

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady

z dnia 24 października 1995 r.

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

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

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

uwzględniając wniosek Komisji [1],

uwzględniając opinię Komitetu Ekonomiczno-Społecznego [2],

stanowiąc zgodnie z procedurą określoną w art. 189b Traktatu [3],

a także mając na uwadze, co następuje:

(1) Cele Wspólnoty, określone w Traktacie, zmienionym Traktatem o Unii Europejskiej, obejmują tworzenie coraz ściślejszego związku między narodami Europy, kształtowanie bliższych stosunków między państwami należącymi do Wspólnoty, zapewnienie postępu gospodarczego i społecznego poprzez wspólne działania na rzecz likwidacji barier dzielących Europę, pobudzanie ciągłej poprawy warunków życia jej narodów, ochronę i umacnianie pokoju i wolności oraz wspieranie demokracji w oparciu o prawa podstawowe uznane w konstytucji 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; muszą one, niezależnie od obywatelstwa czy miejsca stałego zamieszkania osób fizycznych, szanować ich podstawowe prawa i wolności, szczególnie prawo do prywatności, oraz przyczyniać się do postępu gospodarczego i społecznego, rozwoju handlu oraz dobrobytu jednostek.

(3) Ustanowienie i funkcjonowanie rynku wewnętrznego, na którym zgodnie z art. 7a Traktatu, zapewniony jest swobodny przepływ towarów, osób, usług i kapitału, wymaga nie tylko zapewnienia swobodnego przepływu danych osobowych z jednego Państwa Członkowskiego do drugiego, lecz również ochrony praw podstawowych osób fizycznych.

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

(5) Integracja gospodarcza i społeczna będąca wynikiem ustanowienia i funkcjonowania rynku wewnętrznego w rozumieniu art. 7a Traktatu będzie prowadzić do znacznego zwiększenia transgranicznego przepływu danych osobowych między wszystkimi podmiotami zaangażowanymi prywatnie lub publicznie w działalność gospodarczą i społeczną w Państwach Członkowskich; wzrośnie wymiana danych osobowych między przedsiębiorstwami działającymi w różnych Państwach Członkowskich; władze krajowe poszczególnych Państw Członkowskich podejmują się na mocy prawa wspólnotowego współpracy i wymiany danych osobowych dla celu 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 naukowej i technicznej oraz proces skoordynowanego wprowadzania nowych sieci telekomunikacyjnych we Wspólnocie narzuca konieczność i ułatwia transgraniczny przepływ danych osobowych.

(7) Różnica w stopniu ochrony praw i wolności 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 poziomie wspólnotowym, zakłócać konkurencję i utrudniać władzom wykonywanie ich obowiązków wynikających z przepisów prawa wspólnotowego; wspomniana różnica w stopniu ochrony

jest wynikiem istnienia wielkiej różnorodności krajowych przepisów ustawowych, wykonawczych i administracyjnych.

(8) W celu zniesienia przeszkód w przepływie danych osobowych, stopień ochrony praw i wolności jednostek 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 odpowiednimi ustawodawstwami krajowymi oraz potrzebę dokonania koordynacji ustawodawstw Państw Członkowskich w celu zapewnienia jednolitej regulacji transgranicznego przepływu danych osobowych, zgodnie z celem rynku wewnętrznego przewidzianego w art. 7a Traktatu; konieczne są wspólnotowe działania na rzecz zbliżenia ustawodawstw.

(9) Biorąc pod uwagę równoważną ochronę wynikającą ze zbliżenia ustawodawstw krajowych, 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 wykonania dyrektywy korzystać partnerzy handlowi i społeczni; Państwa Członkowskie będą zatem mogły określić w swoim ustawodawstwie ogólne zasady regulujące legalność procesu przetwarzania danych; podejmując te działania, Państwa Członkowskie będą dokładać starań w celu poprawy ochrony gwarantowanej przez ich obecne ustawodawstwo; w granicach wspomnianego marginesu swobody działania oraz zgodnie z prawem wspólnotowym mogą wystąpić rozbieżności w wykonaniu dyrektywy, co może mieć wpływ na przepływ danych w Państwie Członkowskim jak również we Wspólnocie.

(10) Celem krajowych przepisów prawa dotyczących 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 zasadach ogólnych prawa wspólnotowego; z tego powodu zbliżenie przepisów prawa 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 wolności 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 r. 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 wspólnotowego; należy wyłączyć przetwarzanie danych dokonywane przez osobę fizyczną w wykonywaniu działań o charakterze wyłącznie osobistym lub domowym, jak np. korespondencja i przechowywanie spisów adresów.

(13) Działania określone w tytułach V i VI Traktatu o Unii Europejskiej dotyczące bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa w dziedzinie prawa karnego nie wchodzą w zakres stosowania prawa wspólnotowego, bez wpływu na obowiązki nałożone na Państwa Członkowskie na mocy art. 56 ust. 2, art. 57 i art. 100a Traktatu ustanawiającego Wspólnotę Europejską; przetwarzanie danych osobowych konieczne dla zapewnienia ochrony dobrego stanu gospodarczego państwa nie wchodzi w zakres stosowania niniejszej dyrektywy, o ile takie przetwarzanie 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 stosowania niniejszej dyrektywy, jeśli dokonywane jest dla potrzeb bezpieczeństwa publicznego, obronności, bezpieczeństwa narodowego lub też w

trakcie działań państwowych w dziedzinie prawa karnego lub innych działań niewchodzących w zakres prawa wspólnotowego.

(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 ograniczone zastosowanie, zgodnie z przepisami przewidzianymi 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 być przeprowadzane zgodnie z ustawodawstwem jednego z Państw Członkowskich; w związku z tym przetwarzanie danych przeprowadzane na odpowiedzialność administratora danych, który prowadzi działalność gospodarczą na terenie Państwa Członkowskiego, powinno być regulowane przez ustawodawstwo tego państwa.

(19) Prowadzenie działalności gospodarczej na terytorium Państwa Członkowskiego zakłada efektywne i rzeczywiste prowadzenie działań poprzez stabilne rozwiązania; forma prawna prowadzonej działalności gospodarczej, niezależnie czy jest to oddział lub filia posiadająca osobowość prawną, nie jest w tym względzie czynnikiem decydującym; w przypadku ustanowienia jednego administratora danych na terytorium kilku Państw Członkowskich, szczególnie w postaci filii, musi on zapewnić, w celu uniknięcia obejścia przepisów krajowych, że każda z prowadzonych działalności gospodarczych będzie spełniać obowiązki wynikające z prawa krajowego.

(20) Przetwarzanie danych przez osobę prowadzącą działalność w państwie trzecim nie może 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 pozostaje bez uszczerbku dla zasad terytorialności, stosowanych w sprawach karnych.

(22) Państwa Członkowskie dokładniej sprecyzują w ogłaszanych prawach lub przy wprowadzaniu w życie środków podjętych na podstawie niniejszej dyrektywy ogólne warunki, w których przetwarzanie danych jest zgodne z prawem; w szczególności art. 5 w połączeniu z art. 7 i 8, umożliwi Państwom Członkowskim, niezależnie od zasad ogólnych, zapewnienie szczególnych warunków przetwarzania danych dla poszczególnych sektorów oraz dla różnych kategorii danych objętych art. 8.

(23) Państwa Członkowskie są upoważnione do zapewnienia ochrony osobom fizycznym zarówno poprzez ogólne przepisy prawa o ochronie jednostek w odniesieniu do przetwarzania danych osobowych oraz poprzez ustawodawstwo sektorowe, 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 muszą 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 nadzorczego 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 mają zastosowania do 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, nie jest dłużej możliwa.

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

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

(29) Dalsze przetwarzanie danych osobowych do 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 środków zabezpieczających; środki te muszą w szczególności wykluczać wykorzystywanie danych na rzecz działań lub decyzji dotyczących konkretnej osoby.

(30) Zgodnie z prawem proces 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 kontekście uprawnionych zwykłych czynności handlowych spółek i innych instytucji; Państwa Członkowskie mogą w podobny sposób określać warunki, w jakich dane osobowe mogą być ujawnione osobie trzeciej do celów marketingu o charakterze komercyjnym, lub realizowanego przez organizację charytatywną, lub też przez inne stowarzyszenie lub fundację, np. o charakterze politycznym, z zastrzeżeniem przepisów 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 określić, 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 wolności 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 wolności.

(34) Państwa Członkowskie muszą być również uprawnione, w sytuacjach, kiedy jest to uzasadnione ważnym interesem publicznym, do uchylania zakazu przetwarzania sensytywnych kategorii danych w takich dziedzinach, jak zdrowie publiczne i ochrona socjalna – szczególnie w celu zapewnienia odpowiedniej jakości i zasadności ekonomicznej procedur stosowanych do rozstrzygnięcia roszczeń w sprawie świadczeń i usług w ramach

systemu ubezpieczeń zdrowotnych – 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) W przypadku gdy 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 ustanowienia odpowiednich środków zabezpieczających.

(37) Przetwarzanie danych osobowych dla potrzeb dziennikarstwa lub wypowiedzi o charakterze literackim lub artystycznym, zwłaszcza w dziedzinie techniki audiowizualnej, powinno kwalifikować się do zwolnienia z wymagań niektórych przepisów niniejszej dyrektywy, o ile jest to konieczne, aby pogodzić prawa podstawowe 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 prawami podstawowymi odnoszącymi się do ogólnych środków w sprawie legalności przetwarzania danych, środków w sprawie przesyłania danych do państw trzecich i kompetencjami organów nadzorczych; nie powinno to jednak powodować wprowadzenia przez Państwa Członkowskie uregulowań stanowiących odstępstwo od obowiązku zapewnienia bezpieczeństwa przetwarzania danych; przynajmniej organ nadzorczy odpowiedzialny za tę dziedzinę powinien być również wyposażony w niektóre uprawnienia ex post, np. publikowania regularnych sprawozdań lub kierowania spraw do władz sądowych.

(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 niej, 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 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 do 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 jej dotyczą, przynajmniej w przypadku zautomatyzowanego procesu decyzyjnego określonego 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 wolności 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 administratora danych 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 dla ochrony dochodzenia i prowadzenia spraw karnych oraz działań w związku z naruszeniem zasad etyki w zawodach podlegających regulacji; wykaz wyłączeń i ograniczeń powinien obejmować zadania z zakresu monitorowania, kontroli i regulacji koniecznych w trzech wymienionych wyżej dziedzinach dotyczących bezpieczeństwa publicznego, interesów ekonomicznych lub finansowych oraz walki z przestępczością; sporządzenie wykazu 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 przepisów prawa wspólnotowego, odstąpić od przepisów niniejszej dyrektywy odnośnie do prawa dostępu, obowiązku informowania obywateli oraz jakości danych w celu zapewnienia realizacji niektórych celów określonych powyżej.

(45) W przypadkach gdy dane mogą być legalnie przetwarzane ze względu na interes publiczny, władzę publiczną, oficjalne uprawnienia lub uzasadnione prawo osoby fizycznej lub prawnej, osoba, której dane te dotyczą powinna jednakże mieć prawo do sprzeciwienia się przetwarzaniu tych danych, ze względu na uzasadnione i ważne przyczyny związane z jej sytuacją; Państwa Członkowskie mogą jednak ustalić przepisy prawa krajowego 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 w odniesieniu do przetwarzania dodatkowych danych osobowych potrzebnych do wykonywania usług.

(48) Procedury dotyczące zawiadamiania organu nadzorczego są skonstruowane w taki sposób, aby zapewnić ujawnienie celów i głównych cech operacji przetwarzania danych dla ustalenia, czy operacja taka jest zgodna z krajowymi przepisami 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, jeżeli jest to zgodne ze środkiem podjętym przez Państwo Członkowskie określającym jego zakres; Państwa Członkowskie mogą również wprowadzić zwolnienia i uproszczenia w przypadku gdy osoba wyznaczona przez administratora zapewni, że przetwarzanie danych wpłynie niekorzystnie na prawa i wolności osób, których dane dotyczą; urzędnik odpowiedzialny za ochronę danych będący lub niebędący 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 wykazującej uzasadniony interes.

(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 organy musi z reguły być uznawana za wystarczający środek.

(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, określenie takich zagrożeń 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 środka ustawodawczego wydanego przez parlament narodowy lub środka opartego na takim środku prawnym, który określa charakter przetwarzania danych oraz stwarza odpowiednie zabezpieczenia.

(55) Na wypadek nieprzestrzegania przez administratora danych praw osób, których dane dotyczą, ustawodawstwa krajowe muszą przewidywać odpowiednie środki zaskarżenia; szkody, jakie osoba może ponieść wskutek niezgodnego z prawem przetwarzania danych, muszą być wyrównane 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 spełnia wymagań wynikających z przyjętych krajowych przepisów wprowadzonych na podstawie niniejszej dyrektywy.

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

(57) Z drugiej strony należy zakazać przekazywania danych osobowych do państwa trzeciego, które nie zapewnia odpowiedniego stopnia ochrony.

(58) Należy ustanowić, w niektórych okolicznościach, przepisy dla zwolnienia 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 lub administrację celną 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 wykazujących uzasadniony interes; w tym przypadku przekazanie danych nie powinno obejmować ich całości lub całych kategorii danych oraz, jeżeli rejestr jest przeznaczony do wglądu dla osób wykazujących uzasadniony interes, przekazanie danych powinno nastąpić jedynie na wniosek tych osób, lub wówczas gdy osoby te mają być odbierającymi dane.

(59) Podejmowane mogą być konkretne działania w celu zrekompensowania braku ochrony w państwie trzecim, jeżeli administrator danych oferuje właściwe środki zabezpieczające; ponadto, należy uwzględnić procedury negocjacji między Wspólnotą a państwami trzecimi.

(60) W każdym przypadku przekazywanie danych do państw trzecich może następować jedynie w pełnej zgodności z przepisami przyjętymi przez Państwa Członkowskie na podstawie niniejszej dyrektywy, w szczególności jej art. 8.

(61) Państwa Członkowskie i Komisja muszą, w zakresie swoich kompetencji, zachęcać zainteresowane stowarzyszenia handlowe i inne zainteresowane organizacje reprezentatywne do opracowania kodeksów postępowania w celu ułatwienia stosowania niniejszej dyrektywy, biorąc pod uwagę szczególnie cechy procesu przetwarzania danych w niektórych sektorach, z poszanowaniem przepisów prawa krajowego przyjętych w celu jej wykonania.

(62) Utworzenie w Państwach Członkowskich organów nadzorczych, wykonujących swoje funkcje w sposób całkowicie niezależny jest zasadniczym elementem ochrony osób fizycznych 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 brania udziału w postępowaniu sądowym; organy te muszą przyczyniać się do zapewnienia przejrzystości przetwarzania danych w Państwach Członkowskich, których 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 poziomie wspólnotowym 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 szczególny charakter, musi on służyć radą Komisji oraz, w szczególności, przyczyniać się do jednolitego stosowania przepisów krajowych przyjętych na mocy niniejszej dyrektywy.

(66) W odniesieniu do przekazywania danych do państw trzecich, stosowanie niniejszej dyrektywy wymaga nadania Komisji uprawnień wykonawczych oraz ustanowienia procedury zgodnie z decyzją Rady 87/373/EWG [4].

(67) Dnia 20 grudnia 1994 r. zawarta została między Parlamentem Europejskim, Radą i Komisją umowa w sprawie modus vivendi dotycząca środków wykonawczych do aktów przyjętych w trybie określonym w art. 189b Traktatu WE.

(68) Zasady ustanowione w niniejszej dyrektywie dotyczące 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 sektorów, w formie szczegółowych przepisów opartych na wspomnianych zasadach.

Należy wyznaczyć Państwom Członkowskim okres nie dłuższy niż trzy lata od wejścia w życie krajowych środków wykonujących dyrektywę, w którym będą one zobowiązane do (69) progresywnego stosowania nowych przepisów krajowych w odniesieniu do wszystkich realizowanych już operacji przetwarzania danych; dla ułatwienia ich realizacji przy uzasadnionych ekonomicznie kosztach, kolejny okres 12 lat od daty przyjęcia niniejszej dyrektywy wyznaczony zostanie Państwom Członkowskim w celu zapewnienia zgodności istniejących ręcznych systemów ewidencji danych z niektórymi przepisami dyrektywy; jeżeli we wspomnianym przedłużonym okresie przejściowym dane zawarte w owych systemach będą przetwarzane ręcznie, konieczne będzie doprowadzenie do zgodności tych systemów ze wspomnianymi przepisami w czasie przetwarzania danych.

(70) Nie jest konieczne, aby osoba, której dane dotyczą, udzieliła ponownej zgody dla umożliwienia administratorowi danych dalsze przetwarzanie, po wejściu w życie krajowych przepisów przyjętych na mocy niniejszej dyrektywy, wszelkich sensytywnych 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 ustanowionych w niniejszej dyrektywie,

PRZYJMUJĄ NINIEJSZĄ DYREKTYWĘ:

ROZDZIAŁ I

PRZEPISY OGÓLNE

Artykuł 1

Cel dyrektywy

1. Zgodnie z przepisami niniejszej dyrektywy, Państwa Członkowskie zobowiązują się chronić podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do prywatności w odniesieniu do przetwarzania danych osobowych.

2. Państwa Członkowskie nie będą ograniczać ani zakazywać swobodnego przepływu danych osobowych między Państwami Członkowskimi ze względów związanych z ochroną przewidzianą w ust. 1.

Artykuł 2

Definicje

Do celów niniejszej dyrektywy:

- a) "dane osobowe" oznacza wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej ("osoby, której dane dotyczą"); osoba możliwa do zidentyfikowania to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, szczególnie przez powołanie się na numer identyfikacyjny lub jeden bądź kilka szczególnych czynników określających jej fizyczną, fizjologiczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość;
- b) "przetwarzanie danych osobowych" ("przetwarzanie") oznacza każdą operację lub zestaw operacji dokonywanych na danych osobowych 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, blokowanie, usuwanie lub niszczenie;
- c) "zbiór danych" ("zbiór") 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, władzę publiczną, agencję 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 przepisach ustawowych i wykonawczych lub przepisach wspólnotowych, administrator danych może być powoływany lub kryteria jego powołania mogą być ustalane przez ustawodawstwo krajowe lub wspólnotowe;
- e) "przetwarzający" oznacza osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ przetwarzający dane osobowe w imieniu administratora danych;
- f) "osoba trzecia" oznacza osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ niebędący 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) "odbierający dane" oznacza osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ, któremu ujawniane są dane, będący lub niebędący 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 odnoszących się do niej danych osobowych.

Artykuł 3

Zakres obowiązywania

1. Niniejsza dyrektywa stosuje się do 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 ma zastosowania do przetwarzania danych osobowych:

- w ramach działalności wykraczającej poza zakres prawa Wspólnoty, jak np. dane, o których stanowi tytuł V i VI Traktatu o Unii Europejskiej, a w żadnym razie do działalności na rzecz bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (łącznie z dobrą kondycją

gospodarcza państwa, gdy działalność ta dotyczy spraw związanych z bezpieczeństwem państwa) oraz działalności państwa w obszarach prawa karnego,

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

Artykuł 4

Odpowiednie prawo krajowe

1. Każde Państwo Członkowskie stosuje, w odniesieniu do przetwarzania danych osobowych, przepisy prawa krajowego przyjmowane na mocy niniejszej dyrektywy wówczas, gdy:

a) przetwarzanie danych odbywa 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 każde z tych przedsiębiorstw wywiązuje się z obowiązków przewidzianych w odpowiednich przepisach prawa krajowego;

b) administrator danych nie prowadzi działalności gospodarczej na terytorium Państwa Członkowskiego, lecz w miejscu, gdzie jego prawo krajowe obowiązuje na mocy międzynarodowego prawa publicznego;

c) administrator danych nie prowadzi działalności gospodarczej na terytorium Wspólnoty a do 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 określonych w ust. 1 lit. c), administrator danych musi wyznaczyć swojego przedstawiciela na terytorium tego Państwa Członkowskiego, bez uszczerbku dla postępowañ sądowych, jakie mogłyby być podjęte przeciwko samemu administratorowi danych.

ROZDZIAŁ II

OGÓLNE ZASADY LEGALNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

Artykuł 5

Państwa Członkowskie określają, w granicach przepisów zawartych w niniejszym rozdziale, bardziej szczegółowe warunki ustalania legalności przetwarzania danych osobowych.

SEKCJA 1

ZASADY DOTYCZĄCE JAKOŚCI DANYCH

Artykuł 6

1. Państwa Członkowskie zapewniają, aby dane osobowe były:

a) przetwarzane rzetelnie i legalnie;

b) gromadzone do określonych, jednoznacznych i legalnych celów oraz nie były poddawane dalszemu przetwarzaniu w sposób niezgodny z tym celem. Dalsze przetwarzanie danych w celach historycznych, statystycznych lub naukowych nie jest uważane za niezgodne z przepisami pod warunkiem ustanowienia przez Państwa Członkowskie odpowiednich środków zabezpieczających;

c) prawidłowe, stosowne oraz nienadmierne ilościowo w stosunku do celów, dla których zostały zgromadzone i/lub dalej przetworzone;

d) prawidłowe oraz, w razie konieczności, aktualizowane; należy podjąć wszelkie uzasadnione działania, aby zapewnić usunięcie lub poprawienie nieprawidłowych lub niekompletnych danych, biorąc pod uwagę cele, dla których zostały zgromadzone lub dla których są dalej przetwarzane;

e) przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez czas nie dłuższy niż jest to konieczne do celów, dla których dane zostały zgromadzone lub dla których są dalej przetwarzane. Państwa Członkowskie ustanowią odpowiednie środki

zabezpieczające dla danych przechowywanych przez dłuższe okresy dla potrzeb historycznych, statystycznych i naukowych.

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

SEKCJA II

KRYTERIA LEGALNOŚCI PRZETWARZANIA DANYCH

Artykuł 7

Państwa Członkowskie zapewniają, że dane osobowe mogą 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 wykonania zobowiązania prawnego, 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 wykonywania 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, lub osobom, którym dane są ujawniane, z wyjątkiem sytuacji, kiedy interesy takie podporządkowane są interesom związanym z podstawowymi prawami i wolnościami osoby, której dane dotyczą, które gwarantują ochronę na podstawie art. 1 ust. 1.

SEKCJA III

SZCZEGÓLNE KATEGORIE PRZETWARZANIA DANYCH

Artykuł 8

Przetwarzanie szczególnych kategorii danych

1. Państwa Członkowskie zabraniają przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, opinie polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych, jak również przetwarzanie danych dotyczących zdrowia i życia seksualnego.

2. Ustęp 1 nie ma zastosowania w przypadku gdy:

- a) osoba, której dane dotyczą, udzieliła wyraźnej zgody na ich przetwarzanie, chyba że ustawodawstwo Państwa Członkowskiego przewiduje, że zakaz określony 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 środki zabezpieczające; 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 w ramach legalnej działalności wspartej odpowiednimi gwarancjami przez fundację, stowarzyszenie lub inną instytucję nienastawioną na osiągnięcie zysku, 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 ochrony roszczeń prawnych.

3. Ustęp 1 nie ma zastosowania w przypadku gdy przetwarzanie danych wymagane jest do 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 ustanowienia odpowiednich środków zabezpieczających, Państwa Członkowskie mogą, ze względu na istotny interes publiczny, ustalić dodatkowe wyłączenia, poza tymi, które zostały przewidziane w ust. 2, na mocy ustawy krajowej lub decyzji organu nadzorczego.

5. Przetwarzanie danych dotyczących przestępstw, wyroków skazujących lub środków bezpieczeństwa może być dokonywane jedynie pod kontrolą władz publicznych, lub też, jeżeli zgodnie z prawem krajowym ustanowiono określone środki zabezpieczające, z zachowaniem odstępstw, które Państwo Członkowskie może udzielić zgodnie z obowiązującymi przepisami prawa krajowego, zapewniając zachowanie odpowiednich zabezpieczeń. Jednak kompletny rejestr przestępstw kryminalnych może być prowadzony tylko pod kontrolą władzy publicznej.

Państwa Członkowskie mogą ustanowić przepisy zobowiązujące oficjalny organ do sprawowania kontroli nad przetwarzaniem danych dotyczących sankcji administracyjnych lub orzeczeń w sprawach cywilnych.

6. Odstępstwa od ust. 1, przewidziane w ust. 4 i 5, są 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 wprowadzają możliwość wyłączenia lub odstąpienia od przepisów niniejszego rozdziału, rozdziału IV i 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 do zachowania prywatności z przepisami dotyczącymi wolności wypowiedzi.

SEKCJA IV

PRZEKAZYWANIE INFORMACJI OSOBIE, KTÓREJ DANE DOTYCZĄ

Artykuł 10

Informacje w przypadku gromadzenia danych od osoby, której dane dotyczą

Państwa Członkowskie zapewniają, aby administrator danych lub jego przedstawiciel miał obowiązek przedstawienia osobie, której dane dotyczą i od której gromadzone są dane, co najmniej następujących informacji, z wyjątkiem przypadku, kiedy informacje takie już posiada:

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 odbierających dane,

- tego, czy odpowiedzi na pytania są obowiązkowe czy dobrowolne oraz ewentualne konsekwencje nieudzielenia odpowiedzi,

- istnienie prawa wglądu do swoich danych oraz ich sprostowania,

o ile takie dalsze informacje są potrzebne, biorąc od uwagę szczególne okoliczności, w których dane są gromadzone, w celu zagwarantowania rzetelnego przetwarzania danych w stosunku do osoby, 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 zapewniają, aby administrator danych lub jego przedstawiciel był zobowiązany od początku gromadzenia danych osobowych lub w przypadku ujawnienia danych osobie trzeciej, nie później niż do momentu, gdy dane są ujawniane po raz pierwszy, dostarczyć osobie, której dane dotyczą, co najmniej następujące informacje, z wyjątkiem przypadku, kiedy posiada już ona takie informacje:

- tożsamość administratora i ewentualnie jego przedstawiciela;
- cele przetwarzania danych;
- wszelkie dalsze informacje, jak np.:
- kategorie potrzebnych danych,
- odbiorcy lub kategorie odbierających dane,
- istnienie prawa wglądu do swoich danych oraz ich sprostowania,

o ile takie dalsze informacje są konieczne, biorąc od uwagę szczególne okoliczności, w których dane są gromadzone, w celu zagwarantowania rzetelnego przetwarzania danych w stosunku do osoby, której dane dotyczą.

2. Ustęp 1 nie ma zastosowania w przypadku gdy, szczególnie w przypadku przetwarzania danych do celów statystycznych, historycznych lub naukowych, dostarczenie takich informacji wymagałoby niewspółmiernie dużego wysiłku lub jeżeli gromadzenie lub ujawnianie informacji jest wyraźnie przewidziane przez prawo. W takich przypadkach Państwa Członkowskie zapewniają odpowiednie środki zabezpieczające.

SEKCJA V

PRAWO UZYSKANIA PRZEZ OSOBĘ, KTÓREJ DANE DOTYCZĄ DOSTĘPU DO DANYCH

Artykuł 12

Prawo dostępu do danych

Państwa Członkowskie zapewniają 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,
- wyrażonej w zrozumiałej formie informacji o danych przechodzących przetwarzanie oraz posiadanych informacji o ich źródłach,
- wiadomości na temat zasad automatycznego przetwarzania dotyczących jej danych przynajmniej w przypadku zautomatyzowanego procesu decyzyjnego określonego w art. 15 ust. 1;

b) odpowiednio do przypadku, sprostowania, usunięcia lub zablokowania danych, których przetwarzanie jest niezgodne z przepisami niniejszej dyrektywy, szczególnie ze względu na niekompletność lub niedokładność danych;

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

SEKCJA VI

WYŁĄCZENIA 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, art. 10, art. 11 ust. 1, art. 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 karnych lub sprawach o naruszenie zasad etyki w zawodach podlegających regulacji;
- e) ważnego interesu ekonomicznego lub finansowego Państwa Członkowskiego lub Unii Europejskiej, łącznie z kwestiami pieniężnymi, budżetowymi i podatkowymi;
- f) funkcji kontrolnych, inspekcyjnych i regulacyjnych związanych, nawet sporadycznie, z wykonywaniem władzy publicznej w przypadkach wymienionych w lit. c)–e);
- g) ochrony osoby, której dane dotyczą oraz praw i wolności innych osób.

2. Z zastrzeżeniem obowiązku zapewnienia odpowiedniego stopnia ochrony prawnej, 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, gdy dane są przetwarzane wyłącznie do celów badań naukowych lub przechowywane są w formie osobistej przez okres nieprzekraczający okresu koniecznego wyłącznie w celu sporządzenia statystyk.

SEKCJA 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), w dowolnym czasie z ważnych i uzasadnionych przyczyn wynikających z jego konkretnej sytuacji, sprzeciwu co do przetwarzania dotyczących jej danych, z zastrzeżeniem odmiennych postanowień ustawodawstwa krajowego. 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 jej danych osobowych, dla potrzeb bezpośredniego obrotu, lub prawo bycia poinformowanym przed ujawnieniem danych osobowych po raz pierwszy osobom trzecim lub ich wykorzystaniem w ich imieniu dla potrzeb bezpośredniego obrotu, jak również prawo wyraźnego powoływania się na prawo sprzeciwu, bez opłat, wobec ujawniania lub wykorzystywania danych.

Państwa Członkowskie podejmują konieczne działania, aby osoby, których dane dotyczą, były świadome istnienia praw wymienionych w lit. b) akapit pierwszy.

Artykuł 15

Zautomatyzowane decyzje indywidualne

1. Państwa Członkowskie przyznają każdej osobie prawo do nieobjęcia jej decyzją, która wywołuje skutki prawne, które jej dotyczą 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, zdolność kredytowa, wiarygodność, sposób zachowania itp.

2. Z zastrzeżeniem przepisów innych artykułów niniejszej dyrektywy, Państwa Członkowskie zapewniają, że każda osoba będzie mogła być wyłączona z zakresu objętego decyzją określoną w ust. 1, jeżeli decyzja taka:

a) zostanie podjęta w trakcie zawierania lub realizacji umowy, pod warunkiem że wniosek w sprawie zawarcia lub realizacji umowy, wniesiony przez osobę, której dane dotyczą, zostanie przyjęty, lub że istnieją odpowiednie sposoby zabezpieczenia 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.

SEKCJA VIII

POUFNOŚĆ I BEZPIECZEŃSTWO PRZETWARZANIA DANYCH

Artykuł 16

Poufność przetwarzania danych

Żadna osoba działająca z upoważnienia 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 zapewniają, 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 środki, które zapewnią poziom bezpieczeństwa odpowiedni do zagrożeń wynikających z przetwarzania danych oraz charakteru danych objętych ochroną.

2. Państwa Członkowskie zobowiązują administratora danych, w przypadku przetwarzania danych w jego imieniu, do wybrania przetwarzającego, o wystarczających gwarancjach odnośnie do technicznych środków bezpieczeństwa oraz rozwiązań organizacyjnych, regulujących przetwarzanie danych, oraz 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 działa wyłącznie na polecenie administratora danych,

- obowiązki wymienione w ust. 1, określone przez ustawodawstwo Państwa Członkowskiego, w którym przetwarzający prowadzi działalność gospodarczą, dotyczą również przetwarzającego.

4. Do celów zachowania dowodów, części umowy lub aktu prawnego dotyczącego ochrony danych i wymagań dotyczących środków wymienionych w ust. 1 są sporządzane na piśmie lub w innej równorzędnej formie.

SEKCJA IX

ZAWIADOMIENIE

Artykuł 18

Obowiązek zawiadamiania organu nadzorczego

1. Państwa Członkowskie zobowiązują administratora danych lub jego ewentualnego przedstawiciela do zawiadomienia 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 zawiadomienia 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, określą 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 przepisów prawa krajowego przyjętych na mocy niniejszej dyrektywy,

- za prowadzenie rejestru operacji przetwarzania danych wykonywanych przez administratora danych i zawierających informacje określone 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 przepisami ustawowymi lub wykonawczymi ma służyć za źródło informacji dla społeczeństwa oraz który będzie przeznaczony do wglądu dla ogółu społeczeństwa lub osób wykazujących uzasadniony interes.

4. Państwa Członkowskie mogą wprowadzić wyłączenie odobowiązku zawiadamiania lub uprościć procedurę zawiadamiania w przypadku operacji przetwarzania danych określonych w art. 8 ust. 2 lit. d).

5. Państwa Członkowskie mogą postanowić, że niektóre lub wszystkie nieautomatyzowane operacje przetwarzania danych osobowych będą zgłaszane lub ustalać dla takich operacji uproszczony tryb zawiadamiania.

Artykuł 19

Treść zawiadomienia

1. Państwa Członkowskie ustalają, jakie informacje zostaną podane w zawiadomieniu. Obejmują one, co najmniej:

a) nazwę (nazwisko) i adres administratora danych i ewentualnie jego przedstawiciela;

b) cel lub cele przetwarzania danych;

c) opis 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 państw 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 informacje określone w ust. 1 muszą być zgłaszane organowi nadzorcemu.

Artykuł 20

Kontrola wstępna

1. Państwa Członkowskie definiują operacje przetwarzania danych mogące stwarzać określone zagrożenia dla praw i wolności osób, których dane dotyczą oraz kontrolują, czy dane te są badane przed ich rozpoczęciem.

2. Kontrole wstępne są przeprowadzane przez organ nadzorczy po przyjęciu od administratora danych lub urzędnika odpowiedzialnego za ochronę danych zawiadomienia, którzy w razie wątpliwości powinni zasięgać opinii organu nadzorczego.

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

Artykuł 21

Podawanie do wiadomości publicznej operacji przetwarzania danych

1. Państwa Członkowskie podejmują odpowiednie środki, aby zapewnić podanie do wiadomości publicznej operacji przetwarzania danych.

2. Państwa Członkowskie zapewniają, aby organ nadzorczy prowadził rejestr operacji przetwarzania danych zgłoszonych zgodnie z art. 18.

Rejestr zawiera co najmniej informacje wymienione w art. 19 ust. 1 lit. a)–e).

Rejestr może być sprawdzany przez dowolną osobę.

3. Państwa Członkowskie zapewniają, w odniesieniu do operacji przetwarzania danych niepodlegających zgłoszeniu, aby administratorzy danych lub inne instytucje powołane przez Państwa Członkowskie udostępniały przynajmniej informacje określone w art. 19 ust. 1 lit. a)–e), w odpowiedniej formie każdej osobie na żądanie.

Państwa Członkowskie mogą ustalić, że przepis ten nie będzie dotyczyć przetwarzania danych, którego wyłącznym celem jest prowadzenie rejestru mającego służyć, na mocy przepisów ustawowych i wykonawczych, za źródło informacji dla ogółu społeczeństwa, otwartego dla obywateli i każdej osoby wykazującej uzasadniony interes.

ROZDZIAŁ III

ŚRODKI SĄDOWE, ODPOWIEDZIALNOŚĆ I SANKCJE

Artykuł 22

Środki sądowe

Bez uszczerbku dla wszystkich odwoławczych środków administracyjnych, które mogą być wprowadzone przez organ nadzorczy określony w art. 28, przed wszczęciem postępowania sądowego Państwa Członkowskie zapewnią każdej osobie prawo do korzystania ze środków prawnych w związku z naruszeniem praw zagwarantowanych jej przez przepisy krajowe dotyczące przetwarzania danych.

Artykuł 23

Odpowiedzialność

1. Państwa Członkowskie zapewniają, że każdej osobie, która poniosła szkodę wskutek niezgodnej z prawem operacji przetwarzania danych lub innej czynności niezgodnej z przepisami krajowymi przyjętymi zgodnie z niniejszą dyrektywą, przysługuje od administratora danych odszkodowanie za poniesioną szkodę.

2. Administrator danych może zostać zwolniony od 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 przepisów niniejszej dyrektywy oraz w szczególności określą sankcje, jakie należy nałożyć w przypadku naruszenia przepisów przyjętych zgodnie z niniejszą dyrektywą.

ROZDZIAŁ IV

PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTW TRZECICH

Artykuł 25

Zasady

1. Państwa Członkowskie zapewniają, aby przekazywanie do państwa trzeciego danych osobowych poddawanych przetwarzaniu lub przeznaczonych do przetwarzania po ich przekazaniu mogło nastąpić tylko wówczas gdy, niezależnie od zgodności z krajowymi przepisami przyjętymi na podstawie innych przepisów niniejszej dyrektywy, dane państwo trzecie zapewni odpowiedni stopień ochrony.
2. Odpowiedni stopień ochrony danych zapewnianej przez państwo trzecie należy oceniać w świetle wszystkich okoliczności dotyczących operacji przekazania danych lub zbiorutakich 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 państwie trzecim oraz przepisy zawodowe i środki bezpieczeństwa stosowane w tym państwie.
3. Państwa Członkowskie i Komisja będą informować się wzajemnie o przypadkach, kiedy uznają, że państwo trzecie nie zapewnia odpowiedniego stopnia ochrony w znaczeniu ust. 2.
4. Jeżeli Komisja stwierdzi, na podstawie procedury przewidzianej w art. 31 ust. 2, że państwo trzecie 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 państwa trzeciego.
5. We właściwym czasie Komisja przystąpi do negocjacji w celu zaradzenia sytuacji stwierdzonej na podstawie ust. 4.
6. Komisja może stwierdzić, zgodnie z procedurą określoną w art. 31 ust. 2, że państwo trzecie zapewnia prawidłowy stopień ochrony w znaczeniu ust. 2 niniejszego artykułu, co wynika z jego prawa krajowego lub międzynarodowych zobowiązań, jakie państwo to przyjęło, szczególnie po zakończeniu negocjacji określonych w ust. 5, w zakresie ochrony życia prywatnego i podstawowych praw i wolności osób fizycznych.

Państwa Członkowskie podejmują środki niezbędne w celu wykonania decyzji Komisji.

Artykuł 26

Odstępstwa

1. W drodze odstępstwa od przepisów art. 25 oraz, z zastrzeżeniem odmiennych przepisów prawa krajowego dotyczącego konkretnych przypadków, Państwa Członkowskie zapewnią, że przekazanie lub przekazywanie danych osobowych do państwa 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 między administratorem danych i osobą trzecią, w interesie osoby, której dane dotyczą, 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 ma służyć, zgodnie z obowiązującymi przepisami ustawowymi lub wykonawczymi, za źródło informacji dla ogółu społeczeństwa, udostępnionego do konsultacji obywateli i każdej osoby wykazującej uzasadniony interes, o ile warunki określone przez prawo odnośnie do wglądu do takiego rejestru zostały w danym przypadku spełnione.
2. Bez uszczerbku dla ust. 1, Państwo Członkowskie może zezwolić na przekazanie lub przekazywanie danych osobowych do państwa trzeciego, które nie zapewnia odpowiedniego stopnia ochrony w znaczeniu art. 25 ust. 2, jeżeli administrator danych zaleci odpowiednie

zabezpieczenia odnośnie do ochrony prywatności oraz podstawowych praw i wolności osoby oraz odnośnie do wykonywania odpowiednich praw; takie środki zabezpieczające mogą w szczególności wynikać z odpowiednich klauzul umownych.

3. Państwo Członkowskie powiadamia Komisję i inne Państwa Członkowskie o upoważnieniach wydanych na podstawie ust. 2.

Jeżeli Państwo Członkowskie lub Komisja zgłaszają sprzeciw w oparciu o uzasadnione przyczyny związane z ochroną prywatności oraz podstawowych praw i wolności osób fizycznych, Komisja podejmuje właściwe środki 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 określoną w art. 31 ust. 2, że określone klauzule umowne zapewniają odpowiednie środki zabezpieczające 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 zachęcają do opracowywania kodeksów postępowania, których celem będzie usprawnienie procesu prawidłowego wprowadzania krajowych przepisów przyjętych przez Państwa Członkowskie na mocy niniejszej dyrektywy, uwzględniając szczególne cechy różnych sektorów.

2. Państwa Członkowskie umożliwiają związkom 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 władzy publicznej.

Państwa Członkowskie doprowadzą do ustalenia przez wspomniany organ, m.in. czy przedstawiony mu projekt jest zgodny z przepisami krajowymi przyjętymi zgodnie z niniejszą dyrektywą. Jeżeli wspomniany organ uzna to za stosowne, będzie zwracać się o opinie osób, których dane dotyczą lub ich przedstawicieli.

3. Projekty kodeksów wspólnotowych, jak również zmiany i uzupełnienia istniejących kodeksów wspólnotowych, mogą być przedstawione grupie roboczej określonej w art. 29. Grupa robocza ustali m.in., czy przedstawione jej projekty są zgodne z przepisami krajowymi przyjętymi zgodnie z niniejszą dyrektywą. Komisja może zapewnić odpowiednie rozpowszechnienie kodeksów zatwierdzonych przez grupę roboczą.

ROZDZIAŁ VI

ORGAN NADZORCZY I GRUPA ROBOCZA DS. OCHRONY OSÓB FIZYCZNYCH W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

Artykuł 28

Organ nadzorczy

1. Każde Państwo Członkowskie zapewni, że jeden lub więcej organów władzy publicznej będzie odpowiedzialnych za kontrolę stosowania na jego terytorium przepisów przyjętych przez Państwa Członkowskie na mocy niniejszej dyrektywy.

Organy te postępują w sposób całkowicie niezależny przy wykonywaniu powierzonych im funkcji.

2. Każde Państwo Członkowskie wprowadza obowiązek konsultowania się z organami nadzorczymi przy opracowywaniu środków administracyjnych lub przepisów dotyczących ochrony praw i wolności osób fizycznych w zakresie przetwarzania danych osobowych.

3. Każdy organ jest w szczególności 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 narodowych lub innych instytucji politycznych,

- prawo pozywania w przypadku naruszenia krajowych przepisów przyjętych zgodnie z niniejszą dyrektywą lub powiadomienie organów sądowych o takim naruszeniu.

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

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

Każdy organ nadzorczy w szczególności rozpatruje skargi dotyczące kontroli legalności przetwarzania danych, zgłaszane przez dowolną osobę, kiedy mają zastosowanie krajowe przepisy przyjęte zgodnie z art. 13 niniejszej dyrektywy. Osoba ta zostanie w każdym przypadku poinformowana o przeprowadzeniu kontroli.

5. Każdy organ nadzorczy regularnie sporządza sprawozdanie ze swojej działalności. Sprawozdanie jest podawane do wiadomości publicznej.

6. Każdy organ nadzorczy jest właściwy, niezależnie od krajowych przepisów dotyczących danego przypadku przetwarzania danych, do wykonywania na terytorium Państwa Członkowskiego uprawnień powierzonych mu zgodnie z ust. 3. Do każdego organu można się zwrócić z żądaniem wykonania jego praw przez odpowiedni organ innego Państwa Członkowskiego.

Organy nadzorcze współpracują ze sobą w zakresie koniecznym do wykonywania swoich obowiązków, zwłaszcza poprzez wymianę wszelkich przydatnych informacji.

7. Państwa Członkowskie dopilnują, aby członkowie kierownictwa i personel organu nadzorczego podlegali obowiązkowi zachowania tajemnicy zawodowej również po rozwiązaniu stosunku pracy, w odniesieniu do poufnych informacji, do których mają dostęp.

Artykuł 29

Grupa robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych

1. Niniejszym powołuje się grupę roboczą ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych, zwaną dalej "grupą roboczą".

Ma ona charakter doradczy i działa w sposób niezależny.

2. W skład grupy roboczej wchodzi przedstawiciele organu lub organów nadzorczych, powołanych przez każde Państwo Członkowskie oraz przedstawiciel organu lub organów ustanowionych dla instytucji i organów wspólnotowych, oraz przedstawiciel Komisji.

Każdy członek grupy roboczej jest powoływany przez instytucję, organ lub organy, które reprezentuje. Jeżeli Państwo Członkowskie powoła więcej niż jeden organ nadzorczy, organy te wyznaczają wspólnego przedstawiciela. Ta sama zasada dotyczy organów utworzonych przez instytucje i organy wspólnotowe.

3. Grupa robocza podejmuje decyzje zwykłą większością głosów przedstawicieli organów nadzorczych.

4. Grupa robocza wybiera swojego przewodniczącego. Kadencja przewodniczącego trwa dwa lata. Jego mandat jest odnawialny.

5. Komisja zapewnia obsługę sekretariatu grupy roboczej.

6. Grupa robocza przyjmuje swój regulamin.

7. Grupa robocza rozważa pozycje zamieszczone w porządku dziennym przez przewodniczącego, z jego inicjatywy bądź na wniosek przedstawiciela organu nadzorczego lub na wniosek Komisji.

Artykuł 30

1. Grupa robocza:

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

b) przekazuje Komisji opinie na temat stopnia ochrony we Wspólnocie i w państwach trzecich;

c) doradza Komisji w sprawie wszelkich proponowanych zmian niniejszej dyrektywy, dodatkowych lub szczególnych środków mających na celu zabezpieczenie praw i wolności osób fizycznych w zakresie przetwarzania danych osobowych oraz innych proponowanych środków wspólnotowych dotyczących praw i wolności;

d) wydaje opinie na temat kodeksów postępowania opracowywanych na poziomie wspólnotowym.

2. Jeżeli grupa robocza stwierdza występowanie rozbieżności między przepisami i praktyką przyjętą w poszczególnych Państwach Członkowskich, mogących wpływać na równowagę ochrony osób fizycznych w zakresie przetwarzania danych osobowych we Wspólnocie, grupa powiadamia o tym Komisję.

3. Grupa robocza może z własnej inicjatywy formułować zalecenia we wszystkich sprawach dotyczących ochrony osób fizycznych w zakresie przetwarzania danych osobowych we Wspólnocie.

4. Opinie i zalecenia grupy roboczej są przekazywane Komisji oraz komitetowi, określone w art. 31.

5. Komisja informuje grupę roboczą o podejmowanych działaniach w odpowiedzi na jego opinie i zalecenia. Czyni to w formie sprawozdania, które przekazywane jest również Parlamentowi Europejskiemu i Radzie. Sprawozdanie jest udostępniane opinii publicznej.

6. Grupa robocza sporządza roczne sprawozdanie na temat sytuacji dotyczącej ochrony osób fizycznych w zakresie przetwarzania danych osobowych we Wspólnocie oraz w państwach trzecich, które przekazuje Komisji, Parlamentowi Europejskiemu i Radzie. Sprawozdanie jest udostępniane opinii publicznej.

ROZDZIAŁ VII

WSPÓLNOTOWE ŚRODKI WYKONAWCZE

Artykuł 31

Komitet

1. Komisja wspierana jest przez komitet składający się z przedstawicieli Państw Członkowskich, na którego czele stoi przedstawiciel Komisji.

2. Przedstawiciel Komisji przedstawia komitetowi projekt środków, które należy podjąć. Komitet wydaje opinię o projekcie w terminie wyznaczonym przez przewodniczącego zaleźnie od pilności sprawy.

Opinia zostaje przyjęta większością głosów ustanowioną w art. 148 ust. 2 Traktatu. Głosy przedstawicieli Państw Członkowskich w komitecie są wazone w sposób określony w tym artykule. Przewodniczący nie bierze udziału w głosowaniu.

Komisja przyjmuje środki, które stosuje się niezwłocznie. Jeżeli jednak środki te nie są zgodne z opinią komitetu, Komisja niezwłocznie powiadamia o tym Radę. W takim przypadku:

- Komisja odracza stosowanie podjętych środków o trzy miesiące od daty takiego powiadomienia;

- Rada, stanowiąc większością kwalifikowaną, może podjąć inną decyzję w terminie określonym w tiret pierwsze.

PRZEPISY KOŃCOWE

Artykuł 32

1. Państwa Członkowskie wprowadzą w życie przepisy ustawowe, wykonawcze i administracyjne niezbędne do wykonania niniejszej dyrektywy nie później niż w trzy lata od daty jej przyjęcia.

Wymienione środki zawierają odniesienie do niniejszej dyrektywy lub odniesienie to towarzyszy ich urzędowej publikacji. Metody dokonywania takiego odniesienia ustanawiane są przez Państwa Członkowskie.

2. Państwa Członkowskie zapewniają, aby przetwarzanie danych, będące już w toku w dniu, w którym przepisy krajowe przyjęte zgodnie z niniejszą dyrektywą weszły w życie, zostało dostosowane do tych przepisów w terminie trzech lat od wspomnianej daty.

W drodze odstępstwa od poprzedniego akapitu Państwa Członkowskie mogą wprowadzić wymóg, aby przetwarzanie danych, które są już przechowywane w ręcznych systemach ewidencji w dniu wejścia w życie krajowych przepisów przyjętych w ramach wykonania niniejszej dyrektywy zostały dostosowane do wymogów art. 6–8 niniejszej dyrektywy w ciągu 12 lat od daty ich przyjęcia. Państwa Członkowskie przyznają osobie, której dane dotyczą, prawo uzyskania, na jej wniosek, w szczególności w czasie wykonywania przysługującego jej prawa dostępu, sprostowania, usunięcia lub zablokowania danych, które są niekompletne, nieprawidłowe lub przechowywane w sposób niezgodny z uzasadnionymi celami realizowanymi przez administratora danych.

3. W drodze odstępstwa 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 w dziedzinach objętych niniejszą dyrektywą.

Artykuł 33

Komisja składa Radzie i Parlamentowi Europejskiemu regularne sprawozdania, począwszy nie później niż trzy lata od daty wskazanej w art. 32 ust. 1, na temat wykonania niniejszej dyrektywy, załączając do sprawozdania, w razie potrzeby, odpowiednie propozycje zmian. Sprawozdanie jest podawane do publicznej wiadomości.

Komisja bada w szczególności stosowanie niniejszej dyrektywy w odniesieniu do przetwarzania danych dźwiękowych i obrazowych dotyczących osób fizycznych oraz przedstawia odpowiednie propozycje, jakie okażą się konieczne, biorąc pod uwagę rozwój technologii informatycznych 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

K. Hänsch

Przewodniczący

W imieniu Rady

L. Atienza Serna

Przewodniczący

[1] Dz.U. C 277 z 5.11.1990, str. 3 oraz Dz.U. C 311 z 27.11.1992, str. 30.

[2] Dz.U. C 159 z 17.6.1991, str. 38.

[3] Opinia Parlamentu Europejskiego z dnia 11 marca 1992 r. (Dz.U. C 94 z 13.4.1992, str. 198), potwierdzona dnia 2 grudnia 1993 r. (Dz.U. C 342 z 20.12.1993, str. 30); wspólne stanowisko Rady z dnia 20 lutego 1995 r. (Dz.U. C 93 z 13.4.1995, str. 1) i decyzja Parlamentu Europejskiego z dnia 15 czerwca 1995 r. (Dz.U. C 166 z 3.7.1995).

[4] Dz.U. L 197 z 18.7.1987, str. 33.
