EVROPSKÁ
KOMISE

V Bruselu dne 10.1.2017
COM(2017) 10 final

2017/0003 (COD)

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY

o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích)

(Text s významem pro EHP)

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

DŮVODOVÁ ZPRÁVA

1. SOUVISLOSTI NÁVRHU

1.1 Odůvodnění a cíle návrhu

Cílem **Strategie pro jednotný digitální trh**[1] je zvýšení důvěry a posílení bezpečnosti v oblasti digitálních služeb. V tomto směru byla klíčovou akcí reforma rámce pro ochranu osobních údajů, zejména přijetí nařízení (EU) 2016/679 (**„obecné nařízení o ochraně osobních údajů“**)[2]. Strategie pro jednotný digitální trh rovněž oznámila přezkum směrnice 2002/58/ES (**„směrnice o soukromí a elektronických komunikacích“**)[3] s cílem poskytnout uživatelům služeb elektronických komunikací vysokou úroveň ochrany soukromí a nastolit rovné podmínky pro všechny účastníky trhu. Tento návrh přezkoumává směrnici o soukromí a elektronických komunikacích, přičemž zohledňuje cíle strategie pro jednotný digitální trh a zajišťuje soulad s obecným nařízením o ochraně osobních údajů.

Směrnice o soukromí a elektronických komunikacích zajišťuje ochranu základních práv a svobod, zejména respektování soukromého života, důvěrný charakter sdělení a ochranu osobních údajů v odvětví elektronických komunikací. Zaručuje rovněž volný pohyb dat, zařízení a služeb elektronických komunikací v Unii. Do sekundárního práva Unie provádí základní právo na respektování soukromého života, pokud jde o komunikace, jak je zakotveno v článku 7 Listiny základních práv Evropské unie (dále jen **„Listina“**).

Komise v souladu s požadavky na zlepšování právní úpravy provedla *ex post* hodnocení směrnice o soukromí a elektronických komunikacích v rámci Programu pro účelnost a účinnost právních předpisů (dále jen **„hodnocení REFIT“**). Z hodnocení vyplývá, že cíle a zásady stávajícího rámce jsou i nadále platné. Od poslední revize směrnice o soukromí a elektronických komunikacích v roce 2009 však na trhu došlo k důležitému technologickému a hospodářskému vývoji. Spotřebitelé a podniky namísto tradičních komunikačních služeb stále více spoléhají na nové internetové služby umožňující interpersonální komunikaci, jako například VoIP, výměnu rychlých zpráv (instant messaging) a webové e-mailové služby. Tyto komunikační služby „Over-the-Top“ (**„služby OTT“**) obecně nepodléhají stávajícímu unijnímu rámci pro elektronické komunikace, včetně směrnice o soukromí a elektronických komunikacích. Směrnice tedy nedrží krok s technologickým vývojem, což má za následek absenci ochrany komunikací uskutečňovaných prostřednictvím nových služeb.

1.2 Soulad s platnými předpisy v této oblasti politiky

Tento návrh představuje *lex specialis* k obecnému nařízení o ochraně osobních údajů; upřesní jej a doplní, pokud jde o data elektronických komunikací, která lze považovat za osobní údaje. Na všechny záležitosti týkající se zpracování osobních údajů, které nejsou konkrétně upraveny v tomto návrhu, se vztahuje obecné nařízení o ochraně osobních údajů. Sladění s obecným nařízením o ochraně osobních údajů vedlo ke zrušení některých ustanovení, jako jsou například povinnosti v oblasti bezpečnosti uvedené v článku 4 směrnice o soukromí a elektronických komunikacích.

---

[1] Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů – Strategie pro jednotný digitální trh v Evropě, COM(2015) 192 final.

[2] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1).

[3] Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích) (Úř. věst. L 201, 31.7.2002, s. 37).

1.3 Soulad s ostatními politikami Unie

Směrnice o soukromí a elektronických komunikacích je součástí předpisového rámce pro elektronické komunikace. V roce 2016 přijala Komise návrh směrnice, kterou se stanoví evropský kodex pro elektronické komunikace (dále jen **„kodex“**)[4], kterým se tento rámec reviduje. Stávající návrh není nedílnou součástí kodexu, částečně se však spoléhá na definice v něm uvedené, včetně definice „služeb elektronických komunikací“. Stejně jako kodex i tento návrh do své oblasti působnosti začleňuje poskytovatele služeb OTT, aby odrážel realitu na trhu. Kodex navíc toto nařízení doplňuje tím, že zajišťuje bezpečnost služeb elektronických komunikací.

Směrnice o rádiových zařízeních 2014/53/EU[5] zajišťuje jednotný trh pro rádiová zařízení. Tato směrnice zejména vyžaduje, aby bylo rádiové zařízení před uvedením na trh vybaveno bezpečnostním zařízením, které zajišťuje ochranu osobních údajů a soukromí uživatele. Podle směrnice o rádiových zařízeních a nařízení o evropské normalizaci (EU) č. 1025/2012[6] je Komise oprávněna přijímat opatření. Směrnice o rádiových zařízeních není tímto návrhem dotčena.

Tento návrh nezahrnuje žádná zvláštní ustanovení v oblasti uchovávání údajů. Zachovává hlavní myšlenku článku 15 směrnice o soukromí a elektronických komunikacích a přizpůsobuje ji konkrétnímu znění článku 23 obecného nařízení o ochraně osobních údajů, který členským státům poskytuje důvody pro omezení rozsahu povinností a práv uvedených v konkrétních článcích směrnice o soukromí a elektronických komunikacích. Členské státy tak mohou zachovat nebo vytvořit vnitrostátní rámce pro uchovávání údajů, které mimo jiné stanoví cílená opatření pro uchovávání údajů, pokud jsou tyto rámce v souladu s právem Unie a zohledňují judikaturu Soudního dvora týkající se výkladu směrnice o soukromí a elektronických komunikacích a Listiny základních práv[7].

A konečně, návrh se nevztahuje na činnosti orgánů, institucí a agentur Unie. Jeho zásady a příslušné povinnosti, pokud jde o právo na respektování soukromého života a komunikace v souvislosti se zpracováním dat elektronických komunikací, jsou však zahrnuty v návrhu nařízení o zrušení nařízení (ES) č. 45/2001[8].

---

4 Návrh směrnice Evropského parlamentu a Rady, kterou se stanoví evropský kodex pro elektronické komunikace (přepracované znění), předložený Komisí (COM/2016/0590 final – 2016/0288 (COD)).

5 Směrnice Evropského parlamentu a Rady 2014/53/EU ze dne 16. dubna 2014 o harmonizaci právních předpisů členských států týkajících se dodávání rádiových zařízení na trh a zrušení směrnice 1999/5/ES (Úř. věst. L 153, 22.5.2014, s. 62).

6 Nařízení Evropského parlamentu a Rady (EU) č. 1025/2012 ze dne 25. října 2012 o evropské normalizaci, změně směrnic Rady 89/686/EHS a 93/15/EHS a směrnic Evropského parlamentu a Rady 94/9/ES, 94/25/ES, 95/16/ES, 97/23/ES, 98/34/ES, 2004/22/ES, 2007/23/ES, 2009/23/ES a 2009/105/ES, a kterým se ruší rozhodnutí Rady 87/95/EHS a rozhodnutí Evropského parlamentu a Rady č. 1673/2006/ES (Úř. věst. L 316, 14.11.2012, s. 12).

7 Viz spojené věci C-293/12 a C-594/12 *Digital Rights Ireland a Seitlinger a další*, ECLI:EU:C:2014:238; spojené věci C-203/15 a C-698/15 *Tele2 Sverige AB a Secretary of State for the Home Department*, ECLI:EU:C:2016:970.

8 Nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů (Úř. věst. L 8, 12.1.2001, s. 1).

2. PRÁVNÍ ZÁKLAD, SUBSIDIARITA A PROPORCIONALITA

2.1 Právní základ

Příslušným právním základem návrhu jsou články 16 a 114 Smlouvy o fungování Evropské unie (dále jen **„SFEU“**).

Článek 16 SFEU zavádí zvláštní právní základ pro přijetí pravidel týkajících se ochrany fyzických osob při zpracovávání osobních údajů orgány Unie a členskými státy, pokud vykonávají činnosti spadající do oblasti působnosti práva Unie, a pravidla o volném pohybu těchto údajů. Vzhledem k tomu, že elektronická komunikace, které se účastní fyzická osoba, bude za normálních okolností považována za osobní údaje, měla by být ochrana fyzických osob v souvislosti se soukromím komunikace a zpracováním těchto údajů založena na článku 16.

Kromě toho má návrh za cíl ochranu komunikace a souvisejících oprávněných zájmů právnických osob. Význam a rozsah práv podle článku 7 Listiny je v souladu s čl. 52 odst. 3 Listiny stejný jako v případě práv stanovených v čl. 8 odst. 1 Evropské úmluvy o ochraně lidských práv a základních svobod (dále jen **„EÚLP“**). Co se týče oblasti působnosti článku 7 Listiny, judikatura Soudního dvora Evropské unie[9] a Evropského soudu pro lidská práva[10] potvrzuje, že profesní činnost právnických osob nemůže být vyloučena z ochrany práva zaručeného článkem 7 Listiny a článkem 8 EÚLP.

Vzhledem k tomu, že tato iniciativa sleduje dvojí účel a že komponenta týkající se ochrany komunikací fyzických osob a cíl dosažení vnitřního trhu pro tyto elektronické komunikace a zajištění jeho fungování nemůže být v tomto ohledu považována za pouze vedlejší, měla by být iniciativa rovněž založena na článku 114 SFEU.

2.2 Subsidiarita

Respektování komunikace je základní právo garantované Listinou. Obsah elektronických komunikací může odhalit vysoce citlivé informace o koncových uživatelích, kteří se komunikace účastní. Podobně též metadata odvozená z elektronických komunikací mohou odhalit velmi citlivé a osobní informace, jak výslovně uznal Soudní dvůr Evropské unie[11]. Většina členských států rovněž uznává potřebu chránit komunikace jako zvláštní ústavní právo. I když členské státy mohou přijmout politiky zajišťující, aby právo na ochranu údajů nebylo porušováno, nebylo by možné toho dosáhnout jednotně, pokud by neexistovala pravidla na úrovni Unie, a byly by omezeny přeshraniční toky osobních a jiných než osobních údajů souvisejících s používáním služeb elektronických komunikací. A v neposlední řadě je za účelem zachování souladu s obecným nařízením o ochraně údajů nezbytné přezkoumat směrnici o soukromí a elektronických komunikacích a přijmout opatření na sladění těchto dvou nástrojů.

Technologický vývoj a ambice strategie pro jednotný digitální trh posílily důvody pro opatření na úrovni Unie. Úspěch jednotného digitálního trhu Evropské unie závisí na tom, jak účinně se EU podaří odstranit vnitrostátní izolaci a překážky a využít výhod a ekonomiky

---

9 Viz věc C-450/06 *Varec SA*, ECLI:EU:C:2008:91, bod 48.

10 Viz mimo jiné rozsudek Evropského soudu pro lidská práva ze dne 16. prosince 1992 ve věci *Niemietz v. Německo*, řada A č. 251-B, bod 29; rozsudek ve věci *Société Colas Est a další v. Francie* č. 37971/97, bod 41, *Sbírka rozsudků a rozhodnutí* 2002-III; rozsudek ve věci *Peck v. Spojené království* č. 44647/98, bod 57, *Sbírka rozsudků a rozhodnutí* 2003-I; jakož i rozsudek ze dne 2. dubna 2015 ve věci *Vinci Construction a GTM Génie Civil et Services v. Francie* č. 63629/10 a 60567/10, bod 63.

11 Viz poznámka pod čarou č. 7.

evropského jednotného digitálního trhu. Navíc vzhledem k tomu, že internet a digitální technologie neznají hranice, rozsah tohoto problému přesahuje území jednoho členského státu. Členské státy nemohou problémy za stávající situace účinně vyřešit. Aby jednotný digitální trh řádně fungoval, je nutné zajistit rovné podmínky pro hospodářské subjekty poskytující zaměnitelné služby a rovnou ochranu koncových uživatelů na úrovni Unie.

2.3 Proporcionalita

K zajištění účinné právní ochrany, pokud jde o respektování soukromí a komunikace, je nezbytné rozšířit oblast působnosti tak, aby zahrnovala poskytovatele služeb OTT. I když několik oblíbených poskytovatelů služeb OTT zásadu důvěrného charakteru sdělení plně nebo částečně dodržuje, ochranu základních práv nelze ponechat na samoregulaci odvětví. Vzrůstá rovněž význam účinné ochrany soukromí koncových zařízení, jelikož tato zařízení se v soukromém i pracovním životě stala nezbytná pro ukládání citlivých informací. Provádění směrnice o soukromí a elektronických zařízeních nedokázalo účinně posílit postavení koncových uživatelů. Pro dosažení tohoto cíle je proto nezbytné realizovat tuto zásadu soustředěním souhlasu do softwaru a informováním uživatelů o nastavení ochrany soukromí v softwaru. Prosazování tohoto nařízení se opírá o dozorové úřady a mechanismus jednotnosti podle obecného nařízení o ochraně osobních údajů. Kromě toho návrh členským státům umožňuje pro zvláštní a legitimní účely přijmout vnitrostátní odchylná opatření. Návrh tak nepřekračuje rámec toho, co je nezbytné k dosažení cílů, a je v souladu se zásadou proporcionality podle článku 5 Smlouvy o Evropské unii. Povinnosti kladené na dotčené služby jsou omezeny na nejmenší možnou míru, aniž by byla narušena dotčená základní práva.

2.4 Volba nástroje

Komise předkládá návrh nařízení, aby byl zajištěn soulad s obecným nařízením o ochraně osobních údajů a právní jistota pro uživatele i podniky, a to tím, že se zabrání odchylným interpretacím v členských státech. Nařízení může zajistit rovnou ochranu uživatelů v celé Unii a nižší náklady na dodržování předpisů pro podniky působící přeshraničně.

3. VÝSLEDKY HODNOCENÍ *EX POST*, KONZULTACÍ SE ZÚČASTNĚNÝMI STRANAMI A POSOUZENÍ DOPADŮ

3.1 Hodnocení *ex post* / kontroly účelnosti platných právních předpisů

Hodnocení REFIT zkoumalo, nakolik účinně směrnice o soukromí a elektronických komunikacích přispěla k odpovídající ochraně respektování soukromého života a důvěrného charakteru sdělení v EU. Rovněž usilovalo o identifikaci možných nadbytečností.

Hodnocení REFIT dospělo k závěru, že výše uvedené cíle směrnice jsou i nadále **relevantní**. Zatímco obecné nařízení o ochraně osobních údajů zajišťuje ochranu osobních údajů, směrnice o soukromí a elektronických komunikacích zajišťuje důvěrný charakter sdělení, která mohou obsahovat rovněž jiné než osobní údaje a údaje týkající se právnické osoby. Účinnou ochranu podle článku 7 Listiny by proto měl zajistit samostatný nástroj. Další ustanovení, jako jsou pravidla pro zasílání nevyžádaných marketingových sdělení, se také ukázala být i nadále relevantní.

Pokud jde o **účelnost a účinnost**, hodnocení REFIT konstatovalo, že směrnice nesplnila v plném rozsahu své cíle. Nejasné formulace některých ustanovení a nejednoznačnost právních pojmů ohrozily harmonizaci, čímž došlo ke vzniku obtíží pro podniky působící přeshraničně. Hodnocení dále ukázalo, že některá ustanovení vytvořila zbytečnou zátěž pro podniky a spotřebitele. Například pravidlo o získání souhlasu, které slouží k ochraně

důvěrnosti koncových zařízení, nedosáhlo svých cílů, jelikož koncoví uživatelé čelí žádostem o přijetí sledovacích cookies, aniž by rozuměli jejich významu, a v některých případech jsou dokonce vystaveni cookies, které jsou posílány bez jejich souhlasu. Pravidlo o získání souhlasu je příliš inkluzivní, jelikož se vztahuje i na praktiky, které nenarušují soukromí, a zároveň nedostatečně inkluzivní, jelikož se dostatečně jasně nevztahuje na některé sledovací techniky (např. vytváření digitálních otisků zařízení), které nemusí zahrnovat přístup k datům v zařízení a jejich ukládání. Navíc může být jeho provádění pro podniky nákladné.

Hodnocení dospělo k závěru, že pravidla týkající se soukromí a elektronických komunikací stále mají pro **EU přidanou hodnotu**, a to z hlediska lepšího dosažení cíle, totiž zajištění soukromí na internetu v kontextu trhu elektronických komunikací, který je stále více mezinárodní. Hodnocení rovněž prokázalo, že pravidla jsou celkově **v souladu** s jinými příslušnými právními předpisy, ačkoli bylo s ohledem na nové obecné nařízení o ochraně osobních údajů (viz oddíl 1.2) identifikováno několik nadbytečností.

3.2 Konzultace se zúčastněnými stranami

V období mezi 12. dubnem a 5. červencem 2016 Komise zorganizovala veřejnou konzultaci a obdržela 421 odpovědí[12]. Klíčová zjištění jsou tato[13]:

- **Potřeba zvláštních pravidel pro odvětví elektronických komunikací týkajících se důvěrného charakteru elektronických komunikací:** 83,4 % respondentů z řad občanů, spotřebitelských organizací a organizací občanské společnosti a 88,9 % veřejných orgánů souhlasí, zatímco 63,4 % respondentů z průmyslu nesouhlasí.
- **Rozšíření oblasti působnosti na nové komunikační služby (OTT):** 76 % občanů a organizací občanské společnosti a 93,1 % veřejných orgánů souhlasí, zatímco z průmyslu je tomuto rozšíření nakloněno pouze 36,2 % respondentů.
- **Změna výjimek ze souhlasu se zpracováním provozních a lokalizačních údajů:** 49,1 % občanů, spotřebitelských organizací a organizací občanské společnosti a 36 % veřejných orgánů by upřednostnilo nerozšiřování výjimek, zatímco 36 % průmyslu upřednostňuje rozšíření výjimek a 2/3 průmyslu podporují prosté zrušení příslušných ustanovení.
- **Podpora řešení navržených pro otázku souhlasu s cookies:** 81,2 % občanů a 63 % veřejných orgánů podporuje, aby byly výrobcům koncových zařízení uloženy povinnosti uvádět na trh výrobky, v nichž bude aktivováno standardní nastavení ochrany soukromí, zatímco 58,3 % průmyslu upřednostňuje podporu samoregulace / společné regulace.

Mimo to Evropská komise v dubnu 2016 zorganizovala dva workshopy, jeden otevřený všem zúčastněným stranám a jeden otevřený příslušným vnitrostátním orgánům, na kterých se řešily hlavní otázky z veřejných konzultací. Názory vyjádřené během workshopů odrážely výsledek veřejné konzultace.

Za účelem získání názorů od občanů byl v rámci EU proveden průzkum Eurobarometru o soukromí a elektronických komunikacích[14]. Klíčová zjištění jsou tato[15]:

---

[12] 162 příspěvků od občanů, 33 od organizací občanské společnosti a spotřebitelských organizací, 186 od průmyslu a 40 od veřejných orgánů, včetně orgánů příslušných pro prosazování směrnice o soukromí a elektronických komunikacích.

[13] Celé znění zprávy je k dispozici na adrese: https://ec.europa.eu/digital-single-market/news-redirect/37204.

– 78 % respondentů uvedlo, že je pro ně velmi důležité, aby byly osobní informace na jejich počítači, chytrém telefonu nebo tabletu přístupné pouze s jejich svolením.

– 72 % respondentů uvedlo, že je pro ně velmi důležité, aby byl zaručen důvěrný charakter jejich elektronické pošty a rychlých zpráv vyměňovaných online.

– 89 % respondentů souhlasilo s navrhovanou možností, že by standardní nastavení jejich prohlížeče mělo zamezit sdílení jejich informací.

3.3 Sběr a využití výsledků odborných konzultací

Komise zohlednila následující doporučení externích odborníků:

– Cílené konzultace expertních skupin EU: stanovisko pracovní skupiny zřízené podle článku 29, stanovisko EIOÚ, stanovisko platformy REFIT, názory sdružení BEREC, názory agentury ENISA a názory členů sítě pro spolupráci v oblasti ochrany spotřebitele.

– Externí odborné znalosti, zejména tyto dvě studie:

  – studie „Směrnice o soukromí a elektronických komunikacích: posouzení provádění, účinnosti a slučitelnosti s navrhovaným nařízením o ochraně údajů“ (SMART 2013/007116),

  – studie „Hodnocení a přezkum směrnice 2002/58 o soukromí a odvětví elektronických komunikací“ (SMART 2016/0080).

3.4 Posouzení dopadů

Pro tento návrh, k němuž Výbor pro kontrolu regulace dne 28. září 2016 vydal kladné stanovisko, bylo provedeno posouzení dopadů[16]. S ohledem na doporučení Výboru toto posouzení dopadů lépe vysvětluje oblast působnosti této iniciativy, její soulad s jinými právními nástroji (obecné nařízení o ochraně osobních údajů, evropský kodex pro elektronické komunikace, směrnice o rádiových zařízeních) a potřebu samostatného nástroje. Základní scénář je více rozpracován a vyjasněn. Analýza dopadů je posílená a vyváženější a objasňuje a prohlubuje popis očekávaných nákladů a přínosů.

Na základě kritérií účelnosti, účinnosti a souladu byly přezkoumány tyto možnosti politiky:

– **možnost č. 1:** nelegislativní opatření („měkké“ právo),

– **možnost č. 2:** omezené posílení soukromí/důvěrnosti a zjednodušení,

– **možnost č. 3:** uměřené posílení soukromí/důvěrnosti a zjednodušení,

– **možnost č. 4:** dalekosáhlé posílení soukromí/důvěrnosti a zjednodušení,

– **možnost č. 5:** zrušení směrnice o soukromí a elektronických komunikacích.

Jako **upřednostňovaná možnost** pro dosažení cílů byla ve většině aspektů označena **možnost č. 3**, a to s přihlédnutím k její účinnosti a soudržnosti. K hlavním přínosům patří:

– zvýšení ochrany důvěrného charakteru elektronických komunikací prostřednictvím rozšíření oblasti působnosti právního nástroje tak, aby zahrnoval nové funkčně

---

14 Průzkum Eurobarometru 2016 (EB) 443 o soukromí a elektronických komunikacích (SMART 2016/079).

15 Celé znění zprávy je k dispozici na adrese: https://ec.europa.eu/digital-single-market/news-redirect/37205.

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

rovnocenné služby elektronických komunikací. Kromě toho nařízení zvyšuje kontrolu ze strany koncových uživatelů tím, že vyjasňuje, že souhlas lze vyjádřit prostřednictvím odpovídajícího technického nastavení,

– zvýšení ochrany před nevyžádanými sděleními díky zavedení povinnosti poskytnout u marketingových volání identifikaci volající linky nebo povinné předčíslí a rozšíření možností, jak blokovat volání z nežádoucích čísel,

– zjednodušení a vyjasnění právního prostředí, a to snížením manévrovacího prostoru ponechaného členským státům, zrušením zastaralých ustanovení a rozšířením výjimek z pravidel o získání souhlasu.

Očekává se, že hospodářský dopad možnosti č. 3 bude celkově přiměřený cílům návrhu. Tradičním službám elektronických komunikací se otevírají obchodní příležitosti související se zpracováním dat komunikací, zatímco na poskytovatele služeb OTT se budou vztahovat stejná pravidla. Pro tyto operátory to znamená určité dodatečné náklady na dodržování předpisů. Tato změna nicméně významně neovlivní ty poskytovatele služeb OTT, kteří na základě souhlasu již fungují. A konečně, dopad této možnosti nebude pocítěn v členských státech, které tato pravidla na poskytovatele služeb OTT již rozšířily.

Tím, že se souhlas soustředí do softwaru, jako jsou internetové prohlížeče, a uživatelé budou vybízeni k tomu, aby si zvolili své nastavení ochrany soukromí, jakož i tím, že se rozšíří výjimky z pravidla o získání souhlasu s cookies, bude významná část podniků moci odstranit bannery a oznámení týkající se cookies, což povede k potenciálně významným úsporám nákladů a zjednodušením. Nicméně pokud se velká část uživatelů rozhodne pro nastavení „odmítnout přijímání cookies třetích stran“, může být pro inzerenty cílící na internetové prostředí obtížnější získat souhlas. Soustředění souhlasu však současně provozovatele internetových stránek nezbavuje možnosti získat souhlas prostřednictvím individuálních žádostí adresovaných koncovým uživatelům, a zachovat si tak stávající obchodní model. Některým poskytovatelům prohlížečů nebo podobného softwaru by vznikly dodatečné náklady, jelikož by museli zajistit nastavení podporující ochranu soukromí.

Externí studie určila tři různé scénáře provádění možnosti č. 3, podle toho, který subjekt by zajišťoval dialogové okno mezi uživatelem, který si vybral nastavení „odmítnout přijímání cookies třetích stran“ nebo „nesledovat“, a navštívenými internetovými stránkami, které si přejí, aby uživatel internetu svou volbu přehodnotil. Subjekty, kterým by mohl být tento technický úkol svěřen, jsou: 1) software, jako jsou internetové prohlížeče; 2) sledovače třetích stran; 3) jednotlivé internetové stránky (tj. služba informační společnosti požadovaná uživatelem). V porovnání se základním scénářem by možnost č. 3, která je v tomto návrhu uplatněna v podobě prvního scénáře (řešení pomocí internetových prohlížečů), vedla z hlediska nákladů na dodržování předpisů k celkové úspoře činící 70 % (úspora ve výši 948,8 milionu EUR). U ostatních scénářů by byly úspory nákladů nižší. Vzhledem k tomu, že celkové úspory jsou převážně dány velmi výrazným snížením počtu zasažených podniků, očekává se, že individuální výše nákladů na dodržování předpisů, které by jednomu podniku průměrně vznikly, by byly vyšší než dnes.

3.5 Účelnost a zjednodušování právních předpisů

Opatření politiky navržená v rámci upřednostňované možnosti sledují v souladu se zjištěními hodnocení REFIT a se stanoviskem platformy REFIT[17] cíl, kterým je zjednodušení a snížení administrativní zátěže.

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

Platforma REFIT vydala tři soubory doporučení určené Komisi:

– ochrana soukromého života občanů by měla být posílena sladěním směrnice o soukromí a elektronických komunikacích s obecným nařízením o ochraně osobních údajů,

– účinnost ochrany občanů před nevyžádaným marketingem by měla být zvýšena přidáním výjimek z pravidla o získání souhlasu s cookies,

– Komise se zabývá problémy při vnitrostátním provádění a usnadňuje výměnu osvědčených postupů mezi členskými státy.

Návrh konkrétně zahrnuje:

– využití technologicky neutrálních definic k obsáhnutí nových služeb a technologií, aby se zajistilo, že nařízení bude použitelné i v budoucnosti,

– zrušení bezpečnostních pravidel, aby se zamezilo zdvojení regulačních opatření,

– vyjasnění oblasti působnosti, aby se přispělo k odstranění/snížení rizika odlišného provádění členskými státy (bod 3 stanoviska),

– vyjasnění a zjednodušení pravidla o získání souhlasu s používáním cookies a jiných identifikátorů, jak je vysvětleno v oddílech 3.1 a 3.4 (bod 2 stanoviska),

– sladění dozorových úřadů s orgány příslušnými pro prosazování obecného nařízení o ochraně osobních údajů a využití mechanismu jednotnosti podle obecného nařízení o ochraně osobních údajů.

3.6 Dopad na základní práva

Cílem návrhu je zefektivnění a zvýšení úrovně ochrany soukromí a osobních údajů zpracovávaných v souvislosti s elektronickými komunikacemi v souladu s články 7 a 8 Listiny a zajištění větší právní jistoty. Návrh doplňuje a upřesňuje obecné nařízení o ochraně osobních údajů. Účinná ochrana důvěrného charakteru sdělení je zásadní pro uplatňování svobody projevu a informací a jiných souvisejících práv, jako je například právo na ochranu osobních údajů nebo svoboda myšlení, svědomí a náboženského vyznání.

4. ROZPOČTOVÉ DŮSLEDKY

Návrh nemá žádné důsledky pro rozpočet Unie.

5. OSTATNÍ PRVKY

5.1 Plány provádění a monitorování, hodnocení a podávání zpráv

Komise bude monitorovat uplatňování nařízení a každé tři roky Evropskému parlamentu, Radě a Evropskému hospodářskému a sociálnímu výboru předloží zprávu o svém hodnocení. Tyto zprávy budou veřejné a budou uvádět podrobné informace týkající se účinného uplatňování a prosazování tohoto nařízení.

5.2 Podrobné vysvětlení konkrétních ustanovení návrhu

Kapitola I obsahuje obecná ustanovení: předmět (článek 1), oblast působnosti (články 2 a 3) a definice včetně odkazů na příslušné definice z jiných nástrojů EU, jako například z obecného nařízení o ochraně osobních údajů.

Kapitola II obsahuje klíčová ustanovení zajišťující důvěrný charakter elektronických komunikací (článek 5) a omezené povolené účely a podmínky zpracování dat těchto

komunikací (články 6 a 7). Zabývá se také ochranou koncových zařízení, a to i) zaručením integrity informací uložených v koncovém zařízení a ii) ochranou informací vysílaných z koncového zařízení, jelikož by mohly umožnit identifikaci koncového uživatele tohoto zařízení (článek 8). Článek 9 se pak podrobně zabývá souhlasem koncových uživatelů, který je ústředním zákonným důvodem v tomto nařízení, a výslovně odkazuje na definice a podmínky tohoto souhlasu, jak jsou stanoveny v obecném nařízení o ochraně údajů, přičemž článek 10 ukládá poskytovatelům softwaru umožňujícího elektronickou komunikaci povinnosti, které by měly koncovým uživatelům pomoci účinně se rozhodnout, pokud jde nastavení ochrany soukromí. Článek 11 se podrobně zabývá účely a podmínkami, za nichž členské státy mohou omezit výše uvedená ustanovení.

Kapitola III upravuje práva koncových uživatelů vykonávat kontrolu nad odesíláním a příjmem elektronických komunikací, aby bylo chráněno jejich soukromí: i) právo koncových uživatelů potlačit identifikaci volající linky za účelem zaručení anonymity (článek 12) a omezení tohoto práva (článek 13) a ii) povinnost poskytovatelů veřejně dostupných interpersonálních komunikačních služeb založených na číslech umožnit omezení příjmu nežádoucích volání (článek 14). Tato kapitola rovněž reguluje podmínky, za kterých mohou být koncoví uživatelé zahrnuti do veřejně dostupných seznamů (článek 15), a podmínky, za kterých lze sdělovat nevyžádaná sdělení pro účely přímého marketingu (článek 17). Týká se také bezpečnostních rizik a stanoví povinnost poskytovatelů služeb elektronických komunikací upozornit koncové uživatele v případě, že existuje zvláštní riziko, které by mohlo ohrozit bezpečnost sítí a služeb. Na poskytovatele služeb elektronických komunikací se budou vztahovat povinnosti v oblasti bezpečnosti uvedené v obecném nařízení o ochraně údajů a v evropském kodexu pro elektronické komunikace.

Kapitola IV stanoví dozor nad tímto nařízením a jeho prosazování a s ohledem na silné synergie mezi otázkami obecné ochrany údajů a důvěrným charakterem sdělení svěřuje tyto úkoly dozorovým úřadům odpovědným za úkoly podle obecného nařízení o ochraně údajů (článek 18). Jsou také rozšířeny pravomoci Evropského sboru pro ochranu osobních údajů (článek 19) a stanoveno, že v případě přeshraničních záležitostí souvisejících s tímto nařízením se uplatní spolupráce a mechanismus jednotnosti podle obecného nařízení o ochraně údajů (článek 20).

Kapitola V se podrobně zabývá různými prostředky právní ochrany dostupnými koncovým uživatelům (články 21 a 22) a sankcemi, které lze uložit (článek 24), včetně obecných podmínek pro ukládání správních pokut (článek 23).

Kapitola VI se týká přijímání aktů v přenesené pravomoci a prováděcích aktů v souladu s články 290 a 291 Smlouvy.

Kapitola VII pak obsahuje závěrečná ustanovení tohoto nařízení: zrušení směrnice o soukromí a elektronických komunikacích, monitorování a přezkum, vstup v platnost a použitelnost. Co se přezkumu týče, má Komise v úmyslu mimo jiné posoudit, zda je ve světle technického, hospodářského a právního vývoje a s ohledem na první hodnocení nařízení (EU) 2016/679, které má být provedeno do 25. května 2020, i nadále nezbytný samostatný právní akt.

2017/0003 (COD)

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY

o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích)

(Text s významem pro EHP)

EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na články 16 a 114 této smlouvy,

s ohledem na návrh Evropské komise,

po postoupení návrhu legislativního aktu vnitrostátním parlamentům,

s ohledem na stanovisko Evropského hospodářského a sociálního výboru[1],

s ohledem na stanovisko Výboru regionů[2],

s ohledem na stanovisko evropského inspektora ochrany údajů[3],

v souladu s řádným legislativním postupem,

vzhledem k těmto důvodům:

(1) Článek 7 Listiny základních práv Evropské unie (dále jen „Listina“) chrání základní právo každého jedince na respektování jeho soukromého a rodinného života, obydlí a komunikace. Respektování soukromí komunikace je základním rozměrem tohoto práva. Důvěrný charakter elektronických komunikací zajišťuje, že informace, které si strany mezi sebou vymění, a vnější prvky této komunikace, včetně údajů o tom, kdy byla informace zaslána, odkud a komu, nesmí být vyzrazeny nikomu jinému než stranám, které se komunikace účastní. Zásada důvěrnosti by se měla vztahovat na stávající a budoucí komunikační prostředky, včetně volání, přístupu k internetu, aplikací pro výměnu rychlých zpráv, elektronické pošty, internetových telefonních volání a zasílání osobních zpráv prostřednictvím sociálních médií.

(2) Obsah elektronických komunikací může odhalit vysoce citlivé informace o fyzických osobách, které se komunikace účastní, od osobních zkušeností a emocí až po zdravotní stav, sexuální orientaci a politické názory; zveřejnění těchto informací by mohlo mít za následek osobní či společenskou újmu, hospodářskou ztrátu nebo zahanbení. Podobně i metadata odvozená z elektronických komunikací mohou odhalit velmi citlivé a osobní informace. Mezi tato metadata patří volaná čísla, navštívené internetové stránky, zeměpisná poloha, čas a datum, kdy daná osoba uskutečnila

[1] Úř. věst. C, , s. .
[2] Úř. věst. C, , s. .
[3] Úř. věst. C, , s. .

volání, a jeho doba trvání atd., což umožňuje vyvozovat přesné závěry týkající se osobního života osob účastnících se elektronické komunikace, například jejich sociální vztahy, zvyky a každodenní činnosti, zájmy, vkus atd.

(3) Data elektronických komunikací mohou rovněž odhalit informace týkající se právnických osob, například obchodní tajemství nebo jiné citlivé informace, které mají ekonomickou hodnotu. Ustanovení tohoto nařízení by se proto měla vztahovat na fyzické i právnické osoby. Toto nařízení by dále mělo zajistit, aby se ustanovení nařízení Evropského parlamentu a Rady (EU) 2016/679[4] vztahovala rovněž na koncové uživatele, kteří jsou právnickými osobami. To zahrnuje definici souhlasu podle nařízení (EU) 2016/679. Pokud se odkazuje na souhlas koncového uživatele, včetně právnických osob, měla by se použít tato definice. Mimo to by právnické osoby měly mít stejná práva jako koncoví uživatelé, kteří jsou fyzickými osobami, pokud jde o dozorové úřady; dozorové úřady podle tohoto nařízení by dále měly rovněž odpovídat za monitorování uplatňování tohoto nařízení, pokud jde o právnické osoby.

(4) Podle čl. 8 odst. 1 Listiny a čl. 16 odst. 1 Smlouvy o fungování Evropské unie má každý právo na ochranu osobních údajů, které se ho týkají. Nařízení (EU) 2016/679 stanoví pravidla týkající se ochrany fyzických osob v souvislosti se zpracováním osobních údajů a pravidla týkající se volného pohybu osobních údajů. Data elektronických komunikací mohou obsahovat osobní údaje, jak jsou definovány v nařízení (EU) 2016/679.

(5) Ustanovení tohoto nařízení upřesňují a doplňují obecná pravidla o ochraně osobních údajů, která jsou stanovena v nařízení (EU) 2016/679, pokud jde o data elektronických komunikací, která lze považovat za osobní údaje. Toto nařízení tedy nesnižuje úroveň ochrany, kterou požívají fyzické osoby podle nařízení (EU) 2016/679. Zpracování dat elektronických komunikací poskytovateli služeb elektronických komunikací by mělo být povoleno pouze v souladu s tímto nařízením.

(6) Ačkoli zásady a hlavní ustanovení směrnice Evropského parlamentu a Rady 2002/58/ES[5] zůstávají nadále obecně platné, tato směrnice nedokázala držet plně krok s vývojem technologické a tržní reality, což má za následek nekonzistentní nebo nedostatečnou účinnou ochranu soukromí a důvěrnosti ve vztahu k elektronickým komunikacím. Uvedený vývoj zahrnuje to, že na trh vstoupily služby elektronických komunikací, které mohou z hlediska spotřebitele nahradit tradiční služby, ale které nemusí dodržovat stejný soubor pravidel. Další vývoj se týká nových technik umožňujících sledovat chování koncových uživatelů na internetu, na které se směrnice 2002/58/ES nevztahuje. Směrnice 2002/58/ES by tudíž měla být zrušena a nahrazena tímto nařízením.

(7) Členské státy by měly mít možnost v mezích tohoto nařízení zachovat nebo zavést vnitrostátní ustanovení, která by dále upřesnila a vyjasnila uplatňování pravidel tohoto nařízení, aby se zajistilo jejich účinné uplatňování a výklad. Prostor pro uvážení, který členské státy v tomto ohledu mají, by tudíž měl zachovávat rovnováhu mezi ochranou

---

[4] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1).

[5] Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích) (Úř. věst. L 201, 31.7.2002, s. 37).

soukromého života a osobních údajů a volným pohybem dat elektronických komunikací.

(8) Toto nařízení by se mělo vztahovat na poskytovatele služeb elektronických komunikací, na poskytovatele veřejně dostupných seznamů a na poskytovatele softwaru umožňujícího elektronické komunikace včetně získávání a prezentování informací na internetu. Toto nařízení by se rovněž mělo vztahovat na fyzické a právnické osoby, které služby elektronických komunikací používají k zasílání přímých marketingových obchodních sdělení nebo ke shromažďování informací souvisejících s koncovými zařízeními koncových uživatelů nebo uložených v těchto zařízeních.

(9) Toto nařízení by se mělo vztahovat na data elektronických komunikací zpracovávaná v souvislosti s poskytováním a používáním služeb elektronických komunikací v Unii, bez ohledu na to, zda ke zpracování dochází v Unii, či nikoli. Mimo to, aby nebyli koncoví uživatelé v Unii zbaveni účinné ochrany, mělo by se toto nařízení rovněž vztahovat na data elektronických komunikací zpracovávaná v souvislosti s poskytováním služeb elektronických komunikací koncovým uživatelům v Unii ze zemí mimo Unii.

(10) Rádiová zařízení a jejich software uváděné na vnitřní trh v Unii musí být v souladu se směrnicí Evropského parlamentu a Rady 2014/53/EU[6]. Tímto nařízením by neměla být dotčena použitelnost jakýchkoli požadavků směrnice 2014/53/EU ani pravomoci Komise přijímat akty v přenesené pravomoci podle směrnice 2014/53/EU, která vyžaduje, aby rádiová zařízení v konkrétních třídách byla vybavena bezpečnostním zařízením, které zajišťuje ochranu osobních údajů a soukromí koncových uživatelů.

(11) Služby používané pro komunikační účely a technické prostředky pro jejich poskytování prošly značným vývojem. Koncoví uživatelé stále více nahrazují tradiční hlasová telefonní volání, textové zprávy (SMS) a služby přenosu elektronické pošty funkčně rovnocennými internetovými službami, jako jsou VoIP, služby výměny zpráv a webové e-mailové služby. Toto nařízení za účelem zajištění účinné a rovné ochrany koncových uživatelů při využívání funkčně rovnocenných služeb používá definici služeb elektronických komunikací stanovenou ve [směrnici Evropského parlamentu a Rady, kterou se stanoví evropský kodex pro elektronické komunikace[7]]. Tato definice zahrnuje nejen služby přístupu k internetu a služby, které spočívají zcela nebo částečně v přenosu signálů, ale také interpersonální komunikační služby, které mohou, ale nemusí být založeny na číslech, jako například VoIP, služby výměny zpráv a webové e-mailové služby. Ochrana důvěrného charakteru sdělení je zásadní, i pokud jde o interpersonální komunikační služby, které jsou doplňkem jiných služeb; toto nařízení by se proto mělo vztahovat i na tento typ služeb, mají-li také komunikační funkci.

(12) Propojená zařízení a stroje mezi sebou navzájem stále více komunikují prostřednictvím sítí elektronických komunikací (internet věcí). Přenos komunikace mezi stroji zahrnuje přenos signálů po síti, a obvykle tedy představuje službu elektronických komunikací. Aby se zajistila plná ochrana práv na soukromí a důvěrný charakter sdělení a aby se podpořil důvěryhodný a bezpečný internet věcí na jednotném digitálním trhu, je třeba vyjasnit, že toto nařízení by se mělo vztahovat na

---

6 Směrnice Evropského parlamentu a Rady 2014/53/EU ze dne 16. dubna 2014 o harmonizaci právních předpisů členských států týkajících se dodávání rádiových zařízení na trh a zrušení směrnice 1999/5/ES (Úř. věst. L 153, 22.5.2014, s. 62).

7 Návrh směrnice Evropského parlamentu a Rady, kterou se stanoví evropský kodex pro elektronické komunikace (přepracované znění), předložený Komisí (COM/2016/0590 final – 2016/0288 (COD)).

přenos komunikace mezi stroji. Zásada důvěrnosti zakotvená v tomto nařízení by se proto měla vztahovat rovněž na přenos komunikace mezi stroji. Mohla by být rovněž přijata zvláštní ochranná opatření v rámci odvětvových právních předpisů, jako například směrnice 2014/53/EU.

(13) Vývoj rychlých a účinných bezdrátových technologií podpořil vzrůstající veřejnou dostupnost přístupu k internetu prostřednictvím bezdrátových sítí, k nimž může získat přístup kdokoli ve veřejných a polosoukromých prostorech, jako jsou například „hotspoty“ umístěné na různých místech ve městě, v obchodních domech, nákupních centrech a nemocnicích. Pokud jsou tyto komunikační sítě poskytovány nedefinované skupině koncových uživatelů, měl by být chráněn důvěrný charakter sdělení přenášených prostřednictvím těchto sítí. Skutečnost, že bezdrátové služby elektronických komunikací mohou být doplňkem jiných služeb, by neměla být na překážku ochraně důvěrného charakteru dat komunikací a uplatňování tohoto nařízení. Toto nařízení by se proto mělo vztahovat na data elektronických komunikací přenášená službami elektronických komunikací a veřejnými komunikačními sítěmi. Toto nařízení by se naopak nemělo vztahovat na uzavřené skupiny koncových uživatelů, jako například korporátní sítě, u kterých je přístup omezen na členy dané korporace.

(14) Data elektronických komunikací by měla být definována dostatečně širokým a technologicky neutrálním způsobem, aby zahrnovala veškeré informace týkající se přenášeného nebo vyměňovaného obsahu (obsah elektronických komunikací) a informace týkající se koncového uživatele služeb elektronických komunikací, které jsou zpracovávány pro účely přenášení, šíření nebo umožnění výměny obsahu elektronických komunikací, a to včetně údajů sloužících ke sledování a identifikaci zdroje a cíle komunikace, zeměpisné polohy a data, času, doby trvání a typu komunikace. Bez ohledu na to, zda jsou tyto signály a související údaje přenášeny po vedení, rádiovými, optickými nebo elektromagnetickými prostředky, včetně družicových sítí, kabelových sítí, pevných sítí (s komutací okruhů nebo paketů, včetně internetu), mobilních zemských sítí a sítí pro rozvod elektrické energie, měly by být údaje související s těmito signály považovány za metadata elektronických komunikací, a tudíž by se na ně měla vztahovat ustanovení tohoto nařízení. Metadata elektronických komunikací mohou zahrnovat informace, které jsou součástí přihlášení se k užívání služby, jsou-li tyto informace zpracovávány pro účely přenášení, šíření nebo výměny obsahu elektronických komunikací.

(15) Data elektronických komunikací by měla být považována za důvěrná. To znamená, že by mělo být zakázáno jakkoli zasahovat do přenosu dat elektronických komunikací, ať už přímo lidským zásahem nebo zprostředkovaně automatizovaným strojovým zpracováním, bez souhlasu všech komunikujících stran. Během přenosu, tj. do doby, než obsah elektronické komunikace obdrží zamýšlený adresát, by měl platit zákaz zachycování dat komunikací. K zachycování dat elektronických komunikací může dojít například tehdy, když někdo jiný než komunikující strany poslouchá hovory nebo čte, skenuje či ukládá obsah elektronických komunikací nebo související metadata pro jiné účely, než je výměna komunikace. K zachycování rovněž dochází tehdy, když třetí strany monitorují navštívené internetové stránky, načasování návštěv, interakci s ostatními atd. bez souhlasu dotčeného koncového uživatele. S tím, jak se technologie vyvíjí, došlo také k nárůstu technických možností, jak zachycování uskutečňovat. Tyto možnosti mohou sahat od instalace zařízení, která shromažďují údaje z koncových zařízení v cílových oblastech, jako jsou například zachytávače IMSI, po programy a techniky, které například tajně sledují návyky při prohlížení internetu za účelem

vytváření profilů koncových uživatelů. Další příklady zachycování zahrnují zachycování přenášených dat nebo dat obsahu z nešifrovaných bezdrátových sítí a routerů, včetně návyků při prohlížení internetu, bez souhlasu koncových uživatelů.

(16) Zákaz uchovávání komunikace neznamená zákaz jakéhokoli automatického, přechodného a dočasného uchovávání takových informací, pokud k němu dochází výlučně z důvodu uskutečnění přenosu v síti elektronických komunikací. Nemělo by být zakázáno ani zpracování dat elektronických komunikací za účelem zajištění bezpečnosti a kontinuity služeb elektronických komunikací, včetně kontroly z hlediska bezpečnostních hrozeb, jako je například přítomnost malwaru, nebo zpracování metadat za účelem zajištění nezbytných požadavků na kvalitu služby, jako je například latence, kolísání atd.

(17) Zpracování dat elektronických komunikací může být užitečné pro podniky, spotřebitele a pro společnost jako celek. Ve srovnání se směrnicí 2002/58/ES toto nařízení rozšiřuje možnosti, kdy mohou poskytovatelé služeb elektronických komunikací na základě souhlasu koncových uživatelů zpracovávat metadata elektronických komunikací. Koncoví uživatelé nicméně důvěrnému charakteru svých sdělení, včetně svých on-line aktivit, přikládají velký význam a nad používáním dat elektronických komunikací pro jiné účely, než je přenos komunikace, chtějí mít kontrolu. Toto nařízení by proto mělo požadovat, aby poskytovatelé služeb elektronických komunikací získali souhlas koncových uživatelů se zpracováním metadat elektronických komunikací, a ta by měla zahrnovat údaje o poloze zařízení generovaná pro účely udělení a udržení přístupu a připojení ke službě. Za metadata by neměly být považovány lokalizační údaje, které jsou generovány v jiném kontextu, než je poskytování služeb elektronických komunikací. Mezi příklady, jak mohou poskytovatelé služeb elektronických komunikací komerčně využít metadata elektronických komunikací, patří poskytování teplotních map, tj. grafické znázornění údajů za použití barev k naznačení přítomnosti osob. K zobrazení dopravních pohybů v určitých směrech během určitého časového období je nezbytný identifikátor, aby bylo možné v určitých časových intervalech spojit pozice osob. Pokud by měly být použity anonymní údaje, tento identifikátor by chyběl a daný pohyb by nemohl být zobrazen. Tato využití metadat elektronických komunikací by mohla přinést prospěch například veřejným orgánům a provozovatelům veřejné dopravy, kteří by mohli na základě využití stávající struktury a tlaku na ni určit, kde rozvíjet novou infrastrukturu. Pokud je pravděpodobné, že určitý druh zpracování metadat elektronických komunikací, zejména za použití nových technologií a s ohledem na povahu, rozsah, kontext a účel zpracování, bude mít za následek velké riziko pro práva a svobody fyzických osob, mělo by být před zpracováním provedeno posouzení vlivu na ochranu osobních údajů a případně konzultován dozorový úřad v souladu s články 35 a 36 nařízení (EU) 2016/679.

(18) Koncoví uživatelé mohou souhlasit se zpracováním svých metadat, aby obdrželi konkrétní služby, jako například služby chránící proti podvodným jednáním (prostřednictvím analyzování údajů o používání, poloze a zákaznickém účtu v reálném čase). V digitální ekonomice jsou služby často poskytovány za jiné protiplnění než peníze, například za to, že jsou koncoví uživatelé vystaveni reklamám. Pro účely tohoto nařízení by souhlas koncového uživatele, bez ohledu na to, zda je tímto uživatelem fyzická či právnická osoba, měl mít stejný význam a podléhat stejným podmínkám jako souhlas subjektu údajů podle nařízení (EU) 2016/679. Základní širokopásmový přístup k internetu a hlasové komunikační služby se mají považovat za základní služby, aby jednotlivci mohli komunikovat a podílet se na přínosech digitální

ekonomiky. Souhlas se zpracováním údajů z použití internetové nebo hlasové komunikace nebude platný, pokud subjekt údajů nemá skutečnou a svobodnou volbu nebo nemůže souhlas odmítnout či odvolat, aniž by byl poškozen.

(19) Obsah elektronických komunikací se týká podstaty základního práva na respektování soukromého a rodinného života, obydlí a komunikace chráněného podle článku 7 Listiny. Jakékoli zasahování do obsahu elektronických komunikací by mělo být povoleno pouze za velmi jasně definovaných podmínek a pro konkrétní účely a měly by se na něj vztahovat přiměřené záruky proti zneužití. Toto nařízení umožňuje, aby poskytovatelé služeb elektronických komunikací zpracovávali data elektronických komunikací během tranzitu, a to s informovaným souhlasem všech dotčených koncových uživatelů. Poskytovatelé například mohou nabídnout služby, které zahrnují skenování elektronické pošty za účelem odstranění určitého předem definovaného materiálu. Vzhledem k citlivosti obsahu komunikací toto nařízení stanoví předpoklad, že zpracování těchto dat obsahu bude mít za následek vysoká rizika pro práva a svobody fyzických osob. Při zpracovávání tohoto typu údajů by měl poskytovatel služby elektronických komunikací před zpracováním vždy konzultovat s dozorovým úřadem. Tato konzultace by měla být v souladu s čl. 36 odst. 2 a 3 nařízení (EU) 2016/679. Uvedený předpoklad nezahrnuje zpracování dat obsahu za účelem poskytnutí služby požadované koncovým uživatelem, pokud koncový uživatel s tímto zpracováním souhlasil a pokud je toto zpracování prováděno pro účely a po dobu, které jsou nezbytně nutné a přiměřené pro takovou službu. Poté, co byl obsah elektronických komunikací koncovým uživatelem odeslán a zamýšlený koncový uživatel nebo koncoví uživatelé ho obdrželi, může být zaznamenán nebo uložen koncovým uživatelem, koncovými uživateli nebo třetí stranou, která jimi byla k zaznamenání nebo uložení těchto údajů pověřena. Jakékoli zpracování těchto údajů musí být v souladu s nařízením (EU) 2016/679.

(20) Koncová zařízení koncových uživatelů sítí elektronických komunikací a veškeré informace týkající se využívání těchto koncových zařízení, ať už jsou uchovávané v takových zařízeních, vysílané takovými zařízeními, požadované od těchto zařízení nebo zpracovávané za účelem umožnění připojení těchto zařízení k jinému zařízení a/nebo k síťovému zařízení, tvoří součást soukromí koncových uživatelů, které vyžaduje ochranu v souladu s Listinou základních práv Evropské unie a s Evropskou úmluvou o ochraně lidských práv a základních svobod. Vzhledem k tomu, že taková zařízení obsahují nebo zpracovávají informace, které mohou odhalit podrobnosti o citových, politických a společenských stránkách dané osoby, včetně obsahu komunikace, obrázků, polohy získané přístupem k funkcím GPS v zařízení, seznamů kontaktů a dalších informací již uchovávaných v zařízení, vyžadují informace související s takovými zařízeními zvýšenou ochranu soukromí. Kromě toho tzv. špionážní software („spyware“), webové štěnice („web bugs“), skryté identifikátory, sledovací cookies a jiné podobné nežádoucí nástroje pro sledování mohou pronikat do koncového zařízení koncového uživatele bez jeho vědomí s cílem získat přístup k informacím, uchovávat skryté informace nebo sledovat činnost. Informace související se zařízením koncového uživatele mohou být rovněž shromažďovány dálkově, a to za účelem identifikace a sledování a za použití technik, jako je vytváření digitálních otisků konkrétního zařízení („device fingerprinting“), často bez vědomí koncového uživatele, a mohou vážně zasahovat do soukromí těchto koncových uživatelů. Techniky, které skrytě sledují činnosti koncových uživatelů, například prostřednictvím sledování jejich činností on-line nebo polohy jejich koncových zařízení, nebo které přebírají kontrolu nad fungováním koncových zařízení koncových uživatelů, představují vážnou hrozbu pro soukromí koncových uživatelů. Jakékoli takové

zasahování do koncového zařízení koncového uživatele by proto mělo být povoleno pouze se souhlasem koncového uživatele a za konkrétním a transparentním účelem.

(21) Výjimky z povinnosti získat souhlas s využitím funkcí koncového zařízení pro zpracování a uchovávání nebo s přístupem k informacím uloženým v koncovém zařízení by měly být omezeny na situace, při nichž nedochází k narušení soukromí, nebo se tak děje jen ve velmi omezené míře. Souhlas by například neměl být vyžadován pro technické uchovávání nebo přístup, které jsou nezbytně nutné a přiměřené legitimnímu účelu, kterým je umožnit využití konkrétní služby výslovně požadované koncovým uživatelem. To může zahrnovat uchovávání cookies po dobu trvání jedné navázané relace s internetovou stránkou, aby bylo možné udržovat přehled o informacích zadaných koncovým uživatelem při vyplňování internetových formulářů o více stránkách. Cookies mohou být také legitimním a užitečným nástrojem například při měření návštěvnosti internetové stránky. Za přístup k zařízení koncového uživatele nebo využití jeho funkcí pro zpracování by se neměla považovat kontrola konfigurace ze strany poskytovatelů služeb informační společnosti za účelem poskytnutí služby v souladu s nastavením koncového uživatele a pouhé zaznamenání skutečnosti, že zařízení koncového uživatele není schopno přijmout obsah požadovaný koncovým uživatelem.

(22) Metody používané pro poskytování informací a získání souhlasu koncového uživatele by měly být vůči uživateli co možná nejvstřícnější. Vzhledem k všudypřítomnému využívání sledovacích cookies a dalších sledovacích technik se od koncových uživatelů stále častěji požaduje, aby poskytli souhlas s uchováváním těchto sledovacích cookies ve svém koncovém zařízení. Koncoví uživatelé jsou v důsledku toho přetíženi žádostmi o poskytnutí souhlasu. Tento problém může vyřešit použití technických prostředků k poskytnutí souhlasu, například prostřednictvím transparentního a k uživatelům vstřícného nastavení. Toto nařízení by proto mělo umožnit vyjádření souhlasu prostřednictvím vhodného nastavení prohlížeče nebo jiné aplikace. Volby provedené koncovými uživateli v rámci obecného nastavení ochrany soukromí v prohlížeči nebo jiné aplikaci by měly být pro jakékoli třetí strany závazné a vůči nim vynutitelné. Internetové prohlížeče jsou druhem softwarové aplikace, která umožňuje získávání a prezentování informací na internetu. Tyto funkce mají i další druhy aplikací, jako například aplikace, které umožňují volání a přenos zpráv nebo poskytují navigaci na cestách. Internetové prohlížeče zprostředkovávají většinu toho, k čemu dochází mezi koncovým uživatelem a internetovou stránkou. Z tohoto hlediska se nacházejí v privilegovaném postavení, aby hrály aktivní úlohu při pomáhání koncovým uživatelům kontrolovat tok informací do koncového zařízení a z něj. Internetové prohlížeče mohou zejména sloužit jako „strážci“, a pomoci tak koncovým uživatelům zabránit tomu, aby k informacím z jejich koncových zařízení (například z chytrého telefonu, tabletu nebo počítače) bylo přistupováno nebo aby tyto informace byly ukládány.

(23) Zásady záměrné a standardní ochrany osobních údajů byly kodifikovány v článku 25 nařízení (EU) 2016/679. V současné době je standardní nastavení pro cookies ve většině stávajících prohlížečů nastaveno na „přijímat všechna cookies“. Poskytovatelé softwaru umožňujícího získávání a prezentování informací na internetu by proto měli mít povinnost konfigurovat software tak, aby nabízel možnost zabránit třetím stranám v ukládání informací v koncovém zařízení; toto je často prezentováno jako „odmítnout přijímání cookies třetích stran“. Koncovým uživatelům by měl být nabídnut soubor možností nastavení ochrany soukromí, sahající od vyšší úrovně ochrany (například „nikdy nepřijímat cookies“) přes střední úroveň (například „odmítnout přijímání

cookies třetích stran“ nebo „přijímat pouze cookies prvních stran“) až po nižší úroveň (například „vždy přijímat cookies“). Toto nastavení ochrany soukromí by mělo být prezentováno snadno viditelným a srozumitelným způsobem.

(24) Aby mohly internetové prohlížeče získat souhlas koncových uživatelů, jak jej definuje nařízení (EU) 2016/679, například s ukládáním sledovacích cookies třetích stran, měly by mimo jiné vyžadovat od koncového uživatele koncového zařízení jasnou potvrzující akci, která by stvrzovala jeho svobodně poskytnutý, konkrétně informovaný a jednoznačný souhlas s uchováváním těchto cookies v jeho koncovém zařízení a s přístupem k nim. Taková akce může být považována za potvrzující, pokud je například vyžadováno, aby koncoví uživatelé pro potvrzení svého souhlasu aktivně zvolili možnost „přijímat cookies třetích stran“, a jsou jim poskytnuty informace nezbytné k učinění volby. Za tímto účelem je nezbytné vyžadovat, aby poskytovatelé softwaru umožňujícího přístup k internetu zajistili, že koncoví uživatelé jsou při instalaci informováni, že si mohou vybrat z různých možností nastavení ochrany soukromí, a aby je požádali o učinění volby. Poskytnuté informace by neměly koncové uživatele odrazovat od výběru nastavení vyšší ochrany soukromí a měly by zahrnovat relevantní informace o rizicích souvisejících s povolením toho, aby byly v počítači uchovávány cookies třetích stran, včetně sestavování dlouhodobých záznamů o historii prohlížení internetu danou osobou a využívání těchto záznamů k zasílání cílené reklamy. Internetové prohlížeče se vyzývají k tomu, aby koncovým uživatelů poskytly snadné způsoby, jak kdykoli během používání změnit nastavení ochrany soukromí, a aby uživateli umožnily dělat výjimky pro určité internetové stránky, přidávat takové stránky na seznam povolených stránek nebo upřesnit, pro které internetové stránky jsou cookies (třetích) stran povoleny vždy, nebo nikdy.

(25) Přístup k sítím elektronických komunikací vyžaduje pravidelné vysílání určitých datových paketů za účelem navázání nebo udržování spojení se sítí nebo jinými zařízeními v síti. Zařízení dále musí mít přidělenu jedinečnou adresu, aby bylo v dané síti identifikovatelné. Obdobně normy pro bezdrátové komunikace a mobilní telefony zahrnují vysílání aktivních signálů obsahujících jedinečné identifikátory, jako jsou adresa MAC, identifikátory IMEI a IMSI atd. Každá bezdrátová základnová stanice (tj. vysílač a přijímač), jako např. bezdrátový přístupový bod, má konkrétní dosah, v rámci kterého mohou být tyto informace zachyceny. Objevili se poskytovatelé služeb, kteří nabízejí služby sledování, jež jsou založeny na skenování informací souvisejících se zařízením a poskytují různé funkce, včetně počítání osob, poskytování údajů o počtu osob čekajících ve frontě, zjišťování počtu osob v konkrétní oblasti atd. Tyto informace mohou být použity k více obtěžujícím účelům, jako je zasílání komerčních sdělení s personalizovanými nabídkami koncovým uživatelům, například při vstupu do prodejny. Zatímco některé z těchto funkcí nepředstavují vysoká rizika pro soukromí, jiné funkce, například ty, jejichž součástí je sledování osob v průběhu času, včetně opakovaných návštěv určených míst, tato rizika zahrnují. Poskytovatelé provozující tyto praktiky by měli zobrazovat nápadná oznámení umístěná na okraji oblasti pokrytí, která by koncové uživatele před vstupem do vymezené oblasti informovala o tom, že v této oblasti je v provozu tato technologie, o účelu sledování, o odpovědné osobě a o existenci případných opatření, která může koncový uživatel koncového zařízení učinit, aby shromažďování informací minimalizoval nebo zastavil. Jsou-li shromažďovány osobní údaje, měly by být poskytnuty dodatečné informace podle článku 13 nařízení (EU) 2016/679.

(26) Spadá-li zpracování dat elektronických komunikací ze strany poskytovatelů služeb elektronických komunikací do oblasti působnosti tohoto nařízení, mělo by toto

nařízení Unii nebo členským státům umožnit, aby za určitých podmínek právním předpisem omezily některé povinnosti a práva, jestliže takové omezení představuje nezbytné a přiměřené opatření v demokratické společnosti na ochranu konkrétních veřejných zájmů, včetně národní bezpečnosti, obrany, veřejné bezpečnosti, předcházení trestným činům a jejich vyšetřování, odhalování či stíhání nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení a dalších důležitých cílů obecného veřejného zájmu Unie nebo členského státu, zejména jedná-li se o důležitý hospodářský či finanční zájem Unie nebo členského státu, nebo představuje-li monitorovací, inspekční nebo regulační funkci spojenou s výkonem veřejné moci pro účely těchto zájmů. Toto nařízení by proto nemělo ovlivnit možnost členských států provádět zákonné zachycování elektronických komunikací nebo přijímat jiná opatření, je-li to nezbytné a přiměřené pro ochranu výše uvedených veřejných zájmů a je-li to v souladu s Listinou základních práv Evropské unie a s Evropskou úmluvou o ochraně lidských práv a základních svobod, jak je vykládána Soudním dvorem Evropské unie a Evropským soudem pro lidská práva. Poskytovatelé služeb elektronických komunikací by měli stanovit vhodné postupy usnadňující oprávněné žádosti příslušných orgánů, případně se zohledněním úlohy zástupce určeného podle čl. 3 odst. 3.

(27) S ohledem na identifikaci volající linky je nezbytně nutné chránit právo volajícího potlačit identifikaci linky, ze které se volání uskutečňuje, a právo volaného odmítnout volání z neidentifikovaných linek. Někteří koncoví uživatelé, zejména linky pomoci a obdobné subjekty, mají zájem na zaručení anonymity volajících. S ohledem na identifikaci spojené linky je nezbytně nutné chránit právo a oprávněný zájem volaného potlačit identifikaci linky, se kterou je volající ve skutečnosti spojen.

(28) Ve zvláštních případech je oprávněné nepřihlížet k potlačení identifikace volající linky. Práva koncových uživatelů na soukromí s ohledem na identifikaci volající linky by měla být omezena, je-li to nezbytné pro vysledování obtěžujících volání, a s ohledem na identifikaci volající linky a lokalizační údaje, je-li to nezbytné k tomu, aby záchranné služby, například služba eCall, mohly plnit své úkoly co možná nejefektivněji.

(29) Existuje technologie, která poskytovatelům služeb elektronických komunikací umožňuje různými způsoby omezit přijímání nežádoucích volání koncovými uživateli, včetně blokování tichých volání a jiných podvodných a obtěžujících volání. Poskytovatelé veřejně dostupných interpersonálních komunikačních služeb založených na číslech by tuto technologii měli nasadit a zdarma chránit koncové uživatele před obtěžujícími voláními. Poskytovatelé by měli zajistit, aby koncoví uživatelé byli o existenci těchto funkcí informováni, a to zveřejněním této skutečnosti na svých internetových stránkách.

(30) Veřejně dostupné seznamy koncových uživatelů služeb elektronických komunikací jsou značně rozšířeny. Veřejně dostupným seznamem se rozumí jakýkoli seznam nebo služba, které obsahují informace o koncových uživatelích, jako jsou telefonní čísla (včetně čísel mobilních telefonů) a kontaktní údaje v podobě e-mailové adresy, včetně informačních služeb o účastnických číslech. Právo fyzické osoby na soukromí a na ochranu osobních údajů vyžaduje, aby koncoví uživatelé, kteří jsou fyzickými osobami, byli předtím, než jsou jejich osobní údaje zahrnuty do seznamu, požádáni o souhlas. Oprávněný zájem právnických osob vyžaduje, aby koncoví uživatelé, kteří jsou právnickými osobami, měli právo vznést námitku proti tomu, aby byly do seznamu zahrnuty údaje, které se jich týkají.

(31) Pokud koncoví uživatelé, kteří jsou fyzickými osobami, udělí souhlas s tím, aby byly jejich údaje zahrnuty do těchto seznamů, měli by mít možnost na základě souhlasu určit, které kategorie jejich osobních údajů budou v seznamu zahrnuty (například jméno, e-mailová adresa, adresa bydliště, uživatelské jméno, telefonní číslo). Mimo to by poskytovatelé veřejně dostupných seznamů měli koncové uživatele před tím, než je zahrnou do seznamu, informovat o účelech seznamu a o vyhledávacích funkcích. Koncoví uživatelé by měli mít možnost prostřednictvím souhlasu určit, na základě kterých kategorií osobních údajů lze v jejich kontaktních údajích vyhledávat. Kategorie osobních údajů zahrnutých do seznamu a kategorie osobních údajů, na jejichž základě lze vyhledávat v kontaktních údajích koncového uživatele, by neměly být nutně totožné.

(32) Jako přímý marketing se v tomto nařízení označuje jakákoli forma reklamy, prostřednictvím které fyzická nebo právnická osoba zasílá přímá marketingová sdělení přímo jednomu nebo více identifikovaným nebo identifikovatelným koncovým uživatelům využívajícím služby elektronických komunikací. Kromě nabízení produktů a služeb pro obchodní účely by měl tento pojem zahrnovat také sdělení zasílaná politickými stranami, které kontaktují fyzické osoby prostřednictvím služeb elektronických komunikací za účelem podpory svých stran. Totéž by se mělo vztahovat na sdělení zasílaná jinými neziskovými organizacemi za účelem podpory účelů dané organizace.

(33) Měla by být poskytnuta ochranná opatření na ochranu koncových uživatelů před nevyžádanými sděleními pro účely přímého marketingu, která zasahují do soukromého života koncových uživatelů. Míra narušení soukromí a obtěžování je považována za relativně podobnou nezávisle na široké škále technologií a kanálů používaných k uskutečňování této elektronické komunikace, ať už se používají automatické volací a komunikační systémy, aplikace pro výměnu rychlých zpráv, elektronická pošta, SMS, MMS, Bluetooth atd. Je tedy odůvodněné požadovat, aby před tím, než je koncovým uživatelům zasláno elektronické obchodní sdělení pro účely přímého marketingu, byl získán souhlas koncového uživatele, aby byli jednotlivci účinně chráněni před narušováním svého soukromého života, jakož i aby byly chráněny oprávněné zájmy právnických osob. Právní jistota a potřeba zajistit, že pravidla chránící před nevyžádanými elektronickými sděleními budou nadále použitelná i v budoucnosti, odůvodňují potřebu definovat jednotný soubor pravidel, která se neliší v závislosti na technologii použité k přenosu těchto nevyžádaných sdělení a která zároveň zaručí rovnocennou úroveň ochrany pro všechny občany v celé Unii. Je však rozumné umožnit používání kontaktních údajů pro elektronickou poštu v kontextu existujícího zákaznického vztahu pro nabízení podobných produktů nebo služeb. Tato možnost by se měla vztahovat pouze na tutéž společnost, která získala elektronické kontaktní údaje v souladu s nařízením (EU) 2016/679.

(34) Pokud koncoví uživatelé poskytli svůj souhlas s přijímáním nevyžádaných sdělení pro účely přímého marketingu, měli by mít nadále možnost svůj souhlas jednoduchým způsobem kdykoli odvolat. V zájmu usnadnění účinného prosazování pravidel Unie, která se týkají nevyžádaných zpráv pro účely přímého marketingu, je nezbytné zakázat maskování totožnosti a používání falešných totožností a falešných zpátečních adres nebo čísel při zasílání nevyžádaných obchodních sdělení pro účely přímého marketingu. Nevyžádaná marketingová sdělení by proto měla být jako taková snadno rozpoznatelná a měla by uvádět totožnost právnické nebo fyzické osoby, která sdělení přenáší nebo jejímž jménem je přenášeno, jakož i poskytovat informace nezbytné pro

to, aby příjemci mohli uplatnit své právo nesouhlasit s přijímáním dalších písemných a/nebo ústních marketingových zpráv.

(35) Aby bylo možné snadno odvolat souhlas, měly by právnické nebo fyzické osoby zasílající přímá marketingová sdělení prostřednictvím elektronické pošty uvést odkaz nebo platnou adresu elektronické pošty, které mohou koncoví uživatelé snadno použít k odvolání souhlasu. Právnické nebo fyzické osoby sdělující přímá marketingová sdělení formou hlasových volání a formou volání prostřednictvím automatických volacích a komunikačních systémů by měly zobrazit identitu linky, na kterou lze společnosti zavolat, nebo uvést zvláštní kód označující skutečnost, že se jedná o marketingové volání.

(36) Hlasová volání pro účely přímého marketingu, která nezahrnují používání automatických volacích a komunikačních systémů, jsou nákladnější pro odesílatele a koncovým uživatelům žádné finanční náklady nezpůsobují. Členské státy by proto měly mít možnost zavést nebo zachovat vnitrostátní systémy, které umožňují uskutečňovat taková volání pouze koncovým uživatelům, kteří nevznesli námitky.

(37) Poskytovatelé služeb, kteří nabízejí služby elektronických komunikací, by měli koncové uživatele informovat o opatřeních, která mohou učinit na ochranu bezpečnosti svých komunikací, například tím, že použijí konkrétní druhy softwaru nebo šifrovací technologie. Požadavek informovat koncové uživatele o konkrétních bezpečnostních rizicích nezbavuje poskytovatele služeb povinnosti přijmout na své vlastní náklady přiměřená a okamžitá opatření k odstranění jakéhokoli nového nepředvídaného bezpečnostního rizika a obnovit běžnou úroveň bezpečnosti služby. Informace o bezpečnostních rizicích by měly být účastníkovi poskytovány zdarma. Bezpečnost je posuzována s ohledem na článek 32 nařízení (EU) 2016/679.

(38) Aby byl zajištěn plný soulad s nařízením (EU) 2016/679, mělo by být prosazování ustanovení tohoto nařízení svěřeno stejným orgánům, které odpovídají za prosazování ustanovení nařízení (EU) 2016/679, a toto nařízení se opírá a mechanismus jednotnosti podle nařízení (EU) 2016/679. Členské státy by měly mít možnost mít více než jeden dozorový úřad, aby zohlednily své ústavní, organizační a správní uspořádání. Dozorové úřady by měly být rovněž odpovědné za monitorování uplatňování tohoto nařízení, pokud jde o data elektronických komunikací a právnické osoby. Tyto dodatečné úkoly by neměly ohrozit schopnost dozorových úřadů provádět své úkoly týkající se ochrany osobních údajů podle nařízení (EU) 2016/679 a tohoto nařízení. Každému dozorovému úřadu by měly být poskytnuty dodatečné finanční a lidské zdroje, prostory a infrastruktura potřebné pro účinné plnění jeho úkolů podle tohoto nařízení.

(39) Každý dozorový úřad by měl být na území svého vlastního členského státu příslušný k výkonu pravomocí a plnění úkolů stanovených v tomto nařízení. Aby se zajistilo jednotné monitorování a prosazování tohoto nařízení v celé Unii, měly by mít dozorové úřady v každém členském státě tytéž úkoly a účinné pravomoci, aniž by byly dotčeny pravomoci orgánů příslušných podávat obžalobu podle práva členského státu, pravomoci upozorňovat justiční orgány na porušení tohoto nařízení a obrátit se na soud. Členské státy a jejich dozorové úřady jsou vyzývány k tomu, aby při uplatňování tohoto nařízení zohlednily zvláštní potřeby mikropodniků a malých a středních podniků.

(40) S cílem posílit prosazování pravidel tohoto nařízení by každý dozorový úřad měl mít pravomoc za jakékoli porušení tohoto nařízení ukládat sankce včetně správních pokut, a to vedle nebo namísto odpovídajících opatření podle tohoto nařízení. V tomto

nařízení by měly být uvedeny porušení a maximální hranice a kritéria pro stanovení souvisejících správních pokut, jež by měl v každém jednotlivém případě určit příslušný dozorový úřad při zohlednění všech příslušných okolností konkrétní situace s náležitým přihlédnutím zejména k povaze, závažnosti a době trvání tohoto porušení a k jeho důsledkům a opatřením přijatým v zájmu zajištění souladu s povinnostmi vyplývajícími z tohoto nařízení a v zájmu prevence či zmírnění důsledků tohoto porušení. Pro účely stanovení pokuty podle tohoto nařízení by měl být podnik chápán ve smyslu článků 101 a 102 Smlouvy.

(41) Aby byly splněny cíle tohoto nařízení, zejména chránit základní práva a svobody fyzických osob, a především jejich právo na ochranu osobních údajů, a zajistit volný pohyb osobních údajů v rámci Unie, měla by být na Komisi přenesena pravomoc přijímat akty v souladu s článkem 290 Smlouvy za účelem doplnění tohoto nařízení. Akty v přenesené pravomoci by měly být přijímány zejména s ohledem na informace, které mají být poskytovány mimo jiné pomocí standardizovaných ikon, aby byl poskytnut snadno viditelný a srozumitelný přehled o shromažďování informací vysílaných koncovým zařízením, o účelu tohoto shromažďování, odpovědné osobě a o případných opatřeních, která může koncový uživatel koncového zařízení učinit, aby shromažďování minimalizoval. Akty v přenesené pravomoci jsou rovněž nezbytné pro určení kódu k identifikaci přímých marketingových volání, včetně volání uskutečněných prostřednictvím automatických volacích a komunikačních systémů. Je obzvláště důležité, aby Komise vedla odpovídající konzultace a aby tyto konzultace byly provedeny v souladu se zásadami stanovenými v interinstitucionální dohodě o zdokonalení tvorby právních předpisů ze dne 13. dubna 2016[8]. V zájmu zajištění rovné účasti na vypracovávání aktů v přenesené pravomoci obdrží Evropský parlament a Rada veškeré dokumenty současně s odborníky z členských států a tito odborníci mají systematicky přístup na schůze skupin odborníků Komise zabývajících se vypracováním aktů v přenesené pravomoci. V zájmu zajištění jednotných podmínek pro provádění tohoto nařízení je dále třeba svěřit Komisi prováděcí pravomoci v případech stanovených tímto nařízením. Tyto pravomoci by měly být vykonávány v souladu s nařízením (EU) č. 182/2011.

(42) Jelikož cíle tohoto nařízení, totiž zajištění přiměřené úrovně ochrany fyzických a právnických osob a volného pohybu dat elektronických komunikací v Unii, nemůže být dosaženo uspokojivě členskými státy, ale spíše jej, z důvodu rozsahu nebo účinků tohoto nařízení, může být lépe dosaženo na úrovni Unie, může Unie přijmout opatření v souladu se zásadou subsidiarity stanovenou v článku 5 Smlouvy o Evropské unii. V souladu se zásadou proporcionality stanovenou v uvedeném článku nepřekračuje toto nařízení rámec toho, co je nezbytné pro dosažení tohoto cíle.

(43) Směrnice 2002/58/ES by měla být zrušena,

PŘIJALY TOTO NAŘÍZENÍ:

[8] Interinstitucionální dohoda mezi Evropským parlamentem, Radou Evropské unie a Evropskou komisí ze dne 13. dubna 2016 o zdokonalení tvorby právních předpisů (Úř. věst. L 123, 12.5.2016, s. 1).

KAPITOLA I
OBECNÁ USTANOVENÍ

Článek 1
Předmět

1. Toto nařízení stanoví pravidla týkající se ochrany základních práv a svobod fyzických a právnických osob při poskytování a využívání služeb elektronických komunikací, a zejména práv na respektování soukromého života a komunikace a ochranu fyzických osob v souvislosti se zpracováním osobních údajů.

2. Toto nařízení zajišťuje volný pohyb dat elektronických komunikací a služeb elektronických komunikací v rámci Unie, který nesmí být omezen ani zakázán z důvodů souvisejících s respektováním soukromého života a komunikace fyzických a právnických osob a s ochranou fyzických osob v souvislosti se zpracováním osobních údajů.

3. Ustanovení tohoto nařízení upřesňují a doplňují nařízení (EU) 2016/679 tím, že stanoví konkrétní pravidla pro účely uvedené v odstavcích 1 a 2.

Článek 2
Věcná působnost

1. Toto nařízení se vztahuje na zpracování dat elektronických komunikací prováděné v souvislosti s poskytováním a využíváním služeb elektronických komunikací a na informace související s koncovými zařízeními koncových uživatelů.

2. Toto nařízení se nevztahuje na:

a) činnosti, které nespadají do oblasti působnosti práva Unie;

b) činnosti členských států, které spadají do oblasti působnosti hlavy V kapitoly 2 Smlouvy o Evropské unii;

c) služby elektronických komunikací, které nejsou veřejně dostupné;

d) činnosti příslušných orgánů za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení;

3. Zpracování dat elektronických komunikací orgány, institucemi a jinými subjekty Unie se řídí nařízením (EU) 00/0000 [nové nařízení, které nahrazuje nařízení č. 45/2001].

4. Tímto nařízením není dotčeno uplatňování směrnice 2000/31/ES[9], a zejména pravidel týkajících se odpovědnosti zprostředkujících poskytovatelů služeb stanovených v článcích 12 až 15 uvedené směrnice.

5. Tímto nařízením nejsou dotčena ustanovení směrnice 2014/53/EU.

[9] Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu („směrnice o elektronickém obchodu“) (Úř. věst. L 178, 17.7.2000, s. 1).

Článek 3
Místní působnost a zástupce

1. Toto nařízení se vztahuje na:

a) poskytování služeb elektronických komunikací koncovým uživatelům v Unii bez ohledu na to, zda je od koncového uživatele vyžadována platba;

b) využívání těchto služeb;

c) ochranu informací souvisejících s koncovými zařízeními koncových uživatelů nacházejících se v Unii.

2. Pokud poskytovatel služeb elektronických komunikací není usazen v Unii, určí písemně zástupce v Unii.

3. Tento zástupce je usazen v jednom z členských států, ve kterém se nacházejí koncoví uživatelé těchto služeb elektronických komunikací.

4. Zástupce má pravomoc vedle nebo namísto poskytovatele, kterého zastupuje, zodpovídat dotazy a poskytovat informace, zejména dozorovým úřadům a koncovým uživatelům, ohledně všech otázek souvisejících se zpracováním dat elektronických komunikací za účelem zajištění souladu s tímto nařízením.

5. Určením zástupce podle odstavce 2 nejsou dotčeny právní kroky, které by mohly být zahájeny proti fyzické nebo právnické osobě, která zpracovává data elektronických komunikací v souvislosti s poskytováním služeb elektronických komunikací ze zemí mimo Unii koncovým uživatelům v Unii.

Článek 4
Definice

1. Pro účely tohoto nařízení se použijí tyto definice:

a) definice uvedené v nařízení (EU) 2016/679;

b) definice „sítě elektronických komunikací“, „služby elektronických komunikací“, „interpersonální komunikační služby“, „interpersonální komunikační služby založené na číslech“, „interpersonální komunikační služby nezávislé na číslech“, „koncového uživatele“ a „volání“ v čl. 2 bodu 1, 4, 5, 6, 7, 14 a 21 [směrnice, kterou se stanoví evropský kodex pro elektronické komunikace];

c) definice „koncového zařízení“ v čl. 1 bodě 1 směrnice Komise 2008/63/ES[10].

2. Pro účely odst. 1 písm. b) definice „interpersonální komunikační služby“ zahrnuje služby, které umožňují interpersonální a interaktivní komunikaci pouze jako nepodstatnou pomocnou funkci, která je ze své podstaty spjata s jinou službou.

3. Dále se pro účely tohoto nařízení použijí tyto definice:

a) „daty elektronických komunikací“ se rozumí obsah elektronických komunikací a metadata elektronických komunikací;

b) „obsahem elektronických komunikací“ se rozumí obsah vyměňovaný prostřednictvím služeb elektronických komunikací, jako například text, hlas, video, obrazy a zvuk;

[10] Směrnice Komise 2008/63/ES ze dne 20. června 2008 o hospodářské soutěži na trhu s telekomunikačními koncovými zařízeními (Úř. věst. L 162, 21.6.2008, s. 20).

c) „metadaty elektronických komunikací“ se rozumí údaje zpracovávané v síti elektronických komunikací pro účely přenášení, šíření nebo výměny obsahu elektronických komunikací, a to včetně údajů sloužících k vysledování a identifikaci zdroje a cíle komunikace, údajů o poloze zařízení generovaných v kontextu poskytování služeb elektronických komunikací a data, času, době trvání a typu komunikace;

d) „veřejně dostupným seznamem“ se rozumí seznam koncových uživatelů služeb elektronických komunikací v tištěné nebo elektronické podobě, který je zveřejněn nebo který je k dispozici veřejnosti nebo části veřejnosti, a to i prostřednictvím informační služby o účastnických číslech;

e) „elektronickou poštou“ se rozumí jakákoli elektronická zpráva obsahující informace jako text, hlas, video, zvuk nebo obraz zaslaná prostřednictvím sítě elektronických komunikací, kterou lze uchovávat v síti nebo v souvisejících výpočetních zařízeních, nebo v koncovém zařízení jejího příjemce;

f) „přímým marketingovým sdělením“ se rozumí jakákoli forma reklamy, ať už písemná nebo ústní, která je zaslána jednomu nebo více identifikovaným nebo identifikovatelným koncovým uživatelům služeb elektronických komunikací, a to včetně využití automatických volacích a komunikačních systémů se zásahem člověka nebo bez něj, elektronické pošty, SMS atd.;

g) „hlasovými voláními pro účely přímého marketingu“ se rozumí živá volání, která nezahrnují využití automatických volacích a komunikačních systémů;

h) „automatickými volacími a komunikačními systémy“ se rozumí systémy, které jsou schopné automaticky zahájit volání jednomu nebo více příjemcům v souladu s pokyny stanovenými pro daný systém a přenášet zvuky, které nejsou živým projevem, včetně volání uskutečněných za použití automatických volacích a komunikačních systémů, které spojí volanou osobu s jinou osobou.

KAPITOLA II
OCHRANA ELEKTRONICKÝCH KOMUNIKACÍ FYZICKÝCH A PRÁVNICKÝCH OSOB A INFORMACÍ ULOŽENÝCH V JEJICH KONCOVÝCH ZAŘÍZENÍCH

Článek 5
Důvěrný charakter dat elektronických komunikací

Data elektronických komunikací jsou důvěrná. Jakékoli zasahování do dat elektronických komunikací, jako například příposlech, odposlech, uchovávání, monitorování, skenování nebo jiné druhy zachycování, sledování či zpracování dat elektronických komunikací, osobami jinými než koncovými uživateli se zakazuje, s výjimkou případů povolených tímto nařízením.

Článek 6
Povolené zpracování dat elektronických komunikací

1. Poskytovatelé služeb a sítí elektronických komunikací mohou zpracovávat data elektronických komunikací, pokud:

a) je to nezbytné pro přenos komunikace, po dobu nutnou pro tento účel, nebo

b) je to nezbytné pro zachování nebo obnovení bezpečnosti služeb a sítí elektronických komunikací nebo pro odhalení technických závad a/nebo chyb v přenosu elektronických komunikací, po dobu nutnou pro tento účel.

2. Poskytovatelé služeb elektronických komunikací mohou zpracovávat metadata elektronických komunikací, pokud:

a) je to nezbytné pro splnění povinných požadavků na kvalitu služby podle [směrnice, kterou se stanoví evropský kodex pro elektronické komunikace] nebo nařízení (EU) 2015/2120[11], po dobu nutnou pro tento účel, nebo

b) je to nezbytné pro vyúčtování, výpočet plateb za propojení, odhalení podvodného užívání nebo zneužívání služeb elektronických komunikací, zamezení takovému podvodnému užívání nebo zneužívání nebo pro přihlášení se k užívání těchto služeb, nebo

c) dotčený koncový uživatel udělil svůj souhlas se zpracováním metadat svých komunikací pro jeden nebo více konkrétních účelů, včetně poskytování konkrétních služeb těmto koncovým uživatelům, za předpokladu, že tento účel nebo účely nelze splnit zpracováním anonymizovaných informací.

3. Poskytovatelé služeb elektronických komunikací mohou zpracovávat obsah elektronických komunikací pouze:

a) za účelem poskytování konkrétní služby koncovému uživateli, pokud dotčený koncový uživatel nebo koncoví uživatelé udělili svůj souhlas se zpracováním svého obsahu elektronických komunikací a danou službu nelze bez zpracování tohoto obsahu poskytnout, nebo

b) pokud všichni dotčení koncoví uživatelé udělili svůj souhlas se zpracováním svého obsahu elektronických komunikací pro jeden nebo více konkrétních účelů, které nelze splnit zpracováním anonymizovaných informací, a poskytovatel konzultoval dozorový úřad. Pro konzultaci dozorového úřadu se použije čl. 36 odst. 2 a 3 nařízení (EU) 2016/679.

Článek 7
Uchovávání a výmaz dat elektronických komunikací

1. Aniž jsou dotčeny čl. 6 odst. 1 písm. b) a čl. 6 odst. 3 písm. a) a b), poskytovatel služeb elektronických komunikací po obdržení obsahu elektronických komunikací zamýšleným příjemcem nebo příjemci vymaže obsah elektronických komunikací nebo tato data anonymizuje. Tato data mohou být zaznamenána nebo uchovávána koncovými uživateli nebo třetí stranou, která jimi byla k zaznamenání, uchovávání nebo jinému zpracování těchto dat pověřena v souladu s nařízením (EU) 2016/679.

2. Aniž jsou dotčeny čl. 6 odst. 1 písm. b) a čl. 6 odst. 2 písm. a) a c), poskytovatel služeb elektronických komunikací vymaže metadata elektronických komunikací nebo tato data anonymizuje, nejsou-li již potřebná pro účely přenosu komunikace.

3. Pokud ke zpracování metadat elektronických komunikací dochází za účelem vyúčtování v souladu s čl. 6 odst. 2 písm. b), mohou být příslušná metadata

[11] Nařízení Evropského parlamentu a Rady (EU) 2015/2120 ze dne 25. listopadu 2015, kterým se stanoví opatření týkající se přístupu k otevřenému internetu a mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací a nařízení (EU) č. 531/2012 o roamingu ve veřejných mobilních komunikačních sítích v Unii (Úř. věst. L 310, 26.11.2015, s. 1).

uchovávána do konce období, v němž lze v souladu s vnitrostátními právními předpisy vyúčtování právně napadnout nebo uplatňovat nárok na platbu.

Článek 8

Ochrana informací uchovávaných v koncových zařízeních koncových uživatelů a souvisejících s těmito zařízeními

1. Využití funkcí koncového zařízení pro zpracování a uchovávání, jakož i shromažďování informací z koncových zařízení koncových uživatelů, včetně informací o softwaru a hardwaru, jinými subjekty, než jsou dotčení koncoví uživatelé, se zakazuje, s výjimkou těchto důvodů:

a) pokud je to nezbytné výhradně za účelem uskutečnění přenosu elektronické komunikace prostřednictvím sítě elektronických komunikací, nebo

b) pokud koncový uživatel udělil svůj souhlas, nebo

c) je to nezbytné pro poskytování služby informační společnosti požadované koncovým uživatelem, nebo

d) je to nezbytné pro měření návštěvnosti internetových stránek, za předpokladu, že toto měření je prováděno poskytovatelem služby informační společnosti požadované koncovým uživatelem.

2. Shromažďování informací vysílaných koncovým zařízením za účelem umožnění připojení tohoto zařízení k jinému zařízení a/nebo k síťovému zařízení se zakazuje, ledaže:

a) je tak činěno výhradně pro účely navázání spojení a po dobu, která je k tomu nezbytná, nebo

b) je zobrazeno jasné a nápadné oznámení informující alespoň o způsobech shromažďování, jeho účelu a osobě, která je za ně odpovědná, a podávající další informace požadované podle článku 13 nařízení (EU) 2016/679, pokud jsou shromažďovány osobní údaje, jakož i o případných opatřeních, která může koncový uživatel koncového zařízení učinit, aby shromažďování minimalizoval nebo zastavil.

Shromažďování těchto informací je podmíněno použitím vhodných technických a organizačních opatření, aby byla zajištěna úroveň zabezpečení odpovídající rizikům, jak stanoví článek 32 nařízení (EU) 2016/679.

3. Informace poskytnuté podle odst. 2 písm. b) mohou být doplněny standardizovanými ikonami, aby byl snadno viditelným, srozumitelným a jasným způsobem poskytnut smysluplný přehled o shromažďování.

4. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 27, které určují informace, jež mají být sděleny pomocí standardizovaných ikon, a postupy pro poskytování standardizovaných ikon.

Článek 9

Souhlas

1. Použije se definice souhlasu a podmínky jeho vyjádření podle čl. 4 bodu 11 a článku 7 nařízení (EU) 2016/679.

2. Aniž je dotčen odstavec 1, je-li to technicky možné a proveditelné, může být souhlas pro účely čl. 8 odst. 1 písm. b) vyjádřen za použití odpovídajícího technického nastavení softwarové aplikace umožňující přístup k internetu.

3. Koncoví uživatelé, kteří souhlasili se zpracováním dat elektronických komunikací, jak stanoví čl. 6 odst. 2 písm. c) a čl. 6 odst. 3 písm. a) a b), mají možnost svůj souhlas kdykoli odvolat, jak stanoví čl. 7 odst. 3 nařízení (EU) 2016/679, a tato možnost je jim v pravidelném intervalu 6 měsíců připomínána, dokud zpracování pokračuje.

Článek 10
Informace a možnosti nastavení ochrany soukromí, které mají být poskytnuty

1. Software uváděný na trh, který umožňuje elektronické komunikace včetně získávání a prezentování informací na internetu, musí nabízet možnost zabránit třetím stranám v uchovávání informací v koncovém zařízení koncového uživatele nebo ve zpracovávání informací, které jsou v tomto zařízení již uchovávané.

2. Software při instalaci informuje koncového uživatele o možnostech nastavení ochrany soukromí a k tomu, aby mohla instalace pokračovat, vyžaduje souhlas koncového uživatele s nastavením.

3. V případě softwaru, který byl ke dni 25. května 2018 již instalován, musí být požadavky podle odstavců 1 a 2 splněny při první aktualizaci softwaru, avšak nejpozději dne 25. srpna 2018.

Článek 11
Omezení

1. Právo Unie nebo členského státu může prostřednictvím legislativního opatření omezit rozsah povinností a práv uvedených v článcích 5 až 8, jestliže takové omezení respektuje podstatu základních práv a svobod a představuje nezbytné, vhodné a přiměřené opatření v demokratické společnosti s cílem chránit jeden nebo více obecných veřejných zájmů uvedených v čl. 23 odst. 1 písm. a) až e) nařízení (EU) 2016/679, nebo monitorovací, inspekční nebo regulační funkci spojenou s výkonem veřejné moci pro účely těchto zájmů.

2. Poskytovatelé služeb elektronických komunikací na základě legislativního opatření přijatého podle odstavce 1 stanoví vnitřní postupy pro odpovídání na žádosti o přístup k datům elektronických komunikací koncových uživatelů. Příslušnému dozorovému úřadu na vyžádání poskytnou informace o těchto postupech, počet obdržených žádostí, uplatněný právní důvod a svou odpověď.

KAPITOLA III
PRÁVO FYZICKÝCH A PRÁVNICKÝCH OSOB NA KONTROLU NAD ELEKTRONICKÝMI KOMUNIKACEMI

Článek 12
Uvedení a omezení identifikace volající a spojené linky

1. Je-li nabízeno uvedení volající a spojené linky v souladu s článkem [107] [směrnice, kterou se stanoví evropský kodex pro elektronické komunikace], poskytovatelé

veřejně dostupných interpersonálních komunikačních služeb založených na číslech poskytnou:

a) volajícímu koncovému uživateli možnost zabránit uvedení identifikace volající linky, a to pro dané volání, pro dané spojení nebo trvale;

b) volanému koncovému uživateli možnost zabránit uvedení identifikace volající linky u příchozích volání;

c) volanému koncovému uživateli možnost odmítnout příchozí volání, bylo-li volajícím koncovým uživatelem zabráněno uvést identifikaci volající linky;

d) volanému koncovému uživateli možnost zabránit uvedení identifikace spojené linky volajícímu koncovému uživateli.

2. Možnosti uvedené v odst. 1 písm. a), b), c) a d) se koncovým uživatelům poskytnou jednoduše a zdarma.

3. Ustanovení odst. 1 písm. a) se použije rovněž v případě volání směřujících z Unie do třetích zemí. Ustanovení odst. 1 písm. b), c) a d) se použijí rovněž v případě příchozích volání pocházejících ze třetích zemí.

4. Je-li nabízeno uvedení identifikace volající nebo spojené linky, poskytovatelé veřejně dostupných interpersonálních komunikačních služeb založených na číslech poskytnou veřejnosti informace týkající se možností stanovených v odst. 1 písm. a), b), c) a d).

Článek 13
Výjimky z uvedení a omezení identifikace volající a spojené linky

1. Pokud jde o volání záchranných služeb, poskytovatelé veřejně dostupných interpersonálních komunikačních služeb založených na číslech bez ohledu na to, zda volající koncový uživatel zabránil uvedení identifikace volající linky, pro účely odpovídání na tuto komunikaci nedbají na potlačení identifikace volající linky a na odepření či neexistenci souhlasu koncového uživatele se zpracováním metadat, a to pro jednotlivé linky v případě organizací zabývajících se tísňovými komunikacemi, včetně center tísňového volání.

2. Členské státy zavedou konkrétnější ustanovení, pokud jde o zavedení postupů a stanovení okolností, za kterých poskytovatelé veřejně dostupných interpersonálních komunikačních služeb založených na číslech dočasně nedbají na potlačení identifikace volající linky v případech, kdy koncoví uživatelé požadují vysledování zlovolných či obtěžujících volání.

Článek 14
Blokování příchozích volání

Poskytovatelé veřejně dostupných interpersonálních komunikačních služeb založených na číslech zavedou nejmodernější opatření, aby omezili přijímání nežádoucích volání koncovými uživateli, a koncovým uživatelům rovněž zdarma poskytnou tyto možnosti:

a) blokovat příchozí volání z konkrétních čísel nebo z anonymních zdrojů;

b) zamezit automatickému přesměrování volání třetí stranou na koncové zařízení daného koncového uživatele.

Článek 15
Veřejně dostupné seznamy

1. Poskytovatelé veřejně dostupných seznamů musí získat souhlas koncových uživatelů, kteří jsou fyzickými osobami, se zahrnutím jejich osobních údajů do seznamu a následně musí získat souhlas těchto koncových uživatelů se zahrnutím údajů pro jednotlivé kategorie osobních údajů, a to v rozsahu, ve kterém jsou tyto údaje významné pro účely seznamu stanovené poskytovatelem seznamu. Poskytovatelé koncovým uživatelům, kteří jsou fyzickými osobami, dají možnost ověřit, opravit či odstranit tyto údaje.

2. Poskytovatelé veřejně dostupných seznamů informují koncové uživatele, kteří jsou fyzickými osobami a jejichž osobní údaje jsou v seznamu, o dostupných vyhledávacích funkcích seznamu a před tím, než tyto vyhledávací funkce související s údaji těchto koncových uživatelů povolí, získají jejich souhlas.

3. Poskytovatelé veřejně dostupných seznamů poskytnou koncovým uživatelům, kteří jsou právnickými osobami, možnost vznést námitku proti tomu, aby byly údaje, které se jich týkají, zahrnuty do seznamu. Poskytovatelé těmto koncovým uživatelům, kteří jsou právnickými osobami, dají možnost ověřit, opravit či odstranit tyto údaje.

4. Možnost, aby koncoví uživatelé nebyli zahrnuti do veřejně dostupného seznamu nebo aby ověřili, opravili či odstranili jakékoli údaje s nimi související, se poskytuje zdarma.

Článek 16
Nevyžádaná sdělení

1. Fyzické nebo právnické osoby mohou používat služby elektronických komunikací pro účely zasílání přímých marketingových sdělení koncovým uživatelů, kteří jsou fyzickými osobami a udělili svůj souhlas.

2. Pokud fyzická nebo právnická osoba získá od svých zákazníků v souvislosti s prodejem výrobku nebo služby a v souladu s nařízením (EU) 2016/679 jejich elektronické kontaktní údaje pro elektronickou poštu, může tato fyzická či právnická osoba využít tyto elektronické kontaktní údaje pro účely přímého marketingu svých vlastních obdobných výrobků nebo služeb pouze v případě, že je zákazníkům jasně a zřetelně poskytnuta možnost zdarma a jednoduchým způsobem vznést námitku proti takovému využití. Právo vznést námitku se nabídne v době, kdy jsou údaje shromážděny, a při zaslání každé jednotlivé zprávy.

3. Aniž jsou dotčeny odstavce 1 a 2, fyzické nebo právnické osoby využívající služby elektronických komunikací pro účely uskutečňování přímých marketingových volání musí:

a) uvést identitu linky, na které je lze kontaktovat, nebo

b) uvést konkrétní kód nebo předčíslí identifikující skutečnost, že se jedná o marketingové volání.

4. Bez ohledu na odstavec 1 mohou členské státy právním předpisem stanovit, že uskutečňování hlasových volání pro účely přímého marketingu koncovým uživatelům, kteří jsou fyzickými osobami, je povoleno, pouze pokud jde o koncové uživatele, kteří jsou fyzickými osobami a kteří nevznesli námitku proti přijímání těchto sdělení.

5. Členské státy v rámci unijního práva a platného vnitrostátního práva zajistí, že oprávněné zájmy koncových uživatelů, kteří jsou právnickými osobami, jsou v případě nevyžádaných sdělení zasílaných způsoby stanovenými v odstavci 1 dostatečně chráněny.

6. Jakákoli fyzická nebo právnická osoba používající služby elektronických komunikací k přenášení přímých marketingových sdělení informuje koncové uživatele o marketingovém charakteru sdělení a o totožnosti právnické nebo fyzické osoby, jejímž jménem je sdělení přenášeno, a poskytne příjemcům informace nezbytné pro to, aby mohli jednoduchým způsobem uplatnit své právo odvolat svůj souhlas s přijímáním dalších marketingových sdělení.

7. Komisi je svěřena pravomoc přijímat prováděcí opatření v souladu s čl. 26 odst. 2, která upřesňují kód nebo předčíslí identifikující marketingová volání podle odst. 3 písm. b).

Článek 17
Informace o zjištěných bezpečnostních rizicích

V případě konkrétního rizika, které by mohlo ohrozit bezpečnost sítí a služeb elektronických komunikací, poskytovatel služeb elektronických komunikací informuje o těchto rizicích koncové uživatele a v případě, že riziko nespadá do oblasti působnosti opatření, která může poskytovatel služby přijmout, informuje koncové uživatele o veškeré možné právní ochraně, včetně uvedení pravděpodobných souvisejících nákladů.

KAPITOLA IV
NEZÁVISLÉ DOZOROVÉ ÚŘADY A PROSAZOVÁNÍ

Článek 18
Nezávislé dozorové úřady

1. Nezávislé dozorové úřady nebo úřady odpovědné za monitorování uplatňování nařízení (EU) 2016/679 rovněž odpovídají za monitorování uplatňování tohoto nařízení. Kapitoly VI a VII nařízení (EU) 2016/679 se použijí obdobně. Úkoly a pravomoci dozorových úřadů se vykonávají s ohledem na koncové uživatele.

2. Dozorový úřad nebo úřady uvedené v odstavci 1 v příslušných případech spolupracují s vnitrostátními regulačními orgány zřízenými podle [směrnice, kterou se stanoví evropský kodex pro elektronické komunikace].

Článek 19
Evropský sbor pro ochranu osobních údajů

Evropský sbor pro ochranu osobních údajů zřízený podle článku 68 nařízení (EU) 2016/679 má pravomoc zajišťovat jednotné uplatňování tohoto nařízení. Evropský sbor pro ochranu osobních údajů za tímto účelem plní úkoly stanovené v článku 70 nařízení (EU) 2016/679. Sbor plní také tyto úkoly:

a) poskytuje poradenství Komisi ohledně případných navrhovaných změn tohoto nařízení,

b) prošetřuje z vlastního podnětu, na žádost některého ze svých členů nebo na žádost Komise veškeré otázky týkající se uplatňování tohoto nařízení a vydává pokyny, doporučení a osvědčené postupy, aby podporoval soudržné uplatňování tohoto nařízení.

Článek 20
Spolupráce a postupy pro jednotnost

Každý dozorový úřad přispívá k jednotnému uplatňování tohoto nařízení v celé Unii. Dozorové úřady za tímto účelem v souladu s kapitolou VII nařízení (EU) 2016/679 spolupracují mezi sebou a s Komisí, pokud jde o záležitosti upravené tímto nařízením.

KAPITOLA V
PRÁVNÍ OCHRANA, ODOVĚDNOST A SANKCE

Článek 21
Právní ochrana

1. Aniž jsou dotčeny jakékoli jiné prostředky správní nebo soudní ochrany, má každý koncový uživatel služeb elektronických komunikací stejnou právní ochranu stanovenou v článcích 77, 78 a 79 nařízení (EU) 2016/679.

2. Jakákoli fyzická nebo právnická osoba jiná než koncoví uživatelé, která byla nepříznivě zasažena porušením tohoto nařízení a která má oprávněný zájem na zastavení nebo zákazu domnělých porušení, včetně poskytovatele služeb elektronických komunikací chránícího své oprávněné obchodní zájmy, má právo obrátit se v souvislosti s těmito porušeními na soud.

Článek 22
Právo na náhradu újmy a odpovědnost

Jakýkoli koncový uživatel služeb elektronických komunikací, který v důsledku porušení tohoto nařízení utrpěl hmotnou či nehmotnou újmu, má v souladu s článkem 82 nařízení (EU) 2016/679 právo obdržet od porušitele náhradu utrpěné újmy, pokud porušitel neprokáže, že nenese žádným způsobem odpovědnost za událost, která ke vzniku újmy vedla.

Článek 23
Obecné podmínky pro ukládání správních pokut

1. Pro účely tohoto článku se na porušení tohoto nařízení použije kapitola VII nařízení (EU) 2016/679.

2. Za porušení následujících ustanovení tohoto nařízení lze v souladu s odstavcem 1 uložit správní pokuty až do výše 10 000 000 EUR, nebo jedná-li se o podnik, až do výše 2 % celkového ročního obratu celosvětově za předchozí finanční rok, podle toho, která hodnota je vyšší:

a) povinnosti jakékoli fyzické nebo právnické osoby, která zpracovává data elektronických komunikací, podle článku 8;

b) povinnosti poskytovatele softwaru umožňujícího elektronické komunikace podle článku 10;

c) povinnosti poskytovatelů veřejně dostupných seznamů podle článku 15;

d) povinnosti jakékoli fyzické nebo právnické osoby, která používá služby elektronických komunikací, podle článku 16.

3. Za porušení zásady důvěrného charakteru sdělení, povoleného zpracování dat elektronických komunikací a lhůt pro výmaz podle článků 5, 6 a 7 lze v souladu s odstavcem 1 tohoto nařízení uložit správní pokuty až do výše 20 000 000 EUR, nebo jedná-li se o podnik, až do výše 4 % celkového ročního obratu celosvětově za předchozí finanční rok, podle toho, která hodnota je vyšší.

4. Členské státy stanoví pravidla pro sankce za porušení článků 12, 13, 14 a 17.

5. Za nedodržení příkazu dozorového úřadu uvedeného v článku 18 lze uložit správní pokuty až do výše 20 000 000 EUR, nebo jedná-li se o podnik, až do výše 4 % celkového ročního obratu celosvětově za předchozí finanční rok, podle toho, která hodnota je vyšší.

6. Aniž jsou dotčeny nápravné pravomoci dozorových úřadů podle článku 18, může každý členský stát stanovit pravidla týkající se toho, zda a do jaké míry lze ukládat správní pokuty orgánům veřejné moci a veřejným subjektům usazeným v daném členském státě.

7. Na výkon pravomocí dozorovým úřadem podle tohoto článku se vztahují vhodné procesní záruky v souladu s právem Unie a členského státu, včetně účinné soudní ochrany a spravedlivého procesu.

8. Neumožňuje-li právo členského státu uložení správních pokut, může se použít tento článek tak, aby podnět k uložení pokuty dal příslušný dozorový úřad a aby pokuta byla uložena příslušnými vnitrostátními soudy, a současně je třeba zajistit, aby tyto prostředky právní ochrany byly účinné a aby jejich účinek byl rovnocenný se správními pokutami, jež ukládají dozorové úřady. Uložené pokuty musí být v každém případě účinné, přiměřené a odrazující. Tyto členské státy oznámí Komisi do [xxx] příslušná ustanovení svých právních předpisů, která přijmou podle tohoto odstavce, a bez prodlení jakékoli následné novely nebo změny týkající se těchto ustanovení.

Článek 24
Sankce

1. Členské státy stanoví pravidla pro jiné sankce, jež se mají ukládat za porušení tohoto nařízení, zejména za porušení, na něž se nevztahují správní pokuty podle článku 23, a učiní veškerá opatření nezbytná k zajištění jejich uplatňování. Tyto sankce musí být účinné, přiměřené a odrazující.

2. Každý členský stát oznámí Komisi nejpozději do 18 měsíců od data uvedeného v čl. 29 odst. 2 právní předpisy, které přijme podle odstavce 1, a bez zbytečného odkladu jakékoli následné změny týkající se těchto ustanovení.

KAPITOLA VI
AKTY V PŘENESENÉ PRAVOMOCI A PROVÁDĚCÍ AKTY

Článek 25
Výkon přenesené pravomoci

1. Pravomoc přijímat akty v přenesené pravomoci je svěřena Komisi za podmínek stanovených v tomto článku.

2. Pravomoc přijímat akty v přenesené pravomoci uvedená v čl. 8 odst. 4 je svěřena Komisi na dobu neurčitou počínaje [dnem vstupu tohoto nařízení v platnost].

3. Evropský parlament nebo Rada mohou přenesení pravomoci uvedené v čl. 8 odst. 4 kdykoli zrušit. Rozhodnutím o zrušení se ukončuje přenesení pravomoci v něm blíže určené. Rozhodnutí nabývá účinku prvním dnem po zveřejnění v *Úředním věstníku Evropské unie*, nebo k pozdějšímu dni, který je v něm upřesněn. Nedotýká se platnosti již platných aktů v přenesené pravomoci.

4. Před přijetím aktu v přenesené pravomoci Komise vede konzultace s odborníky jmenovanými jednotlivými členskými státy v souladu se zásadami stanovenými v interinstitucionální dohodě o zdokonalení tvorby právních předpisů ze dne 13. dubna 2016.

5. Přijetí aktu v přenesené pravomoci Komise neprodleně oznámí současně Evropskému parlamentu a Radě.

6. Akt v přenesené pravomoci přijatý podle čl. 8 odst. 4 vstoupí v platnost, pouze pokud proti němu Evropský parlament nebo Rada nevysloví námitky ve lhůtě dvou měsíců ode dne, kdy jim byl tento akt oznámen, nebo pokud Evropský parlament i Rada před uplynutím této lhůty informují Komisi o tom, že námitky nevysloví. Z podnětu Evropského parlamentu nebo Rady se tato lhůta prodlouží o dva měsíce.

Článek 26
Výbor

1. Komisi je nápomocen Komunikační výbor zřízený podle článku 110 [směrnice, kterou se stanoví evropský kodex pro elektronické komunikace]. Tento výbor je výborem ve smyslu nařízení (EU) č. 182/2011[12].

2. Odkazuje-li se na tento odstavec, použije se článek 5 nařízení (EU) č. 182/2011.

KAPITOLA VII
ZÁVĚREČNÁ USTANOVENÍ

Článek 27
Zrušení

1. Směrnice 2002/58/ES se zrušuje s účinkem ode dne 25. května 2018.

2. Odkazy na zrušenou směrnici se považují za odkazy na toto nařízení.

Článek 28
Ustanovení o monitorování a hodnocení

Nejpozději do 1. ledna 2018 Komise zavede podrobný program pro monitorování účinnosti tohoto nařízení.

[12] Nařízení Evropského parlamentu a Rady (EU) č. 182/2011 ze dne 16. února 2011, kterým se stanoví pravidla a obecné zásady způsobu, jakým členské státy kontrolují Komisi při výkonu prováděcích pravomocí (Úř. věst. L 55, 28.2.2011, s. 13).

Nejpozději do tří let ode dne použitelnosti tohoto nařízení a poté každé tři roky Komise provede hodnocení tohoto nařízení a hlavní zjištění předloží Evropskému parlamentu, Radě a Evropskému hospodářskému a sociálnímu výboru. Hodnocení bude případně sloužit jako podklad pro návrh na změnu nebo zrušení tohoto nařízení s ohledem na technický, hospodářský a právní vývoj.

Článek 29
Vstup v platnost a použitelnost

1. Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

2. Použije se ode dne 25. května 2018.

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

V Bruselu dne

Za Evropský parlament	*Za Radu*
předseda / předsedkyně	*předseda / předsedkyně*