KOMISJA
EUROPEJSKA

Bruksela, dnia 10.1.2017 r.
COM(2017) 10 final

2017/0003 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej)

(Tekst mający znaczenie dla EOG)

{SWD(2017) 3 final}
{SWD(2017) 4 final}
{SWD(2017) 5 final}
{SWD(2017) 6 final}

UZASADNIENIE

1. KONTEKST WNIOSKU

1.1 Przyczyny i cele wniosku

Celem strategii jednolitego rynku cyfrowego („**strategia jednolitego rynku cyfrowego**”)[1] jest zwiększenie zaufania względem usług cyfrowych i poprawa ich bezpieczeństwa. Reforma ram ochrony danych, a w szczególności przyjęcie rozporządzenia (UE) 2016/679, ogólnego rozporządzenia o ochronie danych („**ogólne rozporządzenie o ochronie danych**”)[2], stanowiła kluczowe działanie w tym kierunku. W ramach strategii jednolitego rynku cyfrowego ogłoszono również przegląd dyrektywy 2002/58/WE („**dyrektywa o prywatności i łączności elektronicznej**”)[3], mający na celu zapewnienie wysokiego poziomu ochrony prywatności użytkowników usług łączności elektronicznej oraz równych warunków działania dla wszystkich podmiotów na rynku. Niniejszy wniosek stanowi przegląd dyrektywy o prywatności i łączności elektronicznej uwzględniający z wyprzedzeniem cele strategii jednolitego rynku cyfrowego oraz zapewniający spójność z ogólnym rozporządzeniem o ochronie danych.

Dyrektywa o prywatności i łączności elektronicznej zapewnia ochronę podstawowych praw i wolności, w szczególności poszanowania życia prywatnego, poufności komunikacji oraz ochrony danych osobowych w sektorze łączności elektronicznej. Gwarantuje ona również swobodny przepływ danych, sprzętu i usług związanych z łącznością elektroniczną w Unii. Stanowi ona wdrożenie do prawa wtórnego Unii prawa podstawowego, jakim jest poszanowanie życia prywatnego, w odniesieniu do komunikowania się, przewidzianego w art. 7 Karty praw podstawowych Unii Europejskiej („**Karta praw podstawowych**”).

Zgodnie z wymogami lepszego stanowienia prawa Komisja przeprowadziła ocenę *ex post* dyrektywy o prywatności i łączności elektronicznej w ramach programu sprawności i wydajności regulacyjnej („**ocena REFIT**”). Z oceny wynika, że cele i zasady obecnych ram są nadal rozsądne. Niemniej jednak od czasu ostatniego przeglądu dyrektywy o prywatności i łączności elektronicznej dokonanego w 2009 r. na rynku doszło do ważnych zmian technologicznych i gospodarczych. Konsumenci i przedsiębiorstwa w coraz większym stopniu zamiast na tradycyjnych usługach łączności polegają na nowych, opartych na internecie usługach umożliwiających komunikację międzyludzką, takich jak usługi telefonii internetowej (VoIP), komunikatory internetowe, usługi poczty elektronicznej przez internet. Takie usługi łączności OTT („**usługi OTT**”) zasadniczo nie są objęte obecnymi unijnymi ramami dotyczącymi łączności elektronicznej, w tym również dyrektywą o prywatności i łączności elektronicznej. Dyrektywa nie nadąża też za rozwojem technologicznym, co skutkuje brakiem ochrony komunikacji przekazywanej za pośrednictwem nowych usług.

---

[1] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Strategia jednolitego rynku cyfrowego dla Europy”, COM(2015) 192 final.

[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1–88).

[3] 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).

1.2 Spójność z istniejącymi przepisami obowiązującymi w tej dziedzinie polityki

Niniejszy wniosek stanowi *lex specialis* względem ogólnego rozporządzenia o ochronie danych, uszczegóławia je i uzupełnia w kwestii danych pochodzących z łączności elektronicznej, które można zakwalifikować jako dane osobowe. Wszystkie sprawy dotyczące przetwarzania danych osobowych, do których nie odwołano się bezpośrednio we wniosku, są objęte zakresem ogólnego rozporządzenia o ochronie danych. Dostosowanie do ogólnego rozporządzenia o ochronie danych doprowadziło do uchylenia pewnych przepisów, takich jak obowiązek zapewnienia bezpieczeństwa zawarty w art. 4 dyrektywy o prywatności i łączności elektronicznej.

1.3 Spójność z innymi politykami Unii

Dyrektywa o prywatności i łączności elektronicznej jest częścią ram prawnych regulujących łączność elektroniczną. W 2016 r. Komisja przyjęła wniosek w sprawie dyrektywy ustanawiającej Europejski kodeks łączności elektronicznej („**Europejski kodeks łączności elektronicznej**”)[4], w którym to wniosku dokonano przeglądu ram regulacyjnych. Chociaż obecny wniosek nie stanowi integralnej części Europejskiego kodeksu łączności elektronicznej, częściowo opiera się na zawartych tam definicjach, włącznie z definicją „usług łączności elektronicznej”. Podobnie jak w przypadku Europejskiego kodeksu łączności elektronicznej, tak i w przypadku niniejszego wniosku, zakres stosowania obejmuje dostawców usług OTT, aby odzwierciedlić rzeczywistość rynkową. Ponadto Europejski kodeks łączności elektronicznej uzupełnia niniejszy wniosek poprzez zapewnienie bezpieczeństwa usług łączności elektronicznej.

Dyrektywa 2014/53/UE w sprawie urządzeń radiowych („**dyrektywa w sprawie urządzeń radiowych**”)[5] zapewnia jednolity rynek dla urządzeń radiowych. W szczególności zawiera wymóg, aby urządzenia radiowe przed ich wprowadzeniem do obrotu zostały wyposażone w zabezpieczenia w celu zapewnienia ochrony danych osobowych i prywatności użytkownika. Zgodnie z dyrektywą w sprawie urządzeń radiowych oraz rozporządzeniem (UE) 1025/2012[6] w sprawie normalizacji europejskiej Komisja jest upoważniona do przyjmowania środków. Niniejszy wniosek nie wpływa na dyrektywę w sprawie urządzeń radiowych.

Wniosek nie zawiera żadnych konkretnych przepisów w zakresie zatrzymywania danych. Podtrzymano treść art. 15 dyrektywy o prywatności i łączności elektronicznej oraz dopasowano ją do brzmienia art. 23 ogólnego rozporządzenia o ochronie danych, który przewiduje możliwość ograniczenia przez państwa członkowskie zakresu praw i obowiązków zawartych w konkretnych artykułach dyrektywy o prywatności i łączności elektronicznej. Państwa członkowskie mogą zatem utrzymać lub stworzyć krajowe ramy zatrzymywania danych, które umożliwiają – między innymi – stosowanie środków ukierunkowanego zatrzymywania danych, o ile ramy te są spójne z ogólnymi zasadami prawa Unii,

---

[4] Wniosek Komisji w sprawie dyrektywy Parlamentu Europejskiego i Rady ustanawiającej Europejski kodeks łączności elektronicznej (wersja przekształcona) (COM/2016/0590 final – 2016/0288 (COD)).

[5] Dyrektywa Parlamentu Europejskiego i Rady 2014/53/UE z dnia 16 kwietnia 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich dotyczących udostępniania na rynku urządzeń radiowych i uchylająca dyrektywę 1999/5/WE (Dz.U. L 153 z 22.5.2014, s. 62–106).

[6] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1025/2012 z dnia 25 października 2012 r. w sprawie normalizacji europejskiej, zmieniające dyrektywy Rady 89/686/EWG i 93/15/EWG oraz dyrektywy Parlamentu Europejskiego i Rady 94/9/WE, 94/25/WE, 95/16/WE, 97/23/WE, 98/34/WE, 2004/22/WE, 2007/23/WE, 2009/23/WE i 2009/105/WE oraz uchylające decyzję Rady 87/95/EWG i decyzję Parlamentu Europejskiego i Rady nr 1673/2006/WE (Dz.U. L 316 z 14.11.2012, s. 12–33).

uwzględniając przy tym orzecznictwo Trybunału Sprawiedliwości dotyczące wykładni dyrektywy o prywatności i łączności elektronicznej oraz Karty praw podstawowych[7].

Wniosek nie ma zastosowania do działań instytucji, organów i agencji Unii. Niemniej jednak zawarte w nim zasady i właściwe obowiązki związane z prawem do poszanowania życia prywatnego i komunikowania się w związku z przetwarzaniem danych pochodzących z łączności elektronicznej zostały włączone do wniosku w sprawie rozporządzenia uchylającego rozporządzenie (WE) nr 45/2001[8].

2 PODSTAWA PRAWNA, POMOCNICZOŚĆ I PROPORCJONALNOŚĆ

2.1 Podstawa prawna

Właściwymi podstawami prawnymi wniosku są art. 16 i art. 114 Traktatu o funkcjonowaniu Unii Europejskiej („**TFUE”**).

W art. 16 TFUE wprowadzono konkretną podstawę prawną na potrzeby przyjęcia przepisów dotyczących ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje Unii i przez państwa członkowskie przy realizacji działań wchodzących w zakres prawa Unii, jak również przepisów dotyczących swobodnego przepływu takich danych. Ponieważ komunikacja elektroniczna z udziałem osoby fizycznej zazwyczaj będzie kwalifikowana jako dane osobowe, ochrona osób fizycznych w zakresie poufności komunikacji i przetwarzania takich danych powinna opierać się na art. 16.

Ponadto wniosek ma chronić komunikację i powiązane uzasadnione interesy osób prawnych. Znaczenie i zakres praw wynikających z art. 7 Karty praw podstawowych zgodnie z art. 52 ust. 3 Karty praw podstawowych są takie same jak te określone w art. 8 ust. 1 europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności („**EKPC**”). Jeżeli chodzi o zakres art. 7 Karty praw podstawowych, orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej („**TSUE**”)[9] oraz Europejskiego Trybunału Praw Człowieka[10] potwierdza, że działania zawodowe osób prawnych nie mogą być wyłączone z ochrony prawa zagwarantowanego w art. 7 Karty praw podstawowych i art. 8 EKPC.

Ponieważ inicjatywa ta służy dwóm celom, a komponent dotyczący ochrony łączności osób prawnych i cel osiągnięcia rynku wewnętrznego dla takiej łączności elektronicznej i zapewnienia jego funkcjonowania w tym względzie nie może być uznawany za czysto przypadkowy, inicjatywa powinna zatem również opierać się na art. 114 TFUE.

2.2 Pomocniczość

Poszanowanie komunikowania się jest prawem podstawowym uznanym w Karcie praw podstawowych. Zawartość komunikacji elektronicznej może ujawniać dane szczególnie chronione na temat użytkowników końcowych zaangażowanych w taką komunikację.

---

7 Zob. sprawy połączone C-293/12 i C-594/12 *Digital Rights Ireland i Seitlinger i inni*, ECLI:EU:C:2014:238; sprawy połączone C-203/15 oraz C-698/15 *Tele2 Sverige AB i Secretary of State for the Home Department*, ECLI:EU:C:2016:970.

8 Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz.U. L 8 z 12.1.2001, s. 1–22).

9 Zob. C-450/06 *Varec SA*, ECLI:EU:C:2008:91, pkt 48.

10 Zob. m.in. ETPC, wyroki w sprawie *Niemietz przeciwko Niemcom*, wyrok z dnia 16 grudnia 1992 r., Seria A nr°251-B, pkt 29; *Société Colas Est i in. przeciwko Francji*, nr 37971/97, pkt 41; ETPC 2002-III; *Peck przeciwko Zjednoczonemu Królestwu* nr 44647/98, pkt 57, ETPC 2003-I; jak również *Vinci Construction i GTM Génie Civil et Services przeciwko Francji*, nr 63629/10 oraz 60567/10, pkt 63, 2 kwietnia 2015 r.

Podobnie metadane pozyskane z łączności elektronicznej mogą także ujawniać dane szczególnie chronione i dane osobowe, co zostało wprost potwierdzone przez TSUE[11]. Większość państw członkowskich uznaje również potrzebę ochrony komunikowania się jako odrębnego prawa konstytucyjnego. Chociaż państwa członkowskie mogą realizować politykę, która zapewni, aby prawo to nie było naruszane, nie osiągnięto by tego w sposób jednolity ze względu na brak zasad unijnych i powodowałoby to ograniczenia w transgranicznym przepływie danych osobowych i nieosobowych związanych z korzystaniem z usług łączności elektronicznej. Aby zachować spójność z ogólnym rozporządzeniem o ochronie danych, konieczne jest dokonanie przeglądu dyrektywy o prywatności i łączności elektronicznej oraz przyjęcie środków w celu zbliżenia do siebie dwóch instrumentów.

Rozwój technologiczny oraz ambicje strategii jednolitego rynku cyfrowego wzmocniły zasadność działań na szczeblu unijnym. Sukces unijnego jednolitego rynku cyfrowego zależy od tego, jak skutecznie Unia Europejska będzie rozbijać krajowe silosy i bariery oraz wykorzystywać zalety europejskiego jednolitego rynku cyfrowego i płynące z niego oszczędności. Ponadto, jako że internetu i technologii cyfrowych granice nie dotyczą, wymiar problemu wykracza poza terytorium poszczególnych państw członkowskich. Państwa członkowskie nie mogą skutecznie rozwiązywać problemów w obecnej sytuacji. Warunkami właściwego funkcjonowania jednolitego rynku cyfrowego są równe warunki działania dla podmiotów gospodarczych świadczących usługi substytucyjne oraz równa ochrona użytkowników końcowych na szczeblu unijnym.

2.3 Proporcjonalność

Aby zapewnić skuteczną ochronę prawną poszanowania prywatności i komunikacji, konieczne jest rozszerzenie zakresu stosowania, aby obejmował również dostawców usług OTT. Chociaż kilku popularnych dostawców usług OTT postępuje już zgodnie lub częściowo zgodnie z zasadą poufności komunikacji, ochrony praw podstawowych nie można pozostawić samoregulacji branżowej. Ponadto znaczenie skutecznej ochrony prywatności urządzeń końcowych wzrasta, gdyż stają się one nieodzowne w życiu osobistym i zawodowym do celów przechowywania danych szczególnie chronionych. Wdrożenie dyrektywy o prywatności i łączności elektronicznej nie było skuteczne, aby wzmocnić pozycję użytkowników końcowych. Dlatego też dla osiągnięcia tego celu konieczne jest wdrożenie tej zasady przez centralizację zgody w oprogramowaniu i informowanie użytkowników o ustawieniach prywatności oprogramowania. Jeżeli chodzi o egzekwowanie niniejszego rozporządzenia, opiera się ono na organach nadzorczych i mechanizmie spójności przewidzianym ogólnym rozporządzeniem o ochronie danych. Ponadto wniosek umożliwia państwom członkowskim zastosowanie krajowych odstępstw w konkretnych prawnie uzasadnionych celach. Z tego względu wniosek nie wykracza poza to, co jest konieczne do realizacji celów i jest zgodny z zasadą proporcjonalności określoną w art. 5 Traktatu o Unii Europejskiej. Obowiązki nakładane na objęte nimi usługi są utrzymywane na możliwie minimalnym poziomie bez rzutowania na stosowne prawa podstawowe.

2.4 Wybór instrumentu

Komisja przedstawia wniosek dotyczący rozporządzenia, aby zapewnić spójność z ogólnym rozporządzeniem o ochronie danych oraz pewność prawa dla użytkowników i przedsiębiorstw poprzez unikanie rozbieżnych interpretacji w państwach członkowskich. Rozporządzenie może zapewnić użytkownikom równy poziom ochrony w całej Unii oraz niższe koszty przestrzegania przepisów dla przedsiębiorstw działających na terenie różnych państw.

[11] Zob. przypis 7.

3 WYNIKI OCEN *EX POST,* KONSULTACJI Z ZAINTERESOWANYMI STRONAMI I OCEN SKUTKÓW

3.1 Oceny *ex post*/kontrole sprawności istniejącego prawodawstwa

W ramach oceny REFIT przeanalizowano, na ile skutecznie dyrektywa o prywatności i łączności elektronicznej przyczyniła się do odpowiedniej ochrony poszanowania życia prywatnego i poufności komunikacji w Unii Europejskiej. Miała ona również służyć zidentyfikowaniu możliwych powieleń.

Na podstawie oceny REFIT ustalono, że powyższe cele dyrektywy pozostają **istotne**. Chociaż ogólne rozporządzenie o ochronie danych zapewnia ochronę danych osobowych, dyrektywa o prywatności i łączności elektronicznej zapewnia poufność komunikacji, która może zawierać również dane nieosobowe oraz dane dotyczące osób prawnych. Skuteczną ochronę art. 7 Karty praw podstawowych powinien zatem zapewniać oddzielny instrument. Inne przepisy, takie jak zasady dotyczące wysyłania niezamówionych informacji handlowych, również okazały się nadal istotne.

Jeżeli chodzi o **skuteczność i wydajność,** w ramach oceny REFIT ustalono, że dyrektywa nie prowadzi do realizowania w pełni przyświecających jej celów. Niejasne sformułowanie niektórych przepisów oraz niejednoznaczność instytucji prawnych zagraża harmonizacji, powodując tym samym wyzwania dla przedsiębiorstw w działaniu transgranicznym. Ocena pokazała również, że niektóre przepisy powodują zbędne obciążenie dla przedsiębiorstw i konsumentów. Przykładowo zasada wyrażenia zgody w celu ochrony poufności urządzenia końcowego nie prowadzi do realizacji przyświecających jej celów, ponieważ użytkownicy końcowi mają do czynienia z prośbami o zaakceptowanie trwałych plików cookie bez rozumienia ich działania, a w niektórych przypadkach są nawet narażeni na działanie takich plików bez wyrażenia zgody. Zasada wyrażenia zgody jest zbyt szeroka, ponieważ obejmuje ona również praktyki nienaruszające prywatności, a jednocześnie niedostatecznie szeroka, ponieważ nie obejmuje wprost pewnych technik śledzenia (np. pobierania odbitek linii papilarnych przez urządzenie), które niekoniecznie muszą wiązać się z dostępem/przechowywaniem w urządzeniu. Jej wdrożenie może być także kosztowne dla przedsiębiorstw.

W ocenie stwierdzono, że zasady prywatności i łączności elektronicznej nadal mają **europejską wartość dodaną** umożliwiającą lepszą realizację celu zapewnienia prywatności w internecie w świetle coraz bardziej transnarodowego rynku łączności elektronicznej. Wykazano również, że – ogólnie rzecz biorąc – zasady te **są spójne** z innymi stosownymi przepisami, przy czym stwierdzono istnienie kilku powieleń względem nowego ogólnego rozporządzenia o ochronie danych (zob. rozdział 1.2).

3.2 Konsultacje z zainteresowanymi stronami

Między 12 kwietnia a 5 lipca 2016 r. Komisja zorganizowała konsultacje społeczne i otrzymała 421 odpowiedzi[12]. Główne ustalenia są następujące[13]:

[12] 162 opinie od obywateli, 33 – od organizacji społeczeństwa obywatelskiego oraz organizacji konsumenckich; 186 – od podmiotów branżowych oraz 40 – od organów publicznych, w tym właściwych organów egzekwujących dyrektywę o prywatności i łączności elektronicznej.

[13] Pełny tekst sprawozdania jest dostępny na stronie internetowej: https://ec.europa.eu/digital-single-market/news-redirect/37204.

– **Potrzeba specjalnych zasad dla sektora łączności elektronicznej dotyczących poufności komunikacji elektronicznej**: 83,4 % wypowiadających się obywateli, organizacji konsumenckich i organizacji społeczeństwa obywatelskiego oraz 88,9 % organów publicznych zgadza się, natomiast 63,4 % respondentów reprezentujących branżę się nie zgadza.

– **Rozszerzenie zakresu o nowe usługi łączności (usługi OTT)**: 76 % obywateli i organizacji społeczeństwa obywatelskiego oraz 93,1 % organów publicznych zgadza się, natomiast wśród respondentów reprezentujących branżę za takim rozszerzeniem opowiada się jedynie 36,2 %.

– **Zmiana zwolnień ze zgody na przetwarzanie danych o ruchu w sieci i danych dotyczących lokalizacji**: 49,1 % obywateli, organizacji konsumenckich i organizacji społeczeństwa obywatelskiego oraz 36 % organów publicznych wolałoby, aby nie rozszerzano zwolnień, natomiast 36 % branży opowiada się za rozszerzonymi zwolnieniami, a 2/3 branży popiera po prostu uchylenie tych przepisów.

– **Wsparcie dla rozwiązań zaproponowanych w związku z problemem zgody na pliki cookie**: 81,2 % obywateli i 63 % organów publicznych popiera nałożenie na producentów urządzeń końcowych obowiązków wprowadzania do obrotu produktów z aktywowanymi domyślnymi ustawieniami prywatności, podczas gdy 58,3 % branży opowiada się za poparciem samoregulacji/współregulacji.

Komisja Europejska zorganizowała też w kwietniu 2016 r. dwie sesje warsztatów: jedną otwartą dla wszystkich zainteresowanych stron i jedną otwartą dla krajowych właściwych organów, w której poruszono główne zagadnienia z konsultacji społecznych. Opinie wyrażone podczas warsztatów odpowiadały wynikom konsultacji społecznych.

Aby uzyskać opinie obywateli, w całej UE przeprowadzono badanie Eurobarometr dotyczące prywatności i łączności elektronicznej[14]. Główne ustalenia są następujące[15]:

– 78 % respondentów uważa, że jest bardzo ważne, aby dostęp do danych osobowych na ich komputerze, smartfonie lub tablecie był możliwy tylko za ich pozwoleniem;

– 73 % respondentów uważa za bardzo ważne zagwarantowanie poufności ich wiadomości e-mail i wiadomości na komunikatorach internetowych;

– 89 % respondentów zgadza się z zasugerowanym rozwiązaniem, w myśl którego domyślne ustawienia przeglądarki powinny wstrzymywać przekazywanie ich danych.

3.3 Gromadzenie i wykorzystanie wiedzy eksperckiej

Komisja uwzględniła następujące dokumenty zawierające opinie ekspertów zewnętrznych:

– ukierunkowane konsultacje z unijnymi grupami ekspertów: opinia Grupy Roboczej Art. 29; opinia EIOD; opinia platformy REFIT; poglądy Organu Europejskich Regulatorów Łączności Elektronicznej (BEREC); poglądy Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz poglądy członków sieci współpracy w zakresie ochrony konsumenta;

[14] Badanie Eurobarometr (EB) 443 z 2016 r. dotyczące prywatności i łączności elektronicznej (SMART 2016/079).

[15] Pełny tekst sprawozdania jest dostępny na stronie internetowej: https://ec.europa.eu/digital-single-market/news-redirect/37205.

– zewnętrzna wiedza fachowa, w szczególności następujące dwie ekspertyzy:

  – ekspertyza „Dyrektywa o prywatności i łączności elektronicznej”: ocena transpozycji, skuteczności i kompatybilności z proponowanym rozporządzeniem o ochronie danych (SMART 2013/007116);

  – ekspertyza „Ocena i przegląd dyrektywy 2002/58 o prywatności i łączności elektronicznej” (SMART 2016/0080).

3.4 Ocena skutków

W odniesieniu do niniejszego wniosku przeprowadzono ocenę skutków, a w dniu 28 września 2016 r. Rada ds. Kontroli Regulacyjnej pozytywnie zaopiniowała wniosek[16]. Aby odnieść się do zaleceń Rady, w ocenie skutków lepiej wyjaśniono zakres inicjatywy, jej spójność z innymi instrumentami prawnymi (ogólne rozporządzenie o ochronie danych, Europejski kodeks łączności elektronicznej, dyrektywa w sprawie urządzeń radiowych) oraz potrzebę odrębnego instrumentu. Scenariusz odniesienia jest dalej opracowywany i doprecyzowywany. Analizę skutków wzmocniono i bardziej wyważono, doprecyzowano i wzmocniono opis oczekiwanych kosztów i korzyści.

W odniesieniu do kryteriów skuteczności, wydajności i spójności przeanalizowano następujące warianty strategiczne:

– **Wariant 1:** Środki nielegislacyjne („prawo miękkie”);

– **Wariant 2:** Ograniczone wzmocnienie prywatności/poufności i uproszczenie;

– **Wariant 3:** Wymierne wzmocnienie prywatności/poufności i uproszczenie;

– **Wariant 4:** Daleko idące wzmocnienie prywatności/poufności i uproszczenie;

– **Wariant 5:** Uchylenie dyrektywy o prywatności i łączności elektronicznej.

Wariant 3 w większości aspektów został wyróżniony jako **wariant preferowany** do realizacji celów przy uwzględnieniu jego wydajności i spójności. Główne korzyści to:

– lepsza ochrona poufności komunikacji elektronicznej poprzez rozszerzenie zakresu stosowania przedmiotowego instrumentu prawnego w celu uwzględnienia nowych, funkcjonalnie równoważnych usług łączności elektronicznej. Ponadto rozporządzenie wzmacnia kontrolę użytkowników końcowych przez doprecyzowanie, że zgoda może być wyrażona poprzez stosowne ustawienia techniczne;

– wzmocnienie ochrony przed niezamówionymi komunikatami, wraz z wprowadzeniem obowiązku zapewnienia identyfikacji rozmów przychodzących lub obowiązkowego prefiksu dla połączeń marketingowych i lepsze możliwości blokowania połączeń z niepożądanych numerów;

– uproszczenie i doprecyzowanie otoczenia regulacyjnego poprzez ograniczenie pola manewru państw członkowskich, uchylenie przestarzałych przepisów i rozszerzenie wyjątków od zasad wyrażenia zgody.

Oczekuje się, że skutek gospodarczy wariantu 3 będzie zasadniczo proporcjonalny w stosunku do celów wniosku. Możliwości biznesowe związane z przetwarzaniem danych komunikacyjnych otwierają się dla tradycyjnych usług łączności elektronicznej, w sytuacji gdy dostawcy usług OTT zaczynają podlegać tym samym zasadom. Oznacza to dla tych

[16] http://ec.europa.eu/transparency/regdoc/?fuseaction=ia.

operatorów pewne dodatkowe koszty przestrzegania przepisów. Niemniej jednak zmiana ta nie wpłynie w znaczny sposób na tych dostawców usług OTT, którzy już funkcjonują w oparciu o zasadę wyrażenia zgody. Wpływ tego wariantu nie byłby odczuwany w państwach członkowskich, które już rozszerzyły swoje przepisy na dostawców usług OTT.

W przypadku centralizacji zgody w oprogramowaniu, takim jak przeglądarki internetowe, i nakłaniania użytkowników do wyboru ustawień prywatności oraz dzięki rozszerzeniu wyjątków od zasady wyrażania zgody na pliki cookie znaczna część przedsiębiorstw byłaby w stanie pozbyć się banerów i powiadomień o plikach cookie, co potencjalnie powodowałoby istotne oszczędności kosztów i uproszczenie. Niemniej jednak internetowym dostawcom reklam ukierunkowanych może być trudniej uzyskać zgodę, w sytuacji gdy duża część użytkowników wybierze ustawienie „odrzuć pliki cookie osoby trzeciej". Jednocześnie scentralizowana zgoda nie pozbawia operatorów stron internetowych możliwości uzyskania zgody w drodze indywidualnych próśb skierowanych do użytkowników końcowych, dzięki czemu utrzymaliby oni swój obecny model biznesowy. Niektórzy dostawcy przeglądarek lub podobnego oprogramowania mieliby do czynienia z dodatkowymi kosztami, ponieważ przeglądarki i programy musiałyby zapewnić ustawienia chroniące prywatność.

W ekspertyzie zewnętrznej opracowano trzy odrębne scenariusze wdrożenia wariantu 3, zależnie od podmiotu, który ustanowi okno dialogowe między użytkownikiem wybierającym ustawienia „odrzuć pliki cookie osoby trzeciej" lub ustawienia uniemożliwiające śledzenie a odwiedzonymi stronami internetowymi, na których prosi się użytkownika internetu o ponowne rozważenie decyzji. Podmioty, którym może zostać powierzone to zadanie techniczne, to: 1) oprogramowanie, takie jak przeglądarki internetowe; 2) osoba trzecia dokonująca śledzenia; 3) poszczególne strony internetowe (tj. usługa społeczeństwa informacyjnego żądana przez użytkownika) Wariant 3 przy pierwszym scenariuszu (rozwiązanie zakładające przeglądarkę) wdrożonym w niniejszym wniosku prowadziłby do ogólnych oszczędności pod względem kosztów przestrzegania przepisów w porównaniu do scenariusza odniesienia na poziomie 70 % (948,8 mln EUR oszczędności). Oszczędności kosztów w innych scenariuszach byłyby mniejsze. Ponieważ ogólne oszczędności wynikają w dużej mierze z bardzo istotnego spadku liczby przedsiębiorstw, na które przepisy mają wpływ, indywidualna kwota kosztów przestrzegania przepisów dla jednego przedsiębiorstwa byłaby – średnio – wyższa niż dziś.

3.5 Sprawność regulacyjna i uproszczenie

Środki z zakresu polityki proponowane w ramach preferowanego wariantu stanowią odpowiedź na cel uproszczenia i zmniejszenia obciążenia administracyjnego zgodnie z ustaleniami z oceny REFIT oraz opinią platformy REFIT[17].

Platforma REFIT wydała trzy zestawy zaleceń skierowanych do Komisji:

– ochrona życia prywatnego obywateli powinna być wzmocniona poprzez dopasowanie dyrektywy o prywatności i łączności elektronicznej oraz ogólnego rozporządzenia o ochronie danych;

– skuteczność ochrony obywateli przed niezamówionymi informacjami marketingowymi należy zwiększyć poprzez dodanie większej liczby wyjątków od zasady zgody na pliki cookie*;*

– Komisja reaguje na krajowe problemy z wdrożeniem i usprawnia wymianę najlepszych praktyk pomiędzy państwami członkowskimi.

[17] http://ec.europa.eu/smart-regulation/refit/refit-platform/docs/recommendations/opinion_comm_net.pdf

Wniosek obejmuje konkretnie:

– zastosowanie definicji neutralnych pod względem technologicznym w celu ujęcia nowych usług i technologii, co zagwarantuje, że rozporządzenie będzie aktualne również w przyszłości;

– uchylenie zasad bezpieczeństwa w celu wyeliminowania powielania przepisów;

– doprecyzowanie zakresu stosowania, aby pomóc wyeliminować/ograniczyć ryzyko rozbieżnego wdrożenia przepisów przez państwa członkowskie (pkt 3 opinii);

– doprecyzowanie i uproszczenie zasady wyrażania zgody na zastosowanie plików cookie i innych identyfikatorów, co wyjaśniono w rozdziale 3.1 i 3.4 (pkt 2 opinii);

– dopasowanie organów nadzorczych do organów właściwych do egzekwowania ogólnego rozporządzenia o ochronie danych oraz oparcie się na mechanizmie spójności określonym w ogólnym rozporządzeniu o ochronie danych.

3.6 Wpływ na prawa podstawowe

Wniosek ma poprawić skuteczność i zwiększyć poziom ochrony prywatności i danych osobowych przetwarzanych w związku z łącznością elektroniczną zgodnie z art. 7 i 8 Karty praw podstawowych oraz zapewnić większą pewność prawa. Wniosek stanowi uzupełnienie i uszczegółowienie ogólnego rozporządzenia o ochronie danych. Skuteczna ochrona poufności komunikacji jest kluczowa dla korzystania z prawa wolności wypowiedzi i informacji oraz innych powiązanych praw, takich jak prawo do ochrony danych osobowych bądź wolność myśli, sumienia i religii.

4 WPŁYW NA BUDŻET

Wniosek nie ma wpływu na budżet Unii.

5 ELEMENTY FAKULTATYWNE

5.1 Plany wdrożenia i monitorowanie, ocena i sprawozdania

Komisja będzie monitorować stosowanie rozporządzenia i przedkładać sprawozdanie ze swojej oceny Parlamentowi Europejskiemu i Radzie oraz Europejskiemu Komitetowi Ekonomiczno-Społecznemu co trzy lata. Sprawozdania te będą dostępne dla opinii publicznej i będą zawierały szczegółowy opis skutecznego stosowania i egzekwowania niniejszego rozporządzenia.

5.2 Szczegółowe objaśnienia poszczególnych przepisów wniosku

Rozdział I zawiera przepisy ogólne: przedmiot (art. 1), zakres stosowania (art. 2 i 3) oraz definicje, w tym odniesienia do stosownych definicji z innych instrumentów unijnych, takich jak ogólne rozporządzenie o ochronie danych.

Rozdział II zawiera najważniejsze przepisy zapewniające poufność komunikacji elektronicznej (art. 5) oraz ograniczone dozwolone cele i warunki przetwarzania takich danych komunikacyjnych (art. 6 i 7). Obejmuje on również kwestię ochrony urządzenia końcowego poprzez (i) gwarantowanie integralności przechowywanych w nim informacji oraz (ii) ochronę informacji emitowanych przez urządzenie końcowe, ponieważ mogą one umożliwić identyfikację użytkowników końcowych (art. 8). Z kolei art. 9 zawiera szczegółowe elementy zgody użytkowników końcowych, a więc centralną, zgodną z prawem podstawę niniejszego rozporządzenia, odnosząc się wprost do jej definicji i warunków przewidzianych w ogólnym rozporządzeniu o ochronie danych, natomiast art. 10 nakłada na

dostawców oprogramowania umożliwiającego łączność elektroniczną obowiązek wsparcia użytkowników końcowych w dokonywaniu skutecznych wyborów dotyczących ustawień prywatności. Art. 11 określa cele i warunki, jakie muszą spełnić państwa członkowskie, aby ograniczyć powyższe przepisy.

Rozdział III dotyczy praw użytkowników końcowych do kontrolowania wysyłania i odbioru komunikacji elektronicznej w celu ochrony ich prywatności: (i) prawo użytkowników końcowych do zapobiegania przedstawianiu identyfikacji rozmów przychodzących w celu zagwarantowania anonimowości (art. 12), wraz z ograniczeniami (art. 13); oraz (ii) obowiązek zapewnienia przez dostawców publicznie dostępnej komunikacji interpersonalnej opartej na numerach możliwości ograniczenia otrzymywania niechcianych połączeń (art. 14). Rozdział ten reguluje również warunki, na jakich użytkowników końcowych można uwzględnić w publicznie dostępnych spisach numerów (art. 15) oraz warunki, na jakich możliwe jest prowadzenie niezamówionej komunikacji na potrzeby marketingu bezpośredniego (art. 17). Obejmuje on również kwestię ryzyka związanego z bezpieczeństwem i przewiduje obowiązek ostrzegania użytkowników końcowych przez dostawców usług łączności elektronicznej w przypadku szczególnego ryzyka, które może zagrozić bezpieczeństwu sieci i usług. Obowiązki w zakresie bezpieczeństwa przewidziane w ogólnym rozporządzeniu o ochronie danych i w Europejskim kodeksie łączności elektronicznej będą miały zastosowanie do dostawców usług łączności elektronicznej.

Rozdział IV odnosi się do nadzorowania i egzekwowania niniejszego rozporządzenia oraz zawiera przepisy, w myśl których obowiązki te powierza się organom nadzorczym odpowiedzialnym za ogólne rozporządzenie o ochronie danych ze względu na silną synergię między ogólnymi problemami związanymi z ochroną danych i poufnością komunikacji (art. 18). Uprawnienia Europejskiej Rady Ochrony Danych są rozszerzone (art. 19), natomiast mechanizm współpracy i spójności przewidziany w ogólnym rozporządzeniu o ochronie danych będzie mieć zastosowanie w przypadku spraw transgranicznych związanych z niniejszym rozporządzeniem (art. 20).

W rozdziale V szczegółowo określa się różne środki zaradcze dostępne dla użytkowników końcowych (art. 21 i 22) oraz kary, jakie można nakładać (art. 24), w tym ogólne warunki nakładania kar administracyjnych (art. 23).

Rozdział VI dotyczy przyjęcia aktów delegowanych i wykonawczych zgodnie z art. 290 i 291 Traktatu.

Rozdział VII zawiera przepisy końcowe niniejszego rozporządzenia: uchylenie dyrektywy o prywatności i łączności elektronicznej, monitorowanie i przegląd, wejście w życie oraz stosowanie. Jeżeli chodzi o przegląd, Komisja zamierza ocenić – między innymi – czy odrębny akt prawny pozostaje nadal konieczny w świetle rozwoju okoliczności prawnych, technicznych lub gospodarczych, uwzględniając pierwszą ocenę rozporządzenia (UE) 2016/679, która ma zostać przeprowadzona do 25 maja 2020 r.

2017/0003 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej)

(Tekst mający znaczenie dla EOG)

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 16 i 114,

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego[1],

uwzględniając opinię Komitetu Regionów[2],

uwzględniając opinię Europejskiego Inspektora Ochrony Danych[3],

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

a także mając na uwadze, co następuje:

(1) Art. 7 Karty praw podstawowych Unii Europejskiej („Karta praw podstawowych”) chroni podstawowe prawo każdej osoby do poszanowania jej życia prywatnego i rodzinnego, domu i komunikowania się. Poszanowanie prywatności komunikacji jest jednym z kluczowych aspektów tego prawa. Poufność komunikacji elektronicznej zapewnia, że informacji przekazywanych między stronami i zewnętrznych elementów takiej komunikacji, w tym danych dotyczących czasu wysłania informacji, miejsca nadania i adresata, nie ujawnia się żadnej innej osobie poza stronami zaangażowanymi w dany akt komunikacji. Zasada poufności powinna obowiązywać w stosunku do obecnych i przyszłych środków komunikacji, w tym rozmów, dostępu do internetu, komunikatorów internetowych, poczty elektronicznej, rozmów telefonii internetowej oraz wiadomości przesyłanych przed media społecznościowe.

(2) Zawartość komunikacji elektronicznej może ujawniać dane szczególnie chronione na temat osób fizycznych zaangażowanych w taką komunikację, od osobistych doświadczeń i uczuć po stan zdrowia, orientację seksualną i poglądy polityczne, których ujawnienie mogłoby spowodować osobistą i społeczną szkodę, stratę ekonomiczną lub zażenowanie. Podobnie metadane pozyskane z łączności elektronicznej mogą także ujawniać dane szczególnie chronione i dane osobowe. Do

[1] Dz.U. C z , s. .
[2] Dz.U. C z , s. .
[3] Dz.U. C z , s. .

takich metadanych należą wybierane numery, odwiedzane strony internetowe, lokalizacja geograficzna, godzina, data i czas trwania połączenia itp., pozwalające na wyciągnięcie konkretnych wniosków dotyczących prywatnego życia osób zaangażowanych w komunikację elektroniczną, takich jak ich relacje towarzyskie, zwyczaje bądź aktywności codziennego życia, zainteresowania, gusty itp.

(3) Dane pochodzące z łączności elektronicznej mogą również ujawniać informacje dotyczące podmiotów prawnych, takie jak tajemnice przedsiębiorstwa lub inne dane szczególnie chronione o wartości ekonomicznej. Z tego względu przepisy niniejszego rozporządzenia powinny mieć zastosowanie zarówno do osób fizycznych, jak i do osób prawnych. Ponadto niniejsze rozporządzenie powinno zapewniać, aby przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679[4] miały zastosowanie również do użytkowników końcowych będących osobami prawnymi. Dotyczy to również definicji zgody zawartej w rozporządzeniu (UE) 2016/679. Ilekroć mowa jest o zgodzie użytkownika końcowego, w tym osób prawnych, zastosowanie powinna mieć ta definicja. Ponadto osobom prawnym powinny przysługiwać takie same prawa w kwestii organów nadzorczych jak użytkownikom końcowym będącym osobami fizycznymi. Co więcej, organy nadzorcze powinny – zgodnie z niniejszym rozporządzeniem – odpowiadać również za monitorowanie stosowania niniejszego rozporządzenia w stosunku do osób prawnych.

(4) Na podstawie art. 8 ust. 1 Karty praw podstawowych oraz art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej każdy ma prawo do ochrony dotyczących go danych osobowych. W rozporządzeniu (UE) 2016/679 ustanowiono przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych oraz przepisy o swobodnym przepływie danych osobowych. Dane pochodzące z łączności elektronicznej mogą zawierać dane osobowe zdefiniowane w rozporządzeniu (UE) 2016/679.

(5) Przepisy niniejszego rozporządzenia stanowią uszczegółowienie i uzupełnienie ogólnych przepisów w zakresie ochrony danych osobowych ustanowionych na mocy rozporządzenia (UE) 2016/679 w odniesieniu do danych pochodzących z łączności elektronicznej kwalifikujących się jako dane osobowe. Niniejsze rozporządzenie nie obniża zatem poziomu ochrony przysługującego osobom fizycznym na mocy rozporządzenia (UE) 2016/679. Przetwarzanie danych pochodzących z łączności elektronicznej przez dostawców usług łączności elektronicznej powinno być dozwolone jedynie zgodnie z niniejszym rozporządzeniem.

(6) Chociaż zasady i główne przepisy dyrektywy Parlamentu Europejskiego i Rady 2002/58/WE[5] pozostają co do zasady rozsądne, dyrektywa nie nadąża w pełni za rozwojem technologicznym i rzeczywistością rynkową, co skutkuje niespójną lub niedostatecznie skuteczną ochroną prywatności i poufności w związku z łącznością elektroniczną. Rozwój, o którym mowa, obejmuje wejście na rynek usług łączności elektronicznej, które z perspektywy konsumenta są usługami zastępującymi usługi tradycyjne, ale nie muszą być godne z tym samym zestawem przepisów. Innym

[4] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1–88).

[5] 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).

przejawem rozwoju są nowe techniki, które umożliwiają śledzenie aktywności użytkowników końcowych w internecie, a również nie są objęte zakresem stosowania dyrektywy 2002/58/WE. Dyrektywę 2002/58/WE należy zatem uchylić i zastąpić niniejszym rozporządzeniem.

(7) Państwa członkowskie powinny mieć możliwość utrzymania lub wprowadzenia przepisów krajowych w granicach przewidzianych niniejszym rozporządzeniem w celu dalszego określenia i doprecyzowania stosowania przepisów niniejszego rozporządzenia, aby zapewnić skuteczne stosowanie i interpretowanie tych przepisów. Z tego względu margines swobody, jaki państwa członkowskie mają w tym zakresie, powinien utrzymywać równowagę między ochroną życia prywatnego i danych osobowych a swobodnym przepływem danych pochodzących z łączności elektronicznej.

(8) Niniejsze rozporządzenie powinno mieć zastosowanie do dostawców usług łączności elektronicznej, dostawców publicznie dostępnych spisów numerów oraz dostawców oprogramowania umożliwiającego łączność elektroniczną, łącznie z odzyskiwaniem i przedstawianiem informacji w internecie. Niniejsze rozporządzenie powinno również mieć zastosowanie do osób fizycznych i prawnych, które korzystają z usług łączności elektronicznej, aby wysyłać materiały handlowe do celów marketingu bezpośredniego, lub gromadzą informacje związane z urządzeniem końcowym użytkowników końcowych bądź przechowywane na takim urządzeniu.

(9) Niniejsze rozporządzenie powinno mieć zastosowanie do danych pochodzących z łączności elektronicznej przetwarzanych w związku z zapewnieniem i zastosowaniem usług łączności elektronicznej w Unii, niezależnie od tego, czy przetwarzanie odbywa się na terytorium Unii. Ponadto, aby uniknąć pozbawienia użytkowników końcowych w Unii skutecznej ochrony, niniejsze rozporządzenie powinno mieć zastosowanie również do danych pochodzących z łączności elektronicznej przetwarzanych w związku ze świadczeniem użytkownikom końcowym w Unii usług łączności elektronicznej pochodzących spoza Unii.

(10) Urządzenia radiowe i ich oprogramowanie, które wprowadzono na rynek wewnętrzny Unii, muszą być zgodne z dyrektywą 2014/53/UE Parlamentu Europejskiego i Rady[6]. Niniejsze rozporządzenie nie powinno wpływać na możliwość zastosowania jakiegokolwiek z wymogów dyrektywy 2014/53/UE ani na uprawnienie Komisji do przyjęcia aktów delegowanych na podstawie dyrektywy 2014/53/UE, zgodnie z którą wymaga się, aby konkretne kategorie lub klasy urządzeń radiowych były wyposażone w zabezpieczenia w celu zapewnienia ochrony danych osobowych i prywatności użytkowników końcowych.

(11) Usługi wykorzystywane w celach komunikacyjnych oraz techniczne środki ich dostawy rozwinęły się w znacznym stopniu. Użytkownicy końcowi coraz częściej zastępują tradycyjną telefonię głosową, wiadomości tekstowe (SMS) oraz usługi elektronicznego przekazywania poczty usługami internetowymi będącymi ich funkcjonalnymi odpowiednikami, takimi jak telefonia internetowa (VoIP), komunikatory internetowe i usługi poczty elektronicznej przez internet. Aby zapewnić skuteczną i równą ochronę użytkowników końcowych podczas korzystania z usług równoważnych pod względem funkcjonalnym, niniejsze rozporządzenie wykorzystuje

[6] Dyrektywa Parlamentu Europejskiego i Rady 2014/53/UE z dnia 16 kwietnia 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich dotyczących udostępniania na rynku urządzeń radiowych i uchylająca dyrektywę 1999/5/WE (Dz.U. L 153 z 22.5.2014, s. 62).

definicję usług łączności elektronicznej zawartą w [dyrektywie Parlamentu Europejskiego i Rady ustanawiającej Europejski kodeks łączności elektronicznej[7]]. Definicja ta obejmuje nie tylko usługi dostępu do internetu i usługi polegające w całości lub częściowo na przekazywaniu sygnałów, lecz również usługi łączności interpersonalnej, z wykorzystaniem numerów lub bez ich wykorzystania, takie jak przykładowo telefonia internetowa, komunikatory internetowe i usługi poczty elektronicznej przez internet. Ochrona poufności komunikacji jest kluczowa również w odniesieniu do usług łączności interpersonalnej, które są usługami pomocniczymi względem innej usługi. Tego rodzaju usługi, które mają również funkcję komunikacyjną, powinny być zatem objęte niniejszym rozporządzeniem.

(12) Urządzenia i maszyny podłączone do internetu na coraz większą skalę komunikują się ze sobą, wykorzystując sieci łączności elektronicznej (internet rzeczy). Przesył komunikatów w trybie maszyna-maszyna wiąże się z przekazywaniem sygnałów w ramach sieci, a przez to stanowi zazwyczaj usługę łączności elektronicznej. W celu zapewnienia pełnej ochrony prawa do prywatności i poufności komunikacji oraz w celu propagowania zaufanego i bezpiecznego internetu rzeczy na jednolitym rynku cyfrowym konieczne jest doprecyzowanie, że rozporządzenie powinno mieć zastosowanie do przesyłu komunikatów w trybie maszyna-maszyna. Z tego względu zasada poufności zapisana w niniejszym rozporządzeniu powinna obowiązywać również w odniesieniu do przesyłu komunikatów w trybie maszyna-maszyna. Można by przyjąć również konkretne zabezpieczenia w ramach sektorowych aktów prawnych, takich jak na przykład dyrektywa 2014/53/UE.

(13) Rozwój szybkich i wydajnych technologii bezprzewodowych spowodował przyspieszenie wzrostu dostępu społeczeństwa do internetu za pośrednictwem sieci bezprzewodowych dostępnych dla każdego w przestrzeniach publicznych i pół-prywatnych, takich jak „hotspoty" usytuowane w różnych miejscach w obrębie miasta, centrach handlowych, galeriach handlowych i szpitalach. W zakresie, w jakim takie sieci łączności są udostępniane nieokreślonej grupie użytkowników końcowych, należy chronić poufność komunikacji przekazywanej przez takie sieci. Fakt, iż bezprzewodowe usługi łączności elektronicznej mogą być pomocnicze względem innych usług, nie powinien stać na przeszkodzie zapewnieniu ochrony poufności danych pochodzących z łączności i zastosowaniu niniejszego rozporządzenia. Z tego względu niniejsze rozporządzenie powinno mieć zastosowanie do danych pochodzących z łączności elektronicznej wykorzystującej usługi łączności elektronicznej i publiczne sieci łączności. Z kolei niniejsze rozporządzenie nie powinno mieć zastosowania do zamkniętych grup użytkowników końcowych, takich jak sieci firmowe, do których dostęp mają wyłącznie członkowie danej instytucji.

(14) Dane pochodzące z łączności elektronicznej należy zdefiniować w dostatecznie szeroki i neutralny technologicznie sposób, aby ich definicja obejmowała wszelkie informacje dotyczące przesyłanych lub przekazywanych treści (treści łączności elektronicznej) oraz informacje dotyczące użytkowników końcowych usług łączności elektronicznej przetwarzane w celu przesyłania, dystrybuowania lub umożliwienia wymiany treści łączności elektronicznej; w tym dane służące do śledzenia i zidentyfikowania źródła i miejsca docelowego przypadku łączności, lokalizacji geograficznej oraz daty, godziny, czasu trwania oraz rodzaju łączności. Niezależnie od tego, czy sygnały i powiązane dane są przekazywane drogą telegraficzną, radiową,

[7] Wniosek Komisji w sprawie dyrektywy Parlamentu Europejskiego i Rady ustanawiającej Europejski kodeks łączności elektronicznej (wersja przekształcona) (COM/2016/0590 final – 2016/0288 (COD)).

światłowodową czy elektromagnetyczną, w tym przez sieci satelitarne, sieci kablowe, stacjonarne (z komutacją łączy i komutacją pakietów, w tym internet) oraz komórkowe sieci naziemne, elektryczne systemy przewodowe, dane dotyczące takich sygnałów należy uznać za metadane pochodzące z łączności elektronicznej, a zatem powinny one podlegać przepisom niniejszego rozporządzenia. Metadane pochodzące z łączności elektronicznej mogą zawierać informacje stanowiące część abonamentu na usługę, gdy takie informacje są przetwarzane na potrzeby przesyłania, dystrybuowania lub wymiany treści łączności elektronicznej.

(15) Dane pochodzące z łączności elektronicznej należy traktować jako poufne. Oznacza to, że jakiekolwiek ingerowanie w przesył danych pochodzących z łączności elektronicznej, czy to za sprawą bezpośredniej ingerencji człowieka, czy za pośrednictwem zautomatyzowanego przetwarzania przez maszyny, dokonywane bez zgody wszystkich komunikujących się stron, powinno być zakazane. Zakaz przechwytywania danych pochodzących z łączności powinien obowiązywać podczas ich przekazywania, tj. do czasu otrzymania treści łączności elektronicznej przez docelowego odbiorcę. Przechwytywanie danych pochodzących z łączności elektronicznej może na przykład nastąpić, gdy ktoś inny niż komunikujące się strony słucha rozmów, czyta, skanuje lub przechowuje treść łączności elektronicznej lub powiązane metadane dla celów innych niż wymiana komunikatów. Przechwytywanie ma miejsce również wówczas, gdy osoby trzecie bez zgody danego użytkownika końcowego monitorują odwiedzane strony internetowe, godziny wizyt, interakcje użytkownika z innymi itp. Wraz z rozwojem technologii zwiększyły się również techniczne możliwości dokonywania przechwytywania. Takie sposoby mogą obejmować działania od instalowania sprzętu, który gromadzi dane z urządzeń końcowych na obszarach docelowych, takie jak tzw. IMSI Catcher (IMSI – międzynarodowy numer tożsamości telefonicznej abonenta mobilnego), po programy i techniki, które – przykładowo – w sposób zakamuflowany monitorują korzystanie z przeglądarki w celu tworzenia profilów użytkownika końcowego. Inne przykłady przechwytywania obejmują wychwytywanie bez zgody użytkownika końcowego danych właściwych (*payload*) lub danych dotyczących treści z niezaszyfrowanych sieci bezprzewodowych i routerów, w tym danych dotyczących korzystania z przeglądarki.

(16) Zakaz przechowywania komunikatów nie ma na celu zakazania jakiegokolwiek automatycznego, pośredniego i tymczasowego przechowywania tych informacji, o ile odbywa się to wyłącznie w celu dokonania przesyłu w ramach sieci łączności elektronicznej. Nie powinno się zakazywać przetwarzania danych pochodzących z łączności elektronicznej prowadzonego w celu zapewnienia bezpieczeństwa i ciągłości usług łączności elektronicznej, w tym sprawdzenia zagrożeń bezpieczeństwa, takich jak obecność złośliwego oprogramowania, ani przetwarzania metadanych prowadzonego w celu zapewnienia spełnienia wymogów koniecznej jakości usług, np. opóźnienia, zmienności opóźnienia przekazu pakietów itp.

(17) Przetwarzanie danych pochodzących z łączności elektronicznej może być użyteczne dla przedsiębiorstw, konsumentów i społeczeństwa ogółem. W stosunku do dyrektywy 2002/58/WE niniejsze rozporządzenie rozszerza możliwości dostawców usług łączności elektronicznej w zakresie przetwarzania metadanych pochodzących z łączności elektronicznej na podstawie zgody użytkowników końcowych. Niemniej jednak użytkownicy końcowi przywiązują dużą wagę do poufności komunikacji, w tym aktywności w internecie, oraz chcą kontrolować korzystanie z danych pochodzących z łączności elektronicznej do celów innych niż przekazywanie

komunikatu. Z tego względu niniejsze rozporządzenie powinno zobowiązywać dostawców usług łączności elektronicznej do uzyskania zgody użytkowników końcowych na przetwarzanie metadanych pochodzących z łączności elektronicznej, które powinny obejmować dane dotyczące lokalizacji urządzenia wygenerowane na potrzeby udzielenia i utrzymania dostępu do usługi oraz połączenia z nią. Danych dotyczących lokalizacji generowanych w inny sposób niż w okolicznościach związanych z przypadkiem łączności nie powinno się uznawać za metadane. Przykłady komercyjnego korzystania z metadanych pochodzących z łączności elektronicznej przez dostawców usług łączności elektronicznej mogą obejmować dostarczanie tzw. mapy aktywności; graficznej reprezentacji danych, na której kolory wskazują obecność osób. Aby wyświetlić ruch drogowy w danym kierunku w określonym czasie, konieczny jest identyfikator wiążący pozycje osób w pewnych interwałach czasowych. Takiego identyfikatora zabrakłoby, gdyby korzystano z anonimowych danych, i taki ruch nie byłby wyświetlany. Tego rodzaju wykorzystanie metadanych pochodzących z łączności elektronicznej mogłoby na przykład przynosić korzyść organom publicznym i operatorom transportu publicznego, pozwalając im określić, gdzie rozwinąć nową infrastrukturę, w oparciu o wykorzystanie istniejącej struktury i presji na nią. W sytuacji gdy rodzaj przetwarzania metadanych pochodzących z łączności elektronicznej, w szczególności przy korzystaniu z nowych technologii, z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania, z dużym prawdopodobieństwem może skutkować dużym zagrożeniem dla praw i wolności osób fizycznych, przed przetwarzaniem należy przeprowadzić ocenę skutków w zakresie ochrony danych oraz – w stosownych przypadkach – powinny odbyć się konsultacje z organem nadzorczym, zgodnie z art. 35 i 36 rozporządzenia (UE) 2016/679.

(18) Użytkownicy końcowi mogą wyrazić zgodę na przetwarzanie swoich metadanych w celu uzyskania konkretnych usług, takich jak usługi ochrony przed oszustwami (poprzez analizowanie danych o korzystaniu, lokalizacji i koncie klienta w czasie rzeczywistym). W gospodarce cyfrowej usługi świadczy się często w zamian za świadczenie wzajemne inne niż pieniądze, na przykład w zamian za to, że użytkownicy końcowi są narażeni na reklamy. Do celów niniejszego rozporządzenia zgoda użytkownika końcowego, niezależnie od tego, czy jest on osobą fizyczną, czy prawną, powinna mieć takie samo znaczenie i podlegać takim samym warunkom jak zgoda osoby, której dane dotyczą, zgodnie z rozporządzeniem (UE) 2016/679. Podstawowe usługi dostępu szerokopasmowego do internetu i usługi komunikacji głosowej są uważane za usługi kluczowe dla osób fizycznych, aby mogły się one komunikować i czerpać korzyści z gospodarki cyfrowej. Zgoda na przetwarzanie danych związanych z korzystaniem z internetu lub komunikacją głosową nie będzie ważna, jeżeli osoba, której dane dotyczą, nie ma rzeczywistego i swobodnego wyboru lub nie może odmówić bądź wycofać zgody bez szkody.

(19) Treść łączności elektronicznej dotyczy kwintesencji prawa podstawowego, jakim jest poszanowanie życia prywatnego i rodzinnego, domu i komunikowania się na mocy art. 7 Karty praw podstawowych. Jakakolwiek ingerencja w treść łączności elektronicznej powinna być dozwolona jedynie w bardzo jasno określonych warunkach i w konkretnych celach oraz powinna podlegać odpowiednim zabezpieczeniom przed nadużyciami. W niniejszym rozporządzeniu przewidziano możliwość przetwarzania przez dostawców usług łączności elektronicznej danych pochodzących z łączności elektronicznej za świadomą zgodą wszystkich zainteresowanych użytkowników końcowych. Dostawcy mogą na przykład oferować usługi, które wiążą się ze skanowaniem poczty elektronicznej w celu usunięcia

pewnego zdefiniowanego wcześniej materiału. Z uwagi na wrażliwy charakter treści łączności w niniejszym rozporządzeniu zakłada się, że przetwarzanie takich danych dotyczących treści będzie skutkować dużym zagrożeniem dla praw i wolności osób fizycznych. Dostawca usług łączności elektronicznej, przetwarzając tego typu dane, powinien zawsze przed przetwarzaniem konsultować się z organem nadzorczym. Takie konsultacje powinny być zgodne z art. 36 ust. 2 i 3 rozporządzenia (UE) 2016/679. Założenie to nie obejmuje przetwarzania danych dotyczących treści w celu świadczenia usługi zamówionej przez użytkownika końcowego, gdy użytkownik końcowy zgodził się na takie przetwarzanie i jest ono dokonywane na potrzeby takiej usługi i przez okres absolutnie dla niej niezbędny i proporcjonalny. Po przesłaniu treści łączności elektronicznej przez użytkownika końcowego i otrzymaniu jej przez docelowego użytkownika końcowego lub docelowych użytkowników końcowych treść ta może być zapisywana lub przechowywana przez użytkownika końcowego, użytkowników końcowych lub osobę trzecią, której użytkownicy końcowi powierzyli zapisanie lub przechowywanie takich danych. Wszelkie przetwarzanie takich danych musi odbywać się zgodnie z rozporządzeniem (UE) 2016/679.

(20) Urządzenie końcowe użytkowników końcowych sieci łączności elektronicznej oraz wszelkie informacje związane z korzystaniem z takiego urządzenia końcowego, czy to w szczególności przechowywane na takim urządzeniu lub przez nie wysyłane, stanowiące przedmiot zapytania kierowanego do urządzenia bądź przetwarzane w celu umożliwienia połączenia z innym urządzeniem lub sprzętem sieciowym, stanowią część prywatnej sfery użytkowników końcowych wymagającej ochrony zgodnie z Kartą praw podstawowych Unii Europejskiej oraz europejską Konwencją o ochronie praw człowieka i podstawowych wolności. Ponieważ taki sprzęt zawiera lub przetwarza informacje, które mogą ujawnić szczegóły dotyczące emocji, poglądów politycznych i sytuacji społecznej osoby fizycznej, w tym treść łączności, zdjęcia, lokalizację osób przez dostęp do funkcji GPS urządzenia, listę kontaktów i inne informacje już przechowywane w urządzeniu, informacje związane z takim sprzętem wymagają zwiększonej ochrony prywatności. Ponadto tak zwane oprogramowanie szpiegujące, robaki internetowe, ukryte identyfikatory, trwałe pliki cookie oraz inne podobne niepożądane narzędzia umożliwiające śledzenie mogą uzyskać dostęp do urządzenia końcowego użytkownika końcowego bez jego zgody w celu uzyskania dostępu do informacji, przechowywania ukrytych informacji i śledzenia aktywności użytkownika. Informacje dotyczące urządzenia użytkownika końcowego mogą być również gromadzone zdalnie w celu identyfikacji i śledzenia z zastosowaniem technik takich jak pobieranie odbitek linii papilarnych przez urządzenie (*device fingerprinting*), często bez wiedzy użytkownika końcowego, a także mogą poważnie naruszyć prywatność takich użytkowników końcowych. Techniki służące do zakamuflowanego monitorowania działań użytkowników końcowych, na przykład poprzez śledzenie ich aktywności w internecie lub lokalizacji ich urządzenia końcowego, bądź przerwania operacji wykonywanych na urządzeniach końcowych użytkowników końcowych stanowią poważne zagrożenie dla prywatności użytkowników końcowych. Z tego względu jakakolwiek ingerencja tego typu w urządzenie końcowe użytkownika końcowego powinna być dozwolona jedynie za zgodą użytkownika końcowego oraz w konkretnych i przejrzystych celach.

(21) Wyjątki od obowiązku uzyskania zgody na korzystanie z możliwości przetwarzania i przechowywania, jakie daje urządzenie końcowe, lub dostępu do informacji przechowywanych w urządzeniu końcowym powinny ograniczać się do sytuacji, które nie wiążą się z żadną ingerencją w prywatność lub ingerencja ta jest bardzo ograniczona. Nie powinno się na przykład żądać zgody na zezwolenie na techniczne

przechowywanie lub dostęp, gdy jest to absolutnie niezbędne i proporcjonalne w prawnie uzasadnionym celu umożliwienia korzystania z konkretnej usługi wprost żądanej przez użytkownika końcowego. Może to obejmować przechowywanie plików cookie przez okres jednej ustanowionej sesji na stronie internetowej w celu śledzenia wpisów użytkownika przy wypełnianiu formularzy online zajmujących kilka stron. Pliki cookie mogą być również zgodnym z prawem i użytecznym narzędziem, na przykład przy pomiarze ruchu w sieci na stronie internetowej. Zaangażowanie dostawców usług z zakresu społeczeństwa informacyjnego w sprawdzanie konfiguracji w celu zapewnienia usług zgodnych z ustawieniami użytkownika końcowego, a także samo odnotowanie w rejestrach faktu, że urządzenie użytkownika końcowego nie może otrzymać treści żądanych przez użytkownika końcowego, nie stanowią dostępu do takiego urządzenia ani korzystania z możliwości urządzenia w zakresie przetwarzania.

(22) Metody stosowane w celu przedstawienia informacji i uzyskania zgody użytkownika końcowego powinny być możliwie przyjazne dla użytkownika. Z uwagi na wszechobecność trwałych plików cookie oraz innych technik umożliwiających śledzenie użytkownicy końcowi są coraz częściej proszeni o wyrażenie zgody na przechowywanie takich trwałych plików cookie na ich urządzeniach końcowych. W rezultacie użytkownicy końcowi są zasypywani prośbami o wyrażenie zgody. Problem ten można rozwiązać przez zastosowanie technicznych środków umożliwiających wyrażenie zgody, na przykład poprzez przejrzyste i przyjazne dla użytkownika ustawienia. Z tego względu niniejsze rozporządzenie powinno zapewniać możliwość wyrażenia zgody poprzez zastosowanie odpowiednich ustawień przeglądarki lub innych aplikacji. Wybór dokonany przez użytkowników końcowych przy ustanawianiu ogólnych ustawień prywatności przeglądarki lub innej aplikacji powinien być wiążący i wykonalny względem osób trzecich. Przeglądarki internetowe są rodzajem aplikacji oprogramowania, która pozwala na wyszukiwanie i przedstawianie informacje w internecie. Inne typy aplikacji, takie jak aplikacje umożliwiające wykonywanie połączeń, przesyłanie wiadomości lub wyznaczenie trasy, mają takie same możliwości. Przeglądarki internetowe pośredniczą w tym, co odbywa się między użytkownikiem końcowym a stroną internetową. Z tej perspektywy są one na uprzywilejowanej pozycji, aby odgrywać aktywną rolę we wspomaganiu użytkownika końcowego w kontrolowaniu przepływu informacji do urządzenia końcowego i z niego. Ściślej mówiąc, przeglądarki internetowe mogą być wykorzystywane jako blokady, które umożliwiają użytkownikom końcowym zapobieganie dostępowi do informacji lub przechowywaniu informacji z ich urządzenia końcowego (na przykład smartfona, tabletu lub komputera).

(23) Zasadę uwzględniania ochrony danych już w fazie projektowania oraz domyślnej ochrony danych skodyfikowano w art. 25 rozporządzenia (UE) 2016/679. Obecnie ustawieniem domyślnym dla plików cookie w większości obecnych przeglądarek jest „akceptuj wszystkie pliki cookie”. Dostawcy oprogramowania umożliwiającego wyszukiwanie i przedstawianie informacji w internecie powinni mieć zatem obowiązek skonfigurowania oprogramowania, aby oferowało ono opcję uniemożliwienia osobom trzecim przechowywania informacji na urządzeniach końcowych; często przedstawia się to jako opcję „odrzuć pliki cookie osób trzecich”. Użytkownicy końcowi powinni mieć możliwość wyboru spośród szeregu ustawień prywatności, od najwyższych (na przykład „nigdy nie akceptuj plików cookie”) po najniższe (na przykład„zawsze akceptuj pliki cookie) oraz pośrednie (na przykład „odrzuć pliki cookie osób trzecich” lub „akceptuj tylko pliki cookie administratora”).

Takie ustawienia prywatności powinny być przedstawione w sposób widoczny i zrozumiały.

(24) W przypadku przeglądarek internetowych w celu uzyskania zgody użytkowników końcowych zdefiniowanej w rozporządzeniu (UE) 2016/679, na przykład na przechowywanie trwałych plików cookie osób trzecich, konieczne jest między innymi wyraźne działanie potwierdzające ze strony użytkownika końcowego urządzenia końcowego w celu wyrażenia dobrowolnej i świadomej oraz jednoznacznej zgody na przechowywanie takich plików cookie na urządzeniu końcowym i ich dostęp z tego urządzenia. Takie działanie można uznać za potwierdzające, jeżeli – przykładowo – użytkownicy końcowi mają obowiązek aktywnie wybrać opcję „akceptuj pliki cookie osób trzecich" w celu potwierdzenia zgody i otrzymują niezbędne informacje, aby dokonać wyboru. W tym celu konieczne jest zobowiązanie dostawców oprogramowania umożliwiających dostęp do internetu, aby informowali użytkowników końcowych w momencie instalacji o możliwości wyboru ustawień prywatności spośród różnych opcji i prosili użytkowników o dokonanie wyboru. Przekazane informacje nie powinny zniechęcać użytkowników końcowych do wyboru wyższego poziomu ustawień prywatności i powinny zawierać istotne informacje o zagrożeniach związanych z wyrażeniem zgody na przechowywanie plików cookie osób trzecich na komputerze, w tym o kompilowaniu danych z historii wyszukiwania użytkownika obejmującej długi okres oraz wykorzystywaniu takich rejestrów do wysyłania reklam ukierunkowanych. Zachęca się, aby przeglądarki internetowe umożliwiały użytkownikom końcowym łatwą zmianę ustawień prywatności w dowolnym momencie podczas korzystania z nich i umożliwiały użytkownikowi wprowadzanie wyjątków lub wyłączanie z ustawień pewnych stron internetowych bądź określanie, na pliki cookie osób trzecich których stron internetowych należy zawsze zezwalać, a na które nigdy nie należy zezwalać.

(25) Dostęp do sieci łączności elektronicznej wymaga regularnego wysyłania pewnych pakietów danych w celu odnalezienia lub utrzymania połączenia z siecią lub innymi urządzeniami w obrębie sieci. Ponadto aby urządzenia mogły być rozpoznawane w tej sieci, muszą mieć przypisany niepowtarzalny adres. Standardy rozwiązań bezprzewodowych i telefonii komórkowej podobnie wiążą się z wysyłaniem aktywnych sygnałów zawierających niepowtarzalne identyfikatory, takie jak adres MAC, numer IMEI (międzynarodowy numer fabryczny mobilnego aparatu telefonicznego), IMSI itp. Pojedyncza bezprzewodowa stacja bazowa (tj. nadajnik i odbiornik), taka jak punkt dostępu bezprzewodowego, ma określony zasięg, w jakim można przechwycić takie informacje. Pojawili się dostawcy usług internetowych, którzy oferują usługi śledzenia w oparciu o skanowanie informacji związanych z urządzeniem, które to usługi obejmują różne funkcje, w tym liczenie osób, udostępnianie danych o osobach czekających w kolejce, potwierdzenie liczby osób na konkretnym obszarze itp. Te informacje można wykorzystywać w celach bardziej natarczywych, takich jak wysyłanie informacji handlowych ze spersonalizowanymi ofertami do użytkowników końcowych, na przykład gdy wchodzą oni do sklepów. Chociaż część tych funkcji nie wiąże się z dużym zagrożeniem dla prywatności, inne mogą wiązać się na przykład ze śledzeniem osób przez dłuży czas, w tym ze śledzeniem ponownych wizyt w określonych miejscach. Dostawcy zaangażowani w takie praktyki powinni wyświetlać widoczne zawiadomienia zamieszczone na granicy obszaru zasięgu, informujące użytkowników końcowych przed wejściem na taki określony obszar, że w danym okręgu funkcjonuje dana technologia, a także wskazujące cel śledzenia, osobę za nie odpowiedzialną oraz istnienie środków umożliwiających użytkownikowi końcowemu urządzenia końcowego ograniczenie lub

wstrzymanie gromadzenia danych. Dodatkowo powinno się poinformować, gdzie zbierane są dane osobowe, zgodnie z art. 13 rozporządzenia (UE) 2016/679.

(26) Jeżeli przetwarzanie danych pochodzących z łączności elektronicznej przez dostawców usług łączności elektronicznej objęte jest zakresem stosowania niniejszego rozporządzenia, powinno ono na określonych warunkach umożliwiać Unii lub państwom członkowskim prawne ograniczenie niektórych obowiązków i praw, o ile takie ograniczenie stanowi w demokratycznym społeczeństwie niezbędny i proporcjonalny środek do ochrony określonych interesów publicznych, w tym bezpieczeństwa narodowego, obrony, bezpieczeństwa publicznego, oraz zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych lub też wykonywania sankcji karnych, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, jak również innych ważnych celów ogólnego interesu publicznego Unii lub państwa członkowskiego, w szczególności ważnego interesu gospodarczego lub finansowego Unii lub państwa członkowskiego bądź monitorowania, kontrolowania lub pełnienia funkcji regulacyjnej w związku z wykonywaniem władzy publicznej na potrzeby takich interesów. Z tego względu niniejsze rozporządzenie nie powinno wpływać na możliwość prowadzenia przez państwa członkowskie zgodnego z prawem przechwytywania komunikacji elektronicznej lub podejmowania innych środków, jeżeli jest to konieczne i proporcjonalne do zabezpieczenia interesów publicznych wskazanych powyżej, zgodnie z Kartą praw podstawowych Unii Europejskiej i europejską Konwencją o ochronie praw człowieka i podstawowych wolności, w myśl wykładni Trybunału Sprawiedliwości Unii Europejskiej i Europejskiego Trybunału Praw Człowieka. Dostawcy usług łączności elektronicznej powinni zapewnić odpowiednie procedury, aby ułatwić prawnie uzasadnione kierowanie zapytań przez właściwe organy, uwzględniając w stosownych przypadkach również rolę przedstawiciela powołanego na podstawie art. 3 ust. 3.

(27) Jeżeli chodzi o identyfikację rozmów przychodzących, konieczna jest ochrona prawa strony wywołującej do niedopuszczenia do wyświetlania identyfikacji numeru linii wywołującej, z której wychodzi połączenie, oraz prawa strony wywoływanej do odrzucenia połączeń z niezidentyfikowanych linii. W interesie niektórych użytkowników końcowych, w szczególności linii telefonów zaufania lub podobnych organizacji, leży zagwarantowanie anonimowości swoim rozmówcom. Jeżeli chodzi o identyfikację linii, z którą się połączono, konieczna jest ochrona prawa i uzasadnionego interesu strony wywoływanej do niedopuszczenia do wyświetlenia identyfikacji linii, z jaką faktycznie połączyła się strona wywołująca.

(28) W niektórych przypadkach uzasadnione jest nieuwzględnienie wyeliminowania identyfikacji rozmów przychodzących. Prawa użytkowników końcowych do prywatności w odniesieniu do identyfikacji rozmów przychodzących powinny być ograniczone, gdy takie ograniczenie praw jest niezbędne do śledzenia uciążliwych połączeń oraz identyfikacji rozmów przychodzących i danych dotyczących lokalizacji w sytuacji, gdy jest to konieczne do umożliwienia służbom ratunkowym wykonywania ich zadań, takich jak obsługa zgłoszeń eCall, w możliwie najbardziej efektywny sposób.

(29) Istnieje technologia, która umożliwia dostawcom usług łączności elektronicznej ograniczanie na różne sposoby otrzymywania przez użytkowników końcowych niepożądanych połączeń, w tym blokowanie głuchych telefonów oraz innych połączeń stanowiących oszustwa i połączeń uciążliwych. Dostawcy publicznie dostępnych usług łączności interpersonalnej wykorzystującej numery powinni wdrożyć tę

technologię i bezpłatnie chronić użytkowników końcowych przed uciążliwymi połączeniami. Dostawcy powinni zapewnić, aby użytkownicy końcowi byli świadomi istnienia takich funkcji, np. publikując informację na ten temat na swojej stronie internetowej.

(30) Publicznie dostępne spisy numerów użytkowników końcowych usług łączności elektronicznej są dystrybuowane na szeroką skalę. Publicznie dostępne spisy numerów oznaczają wszelkie spisy numerów lub usługi zawierające informacje o użytkownikach końcowych, takie jak numer telefonu (w tym numer telefonu komórkowego) i adres e-mail, oraz obejmują usługę informacyjną. Prawo do prywatności i ochrony danych osobowych osób fizycznych wymaga, aby użytkownicy końcowi będący osobami fizycznymi wyrazili zgodę przed włączeniem ich danych osobowych do spisu numerów. Uzasadniony interes osób prawnych wymaga, aby użytkownicy końcowi będący osobami prawnymi mieli prawo sprzeciwić się zamieszczeniu dotyczących ich danych w spisie numerów.

(31) Jeżeli użytkownicy końcowi będący osobami fizycznymi udzielają zgody na umieszczenie swoich danych w takich spisach numerów, powinni móc określić, w formie zgody, jakie kategorie danych osobowych mają być zamieszczone w spisie numerów (na przykład imię i nazwisko, adres e-mail, adres domowy, nazwa użytkownika, numer telefonu). Ponadto dostawcy publicznie dostępnych spisów numerów powinni informować użytkowników końcowych o celach spisu numerów i funkcji przeszukiwania spisu numerów przed uwzględnieniem ich w tym spisie. Użytkownicy końcowi powinni być w stanie określić w formie zgody, na podstawie jakich kategorii danych osobowych można wyszukiwać ich dane kontaktowe. Kategorie danych osobowych zawartych w spisie numerów i kategorie danych osobowych, na podstawie których można wyszukiwać dane kontaktowe użytkowników końcowych, nie muszą być jednakowe.

(32) W niniejszym rozporządzeniu pojęcie „marketing bezpośredni” odnosi się do wszelkich form reklamy, w ramach których osoba fizyczna lub prawna wysyła materiały do celów marketingu bezpośredniego, kierując je bezpośrednio do jednego zidentyfikowanego użytkownika końcowego lub większej liczby zidentyfikowanych użytkowników końcowych lub do możliwych do zidentyfikowania użytkowników końcowych przy użyciu usług łączności elektronicznej. Poza oferowaniem produktów i usług w celach komercyjnych powinno to obejmować również wiadomości wysyłane przez partie polityczne, które kontaktują się z osobami fizycznymi za pośrednictwem usług łączności elektronicznej, aby promować swoje partie. To samo powinno dotyczyć wiadomości wysyłanych przez inne organizacje nienastawione na zysk w celu promowania działalności organizacji.

(33) Należy zapewnić zabezpieczenia, aby chronić użytkowników końcowych przed niezamówionymi komunikatami rozsyłanymi w celu prowadzenia marketingu bezpośredniego, które stanowią ingerencję w życie prywatne użytkowników końcowych. Stopień naruszenia prywatności i uciążliwości jest uważany za stosunkowo podobny niezależnie od szerokiego zakresu technologii i kanałów wykorzystywanych do prowadzenia takiej łączności elektronicznej, czy to z zastosowaniem zautomatyzowanych systemów wywoływania i łączności, czy komunikatorów internetowych, poczty elektronicznej, wiadomości tekstowych, wiadomości graficznych, technologii Bluetooth itp. Z tego względu uzasadnione jest wymaganie uzyskania zgody użytkownika końcowego przed wysłaniem komercyjnych materiałów elektronicznych do celów marketingu bezpośredniego do użytkowników końcowych, aby skutecznie chronić osoby fizyczne przed

ingerowaniem w ich życie prywatne, a osoby prawne – przed ingerowaniem w ich uzasadniony interes. Pewność prawa i potrzeba zapewnienia, aby przepisy chroniące przed niezamawianymi materiałami elektronicznymi pozostały aktualne w przyszłości uzasadnia potrzebę zdefiniowania jednego zestawu przepisów, które nie zmieniają się w zależności od technologii stosowanej do przekazywania niezamówionych komunikatów, a jednocześnie gwarantują równoważny poziom ochrony wszystkim obywatelom w całej Unii. Niemniej jednak zasadne jest zezwolenie na korzystanie z danych kontaktowych w postaci adresu e-mail w odniesieniu do istniejącej relacji z klientem w celu oferowania podobnych produktów lub usług. Taka możliwość powinna dotyczyć wyłącznie tego przedsiębiorstwa, które uzyskało elektroniczne dane kontaktowe zgodnie z rozporządzeniem (UE) 2016/679.

(34) Gdy użytkownicy końcowi wyrazili zgodę na otrzymanie niezamówionych komunikatów do celów marketingu bezpośredniego, nadal powinni mieć możliwość łatwego wycofania zgody w dowolnym momencie. Aby ułatwić skuteczne wykonanie przepisów unijnych dotyczących niezamówionych wiadomości do celów marketingu bezpośredniego, należy zakazać maskowania tożsamości i korzystania z fałszywej tożsamości, fałszywych adresów zwrotnych lub numerów przy wysyłaniu niezamówionych informacji handlowych do celów marketingu bezpośredniego. Niezamówione komunikaty marketingowe powinny być zatem wyraźnie rozpoznawalne jako takie i powinny wskazywać tożsamość osoby prawnej lub fizycznej, która je przesyła lub w imieniu której są przesyłane, oraz zapewniać informacje niezbędne dla odbiorców do wykonania ich prawa do sprzeciwienia się otrzymywaniu dalszych pisemnych lub ustnych wiadomości marketingowych.

(35) Aby umożliwić łatwe wycofanie zgody, osoby prawne lub fizyczne wysyłające materiały do celów marketingu bezpośredniego za pośrednictwem poczty elektronicznej powinny podawać link lub działający adres poczty elektronicznej, przez który użytkownicy końcowi mogą wycofać zgodę. Osoby prawne lub fizyczne prowadzące łączność do celów marketingu bezpośredniego przez połączenia głosowe oraz połączenia dokonywane w ramach zautomatyzowanych systemów wywoływania i łączności powinny wyświetlać swój identyfikator linii, który może służyć do skontaktowania się z przedsiębiorstwem, lub konkretny kod wskazujący, że dane połączenie jest połączeniem marketingowym.

(36) Połączenia głosowe w ramach marketingu bezpośredniego, które nie wiążą się ze stosowaniem zautomatyzowanych systemów wywoływania i łączności są kosztowniejsze dla nadawcy i nie wiążą się z kosztami finansowymi dla użytkowników końcowych. Państwa członkowskie powinny zatem móc ustanowić lub utrzymać krajowe systemy zezwalające na wykonywanie takich połączeń wyłącznie do użytkowników końcowych, którzy nie wyrazili sprzeciwu w tej kwestii.

(37) Dostawcy usług oferujący usługi łączności elektronicznej powinni informować użytkowników końcowych o środkach, jakie mogą podjąć, aby chronić bezpieczeństwo swoich łączności, przykładowo poprzez stosowanie konkretnych rodzajów oprogramowania lub technologii szyfrowania. Wymóg informowania użytkowników końcowych 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 z obowiązku przywrócenia normalnego poziomu bezpieczeństwa usług. Udzielanie abonentowi informacji na temat zagrożeń bezpieczeństwa powinno odbywać się bezpłatnie. Poziom bezpieczeństwa ocenia się w świetle art. 32 rozporządzenia (UE) 2016/679.

(38) Aby zapewnić pełną spójność z rozporządzeniem (UE) 2016/679, egzekwowanie przepisów niniejszego rozporządzenia należy powierzyć tym samym organom, które odpowiadają za egzekwowanie przepisów rozporządzenia (UE) 2016/679, a niniejsze rozporządzenie opiera się na mechanizmie spójności określonym w rozporządzeniu (UE) 2016/679. Aby uwzględnić swoją strukturę konstytucyjną, organizacyjną i administracyjną, państwa członkowskie powinny mieć możliwość posiadania więcej niż jednego organu nadzorczego. Organy nadzorcze powinny również odpowiadać za monitorowanie stosowania niniejszego rozporządzenia dotyczącego danych pochodzących z łączności elektronicznej w odniesieniu do osób prawnych. Takie dodatkowe zadania nie powinny zagrażać zdolności organu nadzorczego do realizacji jego zadań dotyczących ochrony danych osobowych na mocy rozporządzenia (UE) 2016/679 i niniejszego rozporządzenia. Każdy organ nadzorczy powinien dysponować dodatkowymi zasobami finansowymi i osobowymi, lokalami oraz infrastrukturą, które są niezbędne do skutecznej realizacji zadań wynikających z niniejszego rozporządzenia

(39) Każdy organ nadzorczy powinien mieć kompetencje, aby wykonywać uprawnienia i realizować zadania określone w niniejszym rozporządzeniu na terytorium własnego państwa członkowskiego. Aby zapewnić spójne monitorowanie i wykonywanie niniejszego rozporządzenia w całej Unii, bez uszczerbku dla uprawnień organów ścigania wynikających z przepisów państwa członkowskiego, organy nadzorcze w każdym państwie członkowskim powinny mieć takie same zadania i skuteczne uprawnienia, aby zwracać uwagę organów sądowych na naruszenia niniejszego rozporządzenia oraz angażować się w postępowania sądowe. Zachęca się państwa członkowskie i ich organy nadzorcze, aby przy stosowaniu niniejszego rozporządzenia uwzględniały szczególne potrzeby mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.

(40) Aby wzmocnić egzekwowanie przepisów niniejszego rozporządzenia, każdy organ nadzorczy powinien mieć prawo nakładania sankcji, w tym administracyjnych kar pieniężnych, za wszelkie naruszenia niniejszego rozporządzenia, w uzupełnieniu lub zamiast innych właściwych środków wynikających z niniejszego rozporządzenia. W niniejszym rozporządzeniu należy wymienić rodzaje naruszeń oraz wskazać górną granicę i kryteria ustalania związanych z nimi administracyjnych kar pieniężnych, które właściwy organ nadzorczy powinien określać indywidualnie dla każdego przypadku, biorąc pod uwagę wszystkie stosowne okoliczności danej sytuacji, z należytym uwzględnieniem w szczególności charakteru, wagi, czasu trwania naruszenia i jego konsekwencji, a także środków podjętych w celu zastosowania się do obowiązków wynikających z niniejszego rozporządzenia oraz w celu zapobieżenia konsekwencjom naruszenia bądź w celu zminimalizowania tych konsekwencji. Do celów ustalenia kary finansowej na mocy niniejszego rozporządzenia przedsiębiorstwo należy rozumieć jako przedsiębiorstwo w myśl art. 101 i 102 Traktatu.

(41) Aby spełnić cele niniejszego rozporządzenia, mianowicie chronić podstawowe prawa i wolności osób fizycznych, w szczególności prawo do ochrony danych osobowych, oraz zapewnić swobodny przepływ danych osobowych w Unii, należy przekazać Komisji uprawnienia do przyjmowania aktów zgodnie z art. 290 Traktatu celem uzupełniania niniejszego rozporządzenia. W szczególności należy przyjmować akty delegowane odnoszące się do informacji, jakie mają być przedstawiane, w tym poprzez standardowe znaki graficzne, w celu zapewnienia widocznego i czytelnego przedstawienia zbioru informacji wysyłanych przez urządzenie końcowe, celu takiego działania, osoby odpowiedzialnej oraz wszelkich działań, jakie użytkownik końcowy

urządzenia końcowego może podjąć, aby ograniczyć takie gromadzenie. Akty delegowane są również konieczne, aby określić kod służący identyfikacji połączeń wykonywanych w ramach marketingu bezpośredniego, w tym połączeń wykonywanych przez zautomatyzowane systemy wywoływania i łączności. Szczególnie ważne jest, aby Komisja prowadziła odpowiednie konsultacje i aby odbywały się one zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa[8]. W szczególności, aby zapewnić udział na równych zasadach Parlamentu Europejskiego i Rady w przygotowaniu aktów delegowanych, instytucje te otrzymują wszelkie dokumenty w tym samym czasie co eksperci państw członkowskich, a eksperci tych instytucji mogą systematycznie brać udział w posiedzeniach grup ekspertów Komisji zajmujących się przygotowaniem aktów delegowanych. Ponadto aby zapewnić jednolite warunki wdrażania niniejszego rozporządzenia, należy powierzyć Komisji uprawnienia wykonawcze, tak jak to przewiduje niniejsze rozporządzenie. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem (UE) nr 182/2011.

(42) Ponieważ celu niniejszego rozporządzenia, mianowicie zapewnienia równoważnego stopnia ochrony osób fizycznych i prawnych oraz swobodnego przepływu danych pochodzących z łączności elektronicznej w całej Unii, nie mogą w wystarczającym stopniu osiągnąć państwa członkowskie,z uwagi na zakres i skutki proponowanego działania możliwe jest natomiast lepsze jego osiągnięcie na szczeblu unijnym, Unia może przyjąć środki zgodnie z zasadą pomocniczości, o której mowa w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tego celu.

(43) Należy uchylić dyrektywę 2002/58/WE,

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

[8] Porozumienie międzyinstytucjonalne pomiędzy Parlamentem Europejskim, Radą Unii Europejskiej i Komisją Europejską z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa (Dz.U. L 123 z 12.5.2016, s. 1–14).

ROZDZIAŁ I
PRZEPISY OGÓLNE

Artykuł 1
Przedmiot

1. Niniejszym rozporządzeniem ustanawia się zasady dotyczące ochrony podstawowych praw i wolności osób fizycznych i prawnych w odniesieniu do świadczenia usług łączności elektronicznej i korzystania z takich usług, w szczególności prawa do poszanowania życia prywatnego i komunikowania się oraz prawa do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.

2. Niniejsze rozporządzenie zapewnia swobodny przepływ danych pochodzących z łączności elektronicznej i usług łączności elektronicznej w obrębie Unii, który to przepływ nie będzie ani ograniczany, ani zakazywany ze względów związanych z poszanowaniem życia prywatnego i komunikowania się osób fizycznych i prawnych oraz ochroną osób fizycznych w związku z przetwarzaniem danych osobowych.

3. Przepisy niniejszego rozporządzenia uszczegóławiają i uzupełniają rozporządzenie (UE) 2016/679 poprzez określenie konkretnych zasad do celów wspomnianych w ust. 1 i 2.

Artykuł 2
Zakres przedmiotowy

1. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych pochodzących z łączności elektronicznej prowadzonej w związku ze świadczeniem usług łączności elektronicznej i korzystaniem z tych usług oraz do informacji związanych z urządzeniem końcowym użytkowników końcowych.

2. Niniejsze rozporządzenie nie ma zastosowania do:

a) działań nieobjętych zakresem prawa Unii;

b) działań państw członkowskich, które są objęte zakresem rozdziału 2 tytułu V Traktatu o Unii Europejskiej;

c) usług łączności elektronicznej, które nie są dostępne publicznie;

d) działań prowadzonych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania sankcji karnych, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom;

3. Przetwarzanie danych pochodzących z łączności elektronicznej przez instytucje, organy, urzędy i agencje Unii reguluje rozporządzenie (UE) 00/0000 [nowe rozporządzenie zastępujące rozporządzenie 45/2001].

4. Niniejsze rozporządzenie nie powoduje uszczerbku dla stosowania dyrektywy 2000/31/WE[9], w szczególności zasad odpowiedzialności usługodawców będących pośrednikami zawartych w art. 12–15 tej dyrektywy.

[9] Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu

5. Niniejsze rozporządzenie nie narusza przepisów dyrektywy 2014/53/UE.

Artykuł 3
Zakres terytorialny i przedstawiciel

1. Niniejsze rozporządzenie ma zastosowanie do:

a) świadczenia usług łączności elektronicznej na rzecz użytkowników końcowych w Unii, niezależnie od tego, czy od użytkownika końcowego wymaga się płatności;

b) korzystania z takich usług;

c) ochrony informacji związanych z urządzeniem końcowym użytkowników końcowych znajdujących się w Unii.

2. Jeżeli dostawca usług łączności elektronicznej nie ma siedziby w Unii, powołuje na piśmie swojego przedstawiciela w Unii.

3. Przedstawiciel zostaje ustanowiony w jednym z państw członkowskich, w którym znajdują się użytkownicy końcowi takich usług łączności elektronicznej.

4. Przedstawiciel jest upoważniony do udzielania odpowiedzi na pytania i informacji dodatkowo względem dostawcy, którego reprezentuje, lub zamiast niego, w szczególności organom nadzorczym i użytkownikom końcowym, we wszystkich kwestiach związanych z przetwarzaniem danych pochodzących z łączności elektronicznej do celów zapewnienia zgodności z niniejszym rozporządzeniem.

5. Powołanie przedstawiciela zgodnie z ust. 2 odbywa się bez uszczerbku dla kroków prawnych, jakie mogą zostać podjęte wobec osoby fizycznej lub prawnej, która przetwarza dane pochodzące z łączności elektronicznej w związku ze świadczeniem usług łączności elektronicznej spoza Unii na rzecz użytkowników końcowych w Unii.

Artykuł 4
Definicje

1. Do celów niniejszego rozporządzenia stosuje się następujące definicje:

a) definicje z rozporządzenia (UE) 2016/679;

b) definicje: „sieci łączności elektronicznej”, „usługi łączności elektronicznej”, „usługi łączności interpersonalnej”, „usługi łączności interpersonalnej wykorzystującej numery”, „usługi łączności interpersonalnej niewykorzystującej numerów”, „użytkownika końcowego” oraz „wywołania” zawarte odpowiednio w art. 2 pkt 1), 4), 5), 6), 7), 14) i 21) [dyrektywy ustanawiającej Europejski kodeks łączności elektronicznej];

c) definicja „urządzenia końcowego” z art. 1 pkt 1 dyrektywy Komisji 2008/63/WE[10].

2. Dla celów pkt 1 lit. b) definicja „usługi łączności interpersonalnej” obejmuje usługi, które umożliwiają komunikację interpersonalną i interaktywną chociażby w ramach pomniejszej funkcji wspomagającej, która jest nieodłącznie powiązana z inną usługą.

---

elektronicznego w ramach rynku wewnętrznego („dyrektywa o handlu elektronicznym”) (OJ L 178 z 17.7.2000, s. 1–16).

[10] Dyrektywa Komisji 2008/63/WE z dnia 20 czerwca 2008 r. w sprawie konkurencji na rynkach końcowych urządzeń telekomunikacyjnych (Dz.U. L 162 z 21.6.2008, s. 20–26).

3. Dodatkowo dla celów niniejszego rozporządzenia mają zastosowanie następujące definicje:

a) „dane pochodzące z łączności elektronicznej” oznaczają treść łączności elektronicznej oraz metadane pochodzące z łączności elektronicznej;

b) „treść łączności elektronicznej” oznacza treści przekazywane z wykorzystaniem usług łączności elektronicznej, takie jak tekst, głos, wideo, obrazy i dźwięk;

c) „metadane pochodzące z łączności elektronicznej” oznaczają dane przetwarzane w sieci łączności elektronicznej do celów przesyłania, dystrybuowania lub wymiany treści łączności elektronicznej; w tym dane służące do śledzenia i zidentyfikowania źródła i miejsca docelowego przypadku łączności, dane dotyczące lokalizacji urządzenia wygenerowane w związku ze świadczeniem usług łączności elektronicznej oraz daty, godziny, czasu trwania oraz rodzaju łączności;

d) „publicznie dostępny spis numerów” oznacza spis numerów użytkowników końcowych usług łączności elektronicznej, w formie papierowej lub elektronicznej, który jest publikowany lub udostępniany ogółowi społeczeństwa lub części społeczeństwa, między innymi za pośrednictwem biura numerów;

e) „poczta elektroniczna” oznacza dowolną wiadomość elektroniczną zawierającą informację, taką jak tekst, głos, wideo, dźwięk lub obraz, przesyłaną przez sieć łączności elektronicznej, która to wiadomość może być przechowywana w sieci lub w powiązanej infrastrukturze obliczeniowej lub w urządzeniu końcowym odbiorcy takiej wiadomości;

f) „komunikaty marketingu bezpośredniego” oznaczają wszelkie formy reklamowania, pisemne lub ustne, przesyłane jednemu zidentyfikowanemu lub dającemu się zidentyfikować użytkownikowi końcowemu usług łączności elektronicznej lub większej ich liczbie, obejmujące korzystanie ze zautomatyzowanych systemów wywoływania i łączności, z interakcją ludzką lub bez niej, z poczty elektronicznej, wiadomości tekstowych itp.;

g) „połączenia głosowe w ramach marketingu bezpośredniego” oznaczają prowadzone na żywo połączenia, które nie wiążą się z korzystaniem ze zautomatyzowanych systemów wywoływania i łączności;

h) „zautomatyzowane systemy wywoływania i łączności” oznaczają systemy zdolne do automatycznego inicjowania wywołań jednego odbiorcy lub wielu odbiorców zgodnie z instrukcją ustaloną dla danego systemu i przesyłające dźwięki niebędące mową na żywo, w tym wywołań dokonywanych z użyciem zautomatyzowanych systemów wywoływania i łączności, które łączą osobę wywoływaną z inną osobą.

ROZDZIAŁ II
OCHRONA ŁĄCZNOŚCI ELEKTRONICZNEJ OSÓB FIZYCZNYCH I PRAWNYCH ORAZ INFORMACJI PRZECHOWYWANYCH W ICH URZĄDZENIACH KOŃCOWYCH

Artykuł 5
Poufność danych pochodzących z łączności elektronicznej

Dane pochodzące z łączności elektronicznej są poufne. Wszelka ingerencja w dane pochodzące z łączności elektronicznej, taka jak słuchanie, podsłuchiwanie, przechowywanie, monitorowanie, skanowanie lub innego rodzaju przechwytywanie, nadzorowanie lub przetwarzanie danych pochodzących z łączności elektronicznej przez osoby inne niż użytkownicy końcowi, jest zakazana, z wyjątkiem sytuacji dozwolonych niniejszym rozporządzeniem.

Artykuł 6
Dozwolone przetwarzanie danych pochodzących z łączności elektronicznej

1. Dostawcy sieci i usług łączności elektronicznej mogą przetwarzać dane pochodzące z łączności elektronicznej, jeżeli:

a) jest to konieczne do realizacji przesyłu komunikatu – przez okres konieczny do realizacji takiego celu; lub

b) jest to konieczne w celu utrzymania lub przywrócenia bezpieczeństwa sieci i usług łączności elektronicznej lub wykrycia usterek technicznych lub błędów w przesyłaniu komunikatów elektronicznych – przez okres konieczny do realizacji takiego celu.

2. Dostawcy usług łączności elektronicznej mogą przetwarzać metadane pochodzące z łączności elektronicznej, jeżeli:

a) jest to konieczne do spełnienia obowiązkowych wymogów dotyczących jakości usług wynikających z [dyrektywy ustanawiającej Europejski kodeks łączności elektronicznej] lub rozporządzenia (UE) 2015/2120[11] – przez okres konieczny do realizacji takiego celu; lub

b) jest to konieczne w celu naliczania opłat, obliczania płatności międzyoperatorskich, wykrywania lub powstrzymywania oszustw lub nadużyć w zakresie usług łączności elektronicznej lub abonamentu na te usługi; lub

c) użytkownik końcowy, którego to dotyczy, wyraził zgodę na przetwarzanie jego metadanych komunikacyjnych dla jednego celu lub dla kilku celów, w tym dla celu świadczenia konkretnych usług na rzecz takiego użytkownika końcowego, pod warunkiem, że ten cel lub te cele nie mogłyby być zrealizowane przez przetwarzanie informacji poddanych anonimizacji.

[11] rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/2120 z dnia 25 listopada 2015 r. ustanawiające środki dotyczące dostępu do otwartego internetu oraz zmieniające dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, a także rozporządzenie (UE) nr 531/2012 w sprawie roamingu w publicznych sieciach łączności ruchomej wewnątrz Unii (Dz.U. L 310 z 26.11.2015, s. 1–18).

3. Dostawcy usług łączności elektronicznej mogą przetwarzać treść łączności elektronicznej wyłącznie

a) w celu świadczenia konkretnej usługi na rzecz użytkownika końcowego, jeżeli dany użytkownik końcowy lub dani użytkownicy końcowi wyrazili zgodę na przetwarzanie treści ich łączności elektronicznej i usługa ta nie może być świadczona bez przetwarzania tej treści; lub

b) jeżeli wszyscy użytkownicy końcowi, których to dotyczy, wyrazili zgodę na przetwarzanie treści ich łączności elektronicznej dla jednego celu lub dla kilku celów, które nie mogę być zrealizowane przez przetwarzanie informacji poddanych anonimizacji, a dostawca skonsultował się z organem nadzorczym. Do konsultacji z organami nadzorczymi stosuje się art. 36 pkt 2 i 3 rozporządzenia (UE) 2016/679.

Artykuł 7

Przechowywanie i usuwanie danych pochodzących z łączności elektronicznej

1. Nie naruszając przepisów art. 6 ust. 1 lit. b) oraz art. 6 ust. 3 lit. a) i b) dostawca usługi łączności elektronicznej usuwa treść łączności elektronicznej lub dokonuje anonimizacji danych po otrzymaniu treści łączności elektronicznej przez docelowego odbiorcę lub docelowych odbiorców. Dane te mogą być zapisywane lub przechowywane przez użytkowników końcowych lub przez osoby trzecie, którym powierzono ich zapisywanie, przechowywanie lub przetwarzanie w innych sposób, zgodnie z rozporządzeniem (UE) 2016/679.

2. Nie naruszając przepisów art. 6 ust. 1 lit. b) oraz art. 6 ust. 2 lit. a) i c) dostawca usługi łączności elektronicznej usuwa metadane pochodzące z łączności elektronicznej lub dokonuje anonimizacji danych, gdy nie są już one potrzebne dla celów przesyłu komunikatu.

3. Jeżeli przetwarzanie metadanych pochodzących z łączności elektronicznej odbywa się w celu naliczenia płatności zgodnie z art. 6 ust. 2 lit. b), odpowiednie metadane mogą być przechowywane do czasu zakończenia okresu, w jakim można zgodnie z prawem zakwestionować rachunek lub w jakim można egzekwować płatność zgodnie z prawem krajowym.

Artykuł 8

Ochrona informacji przechowywanych w urządzeniu końcowym użytkownika końcowego i dotyczących urządzenia końcowego użytkownika końcowego.

1. Korzystanie z możliwości urządzenia końcowego do przetwarzania i przechowywania oraz gromadzenie informacji z urządzenia końcowego użytkowników końcowych, w tym informacji o oprogramowaniu i sprzęcie, inne niż dokonywane przez użytkownika końcowego, którego dotyczą, jest zakazane, z wyjątkiem wystąpienia następujących podstaw:

a) jest to konieczne jedynie w celu dokonania transmisji komunikatu elektronicznego za pośrednictwem sieci łączności elektronicznej; lub

b) użytkownik końcowy wyraził na to zgodę; lub

c) jest to konieczne do świadczenia usługi społeczeństwa informacyjnego żądanej przez użytkownika końcowego; lub

d) jeżeli jest to konieczne w celu pomiaru odbiorców w sieci web, pod warunkiem, że pomiar taki jest wykonywany przez dostawcę usługi społeczeństwa informacyjnego żądanej przez użytkownika końcowego.

2. Gromadzenie informacji wysyłanych przez urządzenie końcowe w celu umożliwienia podłączenia go do innego urządzenia lub do sprzętu sieciowego jest zakazane, z wyjątkiem sytuacji, w której:

a) wykonuje się to wyłącznie przez czas niezbędny do ustanowienia połączenia i w celu jego ustanowienia; lub

b) w miejscu gromadzenia danych osobowych prezentuje się jasne i wyraźne zawiadomienie informujące przynajmniej o sposobach gromadzenia, celu, osobie odpowiedzialnej oraz zawierające inne informacje wymagane na podstawie art. 13 rozporządzenia (UE) 2016/679, jak również informacje o wszelkich działaniach, jakie może podjąć użytkownik końcowy urządzenia końcowego, aby wstrzymać lub ograniczyć do minimum takie gromadzenie.

Gromadzenie takich informacji jest uzależnione od zastosowania właściwych środków technicznych i organizacyjnych, aby zapewnić poziom bezpieczeństwa właściwy dla ryzyka, jak określono w art. 32 rozporządzenia (UE) 2016/679.

3. Informacje przekazywane zgodnie z ust. 2 lit. b) można przekazywać w połączeniu ze standardowymi znakami graficznymi w celu zapewnienia znaczącego opisu gromadzenia w sposób widoczny, zrozumiały i czytelny.

4. Komisji przysługuje prawo do przyjmowania aktów delegowanych zgodnie z art. 27 określających informacje przedstawiane za pomocą standardowych znaków graficznych oraz procedury ustanowienia standardowych znaków graficznych.

Artykuł 9
Zgoda

1. Zastosowanie mają definicja i warunki zgody przewidziane w art. 4 ust. 11 i art. 7 rozporządzenia (UE) 2016/679/UE.

2. Nie naruszając przepisów ust. 1, gdy jest to techniczne możliwe i wykonalne, dla celów art. 8 ust. 1 lit. b), zgodę można wyrazić poprzez wykorzystanie właściwych ustawień technicznych oprogramowania umożliwiającego dostęp do internetu.

3. Użytkownicy końcowi, którzy wyrazili zgodę na przetwarzanie danych pochodzących z łączności elektronicznej, o czym mowa w art. 6 ust. 2 lit. c) oraz art. 6 ust. 3 lit. a) i b), mają możliwość wycofania swojej zgody w dowolnej chwili zgodnie z art. 7 ust. 3 rozporządzenia (UE) 2016/679 i przypomina im się o takiej możliwości co 6 miesięcy przez cały okres przetwarzania.

Artykuł 10
Informacje dotyczące ustawień prywatności i opcje ustawień prywatności, które należy przekazać

1. Wprowadzane do obrotu oprogramowanie umożliwiające łączność elektroniczną, w tym wyszukiwanie i przedstawianie informacji w internecie, daje możliwość zapobiegania przechowywaniu informacji przez osoby trzecie na urządzeniu końcowym użytkownika końcowego lub przetwarzaniu przez osoby trzecie informacji przechowywanych już na tym urządzeniu.

2. Przy instalacji oprogramowania użytkownik końcowy jest informowany o ustawieniach prywatności i aby kontynuować instalację, musi wyrazić zgodę na ustawienia.

3. W przypadku oprogramowania, które było już zainstalowane w dniu 25 maja 2018 r., wymóg, o którym mowa w ust. 1 i 2, musi być spełniony w czasie pierwszej aktualizacji oprogramowania, ale nie później niż 25 sierpnia 2018 r.

Artykuł 11
Ograniczenia

1. Zakres zobowiązań i praw przewidzianych w art. 5–8 można ograniczyć w drodze środka legislacyjnego w ramach prawa Unii lub prawa krajowego, w sytuacji gdy takie ograniczenie odbywa się z poszanowaniem istoty podstawowych praw i wolności oraz gdy jest to środek konieczny, właściwy i proporcjonalny w demokratycznym społeczeństwie do zabezpieczenia jednego interesu publicznego lub wielu interesów publicznych, o których mowa w art. 23 ust. 1 lit. a)–e) rozporządzenia (UE) 2016/679 lub realizacji funkcji monitorowania, inspekcji lub regulacji w związku z wykonywaniem władzy publicznej na potrzeby takich interesów.

2. Dostawcy usług łączności elektronicznej ustanawiają procedury wewnętrzne dotyczące reagowania na żądania dostępu do danych pochodzących z łączności elektronicznej użytkowników końcowych na podstawie środka legislacyjnego przyjętego zgodnie z ust. 1. Na żądanie przedstawiają oni właściwemu organowi nadzorczemu informacje o tych procedurach, liczbie otrzymanych wniosków, ich uzasadnieniu prawnym oraz udzielonej przez nich odpowiedzi.

ROZDZIAŁ III
PRAWA OSÓB FIZYCZNYCH I PRAWNYCH DO KONTROLOWANIA ŁĄCZNOŚCI ELEKTRONICZNEJ

Artykuł 12
Wyświetlanie i ograniczenie identyfikacji rozmów przychodzących i wychodzących

1. Jeżeli wyświetlanie połączenia i identyfikację rozmów przychodzących oferuje się zgodnie z art. 107 [dyrektywy ustanawiającej Europejski kodeks łączności elektronicznej] dostawcy publicznie dostępnych usług łączności interpersonalnej wykorzystujących numery zapewniają:

a) wywołującemu użytkownikowi końcowemu możliwość zablokowania wyświetlania identyfikacji rozmów przychodzących w odniesieniu do rozmowy, do połączenia lub na stałe;

b) wywoływanemu użytkownikowi końcowemu możliwość zablokowania wyświetlania identyfikacji rozmów przychodzących w odniesieniu do rozmów przychodzących;

c) wywoływanemu użytkownikowi końcowemu możliwość odrzucenia rozmów przychodzących, jeżeli wyświetlanie identyfikacji rozmów przychodzących zostało zablokowane przez wywołującego użytkownika końcowego;

d) wywoływanemu użytkownikowi końcowemu możliwość zablokowania wyświetlania identyfikacji rozmów wychodzących wywołującemu użytkownikowi końcowemu.

2. Możliwości, o których mowa w ust. 1 lit. a), b), c) i d), zapewnia się użytkownikom końcowym prostymi środkami i bezpłatnie.

3. Przepisy ust. 1 lit. a) stosuje się również w odniesieniu do połączeń do państw trzecich wychodzących z Unii. Przepisy ust. 1 lit. b), c) i d) stosuje się również w odniesieniu do połączeń przychodzących wychodzących z państw trzecich.

4. Jeżeli oferuje się wyświetlenie identyfikacji rozmów przychodzących lub wychodzących, dostawcy publicznie dostępnych usług łączności interpersonalnej wykorzystującej numery zapewniają społeczeństwu informacje dotyczące wariantów wskazanych w ust. 1 lit. a), b), c) i d).

Artykuł 13
Wyjątki dotyczące wyświetlania i ograniczenia identyfikacji rozmów przychodzących i wychodzących

1. Niezależnie od tego, czy wywołujący użytkownik końcowy zablokował wyświetlanie identyfikacji rozmów przychodzących, w sytuacji wykonywania połączenia do służb ratunkowych dostawcy publicznie dostępnych usług łączności interpersonalnej wykorzystującej numery pomijają usunięcie wyświetlania identyfikacji rozmów przychodzących oraz odmowę lub brak zgody użytkownika końcowego na przetwarzanie metadanych na poziomie linii na potrzeby organizacji zajmującej się łącznością w sytuacjach nagłych, w tym publicznych punktów przyjmowania zgłoszeń o wypadkach, do celów reagowania na takie zgłoszenia.

2. Państwa członkowskie ustanawiają bardziej szczegółowe przepisy co do ustalenia procedur i okoliczności, w których dostawcy publicznie dostępnych usług łączności interpersonalnej wykorzystującej numery tymczasowo pomijają wyłączenie wyświetlania identyfikacji rozmów przychodzących, jeżeli użytkownicy końcowi zażądają śledzenia złośliwych lub uciążliwych połączeń.

Artykuł 14
Blokowanie połączeń przychodzących

Dostawcy publicznie dostępnych usług łączności interpersonalnej wykorzystującej numery wdrażają najnowocześniejsze środki, aby ograniczyć otrzymywanie przez użytkowników końcowych niepożądanych połączeń, jak również zapewniają – bezpłatnie – wywoływanemu użytkownikowi końcowemu następujące możliwości:

a) blokowanie rozmów przychodzących z konkretnych numerów lub z anonimowych źródeł;

b) zatrzymanie automatycznego przekierowywania połączeń przez osobę trzecią na urządzenie końcowe użytkownika końcowego.

Artykuł 15
Publicznie dostępne spisy numerów

1. Dostawcy publicznie dostępnych spisów numerów uzyskują zgodę użytkowników końcowych, którzy są osobami fizycznymi, na umieszczenie ich danych osobowych w spisie, a przez to uzyskują zgodę tych użytkowników końcowych na włączenie ich danych jako kategorii danych osobowych w zakresie, w jakim takie dane są istotne na potrzeby tego spisu według dostawcy spisu. Dostawcy dają użytkownikom

końcowym, którzy są osobami fizycznymi, środki służące weryfikowaniu, poprawianiu i usuwaniu takich danych.

2. Dostawcy publicznie dostępnego spisu numerów informują użytkowników końcowych będących osobami fizycznymi, których dane osobowe znajdują się w spisie, o dostępności funkcji przeszukiwania spisu i uzyskują zgodę użytkowników końcowych przed aktywowaniem funkcji wyszukiwania w odniesieniu do ich danych.

3. Dostawcy publicznie dostępnych spisów numerów zapewniają użytkownikom końcowym, którzy są osobami prawnymi, możliwość sprzeciwienia się włączeniu do spisu danych, które ich dotyczą. Dostawcy dają takim użytkownikom końcowym, którzy są osobami prawnymi, środki służące do weryfikowania, poprawiania i usuwania takich danych.

4. Możliwość nieuwzględniania użytkowników końcowych w publicznie dostępnych spisach numerów lub zweryfikowania, poprawienia bądź usunięcia danych, które ich dotyczą, oferuje się bezpłatnie.

Artykuł 16
Niezamawiane materiały

1. Osoby fizyczne lub prawne mogą korzystać z usług łączności elektronicznej w celu wysyłania komunikatów do celów marketingu bezpośredniego użytkownikom końcowym będącym osobami fizycznymi, którzy wyrazili na to zgodę.

2. Jeżeli osoba fizyczna lub prawna otrzymuje od swojego klienta elektroniczne dane kontaktowe dotyczące poczty elektronicznej w związku ze sprzedażą produktu lub usługi, zgodnie z rozporządzeniem (UE) 2016/679, taka osoba fizyczna lub prawna może wykorzystywać te elektroniczne dane kontaktowe do celów marketingu bezpośredniego własnych podobnych produktów lub usług jedynie wówczas, gdy klienci mają jasną i wyraźną możliwość wyrażenia – bezpłatnie i w łatwy sposób – sprzeciwu wobec takiego wykorzystania danych. Prawo do wyrażenia sprzeciwu przysługuje w czasie gromadzenia danych i za każdym razem, gdy wysyłana jest wiadomość.

3. Nie naruszając przepisów ust. 1 i 2 osoba fizyczna lub prawna korzystająca z usług łączności elektronicznej w celach wykonywania połączeń w ramach marketingu bezpośredniego:

a) podaje identyfikator linii, pod którą można się z nią skontaktować; lub

b) podaje konkretny kod lub prefiks umożliwiający rozpoznanie, że połączenie jest połączeniem marketingowym.

4. Niezależnie od ust. 1 państwa członkowskie mogą przewidzieć prawem, że wykonywanie połączeń głosowych w ramach marketingu bezpośredniego do użytkowników końcowych, którzy są osobami fizycznymi, jest dozwolone wyłącznie w odniesieniu do użytkowników końcowych będących osobami fizycznymi, którzy nie wyrazili sprzeciwu wobec otrzymywania tych połączeń.

5. Państwa członkowskie zapewniają – w obrębie ram przewidzianych przez prawo Unii i obowiązujące prawo krajowe – dostateczną ochronę uzasadnionego interesu użytkowników końcowych, którzy są osobami prawnymi, co do niezamawianych komunikatów przesyłanych w sposób określony w ust. 1.

6. Wszelkie osoby fizyczne lub prawne wykorzystujące usługi łączności elektronicznej do przekazywania komunikatów do celów marketingu bezpośredniego informują użytkowników końcowych o marketingowym charakterze materiałów i tożsamości osoby prawnej lub fizycznej, w której imieniu przekazywane są komunikaty, jak również podają informacje niezbędne odbiorcom do wykonania ich prawa do wycofania w łatwy sposób zgody na dalsze otrzymywanie komunikatów marketingowych.

7. Komisja jest uprawniona do przyjmowania środków wykonawczych zgodnie z art. 26 ust. 2, określających kod lub prefiks oznaczający połączenia marketingowe, zgodnie z ust. 3 lit. b).

Artykuł 17
Informacje o wykrytym ryzyku w zakresie bezpieczeństwa

W przypadku szczególnego ryzyka, które może zagrozić bezpieczeństwu sieci lub usług łączności elektronicznej, dostawca usługi łączności elektronicznej informuje użytkowników końcowych o takim zagrożeniu, a jeżeli ryzyko występuje poza zakresem środków podejmowanych przez dostawcę usług – informuje użytkowników końcowych o wszelkich możliwych środkach zaradczych, w tym wskazuje prawdopodobne koszty, jakie się z tym wiążą.

ROZDZIAŁ IV
NIEZALEŻNE ORGANY NADZORCZE I EGZEKWOWANIE PRZEPISÓW

Artykuł 18
Niezależne organy nadzorcze

1. Niezależny organ nadzorczy odpowiedzialny za monitorowanie lub niezależne organy nadzorcze odpowiedzialne za monitorowanie stosowania rozporządzenia (UE) 2016/679 są również odpowiedzialne za monitorowanie stosowania niniejszego rozporządzenia. Rozdziały VI i VII rozporządzenia (UE) 2016/679 stosuje się odpowiednio. Zadania i uprawnienia organów nadzorczych są wykonywane w odniesieniu do użytkowników końcowych.

2. Organ nadzorczy lub organy nadzorcze, o których mowa w ust. 1, współpracują, za każdym razem gdy jest to stosowne, z krajowymi organami regulacyjnymi ustanowionymi na podstawie [dyrektywy ustanawiającej Europejski kodeks łączności elektronicznej].

Artykuł 19
Europejska Rada Ochrony Danych

Europejska Rada Ochrony Danych ustanowiona na mocy art. 68 rozporządzenia (UE) 2016/679 ma uprawnienia, aby zapewnić spójne stosowanie niniejszego rozporządzenia. W tym celu Europejska Rada Ochrony Danych wykonuje zadania określone w art. 70 rozporządzenia (UE) 2016/679. Rada wykonuje następujące zadania:

a) doradza Komisji w sprawie proponowanych zmian niniejszego rozporządzenia;

b) z własnej inicjatywy lub na wniosek jednego ze swoich członków lub Komisji bada wszelkie kwestie dotyczące stosowania niniejszego rozporządzenia i wydaje wytyczne, zalecenia oraz określa najlepsze praktyki, aby zachęcić do spójnego stosowania niniejszego rozporządzenia.

Artykuł 20
Współpraca i procedury na rzecz spójności

Każdy organ nadzorczy przyczynia się do spójnego stosowania niniejszego rozporządzenia w całej Unii. W tym celu organy nadzorcze współpracują ze sobą i z Komisją zgodnie z rozdziałem VII rozporządzenia (UE) 2016/679 w kwestiach ujętych w niniejszym rozporządzeniu.

ROZDZIAŁ V
ŚRODKI ZARADCZE, ODPOWIEDZIALNOŚĆ I SANKCJE

Artykuł 21
Środki zaradcze

1. Bez uszczerbku dla innych administracyjnych lub sądowych środków zaradczych każdemu użytkownikowi końcowemu usług łączności elektronicznej przysługują takie same środki zaradcze, jak przewidziano w art. 77, 78 i 79 rozporządzenia (UE) 2016/679.

2. Wszelkie osoby fizyczne lub prawne inne niż użytkownicy końcowi, na które naruszenie niniejszego rozporządzenia miało negatywny wpływ i które mają uzasadniony interes w ustaniu lub zakazaniu domniemanych naruszeń, w tym dostawca usług łączności elektronicznej chroniący swój uzasadniony interes gospodarczy, ma prawo do wytoczenia powództwa w związku z takimi naruszeniami.

Artykuł 22
Prawo do odszkodowania i odpowiedzialność

Każdy użytkownik końcowy usług łączności elektronicznej, który doznał szkody majątkowej lub niemajątkowej w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać rekompensatę od naruszyciela z tytułu poniesionej szkody, chyba że naruszyciel udowodni, że w żaden sposób nie odpowiada za wydarzenie stanowiące podstawę wystąpienia szkody zgodnie z art. 82 rozporządzenia (EU) 2016/679.

Artykuł 23
Ogólne warunki nakładania administracyjnych kar pieniężnych

1. Do celów niniejszego artykułu w odniesieniu do naruszeń niniejszego rozporządzenia stosuje się rozdział VII rozporządzenia (UE) 2016/679.

2. Naruszenia następujących przepisów niniejszego rozporządzenia podlegają – zgodnie z ust. 1 – administracyjnym karom pieniężnym w wysokości do 10 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 2 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa:

a) obowiązki dowolnej osoby prawnej lub fizycznej, która przetwarza dane pochodzące z łączności elektronicznej, zgodnie z art. 8;

b) obowiązki dostawcy oprogramowania umożliwiającego łączność elektroniczną, zgodnie z art. 10;

c) obowiązki dostawców publicznie dostępnych spisów numerów, zgodnie z art. 15;

d) obowiązki dowolnej osoby prawnej lub fizycznej, która korzysta z usług łączności elektronicznej, zgodnie z art. 16.

3. Naruszenia zasady poufności komunikacji, dozwolonego przetwarzania danych pochodzących z łączności elektronicznej, terminów na usunięcie na podstawie art. 5, 6, i 7 podlegają zgodnie z ust. 1 niniejszego artykułu administracyjnym karom pieniężnym w wysokości do 20 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

4. Państwa członkowskie określają zasady nakładania kar za naruszenia art. 12, 13, 14 i 17.

5. Nieprzestrzeganie nakazu wydanego przez organ nadzorczy, o którym mowa w art. 18, podlega administracyjnym karom pieniężnym w wysokości do 20 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

6. Bez uszczerbku dla uprawnień naprawczych organów nadzorczych, o których mowa w art. 18, każde państwo członkowskie może określić w przepisach, czy i w jakim zakresie można nakładać administracyjne kary pieniężne na organy i podmioty publiczne ustanowione w tym państwie członkowskim.

7. Wykonywanie przez organ nadzorczy uprawnień powierzonych mu na mocy niniejszego artykułu podlega odpowiednim zabezpieczeniom proceduralnym zgodnie z prawem Unii i prawem państwa członkowskiego, w tym prawu do skutecznego środka prawnego przed sądem i rzetelnego procesu.

8. Jeżeli ustrój prawny państwa członkowskiego nie przewiduje administracyjnych kar pieniężnych, niniejszy artykuł można stosować w ten sposób, że o zastosowanie kary pieniężnej wnosi właściwy organ nadzorczy, a nakłada ją właściwy sąd krajowy, o ile zapewniona zostaje skuteczność tych środków ochrony prawnej i równoważność ich skutku względem administracyjnych kar pieniężnych nakładanych przez organy nadzorcze. Nakładane kary pieniężne muszą być w każdym przypadku skuteczne, proporcjonalne i odstraszające. Państwa członkowskie zawiadamiają Komisję o przepisach swojego prawa, które przyjęły zgodnie z niniejszym ustępem, do dnia […], a następnie – niezwłocznie – o wszelkich późniejszych aktach zmieniających lub zmianach mających wpływ na te przepisy.

Artykuł 24
Sankcje

1. Państwa członkowskie przyjmują przepisy określające inne sankcje za naruszenia niniejszego rozporządzenia, w szczególności za naruszenia niepodlegające administracyjnym karom pieniężnym na mocy art. 23, oraz podejmują wszelkie

środki niezbędne do zapewnienia ich wykonania. Sankcje te muszą być skuteczne, proporcjonalne i odstraszające.

2. Każde państwo członkowskie zawiadamia Komisję o przepisach prawa, które przyjęło na mocy ust. 1, nie później niż 18 miesięcy po dacie określonej na podstawie art. 29 ust. 2, i bezzwłocznie o każdej kolejnej zmianie mającej na nie wpływ.

ROZDZIAŁ VI
AKTY DELEGOWANE I WYKONAWCZE

Artykuł 25
Wykonywanie przekazanych uprawnień

1. Powierzenie Komisji uprawnień do przyjęcia aktów delegowanych podlega warunkom określonym w niniejszym artykule.

2. Uprawnienia do przyjęcia aktów delegowanych, o których mowa w art. 8 ust. 4, powierza się Komisji na czas nieokreślony od [daty wejścia w życie niniejszego rozporządzenia].

3. Przekazanie uprawnień, o którym mowa w art. 8 ust. 4, może zostać w dowolnym momencie odwołane przez Parlament Europejski lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna od następnego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej* lub w określonym w tej decyzji późniejszym terminie. Nie wpływa ona na ważność jakichkolwiek już obowiązujących aktów delegowanych.

4. Przed przyjęciem aktu delegowanego Komisja konsultuje się z ekspertami wyznaczonymi przez każde państwo członkowskie zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa.

5. Niezwłocznie po przyjęciu aktu delegowanego Komisja przekazuje go równocześnie Parlamentowi Europejskiemu i Radzie.

6. Akt delegowany przyjęty na podstawie art. 8 ust. 4 wchodzi w życie tylko wówczas, gdy ani Parlament Europejski, ani Rada nie wyraziły sprzeciwu w terminie dwóch miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie, lub gdy, przed upływem tego terminu, zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o dwa miesiące z inicjatywy Parlamentu Europejskiego lub Rady.

Artykuł 26
Komitet

1. Komisję wspomaga Komitet ds. Łączności ustanowiony na podstawie art. 110 [dyrektywy ustanawiającej Europejski kodeks łączności elektronicznej]. Komitet ten jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011[12].

2. W przypadku odesłania do niniejszego ustępu stosuje się art. 5 rozporządzenia (UE) nr 182/2011.

ROZDZIAŁ VII
PRZEPISY KOŃCOWE

Artykuł 27
Uchylenie

1. Dyrektywa 2002/58/WE zostaje uchylona ze skutkiem od dnia 25 maja 2018 r.

2. Odesłania do uchylonej dyrektywy należy traktować jako odesłania do niniejszego rozporządzenia.

Artykuł 28
Klauzula o monitorowaniu i ocenie

Najpóźniej do dnia 1 stycznia 2018 r. Komisja ustanowi szczegółowy program monitorowania skuteczności niniejszego rozporządzenia.

Nie później niż trzy lata od daty rozpoczęcia stosowania niniejszego rozporządzenia i co każde trzy lata w późniejszym okresie Komisja dokona oceny niniejszego rozporządzenia i przedstawi główne ustalenia Parlamentowi Europejskiemu, Radzie i Europejskiemu Komitetowi Ekonomiczno-Społecznemu. W stosownych przypadkach ocena stanowi podstawę do wniosku o zmianę niniejszego rozporządzenia lub jego uchylenie w świetle zmian okoliczności prawnych, technicznych lub gospodarczych.

Artykuł 29
Wejście w życie i stosowanie

1. Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

2. Niniejsze rozporządzenie stosuje się od dnia 25 maja 2018 r.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

[12] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 182/2011 z dnia 16 lutego 2011 r. ustanawiające przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję (Dz.U. L 55 z 28.2.2011, s. 13–18).

Sporządzono w Brukseli dnia r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodniczący	*Przewodniczący*