ROZPORZĄDZENIE (WE) NR 45/2001 PARLAMENTU EUROPEJSKIEGO I RADY

z dnia 18 grudnia 2000 r.

o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat ustanawiający Wspólnotę Europejską, w szczególności jego art. 286,

uwzględniając wniosek Komisji[1],

uwzględniając opinię Komitetu Ekonomiczno - Społecznego[2],

stanowiąc zgodnie z procedurą ustanowioną w art. 251 Traktatu[3],

a także mając na uwadze, co następuje:

1) Art. 286 Traktatu wymaga zastosowania aktów wspólnotowych w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu takich danych do instytucji i organów wspólnotowych.

2) Pełny system ochrony danych osobowych wymaga nie tylko ustanowienia praw dla osób fizycznych, których dotyczą te dane i zobowiązań tych, którzy przetwarzają dane osobowe, ale także właściwych sankcji dla tych, którzy naruszają przepisy i monitorowania przez niezależny organ nadzoru.

3) Art. 286 ust. 2 Traktatu wymaga ustanowienia niezależnego organu nadzoru odpowiedzialnego za monitorowanie stosowania takich aktów wspólnotowych do instytucji i organów wspólnotowych.

4) Art. 286 ust. 2 Traktatu wymaga przyjęcia wszelkich innych właściwych przepisów w miarę potrzeb.

5) Konieczne jest rozporządzenie, zapewniające osobie fizycznej prawa prawnie egzekwowalne określające zobowiązania administratorów w instytucjach i organach wspólnotowych odnoszące się do przetwarzania danych osobowych oraz tworzące niezależny organ nadzoru odpowiedzialny za monitorowanie i przetwarzanie danych osobowych przez instytucje i organy wspólnotowe.

6) Przeprowadzono konsultacje z grupą roboczą ds. ochrony osób fizycznych ustanowioną na mocy art. 29 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania

[1] Dz.U. nr C 376E z 28.12.1999, str. 24.
[2] Dz.U. nr C 51 z 23.02.2000, str. 48.
[3] Opinia Parlamentu Europejskiego z dnia 14 listopada 2000 r. oraz decyzja Rady z dnia 30 listopada 2000 r.

danych osobowych i swobodnego przepływu tych danych[4].

7) Chronione mają być osoby, których dane osobowe są przetwarzane przez instytucje i organy wspólnotowe w dowolnym kontekście na przykład, dlatego że są zatrudnione przez te instytucje lub organy.

8) Zasady ochrony danych stosują się do wszelkiej informacji dotyczącej osób zidentyfikowanych przez dane lub mogących być zidentyfikowanymi. Aby określić, czy osoba może być zidentyfikowana należy wziąć pod uwagę wszystkie środki, które mogą być rozsądnie użyte przez administratora lub przez dowolne inne osoby, aby zidentyfikować wspomnianą wyżej osobę. Zasady ochrony nie powinny być stosowane do danych przetworzonych na anonimowe w taki sposób, że obiekt danych przestał być identyfikowalny.

9) Dyrektywa 95/46/WE wymaga, aby Państwa Członkowskie chroniły podstawowe prawa i wolności osób fizycznych, w szczególności ich prawa do prywatności w odniesieniu do przetwarzania danych osobowych, aby zapewnić swobodny przepływ danych osobowych we Wspólnocie.

10) Dyrektywa 97/66/WE Parlamentu Europejskiego i Rady z dnia 15 grudnia 1997 r. dotycząca przetwarzania danych osobowych oraz ochrony prywatności w sektorze telekomunikacyjnym[5] precyzuje i uzupełnia dyrektywę 95/46/WE w odniesieniu do przetwarzania danych osobowych w sektorze telekomunikacyjnym.

11) Różne inne środki wspólnotowe, włącznie ze środkami wzajemnej pomocy między władzami krajowymi i Komisją, są również tworzone, aby sprecyzować i uzupełniać dyrektywę 95/46/WE w sektorach, do których się odnoszą.

12) Spójne i jednolite stosowanie zasad ochrony podstawowych praw i wolności osób fizycznych w odniesieniu do przetwarzania danych osobowych powinno być zapewnione w całej Wspólnocie.

13) Celem jest zapewnienie zarówno efektywnej zgodności z regułami rządzącymi ochroną podstawowych praw i wolności osób fizycznych oraz swobodnego przepływu danych osobowych między Państwami Członkowskimi a instytucjami i organami wspólnotowymi, jak i między instytucjami i organami wspólnotowymi do celów związanych z wykorzystaniem ich kompetencji.

14) W tym celu przyjęte powinny być środki wiążące dla instytucji i organów wspólnotowych. Te środki powinny być stosowane do całości przetwarzania danych osobowych przez wszystkie instytucje i organy wspólnotowe, o ile takie przetwarzanie jest dokonywane podczas wykonywania czynności, które w całości lub częściowo wchodzą w zakres prawa wspólnotowego.

15) Jeżeli takie przetwarzanie jest przeprowadzane przez instytucje i organy wspólnotowe podczas wykonywania czynności wychodzących poza zakres niniejszego rozporządzenia, w szczególności tych, do których odnoszą się tytuły V i VI Traktatu o Unii Europejskiej, ochrona podstawowych praw i wolności osób fizycznych w

[4] Dz.U. nr L 281 z 23.11.1995, str. 31.
[5] Dz.U. nr L 24 z 30.01.1998, str. 1.

odniesieniu do przetwarzania danych osobowych powinna być zapewniona z uwzględnieniem art. 6 Traktatu o Unii Europejskiej. Dostęp do dokumentów, włącznie z warunkami dostępu do dokumentów zawierających dane osobowe, jest zgodny z przepisami przyjętymi na podstawie art. 255 Traktatu WE, którego zakres obejmuje tytuły V i VI Traktatu o Unii Europejskiej.

16) Niniejsze środki nie powinny mieć zastosowania do organów ustanowionych poza ramami Wspólnoty. Europejski inspektor ochrony danych nie powinien mieć uprawnień do monitorowania danych osobowych przetwarzanych przez takie organy.

17) Skuteczność ochrony osoby fizycznej w odniesieniu do przetwarzania danych osobowych w Unii zakłada spójność odpowiednich przepisów i procedur mających zastosowanie do czynności wchodzących w zakres różnych kontekstów prawnych. Rozwój podstawowych zasad ochrony danych osobowych w dziedzinie współpracy sądowej w sprawach karnych i współpracy policji oraz służb celnych, jak również ustanowienie sekretariatu dla połączonych organów nadzoru ustanowionych przez Konwencję o Europolu, Konwencję w sprawie wykorzystania technologii informatycznych do celów odpraw celnych oraz Konwencję z Schengen stanowią pierwszy krok w tym kierunku.

18) Niniejsze rozporządzenie nie ma wpływu na prawa i obowiązki Państw Członkowskich wynikające z dyrektyw 95/46/WE i 97/66/WE. Nie są przewidziane zmiany istniejących procedur i praktyk wprowadzonych w życie przez Państwa Członkowskie w dziedzinie bezpieczeństwa narodowego, zapobiegania niepokojom lub zapobiegania, wykrywania, dochodzeń i ścigania przestępstw karnych zgodnie z Protokołem w sprawie przywilejów i immunitetów Wspólnoty Europejskiej i prawem międzynarodowym.

19) Instytucje i organy wspólnotowe powinny informować właściwe władze w Państwach Członkowskich, jeżeli uważają, że połączenia w ich sieciach telekomunikacyjnych powinny być przechwytywane zgodnie z mającymi zastosowanie przepisami krajowymi.

20) Przepisy mające zastosowanie do instytucji i organów wspólnotowych powinny odpowiadać przepisom ustanowionym w związku z harmonizacją ustawodawstw krajowych i wprowadzeniem w życie innych sposobów postępowania szczególnie w sferze wzajemnej pomocy. Jednakże może być konieczne sprecyzowanie i wzbogacenie tych przepisów w zakresie zapewnienia ochrony w przypadku przetwarzania danych osobowych przez instytucje i organy wspólnotowe.

21) Dotyczy to praw osób fizycznych, których dane są przetwarzane, zobowiązań instytucji i organów wspólnotowych dokonujących przetwarzania i uprawnień nadanych niezależnemu organowi nadzoru odpowiedzialnemu za zapewnienie, że niniejsze rozporządzenie jest stosowane w odpowiedni sposób.

22) Prawa przyznane podmiotowi danych i ich wykonanie nie powinno mieć wpływu na zobowiązania kontrolującego.

23) Niezależny organ nadzoru powinien wykonywać swoje funkcje kontrolne zgodnie z Traktatem i przy poszanowaniu praw człowieka i podstawowych wolności. Powinien prowadzić swoje dochodzenia zgodnie z Protokołem w sprawie przywilejów i

immunitetów oraz regulaminem pracowniczym urzędników Wspólnot Europejskich i warunkami zatrudnienia innych pracowników Wspólnot.

24) Aby zapewnić dostęp do rejestru operacji przetwarzania przeprowadzanych przez inspektorów ochrony danych za pośrednictwem niezależnych organów nadzoru powinny być przyjęte odpowiednie środki techniczne.

25) Decyzje niezależnego organu nadzoru dotyczące wyjątków, gwarancji, upoważnienia i warunków dotyczących operacji przetwarzania danych według definicji niniejszego rozporządzenia powinny być publikowane w sprawozdaniu o działalności. Niezależnie od publikacji rocznego sprawozdania o działalności niezależne organy nadzoru mogą publikować sprawozdania o konkretnych tematach.

26) Niektóre operacje przetwarzania mogące powodować szczególne zagrożenia w odniesieniu do praw i wolności podmiotów danych, są zawczasu sprawdzane przez niezależny organ nadzoru. Opinie wyrażane w kontekście takich uprzednich kontroli, włącznie z opinią wynikającą z braku odpowiedzi, nie powinny mieć wpływu na dalsze stosowanie przez niezależny urząd nadzoru jego uprawnień w odniesieniu do wspomnianej operacji przetwarzania.

27) Przetwarzanie danych osobowych w celu przeprowadzenia czynności wykonywanych w interesie ogólnym przez instytucje i organy wspólnotowe obejmuje przetwarzanie danych osobowych niezbędnych dla zarządzania i funkcjonowania tych instytucji i organów.

28) W niektórych przypadkach przetwarzanie danych powinno być dozwolone przez przepisy wspólnotowe lub przez akty prawne przenoszące do prawa krajowego przepisy wspólnotowe. Niemniej w okresie przejściowym, w którym takie przepisy nie istnieją, oczekując na przyjęcie, europejski inspektor ochrony danych może zezwolić na przetwarzanie takich danych przy założeniu, że przyjęte są odpowiednie środki bezpieczeństwa. Robiąc to powinien w szczególności wziąć pod uwagę przepisy przyjęte przez Państwa Członkowskie w podobnych przypadkach.

29) Powyższe przypadki dotyczą przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, opinie polityczne, przekonania religijne lub filozoficzne oraz przynależność do związków zawodowych i przetwarzania danych dotyczących zdrowia lub życia seksualnego, które są konieczne dla zachowania konkretnych praw i obowiązków administratora w dziedzinie prawa pracy lub dla ważnego interesu społecznego. Dotyczą także przetwarzania danych dotyczących przestępstw, wyroków skazujących za przestępstwa i środków bezpieczeństwa oraz zezwoleń na zastosowanie decyzji do podmiotów danych, które powodują skutki prawne dla tych podmiotów lub mają na nie istotny wpływ, a które oparte są wyłącznie o automatyczne przetwarzanie danych mające na celu ocenę niektórych aspektów osobistych odnośnie podmiotu.

30) Konieczne może być monitorowanie sieci komputerowych działających pod kontrolą instytucji i organów wspólnotowych w celu zapobiegania bezprawnemu użytkowaniu. Europejski inspektor ochrony danych powinien określić, czy i pod jakimi warunkami jest to możliwe.

31) Odpowiedzialność wynikająca z każdego naruszenia niniejszego rozporządzenia

podlega akapitowi drugiemu art. 288 Traktatu.

32) W każdej instytucji lub organie Wspólnoty jeden lub więcej inspektor ochrony danych powinien zapewnić, że stosowane są przepisy niniejszego rozporządzenia i powinien doradzić administratorom w kwestii wypełniania ich zobowiązań.

33) Na mocy art. 21 rozporządzenia Rady (WE) nr 322/97 z dnia 17 lutego 1997 r. w sprawie Statystyki Wspólnoty[6], niniejsze rozporządzenie jest stosowane bez uszczerbku dla dyrektywy 95/46/WE.

34) Na mocy art. 8 ust. 8 rozporządzenia Rady (WE) nr 2533/98 z dnia 23 listopada 1998 r. dotyczącego zbierania informacji statystycznych przez Europejski Bank Centralny[7], niniejsze rozporządzenie jest stosowane bez uszczerbku dla dyrektywy 95/46/WE.

35) Na mocy art. 1 ust. 2 rozporządzenia Rady (Euroatom, EWG) nr 1588/90 z dnia 11 czerwca 1990 r. w sprawie przekazywania do Urzędu Statystycznego Wspólnot Europejskich danych będących przedmiotem poufności informacji statystycznych[8], niniejsze rozporządzenie nie uchyla specjalnych przepisów wspólnotowych lub krajowych dotyczących ochrony poufności innych niż poufność informacji statystycznych.

36) Niniejsze rozporządzenie nie zamierza ograniczać swobody działania Państw Członkowskich przy opracowywaniu ich ustawodawstw krajowych w sprawie ochrony danych na mocy art. 32 dyrektywy 95/46/WE, zgodnie z art. 249 Traktatu,

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I

PRZEPISY OGÓLNE

Artykuł 1

Zakres stosowania rozporządzenia

1. Zgodnie z niniejszym rozporządzeniem instytucje i organy ustanowione przez lub na podstawie Traktatów ustanawiających Wspólnoty Europejskie, zwane dalej „instytucjami lub organami Wspólnoty" chronią podstawowe prawa i wolności osób fizycznych, w szczególności ich prawa do prywatności w odniesieniu do przetwarzania danych osobowych i nie ograniczają ani nie zakazują swobodnego przepływu danych osobowych między nimi a odbiorcami podlegającymi prawu krajowemu Państw Członkowskich wdrażających dyrektywę 95/46/WE.

2. Niezależny organ nadzoru ustanowiony przez niniejsze rozporządzenie, zwany dalej europejskim inspektorem ochrony danych, monitoruje stosowanie przepisów niniejszego rozporządzenia do wszystkich operacji przetwarzania danych przeprowadzanych przez

[6] Dz.U. nr L 52 z 22.02.1997, str. 1.
[7] Dz.U. nr L 318 z 27.11.1998, str. 1.
[8] Dz.U. nr L 151 z 15.06.1990, str. 1. Rozporządzenie zmienione rozporządzeniem (WE) nr 322/97 (Dz.U. nr L 52 z 22.02.1997, str. 1).

instytucje lub organy Wspólnoty.

Artykuł 2

Definicje

Do celów niniejszego rozporządzenia przyjmuje się następujące definicje:

a) „dane osobowe” oznaczają wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej („podmiot danych”), 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, ujawnienie przez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, układanie lub kompilowanie, blokowanie, usuwanie lub niszczenie;

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

d) „administrator danych” oznacza instytucję lub organ Wspólnoty, dyrekcję generalną, oddział lub jakąkolwiek inną jednostkę organizacyjną, która samodzielnie lub wspólnie z innymi określa cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby przetwarzania są określone przez konkretny akt wspólnotowy, administrator i konkretne kryteria jego nominacji mogą być określone przez wspomniany akt wspólnotowy;

e) „przetwarzający” oznacza osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ przetwarzający dane osobowe w imieniu administratora danych;

f) „strona trzecia” oznacza osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ niebędący podmiotem danych, ani administratorem danych, ani przetwarzającym lub jedną z osób, które pod bezpośrednim zwierzchnictwem administratora danych lub przetwarzającego są upoważnione do przetwarzania danych;

g) „odbiorca” oznacza osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ, któremu ujawniane są dane bez względu na to, czy jest osobą trzecią czy nie; jednakże organy władzy, które mogły otrzymać dane w ramach konkretnego dochodzenia nie są uważane za odbiorcę;

h) „zgoda podmiotu danych” oznacza konkretne i świadome, dobrowolne wskazanie przez podmiot danych na to, że wyraża przyzwolenie na przetwarzanie odnoszących się do niego danych osobowych.

Artykuł 3

Zakres obowiązywania

1. Niniejsze rozporządzenie stosuje się do przetwarzania danych osobowych przez wszystkie instytucje i organy wspólnotowe, o ile takie przetwarzanie jest przeprowadzane podczas wykonywania czynności całkowicie lub częściowo podlegających prawu wspólnotowemu.

2. Niniejsze rozporządzenie 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.

ROZDZIAŁ II

OGÓLNE ZASADY LEGALNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

SEKCJA 1

ZASADY DOTYCZĄCE JAKOŚCI DANYCH

Artykuł 4

Jakość danych

1. Dane osobowe muszą być:

a) przetwarzane rzetelnie i legalnie;

b) gromadzone do konkretnych, bezpośrednich i zgodnych z prawem celów i nie przetwarzane dalej w sposób niezgodny z tymi celami. Dalsze przetwarzanie danych osobowych do celów historycznych, statystycznych lub naukowych nie jest uważane za niezgodne pod warunkiem, że administrator danych zapewnia właściwe zabezpieczenia, w szczególności zapewnia, że dane nie są przetwarzane dla żadnych celów innych niż wspomaganie środków i decyzji dotyczących dowolnej konkretnej osoby fizycznej;

c) prawidłowe, stosowne oraz nienadmierne w stosunku do celów, dla których są gromadzone i/lub przetwarzane dalej;

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) przetrzymywane w formie, która pozwala na zidentyfikowanie podmiotów danych dotyczą przez czas nie dłuższy niż jest to konieczne do celów, dla których dane były gromadzone lub dla których są przetwarzane dalej. Instytucja lub organ Wspólnoty zapewnia, że dane osobiste, które mają być przechowywane przez dłuższy czas do użytku historycznego, statystycznego lub naukowego będą przechowywane jedynie w formie anonimowej lub, jeżeli jest to niemożliwe, z zakodowaną tożsamością podmiotu

danych. W każdym razie dane nie zostaną użyte do żadnego celu innego niż cele historyczne, statystyczne lub naukowe.

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

SEKCJA 2

KRYTERIA LEGALNOŚCI PRZETWARZANIA DANYCH

Artykuł 5

Legalność przetwarzania

Dane osobowe mogą być przetwarzane tylko wtedy, gdy:

a) przetwarzanie jest konieczne, aby spełnić zadanie wykonywane w interesie publicznym na podstawie Traktatów ustanawiających Wspólnoty Europejskie bądź innych aktów prawnych przyjętych na ich podstawie lub podczas zgodnego z prawem wykonywania władzy publicznej nadanej instytucji lub organowi Wspólnoty bądź stronie trzeciej, której dane są ujawnione lub

b) przetwarzanie jest konieczne dla zgodności ze zobowiązaniem prawnym, któremu podlega administrator danych lub

c) przetwarzanie jest konieczne dla realizacji umowy, której stroną jest podmiot danych lub w celu podjęcia działań na życzenie podmiotu danych przed zawarciem umowy lub

d) podmiot danych jednoznacznie wyraził na to zgodę lub

e) przetwarzanie danych jest konieczne dla ochrony żywotnych interesów podmiotów danych.

Artykuł 6

Zmiana celu

Bez uszczerbku dla przepisów art. 4, 5 i 10:

1. Dane osobowe są przetwarzane do celów innych niż te, dla których zostały zgromadzone tylko jeżeli zmiana celu jest dozwolona wyraźnie przez wewnętrzne przepisy instytucji lub organów Wspólnoty.

2. Dane osobowe zebrane wyłącznie dla zapewnienia bezpieczeństwa lub kontroli nad systemami przetwarzania i operacjami przetwarzania nie zostaną użyte dla żadnych innych celów z wyjątkiem zapobiegania, dochodzeń, wykrywania i karania poważnych przestępstw kryminalnych.

Artykuł 7

Przekazywanie danych osobowych wewnątrz lub między instytucjami lub organami Wspólnoty

Bez uszczerbku dla przepisów art. 4, 5, 6 i 10:

1. Dane osobowe są przekazywane wewnątrz lub do innych instytucji i organów wspólnotowych tylko jeżeli są konieczne do zgodnego z prawem wykonywania zadań leżących w zakresie kompetencji odbiorcy.

2. Jeżeli dane są przekazywane na życzenie odbiorcy, zarówno administrator danych jak i odbiorca ponoszą odpowiedzialność za zgodność tego przekazania z prawem.

   Administrator danych sprawdza uprawnienia odbiorcy i dokonuje wstępnej oceny konieczności przekazania danych. Jeżeli powstają wątpliwości, co do tej konieczności, administrator danych żąda dalszych informacji od odbiorcy.

   Odbiorca zapewnia, że konieczność przekazania danych może być zweryfikowana po jego dokonaniu.

3. Odbiorca przetwarza dane osobowe tylko do celów, dla których zostały one przekazane.

Artykuł 8

Przekazanie danych osobowych odbiorcom innym niż instytucje i organy wspólnotowe podlegające dyrektywie 95/46/WE

Bez uszczerbku dla przepisów art.. 4, 5, 6 i 10 dane osobowe są przekazywane jedynie odbiorcom podlegającym prawu krajowemu przyjętemu dla wykonania dyrektywy 95/46/WE,

a) jeżeli odbiorca określa, że dane są konieczne, aby spełnić zadanie wykonywane w interesie publicznym bądź w ramach sprawowania władzy publicznej lub

b) jeżeli odbiorca określa konieczność przekazania danych i nie ma powodu zakładać, że uprawniony interes podmiotu danych może być naruszony.

Artykuł 9

Przekazanie danych osobowych odbiorcom innym niż instytucje i organy wspólnotowe nie podlegające dyrektywie 95/46/WE

1. Dane osobowe są przekazywane odbiorcom innym niż instytucje i organy wspólnotowe, a które nie podlegają prawu krajowemu przyjętemu zgodnie z dyrektywą 95/46/WE jedynie wtedy, gdy w kraju odbiorcy lub w organizacji międzynarodowej, do jakiej należy odbiorca, zapewniony jest wystarczający poziom ochrony i dane są przekazywane jedynie w celu spełnienia zadań należących do administratora danych.

2. Prawidłowość stopnia ochrony danych zapewnianej przez państwo trzecie lub organizację międzynarodową należy oceniać w świetle wszystkich okoliczności dotyczących operacji przekazania danych lub zestawu takich operacji; szczególną uwagę należy zwrócić na charakter danych, cel i czas trwania proponowanych operacji przetwarzania, państwo trzecie

będący odbiorcą lub organizację międzynarodową będącą odbiorcą, przepisy prawa, zarówno ogólnego jak i branżowego obowiązującego w państwie trzecim lub organizacji międzynarodowej, o których mowa oraz zasady zawodowe i środki bezpieczeństwa stosowane w tym państwie trzecim lub organizacji międzynarodowej.

3. Instytucje i organy wspólnotowe poinformują Komisję i europejskiego inspektora ochrony danych o przypadkach, kiedy uważają, że państwo trzecie lub organizacja nie zapewniają odpowiedniego poziomu bezpieczeństwa w rozumieniu ust. 2.

4. Komisja poinformuje Państwa Członkowskie o wszelkich przypadkach określonych w ust. 3.

5. Instytucje i organy wspólnotowe podejmą niezbędne środki dla zapewnienia zgodności z decyzjami podjętymi przez Komisję, stwierdzającymi czy zgodnie z art. 25 ust. 4 i 6 dyrektywy 95/46/WE państwo trzecie lub organizacja międzynarodowa zapewnia lub nie zapewnia odpowiedni poziomu bezpieczeństwa.

6. W drodze odstępstwa od ust. 1 i 2 instytucja lub organ Wspólnoty może przekazać dane osobowe jeżeli:

a) podmiot danych jednoznacznie udzieli zgody na proponowane przekazanie danych; lub

b) przekazanie jest konieczne dla realizacji umowy między podmiotem danych a administratorem danych lub wprowadzenia w życie środków poprzedzających umowę na wniosek podmiotu danych; lub

c) przekazanie danych jest konieczne dla zawarcia lub wykonania umowy zawartej między administratorem danych i osobą trzecią w interesie podmiotu danych; 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 jest konieczne dla ochrony żywotnych interesów podmiotu danych; lub

f) przekazanie jest wykonywane z rejestru, który zgodnie z prawem wspólnotowym ma służyć 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 danych przypadku spełnione.

7. Bez uszczerbku dla ust. 6 europejski inspektor ochrony danych może zezwolić na przekazanie lub zestaw przekazań danych osobowych państwu trzeciemu lub organizacji międzynarodowej, która nie zapewnia wystarczającego poziomu ochrony w rozumieniu ust. 1 i 2. Wówczas administrator wprowadza odpowiednie zabezpieczenia w odniesieniu do ochrony prywatności i podstawowych praw i wolności osób fizycznych oraz jeśli chodzi o korzystanie z odpowiednich praw; takie zabezpieczenia mogą w szczególności wynikać z odpowiednich klauzul umownych.

8. Instytucje i organy wspólnotowe informują europejskiego inspektora ochrony danych o kategoriach przypadków, w których stosowano ust. 6 i 7.

SEKCJA 3

SPECJALNE KATEGORIE PRZETWARZANIA DANYCH

Artykuł 10

Przetwarzanie szczególnych kategorii danych

1. Przetwarzanie danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, religijne lub wierzenia filozoficzne, przynależność do związków zawodowych i danych dotyczących zdrowia lub życia seksualnego jest zabronione.

2. Ust. 1 nie ma zastosowania, w przypadku gdy:

a) podmiot danych, udzielił wyraźnej zgody na przetwarzanie takich danych, chyba że wewnętrzne przepisy instytucji lub organu Wspólnoty mówią, że zakaz, do którego odnosi się ust. 1 nie może być uchylony przez zgodę udzieloną przez podmiot danych, lub

b) przetwarzanie jest konieczne do celów wypełnienia konkretnych praw i zobowiązań administratora w dziedzinie prawa pracy, o ile zezwala na to Traktat ustanawiający Wspólnoty Europejskie lub inne akty prawne przyjęte na jego podstawie lub udzieli na to zgody, jeśli jest to konieczne, europejski inspektor ochrony danych przy zapewnieniu odpowiednich zabezpieczeń, lub

c) przetwarzanie jest konieczne dla ochrony żywotnych interesów podmiotu danych lub innej osoby, gdy podmiot danych jest fizycznie lub prawnie niezdolny do udzielenia zgody lub

d) przetwarzanie dotyczy danych, które są podawane do wiadomości publicznej przez podmiot danych, lub jest konieczne do ustalenia, wykonania lub obrony roszczeń prawnych, lub

e) przetwarzanie jest wykonywane w trakcie zgodnych z prawem działań z odpowiednimi zabezpieczeniami przez organ nie działający dla zysku, który stanowi zintegrowaną jednostkę w ramach instytucji lub organu Wspólnoty nie podlegającą krajowemu prawu o ochronie danych na podstawie art. 4 dyrektywy 95/46/WE i ma cele polityczne, filozoficzne, religijne lub związkowe pod warunkiem, że przetwarzanie dotyczy wyłącznie członków tego organu lub do osób, które mają z nim regularny kontakt w związku z jego celami i że dane nie są ujawniane stronom trzecim bez zezwolenia podmiotów danych.

3. Ust. 1 nie ma zastosowania w przypadku, gdy przetwarzanie danych jest konieczne do celów medycyny prewencyjnej, diagnostyki medycznej, świadczenia opieki lub leczenia, lub też zarządzania opieką zdrowotną i gdy powyższe dane są przetwarzane przez pracownika służby zdrowia zobowiązanego do zachowania tajemnicy zawodowej lub przez inną osobą podlegającą równoważnemu zobowiązaniu do zachowania tajemnicy.

4. Z zastrzeżeniem przepisów dotyczących właściwych zabezpieczeń i ze względu na

istotny interes publiczny, dodatkowe zwolnienia, oprócz wynikających z ust. 2., mogą być przewidziane przez Traktaty ustanawiające Wspólnoty Europejskie lub inne akty prawne przyjęte na ich podstawie lub, jeśli to konieczne, przez decyzję europejskiego inspektora ochrony danych.

5. Przetwarzanie danych odnoszących się do przestępstw, wyroków skazujących za przestępstwa lub środków bezpieczeństwa może być przeprowadzone tylko za zezwoleniem Traktatów ustanawiających Wspólnoty Europejskie lub innych aktów prawnych przyjętych na ich podstawie lub, jeśli to konieczne, przez decyzję europejskiego inspektora ochrony danych przy zapewnieniu odpowiednich konkretnych zabezpieczeń.

6. Europejski inspektor ochrony danych określa warunki, które muszą być spełnione, aby osobisty numer identyfikacyjny lub inny identyfikator ogólnego przeznaczenia mogły być przetwarzane przez instytucje lub organ Wspólnoty.

SEKCJA 4

PRZEKAZANIE INFORMACJI PODMIOTOWI DANYCH

Artykuł 11

Informacje w przypadku uzyskiwania danych od podmiotu danych

1. Administrator dostarcza podmiotowi danych, od którego pobierane są dane odnoszące się do niego, przynajmniej następujące informacje chyba, że osoba już je posiada:

a) tożsamość administratora danych;

b) cel przetwarzania danych, do których przeznaczone są dane;

c) odbiorcy lub kategorie odbiorców danych;

d) tego, czy odpowiedzi na pytania są obowiązkowe, czy dobrowolne oraz ewentualne konsekwencje nieudzielenia odpowiedzi;

e) o prawie do dostępu do danych dotyczących tej osoby oraz do ich sprostowania;

f) wszelkich dalszych informacji, jak np.:

(i) podstawa prawna operacji przetwarzania, dla której dane są przeznaczone,

(ii) ramy czasowe, w których przechowywane będą dane,

(iii) prawo do odwołania się w każdej chwili do europejskiego inspektora ochrony danych,

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

2. W drodze odstępstwa od ust. 1 dostarczenie informacji lub jej części z wyjątkiem informacji określonych w ust. 1 lit. a, b i d może być opóźnione na tak długo, jak jest to konieczne do celów statystycznych. Informacja musi być udostępniana gdy tylko powód, dla którego jest ona niedostępna przestaje istnieć.

Artykuł 12

Informacje w przypadku uzyskiwania danych z innych źródeł niż podmiot danych

1. Gdy dane nie zostały uzyskane od podmiotu danych, administrator danych w chwili rozpoczęcia rejestrowania danych osobowych lub, jeśli przewidywane jest ich ujawnienie osobie trzeciej, lecz nie później niż w momencie, gdy dane są ujawnione po raz pierwszy, udostępni przynajmniej następujące informacje chyba, że podmiot danych już je ma:

a) tożsamość administratora danych;

b) cel przetwarzania danych;

c) kategorie potrzebnych danych;

d) odbiorcy lub kategorie odbiorców danych;

e) o prawie do dostępu do danych dotyczących tej osoby oraz do ich sprostowania

f) wszelkich dalszych informacji, jak np.

(i) podstawa prawna operacji przetwarzania, dla której dane są przeznaczone,

(ii) ramy czasowe, w których przechowywane będą dane,

(iii) prawo do odwołania się w każdej chwili do europejskiego inspektora ochrony danych,

(iv) pochodzenie danych, chyba że administrator danych nie może ujawnić tej informacji z powodu tajemnicy zawodowej,

o ile takie dalsze informacje są konieczne, biorąc od uwagę szczególne okoliczności, w których dane są gromadzone, w celu zagwarantowania rzetelnego przetwarzania danych w związku z podmiotem danych.

2. Ust. 1 nie ma zastosowania, gdy, w szczególności dla przetwarzania do celów statystycznych lub do celów historycznych lub badań naukowych, dostarczenie tej informacji okazuje się niemożliwe lub wymagałoby nieproporcjonalnego wysiłku lub, gdy zapis bądź ujawnianie są wyraźnie przewidziane przez prawo wspólnotowe. W tych przypadkach instytucja lub organ Wspólnoty zapewnia odpowiednie zabezpieczenia po konsultacji z europejskim inspektorem ochrony danych.

SEKCJA 5

PRAWA PODMIOTU DANYCH

Artykuł 13

Prawo dostępu do danych

Podmiot danych ma prawo do uzyskania od administratora danych bez ograniczeń, w dowolnym momencie w okresie trzech miesięcy od odebrania takiego życzenia przez administratora i bez opłat:

a) potwierdzenia, czy dane odnoszące się do niego są przetwarzane;

b) informacji co najmniej o celu przetwarzania odnośnych kategorii danych i odbiorców lub kategorii odbiorców, którym dane są ujawnione;

c) przekazania w zrozumiałej formie danych podlegających przetwarzaniu i wszelkich dostępnych informacji o ich źródle;

d) wiedzy o logice związanej z każdym automatycznym procesem decyzyjnym dotyczącym go.

Artykuł 14

Poprawki

Podmiot danych ma prawo uzyskania od administratora danych niezwłocznych poprawek niedokładnych lub niekompletnych danych osobowych.

Artykuł 15

Blokada

1. Podmiot danych ma prawo uzyskania od administratora danych zablokowania danych, gdy:

a) podmiot danych kwestionuje ich dokładność, na czas pozwalający administratorowi na sprawdzenie dokładności włącznie z kompletnością danych lub;

b) administrator przestał ich potrzebować do wykonania swoich zadań, ale muszą być przechowywane do celów dowodowych lub;

c) przetwarzanie jest bezprawne i podmiot danych sprzeciwia się ich wykasowaniu żądając w zamian ich zablokowania.

2. W zautomatyzowanym systemie przechowywania danych, blokowanie powinno zasadniczo być zapewnione za pomocą środków technicznych. Fakt, że dane osobowe są zablokowane powinien być wskazywany przez system w taki sposób, aby było jasne, że dane osobowe nie mogą być używane.

3. Dane osobowe zablokowane na mocy niniejszego artykułu powinny z wyjątkiem przechowywania być przetwarzane jedynie do celów dowodowych lub za zgodą podmiotu

danych lub w celu ochrony praw osoby trzeciej.

4. Podmiot danych, który zażądał i uzyskała blokowanie swoich danych ma być poinformowany przez administratora danych zanim dane zostaną odblokowane.

Artykuł 16

Kasowanie

Podmiot danych ma prawo uzyskać od administratora skasowanie danych, jeżeli ich przetwarzanie jest niezgodne z prawem, szczególnie jeśli naruszone zostały przepisy sekcji 1, 2 i 3 rozdziału II.

Artykuł 17

Powiadomienie osób trzecich

Podmiot danych ma prawo uzyskać od administratora powiadomienie stron trzecich, którym dane zostały ujawnione, o wszelkich poprawkach, skasowaniu lub blokowaniu zgodnie z art. 13 do 16, o ile nie jest to niemożliwe lub nie wymaga nieproporcjonalnego wysiłku.

Artykuł 18

Prawo sprzeciwu przysługujące podmiotowi danych

Podmiot danych ma prawo:

a) sprzeciwić się w dowolnej chwili, ze względu na ważne przyczyny prawne odnoszące się do jej konkretnej sytuacji, przetwarzaniu danych odnoszących się do niego poza przypadkami podlegającymi art. 5 lit. b, c i d. Jeżeli sprzeciw jest uzasadniony, przetwarzanie, o którym mowa, nie może dotyczyć powyższych danych;

b) zostać poinformowanym, zanim dane osobowe zostaną ujawnione osobom trzecim po raz pierwszy lub zanim zostaną użyte w ich imieniu do celów marketingu bezpośredniego i otrzymać wyraźną możliwość sprzeciwu, wolną od opłat, wobec takiego ujawnienia lub użycia.

Artykuł 19

Zautomatyzowane decyzje indywidualne

Podmiot danych ma prawo nie podlegać decyzji, która przynosi skutki prawne, które go dotyczą lub istotnie wpływają na niego i która oparta jest wyłącznie o zautomatyzowane przetwarzanie danych mające ocenić pewne osobiste aspekty odnoszące się do niego, takie jak jego wydajność pracy, solidność czy postępowanie, o ile decyzja nie jest wyraźnie uprawniona zgodnie z prawodawstwem krajowym lub legislacją wspólnotową lub, jeśli to konieczne, wyraźnie uprawomocniona przez europejskiego inspektora ochrony danych. W każdym przypadku użyte muszą być środki ochrony uprawnionych interesów podmiotu danych, takie jak ustalenia pozwalające mu na przedstawienia swojego punktu widzenia.

SEKCJA 6

ZWOLNIENIA I OGRANICZENIA

Artykuł 20

Zwolnienia i ograniczenia

1. Instytucje i organy wspólnotowe mogą ograniczyć stosowanie art. 4 ust. 1, art. 11, art. 12 ust. 1, art. 13-17 i art. 37 ust. 1, jeżeli takie ograniczenie jest środkiem koniecznym, aby chronić:

a) zapobieganie, dochodzenie, wykrywanie i karanie przestępstw;

b) ważnego interesu ekonomicznego lub finansowego Państwa Członkowskiego lub Wspólnot Europejskich, łącznie z kwestiami pieniężnymi, budżetowymi i podatkowymi;

c) ochronę podmiotu danych lub praw i wolności innych osób;

d) bezpieczeństwa narodowego, bezpieczeństwa publicznego lub obronności Państw Członkowskich;

e) funkcji kontrolnych, inspekcyjnych i regulacyjnych związanych nawet sporadycznie ze wykonywaniem władzy publicznej w przypadkach wymienionych w lit. a) i b).

2. Art. 13-16 nie mają zastosowania, gdy dane są przetwarzane jedynie do celów badań naukowych lub są przechowywane w formie osobistej przez okres nie przekraczający okresu koniecznego jedynie do celów opracowania statystyk, pod warunkiem, że jasne jest, iż nie ma ryzyka naruszenia prywatności podmiotu danych i że administrator dostarcza odpowiednie zabezpieczenia prawne, aby zapewnić w szczególności, że dane nie zostaną użyte do podejmowania środków lub decyzji dotyczących konkretnych osób fizycznych.

3. Jeżeli ustanowione jest ograniczenie przewidziane przez ust. 1, podmiot danych zostaje poinformowany zgodnie z prawem wspólnotowym o podstawowych powodach, na których opiera się stosowanie ograniczenia oraz jego prawie do odwołania się do europejskiego inspektora ochrony danych.

4. Jeżeli podmiotowi danych odmówiono dostępu do danych w oparciu o ograniczenie przewidziane przez ust. 1, europejski inspektor ochrony danych po rozważeniu skargi poinformuje go, czy dane zostały przetworzone prawidłowo i jeżeli nie, czy dokonano koniecznych poprawek.

5. Dostarczenie informacji, do których odnoszą się ust. 3 i 4 może być odłożone na tak długo, aby taka informacja nie pozbawiła efektu ograniczenia nałożonego przez ust. 1.

SEKCJA 7

POUFNOŚĆ I BEZPIECZEŃSTWO PRZETWARZANIA DANYCH

Artykuł 21

Poufność przetwarzania danych

Osoba zatrudniona w instytucji lub organie Wspólnoty oraz sam instytucja lub organ Wspólnoty, działające jako jednostka przetwarzająca posiadająca dostęp do danych osobowych, nie będzie przetwarzała ich bez instrukcji od administratora, o ile nie wymaga tego prawo krajowe lub prawo wspólnotowe.

Artykuł 22

Bezpieczeństwo przetwarzania danych

1. Uwzględniając stan wiedzy w tej dziedzinie oraz koszt realizacji, administrator wprowadza w życie właściwe środki techniczne i organizacyjne, aby zapewnić poziom bezpieczeństwa stosowny do zagrożeń stwarzanych przez przetwarzanie i charakteru chronionych danych osobowych.

Środki takie są podejmowane w szczególności, aby zapobiec nieuprawnionemu ujawnieniu lub przypadkowemu udostępnieniu lub bezprawnemu zniszczeniu, przypadkowej utracie lub zmianie i aby zapobiec wszelkim innym bezprawnym formom przetwarzania.

2. Gdy dane osobowe są przetwarzane za pomocą środków automatycznych, należy podjąć odpowiednie ze względu na ryzyko środki, w szczególności, aby:

a) zapobiec uzyskaniu dostępu do systemów komputerowych przetwarzających dane osobowe przez osoby niepowołane;

b) zapobiec wszelkim bezprawnym odczytom, kopiowaniu, zmianie lub usunięciu nośnika informacji;

c) zapobiec wszelkiemu bezprawnemu wprowadzaniu danych do pamięci, jak również wszelkiemu bezprawnemu ujawnieniu, zmianie lub kasowaniu przechowywanych danych osobowych;

d) zapobiec użyciu systemów przetwarzania danych przez osoby niepowołane za pomocą urządzeń służących do transmisji danych;

e) zapewnić, że upoważnieni użytkownicy systemów przetwarzania danych nie mają dostępu do danych osobowych innych niż te, do których odnoszą się ich prawa dostępu;

f) zapisywać, które dane osobowe zostały przekazane, kiedy i komu;

g) zapewnić, że w przyszłości będzie możliwe sprawdzenie, które dane osobowe zostały przetworzone, kiedy i przez kogo;

h) zapewnić, że dane osobowe przetwarzane w imieniu osób trzecich mogą być przetwarzane tylko w sposób przepisany przez zlecający organ lub instytucję;

i) zapewnić, że podczas przekazywania danych osobowych i transportu nośników

informacji dane nie będą czytane, kopiowane lub kasowane bez upoważnienia;

j) zaprojektować strukturę organizacyjną wewnątrz instytucji lub organu w taki sposób, aby spełniała specjalne wymagania dotyczące ochrony danych.

Artykuł 23

Przetwarzanie danych osobowych w imieniu administratorów

1. Jeżeli operacja przetwarzania jest przeprowadzana w imieniu administratora, wybiera on jednostkę przetwarzającą zapewniającą wystarczające pod względem technicznym i organizacyjnym środki bezpieczeństwa wymagane przez art. 22 oraz zapewniającą gwarancję zgodności z tymi środkami.

2. Przeprowadzanie operacji przetwarzania za pomocą jednostki przetwarzającej jest regulowane przez umowę lub akt prawny, na mocy których przetwarzający podlega administratorowi danych i które w szczególności postanawiają, że:

a) jednostka przetwarzająca działa wyłącznie na podstawie instrukcji administratora danych;

b) zobowiązania określone w art. 21 i 22 ciążą także na jednostce przetwarzającej, o ile na mocy art. 16 lub art. 17 ust. 3 tiret drugie dyrektywy 95/46/WE jednostka przetwarzająca podlega już zobowiązaniom w odniesieniu do poufności i bezpieczeństwa ustanowionym przez prawo krajowe jednego z Państw Członkowskich.

3. Do celów dowodowych, części umowy lub aktu prawnego odnoszące się do ochrony danych i wymagania dotyczące środków, do których odnosi się art. 22 są sporządzane na piśmie lub w innej równorzędnej formie.

SEKCJA 8

INSPEKTOR OCHRONY DANYCH

Artykuł 24

Powoływanie i zadania inspektora ochrony danych

1. Każda instytucja Wspólnoty i organ Wspólnoty wyznacza, co najmniej jedną osobę jako inspektora ochrony danych. Zadaniem tej osoby jest:

a) zapewnienie, że administratorzy i podmioty danych są poinformowani o swoich prawach i obowiązkach wynikających z niniejszego rozporządzenia;

b) odpowiadanie na prośby europejskiego inspektora ochrony danych i w ramach jego kompetencji współpraca z europejskim inspektorem ochrony danych na jego życzenie lub z własnej inicjatywy;

c) zapewnienie w sposób niezależny, wewnętrznego stosowania przepisów niniejszego

rozporządzenia;

d) prowadzenie rejestru operacji przetwarzania przeprowadzonych przez administratora, zawierającego informacje, do których mowa w art. 25 ust. 2;

e) powiadamianie europejskiego inspektora ochrony danych o operacjach przetwarzania, które mogą spowodować konkretne zagrożenia w rozumieniu art. 27.

W ten sposób osoba ta zapewnia, że mało prawdopodobne jest, aby operacje przetwarzania wpłynęły negatywnie na prawa i wolności podmiotów danych.

2. Inspektor ochrony danych jest wybierany na podstawie swoich osobistych i zawodowych kwalifikacji, w szczególności swojej wiedzy o ochronie danych.

3. Wybór inspektora ochrony danych nie może powodować konfliktu interesów między jego obowiązkami jako inspektora ochrony danych, a innymi oficjalnymi obowiązkami, w szczególności w odniesieniu do stosowania przepisów niniejszego rozporządzenia.

4. Inspektor ochrony danych zostaje powołany na okres dwóch do pięciu lat. Może on zostać ponownie powołany na maksymalny łączny okres dziesięciu lat. Może być zwolniony ze stanowiska inspektora ochrony danych przez instytucję lub organ Wspólnoty, która go powołała, tylko za zgodą europejskiego inspektora ochrony danych lub, jeśli przestał spełniać warunki konieczne dla wykonywania jego obowiązków.

5. Po powołaniu na stanowisko inspektor ochrony danych zostanie zarejestrowany u europejskiego inspektora ochrony danych przez instytucje lub organ, który go powołał.

6. Instytucja lub organ Wspólnoty, która powołała inspektora ochrony danych dostarczy mu personelu i zasobów koniecznych do wykonywania jego obowiązków.

7. W odniesieniu do wykonywania swoich obowiązków inspektor ochrony danych nie może otrzymywać żadnych instrukcji.

8. Dalsze przepisy wykonawcze dotyczące inspektora ochrony danych będą przyjęte przez każdy instytucję lub organ Wspólnoty zgodnie z przepisami zawartymi w załączniku. Przepisy wykonawcze w szczególności dotyczą zadań, obowiązków i uprawnień inspektora ochrony danych.

Artykuł 25

Powiadomienia skierowane do inspektora ochrony danych

1. Administrator powiadomi zawczasu inspektora ochrony danych o każdej operacji przetwarzania lub zestawie takich operacji, które mają służyć jednemu celowi lub kilku związanym celom.

2. Powyższe informacje zawierają:

a) nazwę i adres administratora i wskazanie organizacyjnej części instytucji lub organu, któremu powierzono przetwarzanie danych osobowych dla danego celu;

b) cel lub cele przetwarzania danych;

c) opis jednej lub wielu kategorii podmiotów danych i odnoszących się do nich danych lub kategorii danych;

d) podstawę prawną operacji przetwarzania, dla której przeznaczone są dane;

e) odbiorcę lub kategorie odbiorców, którym dane mogą być ujawnione;

f) ogólne wskazanie limitów czasowych, w których zostaną zablokowane lub skasowane różne kategorie danych;

g) propozycje przekazania danych do państw trzecich lub organizacji międzynarodowych;

h) ogólny opis pozwalający na wstępną ocenę, czy środki podjęte zgodnie z art. 22 w celu zapewnienia bezpieczeństwa przetwarzania są odpowiednie.

3. Inspektor ochrony danych jest niezwłocznie powiadamiany o każdej zmianie wpływającej na informacje, do których odnosi się ust. 2.

Artykuł 26

Rejestr

Inspektor ochrony danych utrzymuje rejestr operacji przetwarzania, o których został powiadomiony zgodnie z art. 25.

Rejestr zawiera przynajmniej informacje określone w art. 25 ust. 2 lit. a)-g). Rejestr może być poddany inspekcji przez każdą osobę bezpośrednio bądź pośrednio przez europejskiego inspektora przetwarzania danych.

SEKCJA 9

UPRZEDNIE SPRAWDZANIE PRZEZ EUROPEJSKIEGO INSPEKTORA OCHRONY DANYCH ORAZ ZOBOWIĄZANIA DO WSPÓŁPRACY

Artykuł 27

Kontrola wstępna

1. Operacje przetwarzania mogące ze swej natury, przez swój zakres lub swoje cele stworzyć konkretne zagrożenia dla praw i wolności podmiotów danych, podlegają uprzedniemu sprawdzeniu przez europejskiego inspektora ochrony danych.

2. Następujące operacje przetwarzania mogą stworzyć takie zagrożenia:

a) przetwarzanie danych odnoszących się do zdrowia i dotyczących podejrzeń o popełnienie przestępstwa, przestępstw, wyroków karnych lub środków bezpieczeństwa;

b) operacje przetwarzania zmierzające do oceny aspektów osobistych odnoszących się do podmiotu danych, włącznie z jego możliwościami, wydajnością lub postępowaniem;

c) operacje przetwarzania zezwalające na stworzenie powiązań między danymi przetwarzanymi dla różnych celów nieuwzględnionymi w odpowiednim ustawodawstwie krajowym lub legislacji wspólnotowej;

d) operacje przetwarzania w celu pozbawienia jednostki prawa, świadczenia lub wyłączenia jej z umowy.

3. Uprzednie sprawdzanie jest przeprowadzane przez europejskiego inspektora ochrony danych po odebraniu powiadomienia od inspektora ochrony danych, który w przypadkach wątpliwości, co do potrzeby wstępnej kontroli konsultuje się z europejskim inspektorem ochrony danych.

4. Europejski inspektor ochrony danych dostarcza swoją opinię w terminie dwóch miesięcy od odebrania powiadomienia. Ten okres może być zawieszony do momentu, gdy europejski inspektor ochrony danych otrzyma dodatkowe informacje, których mógł zażądać. Jeżeli wymaga tego stopień komplikacji sprawy, okres ten może być wydłużony o następne dwa miesiące decyzją europejskiego inspektora ochrony danych. Administrator zostanie powiadomiony o takiej decyzji przed upływem pierwszego dwumiesięcznego okresu.

Jeżeli opinia nie została dostarczona do końca dwumiesięcznego okresu lub jego przedłużenia przyjmuje się, że jest ona pozytywna.

Jeżeli według opinii europejskiego inspektora ochrony danych przetwarzanie, o którym został powiadomiony może być związane z naruszeniem jakiegokolwiek przepisu niniejszego rozporządzenia, tam gdzie jest to odpowiednie przedstawia on propozycje uniknięcia takiego naruszenia przepisów. Jeżeli administrator nie zmodyfikuje odpowiednio operacji przetwarzania, europejski inspektor ochrony danych może skorzystać z uprawnień nadanych mu na mocy art. 47 ust. 1.

5. Europejski inspektor ochrony danych utrzymuje rejestr wszystkich operacji przetwarzania, o których został powiadomiony zgodnie z ust. 2. Rejestr zawiera informacje określone w art. 25 i jest ogólnodostępny.

Artykuł 28

Konsultacje

1. Instytucje i organy wspólnotowe informują europejskiego inspektora ochrony danych, gdy podejmują środki administracyjne odnoszące się do przetwarzania danych osobowych, w których bierze udział instytucja lub organ Wspólnoty, sama lub razem z innymi.

2. Przyjmując projekty aktu prawnego odnoszącego się do ochrony praw i wolności osoby fizycznej w odniesieniu do przetwarzania danych osobowych, Komisja konsultuje się z europejskim inspektorem ochrony danych.

Artykuł 29

Obowiązek udzielania informacji

Instytucje i organy wspólnotowe informują europejskiego inspektora ochrony danych o środkach podjętych dla realizacji jego decyzji lub upoważnień, określonych w art. 46 lit h).

Artykuł 30

Obowiązek współpracy

Na jego żądanie, administratorzy wspomagają europejskiego inspektora ochrony danych w wykonaniu jego obowiązków, w szczególności przez dostarczanie informacji, do których odnosi się art. 47 ust. 2 lit. a) i przez udzielenie dostępu przewidzianego w art. 47 ust. 2 lit. b).

Artykuł 31

Obowiązek reagowania na skargi

W odpowiedzi na wykonywanie uprawnień przez europejskiego inspektora ochrony danych na mocy art. 47 ust. 1 lit. b) dany administrator informuje inspektora o swoim poglądzie w odpowiednim czasie określonym przez inspektora. Odpowiedź zawiera opis podjętych środków, jeżeli takie zostały podjęte w odpowiedzi na uwagi europejskiego inspektora ochrony danych.

ROZDZIAŁ III

ŚRODKI ODWOŁAWCZE

Artykuł 32

Środki odwoławcze

1. Trybunał Sprawiedliwości Wspólnot Europejskich jest właściwy do orzekania w sporach odnoszących się do przepisów niniejszego rozporządzenia, włącznie z wszelkimi roszczeniami odszkodowawczymi.

2. Bez uszczerbku dla jakiegokolwiek zaskarżenia, każdy podmiot danych może wnieść skargę do europejskiego inspektora ochrony danych, jeżeli uważa, że jego prawa wynikające z art. 286 Traktatu zostały naruszone w wyniku przetwarzania jego danych osobowych przez instytucję lub organ Wspólnoty.

Przy braku odpowiedzi europejskiego inspektora ochrony danych w ciągu sześciu miesięcy, skarga zostaje uznana za odrzuconą.

3. Odwołania od decyzji europejskiego inspektora ochrony danych wnoszone są do Trybunału Sprawiedliwości Wspólnot Europejskich.

4. Każda osoba, która poniosła szkodę w wyniku bezprawnej operacji przetwarzania lub jakiegokolwiek działania niezgodnego z niniejszym rozporządzeniem ma prawo do odszkodowania zgodnie z art. 288 Traktatu.

Artykuł 33

Skargi pracowników Wspólnoty

Każda osoba zatrudniona w instytucji lub organie Wspólnoty może złożyć skargę do europejskiego inspektora ochrony danych, dotyczącą domniemanego naruszenia przepisów niniejszego rozporządzenia regulującego przetwarzanie danych osobowych, bez użycia oficjalnych dróg. Nikt z góry nie przesądza konsekwencji złożenia skargi do europejskiego inspektora ochrony danych, dotyczącego domniemanego naruszenia przepisów rządzących przetwarzaniem danych osobowych.

ROZDZIAŁ IV

OCHRONA DANYCH OSOBOWYCH I PRYWATNOŚCI W KONTEKŚCIE WEWNĘTRZNYCH SIECI TELEKOMUNIKACYJNYCH

Artykuł 34

Zakres

Bez uszczerbku dla innych przepisów niniejszego rozporządzenia, niniejszy rozdział stosuje się do przetwarzania danych osobowych w połączeniu z użyciem sieci telekomunikacyjnych lub urządzeń końcowych, działających pod kontrolą instytucji lub organu Wspólnoty.

Do celów niniejszego rozdziału, „użytkownik” oznacza osobę fizyczną używającą sieci telekomunikacyjnej lub urządzenia końcowego działającego pod kontrolą instytucji lub organu Wspólnoty.

Artykuł 35

Bezpieczeństwo

1. Instytucje i organy wspólnotowe zastosują właściwe środki techniczne i organizacyjne, aby chronić bezpieczne użycie sieci telekomunikacyjnych i urządzeń końcowych, jeśli to konieczne we współpracy z dostawcami ogólnodostępnych usług telekomunikacyjnych i dostawcami publicznych sieci telekomunikacyjnych. Uwzględniając poziom techniki i koszt ich wdrożenia środki te zapewniają poziom bezpieczeństwa odpowiadający stwarzanemu zagrożeniu.

2. W przypadku szczególnego zagrożenia naruszenia bezpieczeństwa sieci i urządzeń końcowych, instytucja lub organ Wspólnoty poinformuje użytkowników o istnieniu takiego zagrożenia oraz o wszelkich środkach odwoławczych i alternatywnych sposobach komunikacji.

Artykuł 36

Poufność komunikacji

Instytucje i organy wspólnotowe zapewniają poufność komunikacji za pomocą sieci telekomunikacyjnych i urządzeń końcowych zgodnie z ogólnymi zasadami prawa

wspólnotowego.

Artykuł 37

Dane o połączeniach i dane billingowe

1. Bez uszczerbku dla przepisów ust. 2, 3 i 4 dane o połączeniach odnoszące się do użytkowników, które są przetwarzane i przechowywane w celu łączenia rozmów i innych połączeń w sieci telekomunikacyjnej są kasowane lub czynione anonimowymi w chwili zakończenia rozmowy lub innego połączenia.

2. Jeśli jest to konieczne, dane o połączeniach wskazane w wykazie, na który wyraził zgodę europejski inspektor ochrony danych mogą być przetwarzane w celu zarządzania budżetem telekomunikacyjnym i połączeniami, włącznie ze sprawdzaniem upoważnionego użycia systemów telekomunikacyjnych. Te dane będą wymazane lub uczynione anonimowymi tak szybko, jak to jest możliwe i nie później niż w sześć miesięcy po ich zebraniu, o ile nie muszą być przechowywane przez czas dłuższy w celu powstania lub zabezpieczenia roszczeń w sporze prawnym toczącym się przed sądem.

3. Przetwarzanie danych o połączeniach wykonują osoby zajmujące się zarządzaniem danymi billingowymi, połączeniami lub budżetem.

4. Użytkownicy sieci telekomunikacyjnych mają prawo otrzymać zbiorcze rachunki lub inne zapisy dotyczące wykonanych połączeń.

Artykuł 38

Spisy użytkowników

1. Dane osobowe zawarte są w drukowanych lub elektronicznych spisach użytkowników i dostęp do takich spisów jest ograniczony do tego, co jest bezwzględnie konieczne do konkretnych celów spisu.

2. Instytucje i organy wspólnotowe podejmą wszelkie dostępne środki, aby zapobiec użyciu danych osobowych zawartych w tych spisach, niezależnie od tego, czy są one ogólnodostępne czy nie, do celów marketingu bezpośredniego.

Artykuł 39

Prezentacja i zastrzeżenie numeru rozmówcy

1. Tam, gdzie oferowana jest identyfikacja rozmówcy, użytkownik dzwoniący ma możliwość prostym sposobem i wolnym od opłat wyeliminować prezentację identyfikacji swojego numeru.

2. Tam, gdzie oferowana jest identyfikacja rozmówcy, użytkownik odbierający rozmowę ma możliwość prostym sposobem i wolnym od opłat wyeliminować identyfikację numeru rozmówcy.

3. Tam, gdzie oferowana jest identyfikacja rozmówcy, użytkownik odbierający rozmowę

ma możliwość prostym sposobem i wolnym od opłat wyeliminować identyfikację swojego numeru.

4. Tam, gdzie oferowana jest identyfikacja rozmówcy, instytucje i organy wspólnotowe informują użytkowników o możliwościach określonych przez ust. 1, 2 i 3.

Artykuł 40

Odstępstwa

Instytucje i organy wspólnotowe zapewniają istnienie przejrzystych procedur regulujących sposób, w który mogą usunąć zastrzeżenie identyfikacji numeru rozmówcy dzwoniącego:

a) tymczasowo na wniosek użytkownika żądającego śledzenia dokuczliwych rozmów lub rozmów zawierających pogróżki;

b) w odniesieniu do linii dla jednostek otrzymujących telefony alarmowe w celu odpowiadania na takie telefony.

ROZDZIAŁ V

NIEZALEŻNY ORGAN NADZORU: EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Artykuł 41

Europejski inspektor ochrony danych

1. Niniejszym ustanawia się niezależny organ nadzoru nazywany europejskim inspektorem ochrony danych.

2. Europejski inspektor ochrony danych jest odpowiedzialny za zapewnienie, że podstawowe prawa i wolności osób fizycznych, w szczególności prawo do prywatności są respektowane przez instytucje i organy wspólnotowe w odniesieniu do przetwarzania danych osobowych.

Europejski inspektor ochrony danych jest odpowiedzialny za monitorowanie i zapewnienie zastosowania przepisów niniejszego rozporządzenia i każdego innego aktu wspólnotowego, odnoszącego się do podstawowych praw i wolności osób fizycznych, w odniesieniu do przetwarzania danych osobowych przez instytucje i organy wspólnotowe oraz za doradzanie instytucjom i organom wspólnotowym i podmiotom danych we wszystkich kwestiach związanych z przetwarzaniem danych osobowych. W tym celu wypełnia on obowiązki przewidziane w art. 46 i korzysta z uprawnień nadanych w art. 47.

Artykuł 42

Powoływanie

1. Parlament Europejski i Rada powołuje europejskiego inspektora ochrony danych w drodze wspólnego Porozumienia na okres pięciu lat, na podstawie listy ustalonej przez

Komisję po ogłoszeniu publicznego naboru dla kandydatów.

Zastępca inspektora, który wspomaga inspektora w wykonywaniu jego obowiązków i zastępuje go, gdy inspektor jest nieobecny lub nie może ich wypełniać, jest powoływany zgodnie z tą samą procedurą i na ten sam okres.

2. Europejski inspektor ochrony danych jest wybierany spośród osób, których niezależność jest niekwestionowana i o których wiadomo, że mają doświadczenie i umiejętności wymagane do spełniania obowiązków europejskiego inspektora ochrony danych, ponieważ na przykład należy lub należała do organów nadzoru określonych w art. 28 dyrektywy 95/46/WE.

3. Europejski inspektor ochrony danych może być powołany ponownie na to stanowiska.

4. Poza przypadkami normalnej rotacji lub śmiercią, obowiązki europejskiego inspektora ochrony danych zakończą się w przypadku rezygnacji lub przymusowej dymisji zgodnie z ust. 5.

5. Europejski inspektor ochrony danych może być zwolniony lub pozbawiony praw do emerytury lub innych świadczeń na jego rzecz przez Trybunał Sprawiedliwości na wniosek Parlamentu Europejskiego, Rady lub Komisji, jeżeli przestanie spełniać warunki wymagane dla wykonania jego obowiązków lub, jeśli jest winny poważnego uchybienia.

6. W przypadku zwykłej zmiany lub dobrowolnej rezygnacji europejski inspektor ochrony danych pełni swoją funkcję do czasu, gdy nie zostanie zastąpiony.

7. Art. 12-15 i 18 Protokołu w sprawie przywilejów i immunitetów Wspólnot Europejskich stosują się także do europejskiego inspektora ochrony danych.

8. Ust. 2-7 stosuje się do zastępcy inspektora.

Artykuł 43

Rozporządzania i ogólne warunki wypełniania obowiązków przez europejskiego inspektora ochrony danych, personel i środki finansowe

1. Parlament Europejski, Rada i Komisja w drodze wspólnego Porozumienia określą rozporządzenia i generalne warunki wykonywania obowiązków europejskiego inspektora ochrony danych, w szczególności jego płacy, przyznanych funduszy i innych świadczeń jako wynagrodzenie.

2. Władze budżetowe zapewnią, że europejski inspektor ochrony danych otrzyma zasoby ludzkie i finansowe konieczne do wykonania swoich zadań.

3. Budżet europejskiego inspektora ochrony danych jest umieszczony w osobnej pozycji budżetu w sekcji VIII ogólnego budżetu Unii Europejskiej.

4. Europejski inspektor ochrony danych jest wspomagany przez sekretariat. Urzędnicy i inny personel sekretariatu jest wyznaczany przez europejskiego inspektora ochrony danych; ich przełożonym jest europejski inspektor ochrony danych i podlegają wyłącznie jemu. Ich

liczba jest wyznaczana każdego roku jako część procedury ustalania budżetów.

5. Urzędnicy i inny personel sekretariatu europejskiego inspektora ochrony danych podlegają zasadom i rozporządzeniom mającym zastosowanie do urzędników i innego personelu Wspólnot Europejskich.

6. W kwestiach dotyczących personelu sekretariatu europejski inspektor ochrony danych posiada ten sam status, jak instytucje w rozumieniu art. 1 regulaminu pracowniczego urzędników Wspólnot Europejskich.

Artykuł 44

Niezależność

1. Europejski inspektor ochrony danych wykonuje swoje obowiązki w sposób całkowicie niezależny.

2. Europejski inspektor ochrony danych podczas wykonywania swoich obowiązków nie oczekuje i nie przyjmuje instrukcji od nikogo.

3. Europejski inspektor ochrony danych powstrzymuje się od wszelkich czynności niezgodnych ze swoimi obowiązkami i podczas swojej kadencji nie wykonuje żadnej innej zarobkowej lub niezarobkowej działalności zawodowej.

4. Europejski inspektor ochrony danych po zakończeniu swojej kadencji zachowuje się z uczciwością i dyskrecją, jeżeli chodzi o przyjmowanie zleceń i korzyści.

Artykuł 45

Tajemnica zawodowa

Europejski inspektor ochrony danych oraz jego personel, w trakcie pełnienia funkcji i po ich zakończeniu, podlega obowiązkowi zachowania tajemnicy zawodowej w odniesieniu do wszelkich poufnych informacji, które uzyskał w trakcie wykonywania oficjalnych obowiązków.

Artykuł 46

Obowiązki

Europejski inspektor ochrony danych:

a) wysłuchuje i bada skargi oraz informuje podmiot danych o wyniku w odpowiednim czasie;

b) przeprowadza dochodzenia zarówno z własnej inicjatywy, jak i na podstawie skarg oraz informuje podmioty danych, o ich wyniku w rozsądnym czasie;

c) monitoruje i zapewnia zastosowanie przepisów niniejszego rozporządzenia i każdego innego aktu wspólnotowego odnoszącego się do ochrony osób fizycznych w

odniesieniu do przetwarzania danych osobowych przez instytucję lub organ Wspólnoty, z wyjątkiem Trybunału Sprawiedliwości Wspólnot Europejskich działającego z mocy prawa;

d) doradza wszystkim instytucjom i organom wspólnotowym, albo z własnej inicjatywy, albo w odpowiedzi na konsultacje, we wszystkich kwestiach dotyczących przetwarzania danych osobowych, w szczególności zanim przyjmą przepisy wewnętrzne związane z ochroną podstawowych praw i wolności w odniesieniu do przetwarzania danych osobowych;

e) monitoruje rozwój w odpowiednich dziedzinach, o ile ma on wpływ na ochronę danych osobowych, w szczególności rozwój technologii informatycznych i telekomunikacyjnych;

f) (i) współpracuje z krajowymi organami nadzoru, do których odnosi się art. 28 dyrektywy 95/46/WE w krajach, do których ta dyrektywa ma zastosowanie, w stopniu koniecznym dla wykonywania ich obowiązków, w szczególności poprzez wymianę wszystkich użytecznych informacji i wnioskowanie, aby taka władza lub organ skorzystała ze swoich uprawnień lub odpowiadając na wniosek takiej władzy lub organu;

(ii) współpracuje także z organami nadzoru w dziedzinie ochrony danych ustanowionymi przez tytuł VI Traktatu o Unii Europejskiej, w szczególności mając na względzie poprawę spójności i zastosowania reguł i procedur, za zapewnienie zgodności z którymi są odpowiednio odpowiedzialne;

g) bierze udział w działalności grupy roboczej ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych, o którym mówi art. 29 dyrektywy 95/46/WE;

h) określa, podaje powody i ogłasza wyłączenia z zabezpieczenia, upoważnienia i warunki wspomniane w art. 10 ust. 2 lit. b), ust. 4, 5 i 6, art. 12 ust. 2, art. 19 i art. 37 ust. 2;

i) prowadzi rejestr operacji przetwarzania, o których został powiadomiony na mocy art. 27 ust. 2 i które zostały zarejestrowane zgodnie z art. 27 ust. 5 oraz zapewnia metody dostępu do rejestrów prowadzonych przez inspektorów ochrony danych na mocy art. 26;

j) przeprowadza wstępne kontrole przetwarzania, o których został powiadomiony;

k) uchwala swój regulamin wewnętrzny.

Artykuł 47

Uprawnienia

1. Europejski inspektor ochrony danych może:

a) doradzać podmiotom danych w kwestii korzystania z ich praw;

b) przekazać sprawę administratorowi w przypadku domniemanego naruszenia przepisów

rządzących przetwarzaniem danych osobowych i w miarę potrzeb, zaproponować środki prawne dla usunięcia tego naruszenia i dla poprawy ochrony podmiotów danych;

c) nakazać, aby przyjęte zostały wnioski o skorzystaniu z pewnych praw w odniesieniu do danych, gdy takie wnioski zostały odrzucone z naruszeniem art. 13-19;

d) ostrzec lub upomnieć administratora danych;

e) nakazać poprawę, zablokowanie, wykasowanie lub zniszczenie wszystkich danych, jeżeli były one przetwarzane z naruszeniem przepisów rządzących przetwarzaniem danych osobowych oraz powiadomienie o takich działaniach osób trzecich, którym dane zostały ujawnione;

f) nałożyć czasowy lub całkowity zakaz przetwarzania;

g) przekazać sprawę odpowiedniej instytucji lub organowi Wspólnoty i jeśli to konieczne Parlamentowi Europejskiemu, Radzie i Komisji;

h) przekazać sprawę Trybunałowi Sprawiedliwości Wspólnot Europejskich zgodnie z warunkami przewidzianymi w Traktacie;

i) interweniować w sprawach wniesionych przed Trybunał Sprawiedliwości Wspólnot Europejskich.

2. Europejski inspektor ochrony danych ma uprawnienia:

a) do uzyskania od administratora lub instytucji bądź organu Wspólnoty dostępu do wszystkich danych osobowych i do wszystkich informacji koniecznych dla prowadzonych przez niego dochodzeń;

b) do uzyskania dostępu do pomieszczeń, w których administrator lub instytucja bądź organ Wspólnoty prowadzi działalność jeżeli są wystarczające powody, aby przypuszczać, że prowadzona jest tam działalność podlegająca niniejszemu rozporządzeniu.

Artykuł 48

Sprawozdanie z działalności

1. Europejski inspektor ochrony danych składa roczne sprawozdanie ze swojej działalności Parlamentowi Europejskiemu, Radzie i Komisji i jednocześnie je publikuje.

2. Europejski inspektor ochrony danych przekazuje sprawozdanie z działalności innym instytucjom i organom wspólnotowym, które mogą dołączyć komentarze mając na względzie możliwe badanie sprawozdania w Parlamencie Europejskim, w szczególności w odniesieniu do opisu środków podjętych w odpowiedzi na uwagi poczynione przez europejskiego inspektora ochrony danych zgodnie z art. 31.

ROZDZIAŁ 6

PRZEPISY KOŃCOWE

Artykuł 49

Sankcje

Niedopełnienie zobowiązań wynikających z niniejszego rozporządzenia, niezależnie od tego czy celowe czy przez zaniedbanie powoduje, że urzędnik lub inny funkcjonariusz Wspólnot Europejskich podlega karze dyscyplinarnej zgodnie z regułami i procedurami ustanowionymi przez regulamin pracowniczy urzędników Wspólnot europejskich lub w warunkach zatrudnienia mających zastosowanie do innych pracowników.

Artykuł 50

Okres przejściowy

Instytucje i organy wspólnotowe zapewnią, że operacje przetwarzania będące w toku w dniu, gdy niniejsze rozporządzenie wchodzi w życie, zostaną doprowadzone do zgodności z niniejszym rozporządzeniem w ciągu roku od tej daty.

Artykuł 51

Wprowadzenie w życie

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Wspólnot Europejskich.*

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich Państwach Członkowskich.

Sporządzono w Brukseli, dnia 18 grudnia 2000 r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
N. FONTAINE	D. VOYNET
Przewodniczący	*Przewodniczący*

ZAŁĄCZNIK

1. Inspektor ochrony danych może formułować zalecenia, w zakresie praktycznego usprawnienia ochrony danych, skierowane do instytucji lub organu Wspólnoty, która go powołała i doradzać temu organowi lub instytucji i odpowiedniemu administratorowi w kwestiach związanych z zastosowaniem przepisów o ochronie danych. Co więcej, może ze swojej własnej inicjatywy lub na wniosek instytucji lub organu Wspólnoty, która go powołała, na wniosek administratora, odpowiedniego komitetu personelu lub dowolnej osoby badać sprawy i zdarzenia odnoszące się bezpośrednio do jego zadań i które zwróciły jego uwagę oraz złożyć sprawozdanie osobie, która zleciła dochodzenie bądź administratorowi.

2. Instytucja lub organ Wspólnoty, która powołała inspektora ochrony danych, odpowiedni administrator, odpowiedni komitet personelu lub dowolna osoba może skonsultować się z nim bez korzystania z kanałów oficjalnych, w każdej sprawie dotyczącej interpretacji i stosowania niniejszego rozporządzenia.

3. Nikt z góry nie przesądza w kwestii spraw, na które zwrócono uwagę odpowiedniego inspektora ochrony danych, dotyczących domniemanego naruszenia przepisów niniejszego rozporządzenia.

4. Każdy właściwy administrator ma wspomagać inspektora ochrony danych w wykonywaniu jego obowiązków i udzielić informacji w odpowiedzi na pytania. Podczas pełnienia swoich obowiązków inspektor ochrony danych ma nieustanny dostęp do wszystkich biur, urządzeń przetwarzających dane i nośników danych.

5. Inspektor ochrony danych, w wymaganym stopniu, jest zwolniony z innej działalności. Inspektor ochrony danych i jego personel, do których stosuje się art. 287 Traktatu, zobowiązani są do nieujawniania informacji lub dokumentów, które uzyskują w ramach swoich obowiązków.