępem, szczególnie wówczas, gdy przetwarzanie danych obejmuje transmisję danych w sieci, jak również przed wszelkimi innymi nielegalnymi formami przetwarzania.

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

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

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

- przetwarzający będzie działać wyłącznie na polecenie administratora danych,
 - obowiązki ustalone w ust. 1, określone przez ustawodawstwo państwa członkowskiego, w którym przetwarzający prowadzi działalność gospodarczą, będą również dotyczyć przetwarzającego.
4. Dla celów dowodowych, części umowy lub aktu prawnego dotyczącego ochrony danych i wymagań dotyczących środków wymienionych w ust. 1 będą sporządzane na piśmie lub w innej równorzędnej formie.

CZĘŚĆ IX

POWIADOMIENIE

Artykuł 18

Obowiązek powiadomienia organu nadzorczego

1. Państwa członkowskie zobowiążą administratora danych lub jego ewentualnego przedstawiciela do powiadomienia organu nadzorczego, wymienionego w art. 28 przed przeprowadzeniem całościowej lub częściowej operacji automatycznego przetwarzania danych lub zestawu takich operacji mających służyć jednemu celowi lub wielu powiązanim ze sobą celom.
2. Państwa członkowskie mogą wprowadzić uproszczenie procedury lub zwolnienie z obowiązku powiadomienia tylko w następujących sytuacjach oraz na następujących warunkach:
 - jeżeli, w przypadku kategorii operacji przetwarzania, co do których mało prawdopodobne jest, biorąc pod uwagę dane przeznaczone do przetworzenia, aby niekorzystnie wpłynęły na prawa i wolności osób, których dane dotyczą, określają cele przetwarzania danych, dane lub kategorie danych przechodzących proces przetwarzania, kategorię lub kategorie osób, których dane dotyczą, odbiorców lub kategorie odbiorców, którym dane mają być ujawnione oraz długość okresu przechowywania danych i/lub
 - jeżeli administrator danych, zgodnie z dotyczącymi go przepisami krajowymi, powoła urzędnika do spraw ochrony danych osobowych, odpowiedzialnego w szczególności:
 - za zapewnienie w niezależny sposób wewnętrznego stosowania krajowych przepisów przyjętych na podstawie niniejszej dyrektywy,
 - za prowadzenie rejestru operacji przetwarzania danych wykonywanych przez administratora danych i zawierających informacje, o których mowa w art. 21 ust. 2, zapewniając przy tym, że nie zostaną naruszone prawa i wolności osób, których dane dotyczą.
3. Państwa członkowskie mogą ustalić, że ust. 1 nie odnosi się do przetwarzania danych, którego wyłącznym celem jest prowadzenie rejestru, który zgodnie z obowiązującymi ustawami lub przepisami ma służyć za źródło informacji dla społeczeństwa oraz który będzie

przeznaczony do wglądu dla ogółu społeczeństwa lub osób posiadających uzasadniony interes w uzyskaniu informacji;

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

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

Artykuł 19 Treść powiadomienia

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

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

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

Artykuł 20

Kontrola wstępna

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

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

3. Państwa członkowskie mogą również przeprowadzać takie kontrole w kontekście opracowywania odpowiedniego uregulowania w parlamencie krajowym lub uregulowania

opartego na takim rozwiązaniu legislacyjnym, które określa charakter przetwarzania danych oraz stwarza odpowiednie zabezpieczenia.

Artykuł 21

Upublicznienie operacji przetwarzania danych

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

2. Państwa członkowskie zapewnią, że organ nadzorczy będzie prowadzić rejestr operacji przetwarzania danych zgłoszonych zgodnie z art.18.

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

Każda osoba może mieć wgląd do rejestru.

3. Państwa członkowskie zapewnią, - w odniesieniu do operacji przetwarzania danych nie podlegających zgłaszaniu – aby administratorzy danych lub inne instytucje powołane przez państwa członkowskie będą udostępniać przynajmniej te informacje, o których mowa w art. 19 ust. 1 lit. a) - e) w odpowiedniej formie każdej osobie na żądanie.

Państwa członkowskie mogą ustalić, że postanowienie to nie będzie dotyczyć przetwarzania danych, którego wyłącznym celem jest prowadzenie rejestru, który zgodnie z ustawami i innymi przepisami ma służyć za źródło informacji dla społeczeństwa i jest udostępniony albo do publicznego wglądu albo do wglądu każdej osoby posiadającej uzasadniony interes w uzyskaniu informacji;

ROZDZIAŁ III

ŚRODKI OCHRONY PRAWNEJ, ODPOWIEDZIALNOŚĆ I SANKCJE

Artykuł 22

Środki ochrony prawnej

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

Artykuł 23

Odpowiedzialność

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

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

Artykuł 24 Sankcje

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

ROZDZIAŁ IV

PRZEKAZYWANIE DANYCH OSOBOWYCH DO KRAJÓW TRZECICH

Artykuł 25 Zasady

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

2. Odpowiedniość stopnia ochrony danych zapewnianej przez kraj trzeci należy oceniać w świetle wszystkich okoliczności dotyczących operacji przekazania danych lub zestawu takich operacji; szczególną uwagę zwracać się będzie na charakter danych, cel i czas trwania proponowanych operacji przetwarzania danych, kraj pochodzenia i kraj ostatecznego przeznaczenia, normy prawne, zarówno ogólne jak i branżowe, obowiązujące w kraju trzecim oraz przepisy zawodowe i środki bezpieczeństwa stosowane w tym kraju.

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

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

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

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

Państwa członkowskie podejmą konieczne działania w celu wykonania decyzji Komisji.

Artykuł 26

Wyłączenia

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

- (a) osoba, której dane dotyczą jednoznacznie udzieli zgody na proponowane przekazanie danych; lub
- (b) przekazanie danych jest konieczne dla realizacji umowy między osobą, której dane dotyczą i administratorem danych lub dla wprowadzenia w życie ustaleń poprzedzających zawarcie umowy na wniosek osoby, której dane dotyczą; lub
- (c) przekazanie danych jest konieczne dla zawarcia lub wykonania umowy zawartej w interesie osoby, której dane dotyczą; między administratorem danych i osobą trzecią; lub
- (d) przekazanie danych jest konieczne lub wymagane przez prawo z ważnych względów publicznych lub w celu ustanowienia, wykonania lub obrony tytułu prawnego; lub
- (e) przekazanie danych jest konieczne dla zapewnienia ochrony żywotnych interesów osoby, której dane dotyczą; lub
- (f) przekazanie danych następuje z rejestru, który zgodnie z obowiązującymi przepisami ma służyć za źródło informacji dla ogółu społeczeństwa i jest udostępniony albo do publicznego wglądu albo każdej osobie posiadającej uzasadniony interes w uzyskaniu informacji, o ile warunki określone przez prawo odnośnie wglądu do takiego rejestru zostały w danym przypadku spełnione.

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

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

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

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

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

ROZDZIAŁ V

REGUŁY POSTĘPOWANIA

Artykuł 27

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

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

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

3. Projekty reguł wspólnotowych, jak również zmiany i uzupełnienia istniejących reguł wspólnotowych mogą być przedstawione zespołowi roboczemu, o którym mowa w art. 29. Zespół roboczy ustali m.in., czy przedstawione mu projekty zgodne są z przepisami krajowymi przyjętymi na podstawie niniejszej dyrektywy. Jeżeli organ uzna to za stosowne, będzie starać się o opinię osób, których dane dotyczą, lub ich przedstawicieli. Komisja może zapewnić odpowiednie rozpowszechnienie reguł zatwierdzonych przez 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 zapewnia, że jeden lub kilka organów publicznych, będzie odpowiedzialnych za kontrolę stosowania na jego terytorium postanowień przyjętych przez państwa członkowskie na podstawie niniejszej dyrektywy.

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

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

3. Każdy organ będzie wyposażony w szczególności w:

- uprawnienia dochodzeniowe, takie jak prawo dostępu do danych stanowiących przedmiot operacji przetwarzania danych oraz prawo gromadzenia wszelkich informacji potrzebnych do wykonywania jego funkcji nadzorczych,
- skuteczne uprawnienia interwencyjne, takie jak np. do wyrażenia opinii przed przystąpieniem do operacji przetwarzania danych zgodnie z art. 20, oraz do zapewnienia odpowiedniej publikacji tych opinii, zarządzania blokady, usunięcia lub zniszczenia danych, nakładania czasowego lub ostatecznego zakazu przetwarzania danych, ostrzegania lub upominania administratora danych, lub też prawo kierowania sprawy do parlamentów krajowych lub innych instytucji politycznych;
- uprawnienia do udziału w postępowaniu sądowym w przypadku naruszenia krajowych przepisów przyjętych na podstawie niniejszej dyrektywy lub zwrócenia uwagi władz sądowniczych na takie naruszenia.

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

4. Każdy organ nadzorczy będzie rozpatrywać skargi zgłaszane przez każdą osobę lub przez stowarzyszenie ją reprezentujące, odnośnie ochrony jej praw i wolności w zakresie przetwarzania danych osobowych. Zainteresowana osoba zostanie poinformowana o wyniku sprawy.

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

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

6. Każdy organ nadzorczy jest władny, niezależnie od krajowych przepisów dotyczących danego przypadku przetwarzania danych, do wykonywania na terytorium państwa członkowskiego kompetencji powierzonych mu zgodnie z ust. 3. Każdy organ może być

poproszony o skorzystanie ze swoich uprawnień przez odpowiedni organ innego państwa członkowskiego.

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

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

Artykuł 29

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

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

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

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

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

3. 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 środków mających na celu zabezpieczenie praw i wolności osób fizycznych w zakresie przetwarzania danych osobowych oraz innych proponowanych przez środki wspólnotowych wpływających na prawa i wolności;
 - (d) wydawać opinie na temat reguł postępowania opracowywanych na szczeblu Wspólnoty.
2. Jeżeli zespół roboczy stwierdzi występowanie rozbieżności między przepisami i praktyką w poszczególnych państwach członkowskich, mogących wpływać na równorzędność ochrony osób fizycznych w zakresie przetwarzania danych osobowych we Wspólnocie, zespół poinformuje o tym Komisję.
3. Zespół roboczy może, z własnej inicjatywy przedstawiać zalecenia we wszystkich sprawach związanych z ochroną osób fizycznych w zakresie przetwarzania danych osobowych we Wspólnocie.
4. Opinie i zalecenia zespołu roboczego będą przekazywane do Komisji oraz do komitetu, o którym mowa w art. 31.
5. Komisja będzie informować zespół roboczy o podejmowanych działaniach w odpowiedzi na jego opinie i zalecenia. Będzie to czynić w formie raportu, który przekazywany będzie również do Parlamentu Europejskiego i do Rady. Raport będzie udostępniony opinii publicznej.
6. Zespół roboczy będzie sporządzać roczny raport na temat sytuacji dotyczącej ochrony osób fizycznych w zakresie przetwarzania danych osobowych we Wspólnocie oraz w krajach trzecich, które będzie przekazywać Komisji, Parlamentowi Europejskiemu i Radzie. Raport będzie udostępniony opinii publicznej.

ROZDZIAŁ VII

ŚRODKI WYKONAWCZE PODEJMOWANE PRZEZ WSPÓLNOTĘ

*Artykuł 31** Komitet

- 1. Komisję wspomaga komitet.
- 2. W przypadku odniesienia się do niniejszego artykułu, art. 4 i 7 decyzji 1999/468/WE** stosuje się z uwagi na przepisy zawarte w jej art. 8.

Okres ustanowiony w art. 4 ust. 3 decyzji 1999/468/WE ustala się na trzy miesiące.

* w brzmieniu ustalonym Rozporządzeniem (WE) Nr 1882/2003 Parlamentu Europejskiego i Rady z dnia 29 września 2003 r. dostosowującym do decyzji Rady 1999/468/WE przepisy odnoszące się do komitetów, które wspomagają Komisję w wykonywaniu jej uprawnień wykonawczych ustanowionych w instrumentach podlegających procedurze określonej w art. 251 Traktatu WE (Dz. U. WE Nr. L 284 z 31.10.2003, str. 1).

** Decyzja Rady 1999/468/WE z dnia 28 czerwca 1999 r. ustanawiająca warunki wykonywania uprawnień wykonawczych przyznanych Komisji (Dz.U. WE L 184 z 17.7.1999, str. 23)."

3. Komitet uchwała swój regulamin wewnętrzny.

POSTANOWIENIA KOŃCOWE

Artykuł 32

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

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

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

Odstępując od poprzedniego akapitu, ustala się, że państwa członkowskie mogą wprowadzić wymóg, aby przetwarzanie danych, które są już przechowywane w ręcznych systemach ewidencji w dniu wejścia w życie krajowych przepisów przyjętych na podstawie niniejszej dyrektywy zostały dostosowane do wymogów art. 6 - 8 dyrektywy w ciągu 12 lat od daty ich przyjęcia. Państwa członkowskie przyznają osobie, której dane dotyczą prawo uzyskania, na jej wniosek, a szczególnie w czasie wykonywania przysługującego mu prawa dostępu, poprawy, usunięcia lub zablokowania danych, które są niekompletne, nieprawidłowe lub przechowywane w sposób niezgodny z uzasadnionymi celami realizowanymi przez administratora danych.

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

4. Państwa członkowskie 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.

W imieniu Parlamentu Europejskiego

Przewodniczący

K. HÄNSCH

W imieniu Rady

Przewodniczący

L. ATIENZA SERNA