

Dokument ten służy wyłącznie do celów informacyjnych i nie ma mocy prawnej. Unijne instytucje nie ponoszą żadnej odpowiedzialności za jego treść. Autentyczne wersje odpowiednich aktów prawnych, włącznie z ich preambułami, zostały opublikowane w Dzienniku Urzędowym Unii Europejskiej i są dostępne na stronie EUR-Lex. Bezpośredni dostęp do tekstów urzędowych można uzyskać za pośrednictwem linków zawartych w dokumencie

► **B** **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)

(Dz.U. L 201 z 31.7.2002, s. 37)

zmieniona przez:

Dziennik Urzędowy

		nr	strona	data
► <u>M1</u>	Dyrektywa Parlamentu Europejskiego i Rady 2006/24/WE z dnia 15 marca 2006 r.	L 105	54	13.4.2006
► <u>M2</u>	Dyrektywa Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r.	L 337	11	18.12.2009

sprostowana przez:

- **C1** Sprostowanie, Dz.U. L 241 z 10.9.2013, s. 9 (2009/136/WE)
- **C2** Sprostowanie, Dz.U. L 162 z 23.6.2017, s. 56 (2009/136/WE)

▼B**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)***Artykuł 1***Zakres i cel****▼M2**

1. 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.

▼B

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.

*Artykuł 2***Definicje**

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) ⁽¹⁾.

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;

⁽¹⁾ Dz.U. L 108 z 24.4.2002, str. 33.

▼ M2

- 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;

▼ B

- 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;

▼ M2**▼ B**

- 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;

▼ M2

- **C1** i) „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.

*Artykuł 3***Usługi**

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.

▼ B*Artykuł 4***► M2 Bezpieczeństwo przetwarzania ◀**

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.

▼ M2

1a. 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.

▼ B

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.

▼ M2

3. 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.

▼ M2

4. 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. 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.

▼ B*Artykuł 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.

▼ M2

3. 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.

▼ B*Artykuł 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 zgodny z prawem zakwestionowany lub w którym należy uiścić opłatę.

▼ M2

3. Do celów wprowadzania na rynek usług łączności elektronicznej lub świadczenia usług tworzących wartość zbogaconą, 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.

▼ B

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 z obowiązującym ustawodawstwem, w celu rozstrzygnięcia sporów, w szczególności sporów dotyczących rozliczeń międzyoperatorskich lub naliczania opłat.

*Artykuł 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.

*Artykuł 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.

▼ B*Artykuł 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.

*Artykuł 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

- 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.

*Artykuł 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.

*Artykuł 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.

▼ M2*Artykuł 13***Komunikaty niezamówione**

1. 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. 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. 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. 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. 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.

► C2 6. 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, a zatem 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

▼ M2

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.

▼ B*Artykuł 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 ⁽¹⁾.

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 ⁽²⁾.

▼ M2*Artykuł 14a***Procedura komitetowa**

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

2. 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. 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.

⁽¹⁾ Dz.U. L 204 z 21.7.1998, str. 37. Dyrektywa zmieniona dyrektywą 98/48/WE (Dz.U. L 217 z 5.8.1998, str. 18).

⁽²⁾ Dz.U. L 36 z 7.2.1987, str. 31. Decyzja ostatnio zmieniona Aktem Przystąpienia z 1994 r.

▼ B*Artykuł 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.

▼ M1

1a. 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 ⁽¹⁾ dla celów określonych w art. 1 ust. 1 tej dyrektywy.

▼ M2

1b. 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.

▼ B

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.

⁽¹⁾ Dz.U. L 105 z 13.4.2006, str. 54.

▼ **M2***Artykuł 15a***Wdrażanie i egzekwowanie**

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 jakiegokolwiek 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.

▼ **B***Artykuł 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.

▼B

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.

*Artykuł 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 prześlą Komisji teksty przepisów prawa krajowego, które przyjmą w dziedzinie regulowanej niniejszą dyrektywą oraz każdej kolejnej zmiany tych przepisów.

*Artykuł 18***Przeгляд**

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.

*Artykuł 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.

▼B

Artykuł 20

Wejście w życie

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

Artykuł 21

Adresaci

Niniejsza dyrektywa skierowana jest do Państw Członkowskich.