brzmienie od 2009-12-19

Dyrektywa 2002/58/WE parlamentu europejskiego i rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)

z dnia 2002-07-12 (Dz.Urz.UE.L 2002 Nr 201, str. 37)
wydanie specjalne Dz.Urz.UE.WS rozdział 13 tom 29, str. 514

Zmiany aktu:

2009-12-19	**Dz.Urz.UE.L 2009**	Nr 337	poz. 11	
2006-05-03	**Dz.Urz.UE.L 2006**	Nr 105	poz. 54	Art. 11

2002-07-31

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,
uwzględniając Traktat ustanawiający Wspólnotę Europejską, w szczególności jego art. 95,
uwzględniając wniosek Komisji[1] ,
uwzględniając opinię Komitetu Ekonomiczno-Społecznego[2] ,
po konsultacji z Komitetem Regionów,
stanowiąc zgodnie z procedurą ustanowioną w art. 251 Traktatu[3] ,
a także mając na uwadze, co następuje:

(1) 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[4] wymaga od Państw Członkowskich zapewnienia osobom fizycznym praw i wolności w zakresie przetwarzania danych osobowych, w szczególności prawa do prywatności, w celu zapewnienia swobodnego przepływu danych osobowych we Wspólnocie.

(2) Niniejsza dyrektywa dąży do poszanowania fundamentalnych praw i jest zgodna z zasadami uznanymi w szczególności przez Kartę Praw Podstawowych Unii Europejskiej. W szczególności niniejsza dyrektywa zmierza do zapewnienia pełnego poszanowania praw określonych w art. 7 i 8 tej Karty.

(3) Poufność komunikacji jest zagwarantowana zgodnie z międzynarodowymi instrumentami dotyczącymi praw człowieka, w szczególności zgodnie z Europejską Konwencją o Ochronie Praw Człowieka i Podstawowych Wolności oraz z konstytucjami Państw Członkowskich.

(4) 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] przełożyła zasady ustanowione w dyrektywie 95/46/WE na zasady szczególne dla sektora telekomunikacji. Dyrektywa 97/66/WE musi zostać dostosowana do rozwoju rynków i technologii w usługach łączności elektronicznej, aby zapewnić równy poziom ochrony danych osobowych i prywatności użytkownikom dostępnych publicznie usług łączności elektronicznej, bez względu na zastosowane technologie. Ta dyrektywa powinna zatem zostać uchylona i zastąpiona niniejszą dyrektywą.

(5) W publicznych sieciach łączności we Wspólnocie wprowadza się obecnie nowe zaawansowane technologie cyfrowe, które uzasadniają wprowadzenie szczególnych wymagań dotyczących ochrony danych osobowych i prywatności użytkownika. Rozwój społeczeństwa informacyjnego charakteryzuje się wprowadzeniem nowych usług łączności elektronicznej. Cyfrowa sieć telefonii ruchomej stała się osiągalna i ogólnodostępna. Sieci cyfrowe charakteryzują się dużą pojemnością i możliwością przetwarzania danych osobowych. Pomyślny

transgraniczny rozwój takich usług jest częściowo uzależniony od pewności użytkowników, że ich prywatność nie będzie zagrożona.

(6) Internet przekształca tradycyjne struktury rynkowe przez udostępnienie ogólnej, globalnej infrastruktury dostarczającej szerokiego spektrum usług łączności elektronicznej. Usługi łączności elektronicznej ogólnodostępne za pośrednictwem internetu stwarzają nowe możliwości użytkownikom, ale również powodują powstanie nowych zagrożeń dotyczących ich danych osobowych i prywatności.

(7) W przypadku publicznych sieci łączności należy wprowadzić szczególne przepisy prawne, wykonawcze i techniczne w celu ochrony podstawowych praw i wolności osób fizycznych oraz uzasadnionego interesu osób prawnych, w szczególności w odniesieniu do zwiększonej pojemności automatycznego przechowywania i przetwarzania danych odnoszących się do abonentów i użytkowników.

(8) Przepisy prawne, wykonawcze i techniczne przyjęte przez Państwa Członkowskie dotyczące ochrony danych osobowych, prywatności i uzasadnionego interesu osób prawnych w sektorze łączności elektronicznej powinny zostać zharmonizowane w celu uniknięcia przeszkód uniemożliwiających rozwój wewnętrznego rynku łączności elektronicznej, zgodnie z art. 14 Traktatu. Harmonizacja powinna zostać ograniczona do wymogów niezbędnych do zagwarantowania, że promocja i rozwój nowych usług łączności elektronicznej oraz sieci między Państwami Członkowskimi nie napotkają przeszkód.

(9) Państwa Członkowskie, dostawcy usług i zainteresowani użytkownicy, wraz z właściwymi organami wspólnotowymi, powinni współpracować przy wprowadzaniu i rozwijaniu odpowiednich technologii w przypadku gdy jest to niezbędne w celu zastosowania gwarancji przewidzianych w niniejszej dyrektywie i ze szczególnym uwzględnieniem celów zminimalizowania przetwarzania danych osobowych oraz wykorzystywania, gdzie możliwe, danych anonimowych lub pseudoanonimowych.

(10) W sektorze łączności elektronicznej dyrektywę 95/46/WE stosuje się w szczególności do wszystkich spraw dotyczących ochrony podstawowych praw i wolności, które nie są szczegółowo objęte przepisami niniejszej dyrektywy, włączając zobowiązania nałożone na kontrolera oraz prawa jednostek. Dyrektywa 95/46/WE ma zastosowanie do niepublicznych usług łączności.

(11) Niniejsza dyrektywa, podobnie jak dyrektywa 95/46/WE, nie odnosi się do kwestii ochrony podstawowych praw i wolności związanych z działalnością, która nie jest regulowana prawem wspólnotowym. Dyrektywa nie zmienia zatem istniejącej równowagi między prawem do prywatności osoby fizycznej a możliwością Państw Członkowskich do podejmowania środków, określonych w art. 15 ust. 1 niniejszej dyrektywy, niezbędnych do ochrony bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (włączając gospodarczy dobrobyt państwa, gdy działania dotyczą zagadnień bezpieczeństwa państwa) i wykonywania prawa karnego. Wskutek tego, niniejsza dyrektywa nie wpływa na możliwości Państw Członkowskich do zgodnego z prawem przejmowania danych w łączności elektronicznej lub podejmowania innych środków, jeżeli jest to konieczne dla któregokolwiek z tych celów i zgodne z Europejską Konwencją o Ochronie Praw Człowieka i Podstawowych Wolności, dla której wykładnię stanowi orzecznictwo Europejskiego Trybunału Praw Człowieka. Środki tego rodzaju muszą być właściwe, współmierne do zamierzonego celu i niezbędne w ramach społeczeństwa demokratycznego oraz powinny podlegać stosownym zabezpieczeniom zgodnie z Europejską Konwencją o Ochronie Praw Człowieka i Podstawowych Wolności.

(12) Abonentami publicznie dostępnych usług łączności elektronicznej mogą być osoby fizyczne lub prawne. Jako uzupełnienie dyrektywy 95/46/WE niniejsza dyrektywa zmierza do ochrony podstawowych praw osób fizycznych, w szczególności ich prawa do prywatności, jak również uzasadnionych interesów osób prawnych. Niniejsza dyrektywa nie nakłada na Państwa Członkowskie obowiązku rozszerzenia zakresu stosowania dyrektywy 95/46/WE na ochronę uzasadnionych interesów osób prawnych, która jest zapewniona w ramach stosowanego prawodawstwa wspólnotowego i krajowego.

(13) Stosunek umowny między abonentem a usługodawcą może pociągać za sobą ponoszenie

opłat okresowych lub opłaty jednorazowej za usługę dostarczoną lub taką, która ma być dostarczona. Stosunek umowny powstaje również na podstawie kart opłacanych z góry.

(14) Dane o lokalizacji mogą się odnosić do szerokości, długości i wysokości terminala użytkownika, kierunku przekazu, poziomu dokładności informacji dla danej lokalizacji, identyfikacji komórki sieciowej, w której znajduje się terminal w danym momencie i do czasu, w którym informacja dla danej lokalizacji została zapisana.

(15) Komunikat może obejmować wszelkiego rodzaju nazwy, liczby lub adresy dostarczone przez nadawcę komunikatu lub użytkownika połączenia w celu przeprowadzenia łączności. Dane o ruchu mogą obejmować wszelkiego rodzaju przekształcanie tej informacji w sieci, przez którą nadawany jest komunikat, do celów przeprowadzenia operacji przesłania danych. Dane o ruchu mogą, między innymi, obejmować dane odnoszące się do wyznaczania trasy, długości, czasu lub pojemności komunikatu, zastosowanego protokołu, lokalizacji terminala nadawcy lub odbiorcy, sieci, w której komunikat powstaje lub zostaje przerwany, początku, końca lub długości połączenia. Mogą również zawierać format, w którym komunikat jest przenoszony przez sieć.

(16) Informacja, która stanowi część usług nadawczych dostarczanych za pomocą publicznej sieci łączności elektronicznej, jest przeznaczona dla potencjalnie nieograniczonej ilości odbiorców i nie stanowi komunikatu w rozumieniu niniejszej dyrektywy. Jednakże w przypadku gdy indywidualny abonent lub użytkownik otrzymujący taką informację może zostać zidentyfikowany, na przykład przez usługi typu „audycja na żądanie", przenoszona informacja stanowi komunikat do celów niniejszej dyrektywy.

(17) Do celów niniejszej dyrektywy, zgoda użytkownika lub abonenta, niezależnie od tego czy abonentem jest osoba fizyczna czy prawna, powinna mieć to samo znaczenie co zgoda podmiotu danych opisana i szerzej określona w dyrektywie 95/46/WE. Zgoda może być udzielona w jakikolwiek sposób umożliwiający swobodne i świadome wyrażenie woli użytkownika, włączając zaznaczenie okna wyboru podczas przeglądania witryny internetowej.

(18) Usługi tworzące wartość dodaną mogą, na przykład, obejmować porady dotyczące najtańszych pakietów taryfowych, zalecanych tras, informacje o ruchu, prognozy pogody i informację turystyczną.

(19) Stosowanie niektórych wymogów dotyczących wyświetlania i ograniczeń identyfikacji rozmów przychodzących i wychodzących oraz automatycznego przekazywania połączeń do łączy abonenckich podłączonych do central analogowych nie powinno być obowiązkowe w szczególnych przypadkach, w których zastosowanie tego typu rozwiązań jest technicznie niemożliwe lub wymaga nieproporcjonalnie wysokich kosztów. Istotne jest informowane zainteresowanych stron o takich przypadkach, a Państwa Członkowskie powinny powiadamiać o nich Komisję.

(20) W razie potrzeby dostawcy usług powinni podjąć, wraz z dostawcą sieci, właściwe środki w celu zagwarantowania bezpieczeństwa świadczonych usług oraz poinformować abonentów o szczególnym ryzyku naruszenia bezpieczeństwa sieci. Tego rodzaju zagrożenia mogą w szczególności pojawiać się w przypadku usług łączności elektronicznej świadczonych za pomocą otwartej sieci takiej jak internet lub analogowa telefonia komórkowa. Szczególnie ważne jest, aby abonenci i użytkownicy takich usług byli w pełni informowani przez usługodawcę o istniejących zagrożeniach bezpieczeństwa, którym zaradzenie leży poza zakresem możliwości usługodawcy. Dostawcy usług, którzy oferują publicznie dostępne usługi łączności elektronicznej przez internet powinni poinformować użytkowników i abonentów o środkach, które mogą podejmować w celu ochrony bezpieczeństwa łączności, na przykład przez zastosowanie szczególnych rodzajów oprogramowania lub technologii kodowania. Wymóg informowania abonentów o szczególnych zagrożeniach bezpieczeństwa nie zwalnia usługodawcy z obowiązku podjęcia, na własny koszt, właściwych i natychmiastowych środków zaradczych wobec nowych nieprzewidzianych rodzajów zagrożeń bezpieczeństwa oraz przywrócenia normalnego poziomu bezpieczeństwa usług. Powiadomienie abonenta o zagrożeniu bezpieczeństwa powinno być wolne od opłat z wyjątkiem kosztów nominalnych ponoszonych przez abonenta w zamian za otrzymywanie i zbieranie informacji, na przykład przez pobieranie wiadomości z poczty elektronicznej. Poziom bezpieczeństwa ocenia się w świetle przepisów art. 17 dyrektywy 95/46/WE.

(21) W celu ochrony przed niedozwolonym dostępem do komunikatów należy podjąć odpowiednie środki, aby zapewnić ochronę poufności łączności, włączając zarówno treść, jak i dane związane z tego rodzaj komunikatem, przy pomocy publicznych sieci łączności i publicznie dostępnych usług łączności elektronicznej. Ustawodawstwo krajowe w niektórych Państwach Członkowskich zabrania jedynie zamierzonego niedozwolonego dostępu do komunikatów.

(22) Zakaz przechowywania komunikatów oraz związanych z nimi danych dotyczących ruchu w sieci przez osoby inne niż użytkownicy lub bez ich zgody nie ma na celu zakazu automatycznego, pośredniego i przejściowego przechowywania takiej informacji wówczas gdy odbywa się to wyłącznie do celu przeprowadzenia transmisji w sieci łączności elektronicznej oraz pod warunkiem że informacja nie jest przechowywana przez okres dłuższy niż jest to konieczne w celu wykonania transmisji i zarządzania ruchem, oraz, że w okresie przechowywania zagwarantowana zostaje poufność. W przypadku gdy jest to niezbędne dla zwiększenia wydajności transmisji jakiejkolwiek dostępnej publicznie informacji do innych odbiorców usług na ich żądanie, niniejsza dyrektywa nie powinna uniemożliwiać dalszego przechowywania takiej informacji, pod warunkiem że informacja jest w każdym przypadku dostępna publicznie bez ograniczeń oraz, że dane o poszczególnych abonentach lub użytkownikach zamawiających taką informację zostaną usunięte.

(23) Poufność komunikacji powinna być również zapewniona w toku legalnej praktyki handlowej. Komunikaty mogą być utrwalane do celów potwierdzenia transakcji handlowych, gdy jest to konieczne i zgodne z prawem. Do tego rodzaju przetwarzania stosuje się dyrektywę 95/46/WE. Strony, do których odnosi się komunikat, powinny być poinformowane o zapisie, jego celu oraz okresie przechowywania przed rozpoczęciem zapisu. Zapisany komunikat powinien zostać usunięty jak najszybciej i w każdym przypadku najpóźniej z końcem okresu, w trakcie którego transakcja może zostać zakwestionowana zgodnie z prawem.

(24) Wyposażenie terminali użytkowników sieci łączności elektronicznej oraz informacje przechowywane na tych urządzeniach stanowią część prywatnej sfery użytkowników podlegającej ochronie na mocy Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności. Programy określane mianem spyware, błędy sieciowe, ukryte identyfikatory i inne podobne narzędzia mogą się znaleźć w terminalu użytkownika bez jego wiedzy w celu uzyskania dostępu do informacji, przechowania ukrytych informacji lub śledzenia czynności użytkownika i mogą w poważny sposób naruszyć jego prywatność. Stosowanie takich narzędzi powinno być dozwolone wyłącznie dla uzasadnionych celów, po powiadomieniu zainteresowanych użytkowników.

(25) Jednakże takie narzędzia, jak na przykład tak zwane „cookies” stanowią prawnie dopuszczalne i użyteczne narzędzie, na przykład, w analizowaniu skuteczności projektu strony internetowej i reklamy oraz w sprawdzaniu tożsamości użytkowników prowadzących transakcje w systemie on-line. W przypadku gdy takie narzędzia, na przykład „cookies”, są przeznaczone do prawnie dopuszczalnych celów, takich jak ułatwienie dostarczania usług społeczeństwa informacyjnego, ich wykorzystywanie powinno być dozwolone pod warunkiem że użytkownicy otrzymają wyraźną i dokładną informację zgodnie z dyrektywą 95/46/WE o celu „cookies” lub podobnego narzędzia w celu zapewnienia, że użytkownicy zostali zapoznani z informacją umieszczaną na użytkowanym przez nich terminalu. Użytkownicy powinni mieć możliwość odmówienia przechowywania „cookies” lub podobnego narzędzia w ich terminalu. Jest to szczególnie ważne w przypadku gdy użytkownicy inni niż użytkownik początkowy mają dostęp do terminali, a przez to do danych zawierających informacje szczególnie chronione ze względu na prywatność przechowywane na tym urządzeniu. Informacja i prawo do odmowy mogą być oferowane jednorazowo dla różnego rodzaju narzędzi instalowanych w terminalu użytkownika w czasie tego samego połączenia oraz mogą obejmować wszelkie dalsze korzystanie z tych narzędzi w trakcie kolejnych połączeń. Metody udostępniania informacji, oferujące prawo do odmowy lub wymagające zgody powinny być jak najbardziej przyjazne dla użytkownika. Dostęp do niektórych treści zamieszczonych na stronach internetowych może być nadal uzależniony od świadomej akceptacji zastosowania „cookie” lub podobnego urządzenia, jeżeli służy ono prawnie dopuszczalnemu celowi.

(26) Dane dotyczące abonentów przetwarzane w ramach sieci łączności elektronicznej w celu ustanowienia połączenia i przenoszenia informacji zawierają informacje dotyczące prywatnego

życia osób fizycznych i dotyczą prawa do poszanowania tajemnicy korespondencji lub dotyczą uzasadnionych interesów osób prawnych. Takie dane mogą być przechowywane tylko przez określony czas i wyłącznie w zakresie umożliwiającym świadczenie usług związanych z naliczaniem opłat i rozliczeń międzyoperatorskich. Wszelkie dalsze przetwarzanie tego rodzaju danych przez dostawcę publicznie dostępnych usług łączności elektronicznej do celów marketingu usług łączności elektronicznej lub w celu dostarczenia usług tworzących wartość dodaną, może być dozwolone tylko w przypadkach, gdy abonent wyraził na to zgodę na podstawie udzielonej mu przez dostawcę usług dokładnej i pełnej informacji o rodzajach zamierzonego dalszego przetwarzania oraz prawie abonenta do nieudzielenia zgody na przetwarzanie lub jej odwołania. Dane dotyczące ruchu wykorzystywane w marketingu usług komunikacyjnych lub dostarczenia usług tworzących wartość dodaną powinny również zostać usunięte lub uczynione anonimowymi po dostarczeniu usług. Dostawcy usług powinni na bieżąco informować abonentów o rodzajach danych przez nich przetwarzanych oraz celach i czasie trwania przetwarzania danych.

(27) Dokładny moment zakończenia transmisji komunikatu, po którym dane o ruchu powinny zostać usunięte, z wyjątkiem danych wykorzystywanych w celu naliczania opłat, może zależeć od rodzaju dostarczonej usługi komunikacji elektronicznej. Na przykład w przypadku połączenia z zastosowaniem telefonii głosowej, transmisja zostaje zakończona w chwili rozłączenia któregokolwiek z użytkowników. W przypadku poczty elektronicznej transmisja zostaje zakończona w chwili pobrania wiadomości przez odbiorcę, zazwyczaj z serwera usługodawcy.

(28) Obowiązek usuwania danych o ruchu lub uczynienia ich anonimowymi, gdy nie są one już potrzebne do celów transmisji komunikatu, nie koliduje z procedurami w internecie takimi jak przechwytywanie numerów IP w systemie nazw domen internetowych lub przechwytywanie numerów IP w celu łączenia ich z adresem fizycznym czy wykorzystywanie informacji dotyczących log-in w celu kontrolowania prawa dostępu do sieci lub usług.

(29) Usługodawca może przetwarzać dane o ruchu odnoszące się do abonentów i użytkowników, gdy w indywidualnych przypadkach jest to konieczne w celu wykrycia usterki technicznej lub błędów w transmisji komunikatów. Dane o ruchu niezbędne do celów naliczenia opłat mogą być również przetwarzane przez dostawcę w celu wykrywania i powstrzymywania nadużyć finansowych polegających na nieodpłatnym korzystaniu z usług łączności elektronicznej.

(30) Systemy dostarczania sieci i usług łączności elektronicznej powinny być zaprojektowane w taki sposób, aby ograniczać ilość niezbędnych danych osobowych do ścisłego minimum. Czynności związane z dostarczaniem usług łączności elektronicznej, które wykraczają poza transmisje komunikatów i naliczenia opłat za te transmisje, powinny opierać się o łączne dane o ruchu, które nie mogą być związane z abonentami i użytkownikami. W przypadku gdy takie czynności nie mogą bazować na danych łącznych, powinny zostać uznane za usługi tworzące wartość dodaną, wymagające zgody abonenta.

(31) Uzyskanie zgody na przetwarzanie danych osobowych w celu dostarczenia usług tworzących wartość dodaną od użytkownika czy od abonenta zależy od rodzaju przetwarzanych danych i rodzaju dostarczanej usługi oraz od tego, czy jest technicznie, proceduralnie i umownie możliwe, rozróżnienie czy korzystająca z usługi łączności elektronicznej osoba będąca abonentem tych usług jest osobą fizyczną czy prawną.

(32) W przypadku gdy dostawca usług łączności elektronicznej lub usług tworzących wartość dodaną zleca przetwarzanie danych osobowych niezbędnych do dostarczenia tych usług innemu podmiotowi, to podwykonawstwo i kolejne przetwarzanie danych powinno być w pełni zgodne z wymogami dotyczącymi kontrolerów i osób przetwarzających dane osobowe określonych w dyrektywie 95/46/WE. W przypadku gdy dostarczenie usług tworzących wartość dodaną wymaga, aby dane o ruchu lub dane lokalizacji były przekazywane przez dostawcę usług łączności elektronicznej dostawcy usług tworzących wartość dodaną, abonenci lub użytkownicy, których dane dotyczą, powinni być również w pełni informowani o takim przesyłaniu danych przed wyrażeniem przez nich zgody na przetwarzanie danych.

(33) Wprowadzenie szczegółowych wykazów połączeń zwiększa możliwość weryfikowania przez abonenta prawidłowości naliczania opłat przez usługodawcę, ale jednocześnie może narazić na

niebezpieczeństwo prywatność użytkownika dostępnych publicznie usług łączności elektronicznej. Dlatego też, w celu ochrony prywatności użytkowników, Państwa Członkowskie powinny zachęcać do rozwoju możliwości stosowania opcji usług łączności elektronicznej takich jak alternatywne udogodnienia w dokonywaniu płatności, które umożliwiają anonimowy lub ściśle prywatny dostęp do publicznie dostępnych usług łączności elektronicznej, na przykład karty telefoniczne i możliwość opłacania rozmów z użyciem kart kredytowych. Państwa Członkowskie mogą, w tym samym celu, wymagać od operatorów oferowania ich abonentom różnego rodzaju szczegółowych wykazów połączeń, w których zostaną usunięte niektóre cyfry wybieranych numerów telefonicznych.

(34) Konieczna jest, w odniesieniu do identyfikacji rozmów przychodzących, ochrona prawa strony wybierającej do niedopuszczenia do wyświetlania identyfikacji numeru linii wywołującej, z której wychodzi połączenie oraz prawa strony, do której połączenie przychodzi do odrzucenia rozmowy z niezidentyfikowanych linii. W niektórych przypadkach uzasadnione jest nieuwzględnienie wyeliminowania identyfikacji rozmów przychodzących. Niektórzy abonenci, w szczególności linie telefonów zaufania lub podobnych organizacji, są zainteresowani zagwarantowaniem anonimowości swoim klientom. W odniesieniu do identyfikacji rozmów wychodzących, konieczna jest ochrona prawa i uzasadnionego interesu strony wybieranej do wstrzymania wyświetlania identyfikacji numeru, z którym strona wybierająca jest aktualnie połączona, w szczególności w przypadkach połączeń przekazywanych. Dostawcy publicznie dostępnych usług łączności elektronicznej powinni informować swoich abonentów o istnieniu w sieci identyfikacji rozmów wychodzących i przychodzących, jak również o wszystkich oferowanych usługach związanych z identyfikacją rozmów wychodzących i przychodzących oraz o możliwych opcjach ochrony prywatności. Pozwoli to abonentom na podejmowanie świadomego wyboru w sprawie rodzajów możliwości ochrony prywatności, z których chcą skorzystać. Opcje ochrony prywatności oferowane dla konkretnej linii jako osobna usługa nie muszą być dostępne jako automatyczna usługa sieci, lecz na podstawie zwykłego wniosku skierowanego do dostawcy publicznie dostępnych usług łączności elektronicznej.

(35) W przypadku cyfrowej sieci telefonii ruchomej dane dotyczące lokalizacji podające położenie geograficzne terminala użytkownika są przetwarzane w celu umożliwienia transmisji komunikatu. Są to dane o ruchu objęte art. 6 niniejszej dyrektywy. Jednakże cyfrowa sieć telefonii ruchomej może posiadać zdolność przetwarzania danych dotyczących lokalizacji, które są bardziej dokładne niż dane potrzebne do transmisji komunikatu i które są stosowane do świadczenia usług tworzących wartość dodaną takich jak: usługi dostarczające indywidualne informacje o ruchu i wskazówki dla kierowców. Przetwarzanie takich danych dla usług tworzących wartość dodaną może być dozwolone wyłącznie w przypadku wyrażenia na nie zgody przez abonentów. Pomimo wyrażenia zgody na przetwarzanie abonenci powinni posiadać możliwość odmowy udzielenia zgody na przetwarzanie danych dotyczących lokalizacji przez określony czas, w prosty i bezpłatny sposób.

(36) Państwa Członkowskie mogą ograniczyć prawa użytkowników i abonentów do ochrony prywatności w odniesieniu do identyfikacji rozmów przychodzących, w przypadku gdy jest to niezbędne do śledzenia dokuczliwych telefonów oraz w odniesieniu do identyfikacji rozmów przychodzących i danych o lokalizacji, w przypadku gdy jest to konieczne do umożliwienia służbom ratunkowym wykonywania ich zadań w możliwie najbardziej efektywny sposób. Do tych celów, Państwa Członkowskie mogą przyjąć przepisy szczególne uprawniające dostawców usług łączności elektronicznej do zapewnienia dostępu do identyfikacji rozmów przychodzących oraz danych dotyczących lokalizacji bez uprzedniej zgody zainteresowanych użytkowników i abonentów.

(37) Należy zapewnić środki zabezpieczające abonentów przed uciążliwościami, które mogą być spowodowane automatycznym przekazywaniem połączeń przez inne podmioty. Ponadto, w takich przypadkach, abonenci muszą mieć możliwość zablokowania przekazywanych na ich terminale połączeń na podstawie prostego wniosku do dostawcy publicznie dostępnych usług łączności elektronicznej.

(38) Spisy abonentów usług łączności elektronicznej są szeroko dystrybuowane i dostępne publicznie. Prawo do prywatności osób fizycznych i uzasadniony interes osób prawnych wymaga,

aby abonenci mieli możliwość ustalenia, czy ich dane osobowe są publikowane w spisach abonentów, a jeśli tak, to które z nich. Dostawcy publicznych spisów abonentów powinni informować abonentów o umieszczeniu ich w tych spisach, o celach spisu i każdym możliwym wykorzystaniu wersji elektronicznej publicznych spisów abonentów, szczególnie przy pomocy dostępnej w oprogramowaniu funkcji wyszukiwania takiej jak wyszukiwanie zwrotne pozwalające użytkownikom spisu ustalenie nazwiska(nazwy) i adresu abonenta wyłącznie na podstawie numeru telefonu.

(39) Obowiązek informowania abonentów o celu(-ach) spisu abonentów w których mają być umieszczone ich dane osobowe powinien być nałożony na stronę zbierającą dane w celu takiego umieszczenia w spisie. W przypadku gdy dane będą mogły być przekazywane jednej lub więcej osób trzecich, abonent powinien zostać poinformowany o takiej możliwości oraz o odbiorcy lub kategoriach możliwych odbiorców. Każde przekazanie danych powinno mieć miejsce tylko pod warunkiem że dane nie zostaną wykorzystane do celów innych niż cele, dla których zostały zebrane. Jeżeli strona zbierająca dane od abonenta lub strona trzecia, której dane zostały przekazane, zamierza wykorzystać dane w innym celu, ponowna zgoda abonenta musi być uzyskana przez stronę zbierającą dane lub przez stronę trzecią, której dane zostały przekazane

(40) Należy zapewnić środki zabezpieczające abonentów przed ingerencją w ich prywatność przez niezamówione komunikaty do celów marketingu bezpośredniego w szczególności przez urządzenia do wywołań automatycznych, telefaksy i wiadomości z poczty elektronicznej (e-maile), w tym wiadomości SMS. Te formy niezamówionych komunikatów handlowych mogą z jednej strony być stosunkowo proste i tanie w przesyłaniu, z drugiej strony zaś mogą powodować obciążenie i/lub koszty dla odbiorcy. Ponadto, w niektórych przypadkach ich pojemność może powodować również problemy w sieci łączności elektronicznej i terminalu. W przypadku takich form niezamówionych komunikatów dotyczących marketingu bezpośredniego, uzasadnione staje się wymaganie uprzedniej wyraźnej zgody odbiorcy przed wysłaniem do niego komunikatu. Jednolity rynek wymaga zharmonizowanego podejścia w celu zapewnienia prostych reguł dla przedsiębiorców i użytkowników na terenie całej Wspólnoty.

(41) W kontekście istniejącej relacji z klientem, uzasadnione staje się zezwolenie wykorzystywania szczegółowych elektronicznych danych kontaktowych w celu oferowania podobnych produktów lub usług, ale jedynie za pośrednictwem tego samego przedsiębiorcy, który uzyskał elektroniczne dane kontaktowe zgodnie z dyrektywą 95/46/WE. Jeżeli szczegółowe elektroniczne dane kontaktowe zostały uzyskane klient powinien zostać poinformowany o przyszłym ich wykorzystywaniu do celów marketingu bezpośredniego w sposób jasny i wyraźny, oraz powinien mieć możliwość wyrażenia sprzeciwu wobec tego rodzaju wykorzystania jego danych. Taka opcja powinna być zawsze oferowana w każdej kolejnej wiadomości nadesłanej w celu marketingu bezpośredniego i powinna być wolna od opłat, z wyjątkiem kosztów transmisji odmowy.

(42) Inne formy marketingu bezpośredniego, które są bardziej kosztowne dla nadawcy i nie obciążają żadnymi kosztami abonenta czy użytkownika, takie jak połączenia telefonii głosowej między jej użytkownikami, mogą uzasadniać zachowanie systemu dającego abonentom i użytkownikom możliwość wskazania, iż nie życzą sobie otrzymywać takich połączeń. Niemniej jednak, aby nie zmniejszać istniejącego poziomu ochrony prywatności, Państwa Członkowskie powinny być uprawnione do utrzymania w mocy systemów krajowych, dopuszczających takie połączenia wyłącznie w odniesieniu do abonentów i użytkowników, którzy wyrazili na nie uprzednią zgodę.

(43) W celu ułatwienia skutecznego wykonywania reguł wspólnotowych dotyczących niezamówionych komunikatów marketingu bezpośredniego, niezbędne jest zakazanie wykorzystywania fałszywych danych określających tożsamość lub fałszywych adresów zwrotnych lub numerów w trakcie wysyłania niezamówionych komunikatów do celów marketingu bezpośredniego.

(44) Niektóre systemy poczty elektronicznej umożliwiają abonentom odczytanie informacji o nadawcy i temacie poczty elektronicznej, a także usunięcie wiadomości, bez potrzeby otwierania treści poczty elektronicznej lub jej załączników, redukując przez to koszty, które mogłyby

wyniknąć z pobrania niezamówionej poczty elektronicznej lub jej załączników. Takie ustawienia mogą być nadal użyteczne w niektórych przypadkach stanowiąc dodatkowe narzędzie w odniesieniu do ogólnych obowiązków ustanowionych w niniejszej dyrektywie.

(45) Niniejsza dyrektywa pozostaje bez uszczerbku dla uzgodnień, które Państwa Członkowskie wprowadzają w celu ochrony uzasadnionych interesów osób prawnych w odniesieniu do niezamawianych komunikatów do celów marketingu bezpośredniego. W przypadku ustanowienia przez Państwa Członkowskie rejestru opt-out w odniesieniu do tego rodzaju komunikatów kierowanych do osób prawnych, głównie użytkowników będących przedsiębiorcami, zastosowanie znajdują w całości przepisy art. 7 dyrektywy 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego, w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym)[6] .

(46) Funkcjonalne rozwiązania technologiczne wykorzystywane w celu dostarczania usług łączności elektronicznej mogą być zintegrowane w sieci lub w części terminala użytkownika, włączając w to oprogramowanie. Ochrona danych osobowych i prywatności użytkownika publicznie dostępnych usług łączności elektronicznej powinna być niezależna od konfiguracji różnego rodzaju komponentów niezbędnych do dostarczenia usługi oraz dystrybucji niezbędnych funkcji między tymi komponentami. Dyrektywa 95/46/WE obejmuje wszelkie formy przetwarzania danych osobowych bez względu na zastosowane technologie. Istnienie szczególnych przepisów dotyczących usług łączności elektronicznej obok ogólnych zasad dotyczących innych składników niezbędnych do dostarczenia tych usług może nie ułatwiać ochrony danych osobowych i prywatności w sposób technologicznie neutralny. Konieczne zatem może stać się przyjęcie środków zobowiązujących producentów niektórych typów urządzeń stosowanych w usługach łączności elektronicznej do konstruowania ich produktów w sposób uwzględniający zabezpieczenia zapewniające ochronę danych osobowych i prywatności użytkownika i abonenta. Przyjęcie tych środków zgodnie z dyrektywą 1999/5/WE Parlamentu Europejskiego i Rady z dnia 9 marca 1999 r. w sprawie urządzeń radiowych i końcowych urządzeń telekomunikacyjnych oraz wzajemnego uznawania ich zgodności[7] zapewni, że wprowadzenie cech technicznych urządzeń łączności elektronicznej, w tym oprogramowania, do celów ochrony danych, jest zharmonizowane z urzeczywistnianiem rynku wewnętrznego.

(47) W przypadku gdy prawa użytkowników i abonentów nie są przestrzegane, ustawodawstwo krajowe powinno zapewnić odpowiednie środki prawne. Kary powinny być nałożone na każdą osobę, niezależnie od tego czy podlega przepisom prawa prywatnego lub publicznego, która nie stosuje się do środków krajowych przyjętych na mocy niniejszej dyrektywy.

(48) W zakresie stosowania niniejszej dyrektywy pomocne jest uwzględnienie doświadczeń Grupy Roboczej ds. Ochrony Osób Fizycznych w Zakresie Przetwarzania Danych Osobowych złożonej z przedstawicieli organów nadzorczych Państw Członkowskich, określonych w art. 29 dyrektywy 95/46/WE.

(49) W celu zapewnienia zgodności z przepisami niniejszej dyrektywy konieczne są niektóre uzgodnienia szczególne dotyczące przetwarzania danych rozpoczętego w dniu wejścia w życie krajowych przepisów wykonawczych wynikających z niniejszej dyrektywy,

PRZYJMUJĄ NINIEJSZĄ DYREKTYWĘ:

Art. 1.

Zakres i cel

1. [8] Niniejsza dyrektywa przewiduje harmonizację przepisów krajowych wymaganych do zapewnienia równoważnego poziomu ochrony podstawowych praw i wolności, w szczególności prawa do prywatności i poufności, w odniesieniu do przetwarzania danych osobowych w sektorze łączności elektronicznej oraz w celu zapewnienia swobodnego przepływu we Wspólnocie tego typu danych oraz urządzeń i usług łączności elektronicznej.

2. Przepisy niniejszej dyrektywy dookreślają i uzupełniają dyrektywę 95/46/WE zgodnie z celami

przedstawionymi w ust. 1. Ponadto zapewniają ochronę uzasadnionych interesów abonentów będących osobami prawnymi.

3. Niniejsza dyrektywa nie ma zastosowania do działalności, która wykracza poza zakres Traktatu ustanawiającego Wspólnotę Europejską, takiej jak działalność określona w tytułach V i VI Traktatu o Unii Europejskiej, ani, w żadnym wypadku do działalności dotyczącej bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (włączając dobrobyt gospodarczy państwa, gdy działalność odnosi się do spraw bezpieczeństwa państwa) i działalności państwa w dziedzinie prawa karnego.

Art. 2.

Definicje

[9] Z zastrzeżeniem innych przepisów, stosuje się definicje z dyrektywy 95/46/WE i dyrektywy 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywa ramowa)[10] .
Stosuje się również następujące definicje:

a) "użytkownik" oznacza każdą osobę fizyczną korzystającą z publicznie dostępnych usług łączności elektronicznej, do celów prywatnych lub handlowych, niekoniecznie na podstawie abonamentu za te usługi;

b) "dane o ruchu" oznaczają wszelkie dane przetwarzane do celów przekazywania komunikatu w sieci łączności elektronicznej lub naliczania opłat za te usługi;

c) "dane dotyczące lokalizacji" oznaczają wszelkie dane przetwarzane w sieci łączności elektronicznej lub w ramach usług łączności elektronicznej, wskazujące położenie geograficzne urządzenia końcowego użytkownika publicznie dostępnych usług łączności elektronicznej;

d) "komunikat" oznacza każdą informację wymienianą lub przekazaną między określoną liczbą stron za pośrednictwem usług publicznie dostępnej łączności elektronicznej. Nie obejmuje on informacji przekazanej jako część publicznych usług nadawczych przez sieć łączności elektronicznej, z wyjątkiem zakresu, w jakim informacja może się odnosić do możliwego do zidentyfikowania abonenta lub użytkownika otrzymującego informację;

e) (*skreślona*)

f) "zgoda" użytkownika lub abonenta odpowiada zgodzie podmiotu danych określonej w dyrektywie 95/46/WE;

g) usługi tworzące wartość dodaną oznaczają wszelkie usługi, które wymagają przetwarzania danych o ruchu lub danych dotyczących lokalizacji innych niż dane o ruchu wykraczające poza dane niezbędne do transmisji komunikatu lub naliczenia za nią opłaty;

h) "poczta elektroniczna" oznacza wiadomość tekstową, głosową, dźwiękową lub obrazkową wysłaną za pośrednictwem publicznej sieci łączności, która może być przechowywana w sieci lub terminalu odbiorcy do chwili jej odebrania przez odbiorcę;

h) "naruszenie danych osobowych" oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub bezprawnego zniszczenia, utraty, zmiany, nieuprawnionego ujawnienia lub dostępu do danych osobowych przekazywanych, przechowywanych lub w inny sposób przetwarzanych w związku ze świadczeniem publicznie dostępnych usług łączności elektronicznej we Wspólnocie.

.

Art. 3.

Usługi

[11] Niniejsza dyrektywa ma zastosowanie do przetwarzania danych osobowych w związku z dostarczaniem publicznie dostępnych usług łączności elektronicznej w publicznych sieciach łączności we Wspólnocie, włącznie z publicznymi sieciami łączności służącymi do zbierania danych i obsługi urządzeń identyfikacyjnych.

Art. 4.

Bezpieczeństwo przetwarzania

[12]

1. Dostawca publicznie dostępnych usług łączności elektronicznej musi podjąć właściwe środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa oferowanych przez siebie usług, jeśli to konieczne, wraz z dostawcą publicznej sieci komunikacyjnej w odniesieniu do bezpieczeństwa sieci. Uwzględniając najnowocześniejsze osiągnięcia techniczne oraz koszty ich wprowadzenia, środki te zapewniają poziom bezpieczeństwa odpowiedni do stopnia ryzyka.

1a. [13] Bez uszczerbku dla dyrektywy 95/46/WE środki, o których mowa w ust. 1, muszą co najmniej:

- zapewniać, aby do danych osobowych mógł mieć dostęp wyłącznie uprawniony personel w dozwolonych prawem celach,
- chronić przechowywane lub przekazywane dane osobowe przed przypadkowym lub bezprawnym zniszczeniem, przypadkową utratą lub zmianą oraz nieuprawnionym lub bezprawnym przechowywaniem, przetwarzaniem, dostępem lub ujawnieniem, oraz
- zapewnić wdrożenie polityki bezpieczeństwa w odniesieniu do przetwarzania danych osobowych.

Właściwe organy krajowe muszą być w stanie kontrolować środki przyjęte przez dostawcę publicznie dostępnych usług łączności elektronicznej oraz wydawanie zaleceń dotyczących najlepszych praktyk dotyczących poziomu bezpieczeństwa, do jakiego środki te powinny prowadzić.

2. W przypadku szczególnego ryzyka naruszenia bezpieczeństwa sieci, dostawca publicznie dostępnych usług łączności elektronicznej musi poinformować abonentów o zaistniałym ryzyku i, w przypadku gdy ryzyko wykracza poza zakres środków zaradczych, które może podjąć dostawca usług, włącznie z wynikającymi z nich ewentualnymi kosztami.

3. [14] W przypadku naruszenia danych osobowych, dostawca publicznie dostępnych usług łączności elektronicznej bez zbędnej zwłoki powiadamia o tym przypadku naruszenia danych osobowych właściwy organ krajowy.

W przypadku gdy naruszenie danych osobowych może wywrzeć niekorzystny wpływ na dane osobowe lub prywatność abonenta lub osoby fizycznej, dostawca bez zbędnej zwłoki powiadamia również o takim naruszeniu abonenta lub osobę fizyczną.

Powiadomienie danego abonenta lub osoby fizycznej o naruszeniu danych osobowych nie jest wymagane, jeżeli dostawca wykazał zgodnie z wymogami właściwego organu, że wdrożył odpowiednie technologiczne środki ochrony oraz że środki te zostały zastosowane do danych, których dotyczyło naruszenie bezpieczeństwa. Tego rodzaju technologiczne środki ochrony muszą sprawiać, że dane stają się nieczytelne dla każdego, kto nie jest uprawniony do dostępu do nich.

Bez uszczerbku dla obowiązku powiadomienia przez dostawcę danych abonentów lub osób fizycznych, jeżeli dostawca nie powiadomił jeszcze abonenta lub osoby fizycznej o naruszeniu danych osobowych, właściwy organ krajowy - po rozważeniu możliwych niekorzystnych skutków tego naruszenia - może wymagać, aby dostawca to uczynił.

Powiadomienie skierowane do abonenta lub osoby fizycznej zawiera co najmniej opis charakteru naruszenia danych osobowych oraz dane punktów kontaktowych, w których można uzyskać więcej informacji; zawiera ono także informacje o zalecanych środkach mających na celu złagodzenie ewentualnych niekorzystnych skutków tego naruszenia danych osobowych. Powiadomienie właściwego organu krajowego zawiera ponadto opis konsekwencji naruszenia danych osobowych i opis proponowanych lub podjętych przez dostawcę środków mających zaradzić naruszeniu.

4. [15] Z zastrzeżeniem wszelkich technicznych środków wykonawczych przyjętych na mocy ust. 5 właściwe organy krajowe mogą przyjąć wytyczne i w razie konieczności wydać instrukcje dotyczące okoliczności, w których dostawcy zobowiązani są do powiadamiania o naruszeniu danych osobowych, a także dotyczące formy takiego powiadomienia oraz sposobu, w jaki ma być dokonane takie powiadomienie. Właściwe organy krajowe muszą mieć również możliwość kontrolowania, czy dostawcy spełniają swoje obowiązki związane z powiadamianiem określone w niniejszym ustępie, oraz nakładają odpowiednie kary w przypadku niewykonywania tych obowiązków.

Dostawcy prowadzą rejestr naruszeń ochrony danych osobowych, w tym faktów towarzyszących naruszeniom, ich skutków i podjętych działań naprawczych; rejestr ten musi być wystarczający, tak aby umożliwić właściwemu organowi krajowemu sprawdzenie zgodności z przepisami ust. 3. Rejestr zawiera wyłącznie informacje niezbędne do realizacji tego celu.

5.[16] W celu zapewnienia spójności we wdrażaniu środków, o których mowa w ust. 2, 3 i 4, Komisja - po konsultacji z Europejską Agencją ds. Bezpieczeństwa Sieci i Informacji (ENISA), Grupą Roboczą ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych powołaną na mocy art. 29 dyrektywy 95/46/WE oraz Europejskim Inspektorem Ochrony Danych - może przyjąć techniczne środki wykonawcze dotyczące okoliczności, formy i trybu mających zastosowanie do wymogów dotyczących informowania i powiadamiania, o których mowa w niniejszym artykule. Przyjmując te środki Komisja angażuje wszystkie zainteresowane strony, aby uzyskać w szczególności informacje o najlepszych dostępnych technicznych i ekonomicznych środkach wdrażania niniejszego artykułu.
Środki te, mające na celu zmianę elementów innych niż istotne niniejszej dyrektywy poprzez jej uzupełnienie, przyjmowane są zgodnie z procedurą regulacyjną połączoną z kontrolą, o której mowa w art. 14a ust. 2.

Art. 5.

Poufność komunikacji

1. Państwa Członkowskie zapewniają, poprzez ustawodawstwo krajowe, poufność komunikacji i związanych z nią danych o ruchu za pośrednictwem publicznie dostępnej sieci łączności i publicznie dostępnych usług łączności elektronicznej. W szczególności zakazują słuchania, nagrywania, przechowywania lub innych rodzajów przejęcia lub nadzoru komunikatu i związanych z nim danych o ruchu przez osoby inne niż użytkownicy, bez zgody zainteresowanych użytkowników, z wyjątkiem upoważnienia zgodnego z art. 15 ust. 1. Niniejszy ustęp nie zabrania technicznego przechowywania, które jest niezbędne do przekazania komunikatu bez uszczerbku dla zasady poufności.

2. Ustęp 1 nie dotyczy jakichkolwiek przypadków prawnie dozwolonego rejestrowania komunikatów i związanych z nimi danych o ruchu stosowanego w zgodnej z prawem praktyce handlowej do celów zapewnienia dowodów transakcji handlowej lub do celów łączności w działalności handlowej.

3.[17] Państwa członkowskie zapewniają, aby przechowywanie informacji lub uzyskanie dostępu do informacji już przechowywanych w urządzeniu końcowym abonenta lub użytkownika było dozwolone wyłącznie pod warunkiem że dany abonent lub użytkownik wyraził zgodę zgodnie z dyrektywą 95/46/WE po otrzymaniu jasnych i wyczerpujących informacji, między innymi o celach przetwarzania. Nie stanowi to przeszkody dla każdego technicznego przechowywania danych ani dostępu do nich jedynie w celu wykonania transmisji komunikatu za pośrednictwem sieci łączności elektronicznej, lub gdy jest to ściśle niezbędne w celu świadczenia usługi przez dostawcę usługi społeczeństwa informacyjnego, wyraźnie zażądanej przez abonenta lub użytkownika.

Art. 6.

Dane o ruchu

1. Dane o ruchu dotyczące abonentów i użytkowników przetwarzane i przechowywane przez dostawcę publicznej sieci łączności lub publicznie dostępnych usług łączności elektronicznej muszą zostać usunięte lub uczynione anonimowymi, gdy nie są już potrzebne do celów transmisji komunikatu, bez uszczerbku dla przepisów ust. 2, 3 i 5 niniejszego artykułu oraz art. 15 ust. 1.

2. Można przetwarzać dane o ruchu niezbędne do celów naliczania opłat abonenta i opłat rozliczeń międzyoperatorskich. Przetwarzanie takie jest dozwolone tylko do końca okresu, w którym rachunek może być zgodnie z prawem zakwestionowany lub w którym należy uiścić opłatę.

3.[18] Do celów wprowadzania na rynek usług łączności elektronicznej lub świadczenia usług tworzących wartość wzbogaconą, dostawca publicznie dostępnych usług łączności elektronicznej może przetwarzać dane określone w ust. 1, w zakresie i przez czas niezbędny dla tego rodzaju usług lub wprowadzania ich na rynek, jeżeli abonent lub użytkownik, których dane dotyczą, uprzednio wyraził na to zgodę.

Użytkownicy lub abonenci mają w każdej chwili możliwość odwołania swojej zgody na przetwarzanie danych o ruchu.

4. Dostawca usług musi poinformować abonenta lub użytkownika o rodzajach danych o ruchu, które są przetwarzane oraz o okresie tego przetwarzania do celów wymienionych w ust. 2 oraz, przed uzyskaniem zgody, do celów wymienionych w ust. 3.

5. Przetwarzanie danych o ruchu, zgodnie z ust. 1-3 i 4, musi być ograniczone do osób działających z upoważnienia dostawców publicznych sieci łączności i publicznie dostępnych usług łączności elektronicznej, zajmujących się naliczaniem opłat lub ruchem, obsługą klienta, systemem wykrywania nadużyć finansowych, marketingiem usług łączności elektronicznej lub świadczeniem usług tworzących wartość dodaną, oraz musi być ograniczone do celów niezbędnych przy takich działaniach.

6. Przepisy ust. 1-3 i 5 stosuje się bez uszczerbku dla możliwości otrzymywania przez właściwe organy informacji na temat danych o ruchu, zgodnie ze obowiązującym ustawodawstwem, w celu rozstrzygania sporów, w szczególności sporów dotyczących rozliczeń międzyoperatorskich lub naliczania opłat.

Art. 7.

Szczegółowe wykazy połączeń

1. Abonenci mają prawo do otrzymywania rachunków, które nie są szczegółowe.

2. Państwa Członkowskie stosują przepisy prawa krajowego w celu pogodzenia praw abonentów otrzymujących szczegółowe wykazy połączeń z prawem do prywatności użytkowników dzwoniących i abonentów wybieranych, na przykład przez uzyskanie pewności, że zapewniono tym użytkownikom i abonentom wystarczające, alternatywne, gwarantujące prywatność metody łączności i uiszczania opłat.

Art. 8.

Wyświetlanie i ograniczenie identyfikacji rozmów przychodzących i wychodzących

1. W przypadku gdy oferowane jest wyświetlanie identyfikacji rozmów przychodzących dostawca usług musi zaoferować użytkownikowi wybierającemu, w sposób prosty i wolny od opłat, zablokowanie wyświetlania identyfikacji rozmów przychodzących przy poszczególnych połączeniach telefonicznych. Abonent wybierający musi mieć taką możliwość w odniesieniu do każdej linii.

2. W przypadku gdy oferowane jest wyświetlanie identyfikacji rozmów przychodzących, dostawca usług musi zaoferować abonentowi wybieranemu, w sposób prosty i wolny od opłat w przypadku uzasadnionego korzystania z tej funkcji, zablokowanie wyświetlania identyfikacji rozmów przychodzących.

3. W przypadku gdy oferowane jest wyświetlanie identyfikacji rozmów przychodzących oraz w przypadku gdy wyświetlenie identyfikacji rozmowy przychodzącej następuje przed rozpoczęciem połączenia, dostawca usługi musi zaoferować abonentowi wybieranemu możliwość odrzucenia, w prosty sposób, rozmów przychodzących, gdy wyświetlanie identyfikacji rozmowy przychodzącej zostało zablokowane przez użytkownika lub abonenta wybierającego.

4. W przypadku gdy oferowane jest wyświetlanie identyfikacji rozmów wychodzących, dostawca usług musi zaoferować abonentowi wybieranemu, w sposób prosty i wolny od opłat, zablokowanie wyświetlania identyfikacji rozmów wychodzących u użytkownika wybierającego.

5. Przepisy ust. 1 stosuje się również w odniesieniu do połączeń do państw trzecich wychodzących ze Wspólnoty. Przepisy ust. 2, 3 i 4 stosuje się również do rozmów przychodzących z państw trzecich.

6. W przypadku gdy oferowane jest wyświetlanie identyfikacji rozmów przychodzących i/lub wychodzących Państwa Członkowskie zapewniają, że dostawcy publicznie dostępnych usług łączności elektronicznej podają do wiadomości publicznej informację na ten temat oraz na temat możliwości określonych w ust. 1-3 i 4.

Art. 9.

Dane dotyczące lokalizacji inne niż dane o ruchu

1. W przypadku gdy dane dotyczące lokalizacji inne niż dane o ruchu, odnoszące się do użytkowników lub abonentów publicznych sieci łączności lub publicznie dostępnych usług łączności elektronicznej, mogą być przetwarzane, przetwarzanie może mieć miejsce tylko wówczas gdy dane te są anonimowe, lub za zgodą użytkowników lub abonentów, w zakresie i przez okres niezbędny do świadczenia usługi tworzącej wartość dodaną. Przed uzyskaniem zgody użytkowników lub abonentów dostawca usług musi ich poinformować o rodzaju danych dotyczących lokalizacji innych niż dane o ruchu, które będą przetwarzane, o celach i okresie ich przetwarzania oraz o tym, czy dane zostaną przekazane stronie trzeciej do celów świadczenia usługi tworzącej wartość dodaną. Użytkownicy lub abonenci mają możliwość odwołania w każdej chwili swojej zgody na przetwarzanie danych dotyczących lokalizacji innych niż dane o ruchu.

2. W przypadku gdy uzyskana została zgoda użytkowników lub abonentów na przetwarzanie danych dotyczących lokalizacji innych niż dane o ruchu, użytkownik lub abonent musi nadal posiadać możliwość, w sposób prosty i wolny od opłat, czasowego odwołania zgody na przetwarzanie tych danych w przypadku każdego połączenia z siecią lub każdej transmisji komunikatu.

3. Przetwarzanie danych dotyczących lokalizacji innych niż dane o ruchu, zgodnie z ust. 1 i 2, musi być ograniczone do osób działających z upoważnienia dostawcy publicznej sieci łączności lub publicznie dostępnych usług łączności elektronicznej lub strony trzeciej świadczącej usługę tworząc a wartość dodaną oraz musi być ograniczone do celów niezbędnych do świadczenia usługi tworzącej wartość dodaną.

Art. 10.

Wyjątki

Państwa Członkowskie zapewniają, że posiadają przejrzyste procedury regulujące sposób, w jaki dostawca publicznej sieci łączności i/lub publicznie dostępnych usług łączności elektronicznej może pominąć:

a) zablokowanie wyświetlania identyfikacji rozmów przychodzących, tymczasowo, na wniosek abonenta o ustalenie numerów linii w przypadku otrzymywania dokuczliwych lub złośliwych telefonów. W takich przypadkach, zgodnie z prawem krajowym, dane zawierające identyfikację abonenta dzwoniącego są przechowywane i mogą być udostępnione przez dostawcę publicznej sieci łączności i/lub publicznie dostępnych usług łączności elektronicznej;

b) zablokowanie wyświetlania identyfikacji rozmów przychodzących i czasową odmowę lub brak zgody abonenta lub użytkownika na przetwarzanie danych o lokalizacji, w przypadku poszczególnych linii dla organizacji zajmujących się połączeniami alarmowymi i uznanymi przez Państwo Członkowskie za organizacje pełniące takie funkcje, włączając organy przestrzegania prawa, pogotowie ratunkowe i straż pożarną, do celów odpowiadania na takie połączenia.

Art. 11.

Automatyczne przekazywanie połączeń

Państwa Członkowskie zapewniają, że każdy abonent, w sposób prosty i wolny od opłat, posiada możliwość zablokowania automatycznego przekazywania połączeń przez stronę trzecią do terminala tego abonenta.

Art. 12.

Spisy abonentów

1. Państwa Członkowskie zapewniają, że abonenci są informowani w sposób wolny od opłat oraz przed umieszczeniem ich danych w spisach abonentów, o celu(-ach) spisów abonentów wydawanych w formie druku lub elektronicznej, publicznie dostępnych lub uzyskiwanych w telefonicznej informacji o numerach, w których ich dane osobowe mogą się znajdować oraz o wszelkich dalszych możliwościach wykorzystania na podstawie funkcji wyszukiwania znajdującej się w wersji elektronicznej spisu.

2. Państwa Członkowskie zapewniają, że abonenci posiadają możliwość ustalenia czy ich dane osobowe znajdują się w publicznym spisie abonentów, a jeżeli tak, to które, w zakresie, w jakim te dane są niezbędne do celu spisu abonentów określonego przez dostawcę spisu abonentów i sprawdzania, poprawiania lub wycofywania tych danych. Zastrzeżenie numeru, sprawdzanie, poprawianie lub wycofywanie danych osobowych ze spisu abonentów jest wolne od opłat.

3. Państwa Członkowskie mogą wymagać, aby dla jakiegokolwiek celu publicznego spisu abonentów innego niż przeszukiwanie danych do kontaktu osób, na podstawie podania ich nazwiska oraz, w miarę potrzeb, minimalnej ilości innych danych identyfikacyjnych, wymagana była dodatkowa zgoda abonentów.

4. Przepisy ust. 1 i 2 stosuje się do abonentów będących osobami fizycznymi. Państwa Członkowskie zapewniają również, że, w ramach prawa wspólnotowego i obowiązującego ustawodawstwa krajowego, uzasadnione interesy abonentów innych niż osoby fizyczne, w odniesieniu do ich umieszczenia w publicznych spisach abonentów, posiadają wystarczającą ochronę.

Art. 13.

Komunikaty niezamówione

[19]

1.[20] Używanie automatycznych systemów wywołujących i systemów łączności bez ludzkiej ingerencji (automatyczne urządzenia wywołujące), faksów lub poczty elektronicznej do celów marketingu bezpośredniego może być dozwolone jedynie wobec abonentów lub użytkowników, którzy uprzednio wyrazili na to zgodę.

2.[21] Niezależnie od przepisów ust. 1, w przypadku gdy osoba fizyczna lub prawna otrzymuje od swoich klientów szczegółowe elektroniczne dane kontaktowe dotyczące kontaktu z nimi za pomocą poczty elektronicznej, w kontekście sprzedaży produktu lub usługi, zgodnie z dyrektywą 95/46/WE, ta sama osoba fizyczna lub prawna może używać tych szczegółowych elektronicznych danych kontaktowych na potrzeby marketingu bezpośredniego swoich własnych podobnych produktów lub usług, pod warunkiem że klienci zostali jasno i wyraźnie poinformowani o możliwości sprzeciwienia się, w prosty i wolny od opłat sposób, takiemu wykorzystywaniu elektronicznych danych kontaktowych w chwili ich pobierania oraz przy każdej okazji otrzymywania wiadomości, w przypadku klientów, którzy początkowo nie sprzeciwili się takiemu wykorzystywaniu.

3.[22] Państwa członkowskie podejmują odpowiednie środki w celu zapewnienia, aby niezamówione komunikaty do celów marketingu bezpośredniego, w przypadkach innych niż określone w ust. 1 i 2, nie były dozwolone bez zgody abonentów lub użytkowników bądź w odniesieniu do abonentów lub użytkowników, którzy nie życzą sobie otrzymywania tego typu komunikatów, przy czym wybór między tymi opcjami zostaje ustalony przez przepisy krajowe, z uwzględnieniem faktu, że obie te opcje muszą być dla abonenta lub użytkownika bezpłatne.

4.[23] W każdym przypadku zakazana jest praktyka wysyłania poczty elektronicznej do celów marketingu bezpośredniego, która ukrywa lub zataja tożsamość nadawcy, w którego imieniu wysyłany jest komunikat, lub która narusza art. 6 dyrektywy 2000/31/WE, oraz bez ważnego adresu, na który odbiorca może wysłać żądanie zaprzestania takich komunikatów, lub która zachęca odbiorców do odwiedzenia stron internetowych naruszających ten artykuł dyrektywy 2000/31/WE.

5.[24] Ust. 1 i 3 stosują się do abonentów będących osobami fizycznymi. Państwa członkowskie zapewniają również, aby - w ramach prawa wspólnotowego oraz mających zastosowanie przepisów krajowych - uzasadnione interesy abonentów innych niż osoby fizyczne były wystarczająco chronione w związku z uciążliwymi komunikatami.

6.[25] Bez uszczerbku dla jakichkolwiek środków administracyjnych, w odniesieniu do których mogą zostać przyjęte przepisy, między innymi na mocy art. 15a ust. 2, państwa członkowskie zapewniają, aby każda osoba fizyczna lub prawna, która odczuła negatywne skutki naruszeń przepisów krajowych przyjętych na mocy niniejszego artykułu i mająca uzasadniony interes w tym, by położyć kres takim naruszeniom lub ich zakazać, w tym także dostawca usług łączności elektronicznej chroniący własne uzasadnione interesy gospodarcze, mogła podjąć działania prawne przeciwko takim naruszeniom.

Państwa członkowskie mogą także ustalić szczególne zasady dotyczące sankcji mających zastosowanie do dostawców usług łączności elektronicznej, którzy przez zaniedbanie przyczyniają się do naruszeń przepisów krajowych przyjętych na podstawie niniejszego artykułu.

Art. 14.

Charakterystyka techniczna i normalizacja

1. Przy wykonywaniu przepisów niniejszej dyrektywy, Państwa Członkowskie zapewniają, z zastrzeżeniem przepisów ust. 2 i 3, że nie zostaną nałożone żadne wymagania obowiązkowe dotyczące szczególnej charakterystyki technicznej terminali lub innych urządzeń łączności elektronicznej, które mogłyby utrudniać wprowadzanie urządzeń na rynek oraz do swobodnego obrotu w i między Państwami Członkowskimi.

2. W przypadkach gdy przepisy niniejszej dyrektywy mogą być wykonywane wyłącznie przez wprowadzenie wymogu szczególnych cech technicznych w sieci łączności elektronicznej, Państwa Członkowskie powiadamiają Komisję, zgodnie z procedurą przewidzianą w dyrektywie 98/34/WE Parlamentu Europejskiego i Rady z dnia 22 czerwca 1998 r. ustanawiającej procedurę udzielania informacji w zakresie norm i przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego[26] .

3. W miarę potrzeb, możliwe jest przyjęcie środków w celu zapewnienia, że terminal jest skonstruowany w sposób zgodny z prawem użytkowników do ochrony i kontroli używania ich danych osobowych, zgodnie z dyrektywą 1999/5/WE i decyzją Rady 87/95/EWG z dnia 22 grudnia 1986 r. w sprawie normalizacji w dziedzinie technologii informatycznych i telekomunikacji[27] .

Art. 14a.

Procedura komitetowa

[28]

1.[29] Komisja wspierana jest przez Komitet ds. Łączności ustanowiony na mocy art. 22 dyrektywy 2002/21/WE (dyrektywa ramowa).

2.[30] W przypadku odesłania do niniejszego ustępu, stosuje się art. 5a ust. 1-4 i art. 7 decyzji 1999/468/WE, z uwzględnieniem przepisów jej art. 8.

3.[31] W przypadku odesłania do niniejszego ustępu, stosuje się art. 5a ust. 1, 2, 4 i 6 oraz art. 7 decyzji 1999/468/WE, z uwzględnieniem przepisów jej art. 8.

Art. 15.

Stosowanie niektórych przepisów dyrektywy 95/46/WE

1. Państwa Członkowskie mogą uchwalić środki ustawodawcze w celu ograniczenia zakresu praw i obowiązków przewidzianych w art. 5, 6, art. 8 ust. 1-4, i art. 9 tej dyrektywy, gdy takie ograniczenia stanowią środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego (i.e. bezpieczeństwa państwa), obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej, jak określono w art. 13 ust. 1 dyrektywy 95/46/WE. W tym celu, Państwa Członkowskie mogą, między innymi, uchwalić środki ustawodawcze przewidujące przechowywanie danych przez określony czas uzasadnione na podstawie zasad ustanowionych w niniejszym ustępie. Wszystkie środki określone w niniejszym ustępie są zgodne z ogólnymi zasadami prawa wspólnotowego, w tym zasadami określonymi w art. 6 ust. 1 i 2 Traktatu o Unii Europejskiej.

1a.[32] Ustępu 1 nie stosuje się do danych, których zatrzymywanie jest wyraźnie wymagane na mocy dyrektywy 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie

zatrzymywania danych wygenerowanych lub przetworzonych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności dla celów określonych w art. 1 ust. 1 tej dyrektywy.

1b. [33] Dostawcy ustanawiają wewnętrzne procedury odpowiedzi na wnioski o dostęp do danych osobowych użytkownika w oparciu o krajowe przepisy przyjęte zgodnie z art. 1. Na żądanie przedstawiają oni właściwemu organowi krajowemu informacje o tych procedurach, liczbie otrzymanych wniosków, ich uzasadnieniu prawnym oraz udzielonej przez nich odpowiedzi.

2. Przepisy rozdziału III dotyczącego środków zaskarżenia, odpowiedzialności i sankcji dyrektywy 95/46/WE stosuje się w odniesieniu do przepisów krajowych przyjętych zgodnie z niniejszą dyrektywą i w odniesieniu do indywidualnych uprawnień wynikających z niniejszej dyrektywy.

3. Grupa Robocza ds. Ochrony Osób Fizycznych w Zakresie Przetwarzania Danych Osobowych powołana zgodnie z art. 29 dyrektywy 95/46/WE podejmuje również zadania ustanowione w art. 30 wspomnianej dyrektywy w odniesieniu do spraw objętych niniejszą dyrektywą, mianowicie ochrony podstawowych praw i wolności oraz uzasadnionego interesu w sektorze łączności elektronicznej.

Art. 15a.

Wdrażanie i egzekwowanie

[34]

1. Państwa członkowskie ustanawiają przepisy dotyczące kar, w tym w stosownych przypadkach sankcji karnych, mających zastosowanie w przypadku naruszeń krajowych przepisów przyjętych zgodnie z niniejszą dyrektywą, i podejmują wszelkie niezbędne środki w celu zapewnienia, aby zasady te zostały wdrożone. Przewidziane sankcje muszą być skuteczne, proporcjonalne i odstraszające oraz mogą być stosowane w odniesieniu do okresu, w którym występowało jakiekolwiek naruszenie, nawet w przypadku gdy naruszenie to następnie naprawiono. Państwa członkowskie powiadamiają Komisję o tych przepisach najpóźniej do dnia 25 maja 2011 r. i powiadamiają ją niezwłocznie o wszelkich późniejszych zmianach mających na nie wpływ.

2. Bez uszczerbku dla wszelkich ewentualnie dostępnych środków prawnych, państwa członkowskie zapewniają, aby właściwy organ krajowy oraz, w stosownych przypadkach, inne podmioty krajowe dysponowały uprawnieniami do nakazania zaprzestania naruszeń, o których mowa w ust. 1.

3. Państwa członkowskie zapewniają, aby właściwe organy krajowe oraz, w stosownych przypadkach, inne podmioty krajowe dysponowały uprawnieniami i środkami niezbędnymi do prowadzenia dochodzeń, w tym uprawnieniami do uzyskiwania wszelkich istotnych informacji, których mogą potrzebować, aby monitorować i egzekwować przestrzeganie przepisów krajowych przyjętych zgodnie z niniejszą dyrektywą.

4. Właściwe krajowe organy regulacyjne mogą przyjmować środki w celu zapewnienia efektywnej współpracy transgranicznej w zakresie egzekwowania przepisów krajowych przyjętych zgodnie z niniejszą dyrektywą oraz tworzenia zharmonizowanych warunków świadczenia usług obejmujących transgraniczny przepływ danych.
Krajowe organy regulacyjne przekazują Komisji - w odpowiednim czasie przed przyjęciem takich środków - podsumowanie podstawy do działania, przewidywane środki i proponowany przebieg działań. Po zbadaniu takich informacji oraz konsultacjach z ENISA i Grupą Roboczą ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych ustanowioną na mocy art. 29 dyrektywy 95/46/WE, Komisja może zgłaszać do nich uwagi lub wydawać zalecenia, w szczególności w celu zapewnienia, aby przewidywane środki nie wpływały niekorzystnie na funkcjonowanie rynku wewnętrznego. Przy podejmowaniu decyzji dotyczącej omawianych środków krajowe organy regulacyjne uwzględniają w jak największym stopniu uwagi lub zalecenia Komisji.

Art. 16.

Przepisy przejściowe

1. Przepisów art. 12 nie stosuje się do publikacji spisów abonentów już wydanych lub wprowadzonych do obrotu w wersji drukowanej lub w elektronicznej formie off-line przed wejściem w życie przepisów krajowych przyjętych stosownie do niniejszej dyrektywy.

2. W przypadku gdy dane osobowe abonentów usług stacjonarnej lub przenośnej publicznej telefonii głosowej są zawarte w publicznym spisie abonentów, zgodnie z przepisami dyrektywy 95/46/WE i art. 11 dyrektywy 97/66/WE, przed wejściem w życie przepisów prawa krajowego przyjętych na mocy niniejszej dyrektywy, dane osobowe tych abonentów mogą pozostać w tym spisie abonentów w wersji drukowanej lub elektronicznej, włączając wersje ze zwrotnymi funkcjami wyszukiwania, chyba że abonenci, po otrzymaniu pełnej informacji o celach i opcjach zgodnie z art. 12 niniejszej dyrektywy, oświadczą inaczej.

Art. 17.

Transpozycja

1. Przed dniem 31 października 2003 r. Państwa Członkowskie wprowadzą w życie przepisy niezbędne do wykonania niniejszej dyrektywy i niezwłocznie powiadomią o tym Komisję.
Przepisy przyjęte przez Państwa Członkowskie zawierają odniesienie do niniejszej dyrektywy lub odniesienia takie towarzyszy ich urzędowej publikacji. Państwa Członkowskie określają metody dokonywania takich odniesień.

2. Państwa Członkowskie przekażą Komisji teksty przepisów prawa krajowego, które przyjmą w dziedzinie regulowanej niniejszą dyrektywą oraz każdej kolejnej zmiany tych przepisów.

Art. 18.

Przegląd

Komisja przekazuje Parlamentowi Europejskiemu i Radzie, najpóźniej trzy lata od dnia, określonego w art. 17 ust. 1, sprawozdanie w sprawie stosowania niniejszej dyrektywy i jej wpływu na podmioty gospodarcze i konsumentów, w szczególności w odniesieniu do przepisów o niezamówionych komunikatach, uwzględniając otoczenie międzynarodowe. W tym celu, Komisja może żądać informacji od Państw Członkowskich, które powinny być dostarczone bez zbędnej zwłoki. Komisja przedkłada, gdzie stosowne, wnioski w sprawie zmian niniejszej dyrektywy, uwzględniając wyniki tego sprawozdania, wszelkie zmiany w sektorze oraz wszelkie inne wnioski, które uzna za niezbędne w celu poprawy skuteczności stosowania niniejszej dyrektywy.

Art. 19.

Uchylenie

Dyrektywa 97/66/WE traci moc z dniem określonym w art. 17 ust. 1.
Odniesienia do uchylonej dyrektywy traktuje się jak odniesienia do niniejszej dyrektywy.

Art. 20.

Wejście w życie

Niniejsza dyrektywa wchodzi w życie z dniem jej opublikowania w *Dzienniku Urzędowym Wspólnot Europejskich.*

Art. 21.

Adresaci

Niniejsza dyrektywa skierowana jest do Państw Członkowskich.

Sporządzono w Brukseli, dnia 12 lipca 2002 r.

W imieniu Parlamentu Europejskiego: P. COX Przewodniczący
W imieniu Rady: T. PEDERSEN Przewodniczący