

V Bruseli 16. januára 2017
(OR. en)

5358/17

**Medziinštitucionálny spis:
2017/0003 (COD)**

TELECOM 12
COMPET 32
MI 45
DATAPROTECT 4
CONSOM 19
JAI 40
DIGIT 10
FREMP 3
CYBER 10
IA 12
CODEC 52

NÁVRH

Od:	Jordi AYET PUIGARNAU, riaditeľ, v zastúpení generálneho tajomníka Európskej komisie
Dátum doručenia:	12. januára 2017
Komu:	Jeppe TRANHOLM-MIKKELSEN, generálny tajomník Rady Európskej únie
Č. dok. Kom.:	COM(2017) 10 final
Predmet:	Návrh NARIADENIA EURÓPSKEHO PARLAMENTU A RADY o rešpektovaní súkromného života a ochrane osobných údajov v elektronických komunikáciách a o zrušení smernice 2002/58/ES (smernica o súkromí a elektronických komunikáciách)

Delegáciám v prílohe zasielame dokument COM(2017) 10 final.

Príloha: COM(2017) 10 final



EURÓPSKA
KOMISIA

V Bruseli 10. 1. 2017
COM(2017) 10 final

2017/0003 (COD)

Návrh

NARIADENIE EURÓPSKEHO PARLAMENTU A RADY

o rešpektovaní súkromného života a ochrane osobných údajov v elektronických komunikáciách a o zrušení smernice 2002/58/ES (smernica o súkromí a elektronických komunikáciách)

(Text s významom pre EHP)

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

DÔVODOVÁ SPRÁVA

1. KONTEXT NÁVRHU

1.1. Dôvody a ciele návrhu

Cieľom stratégie digitálneho jednotného trhu (ďalej len „**stratégia DSM**“)¹ je zvýšiť dôveru v digitálne služby a zlepšiť bezpečnosť digitálnych služieb. V tejto súvislosti boli kľúčovými krokmi reforma rámca ochrany údajov a prijatie nariadenia (EÚ) 2016/679 (ďalej len „**všeobecné nariadenie o ochrane údajov**“)². V rámci stratégie DSM bolo oznámené aj preskúmanie smernice 2002/58/ES (ďalej len „**smernica o súkromí a elektronických komunikáciách**“)³, s cieľom zabezpečiť prísne pravidlá ochrany súkromia pre používateľov elektronických komunikačných služieb a rovnaké podmienky pre všetkých účastníkov trhu. V tomto návrhu sa skúma smernica o súkromí a elektronických komunikáciách z hľadiska dodržiavania cieľov stratégie DSM a zabezpečovania súladu so všeobecným nariadením o ochrane údajov.

Smernicou o súkromí a elektronických komunikáciách sa zabezpečuje ochrana základných práv a slobôd, najmä rešpektovanie súkromného života, dôvernoscť komunikácií a ochrana osobných údajov v sektore elektronických komunikácií. Tiež sa ňou zaručuje voľný pohyb údajov z elektronických komunikácií, ako aj elektronických komunikačných zariadení a služieb v Únii. Do sekundárneho práva Únie sa ňou zavádza základné právo na rešpektovanie súkromného života, pokiaľ ide o komunikácie, ktoré je zakotvené v článku 7 Charty základných práv Európskej únie (ďalej len „**charta**“).

V súlade s požiadavkami lepšej právnej regulácie vykonala Komisia *ex post* Program regulačnej vhodnosti a efektívnosti (ďalej len „**hodnotenie REFIT**“)⁴ smernice o súkromí a elektronických komunikáciách. Z hodnotenia vyplýva, že ciele a zásady aktuálneho rámca zostávajú primerané. Od poslednej revízie smernice o súkromí a elektronických komunikáciách v roku 2009 však došlo k významnému technologickému a hospodárskemu vývoju. Spotrebitelia a podniky čoraz častejšie namiesto tradičných komunikačných služieb využívajú nové internetové služby umožňujúce interpersonálnu komunikáciu, ako sú internetová telefónia, rýchle správy a e-mailové služby založené na webe. Na tieto internetové komunikačné (over-the-top) služby (ďalej len „**OTT**“)⁵ sa vo všeobecnosti nevzťahuje aktuálny rámec elektronických komunikácií Únie a ani smernica o súkromí a elektronických komunikáciách. Smernica teda nedrží krok s technologickým vývojom, v dôsledku čoho nie sú komunikácie uskutočňované prostredníctvom nových služieb chránené.

1.2. Súlad s existujúcimi ustanoveniami politik v oblasti tejto politiky

Tento návrh je vo vzťahu k všeobecnému nariadeniu o ochrane údajov *lex specialis* a špecifikuje a dopĺňa ho v oblasti údajov z elektronických komunikácií, ktoré sa považujú za

¹ Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov Stratégia pre jednotný digitálny trh v Európe, COM(2015) 192 final.

² Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracovávaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1 – 88).

³ Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002, týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) (Ú. v. ES L 201, 31.7.2002, s. 37).

osobné údaje. Všetky záležitosti týkajúce sa spracovávaní osobných údajov, ktoré sa v návrhu osobitne neriešia, sú upravené vo všeobecnom nariadení o ochrane údajov. Zosúladienie so všeobecným nariadením o ochrane údajov malo za následok zrušenie niektorých ustanovení, ako sú bezpečnostné požiadavky z článku 4 smernice o súkromí a elektronických komunikáciách.

1.3. Súlad s ostatnými politikami Únie

Smernica o súkromí a elektronických komunikáciách tvorí súčasť regulačného rámca pre elektronické komunikácie. V roku 2016 prijala Komisia návrh smernice, ktorou sa stanovuje európsky kódex elektronickej komunikácie (ďalej len „kódex **EECC**“)⁴ a ktorou sa tento rámec reviduje. Hoci tento návrh nie je neoddeliteľnou súčasťou kódexu EECC, čiastočne vychádza z jeho vymedzenia pojmov, a to aj v prípade pojmu „elektronické komunikačné služby“. Podobne ako v prípade kódexu EECC, poskytovatelia OTT sú začlenení aj do rozsahu pôsobnosti tohto návrhu, aby sa tak zohľadnila realita na trhu. Kódex EECC okrem toho dopĺňa tento návrh v oblasti zaistenia bezpečnosti elektronických komunikačných služieb.

Smernicou 2014/53/EÚ o rádiových zariadeniach (ďalej len „smernica **RED**“)⁵ sa zabezpečuje jednotný trh pre rádiové zariadenia. Konkrétne sa v nej vyžaduje, aby rádiové zariadenia pred uvedením na trh obsahovali prostriedky na zabezpečenie ochrany osobných údajov a súkromia používateľa. Podľa smernice RED a nariadenia o európskej normalizácii (EÚ) č. 1025/2012⁶ je Komisia oprávnená prijímať opatrenia. Tento návrh nemá vplyv na smernicu RED.

Návrh neobsahuje žiadne osobitné ustanovenia z oblasti uchovávaní údajov. Zachováva podstatu článku 15 smernice o súkromí a elektronických komunikáciách a zosúladuje ho s osobitným znením článku 23 všeobecného nariadenia o ochrane údajov, v ktorom sa stanovujú dôvody, na základe ktorých môžu členské štáty obmedziť rozsah práv a povinností uvedených v konkrétnych článkoch smernice o súkromí a elektronických komunikáciách. S ohľadom na judikatúru Súdneho dvora týkajúcu sa výkladu smernice o súkromí a elektronických komunikáciách a Charty základných práv⁷ si preto členské štáty môžu slobodne ponechať alebo vytvoriť národné rámce pre uchovávanie údajov, v rámci ktorých okrem iného stanovujú opatrenia pre cielené uchovávanie údajov, a to pod podmienkou, že tieto rámce sú v súlade so všeobecnými zásadami práva Únie.

A nakoniec, návrh sa nevzťahuje na činnosti inštitúcií, orgánov a agentúr Únie. Jeho zásady a príslušné povinnosti, pokiaľ ide o právo na rešpektovanie súkromného života a komunikácií

⁴ Návrh smernice Európskeho parlamentu a Rady, ktorou sa stanovuje európsky kódex elektronickej komunikácie (Prepracované znenie) [COM/2016/0590 final – 2016/0288 (COD)].

⁵ Smernica Európskeho parlamentu a Rady 2014/53/EÚ zo 16. apríla 2014 o harmonizácii právnych predpisov členských štátov týkajúcich sa sprístupňovania rádiových zariadení na trhu, ktorou sa zrušuje smernica 1999/5/ES (Ú. v. EÚ L 153, 22.5.2014, s. 62 – 106).

⁶ Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1025/2012 z 25. októbra 2012 o európskej normalizácii, ktorým sa menia a dopĺňajú smernice Rady 89/686/EHS a 93/15/EHS a smernice Európskeho 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 ktorým sa zrušuje rozhodnutie Rady 87/95/EHS a rozhodnutie Európskeho parlamentu a Rady č. 1673/2006/ES (Ú. v. EÚ L 316, 14.11.2012, s. 12 – 33).

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

v súvislosti so spracovávaním údajov z elektronických komunikácií, sú však už začlenené do návrhu nariadenia, ktorým sa zrušuje nariadenie (ES) č. 45/2001⁸.

2. PRÁVNY ZÁKLAD, SUBSIDIARITA A PROPORCIONALITA

2.1. Právny základ

Príslušný právny základ tohto návrhu predstavujú články 16 a 114 Zmluvy o fungovaní Európskej únie (ďalej len „ZFEÚ“).

V článku 16 ZFEÚ sa zavádza osobitný právny základ na prijímanie pravidiel týkajúcich sa ochrany jednotlivcov pri spracúvaní osobných údajov inštitúciami Únie a členskými štátmi počas vykonávania činností patriacich do rozsahu pôsobnosti práva Únie a pravidiel týkajúcich sa voľného pohybu takýchto údajov. Keďže elektronická komunikácia fyzickej osoby sa zvyčajne považuje za osobné údaje, ochrana fyzických osôb, pokiaľ ide o súkromie komunikácií a spracovanie takýchto údajov, by mala vychádzať z článku 16.

Návrh sa okrem toho zameriava aj na ochranu komunikácií a súvisiace oprávnené záujmy právnických osôb. Význam a rozsah pôsobnosti práv z článku 7 charty sú v súlade s článkom 52 ods. 3 charty rovnaké ako význam a rozsah pôsobnosti práv stanovených v článku 8 ods. 1 Európskeho dohovoru o ochrane ľudských práv a základných slobôd (ďalej len „EDLP“). Pokiaľ ide o rozsah pôsobnosti článku 7 charty, v judikatúre Súdneho dvora Európskej únie (ďalej len „Súdny dvor“)⁹ a Európskeho súdu pre ľudské práva¹⁰ sa potvrdzuje, že odborné činnosti právnických osôb nesmú byť vyňaté z ochrany práva zaručeného článkom 7 charty a článkom 8 EDLP.

Keďže iniciatíva má plniť dvojaký účel, a to ochranu komunikácií právnických osôb a cieľ dosiahnutia vnútorného trhu v prípade týchto elektronických komunikácií, a zabezpečenie jeho fungovania v tomto smere nemožno ponechať náhode, mala by preto vychádzať aj z článku 114 ZFEÚ.

2.2. Subsidiarita

Rešpektovanie komunikácií je základným právom, uznaným v charte. Obsahom elektronických komunikácií môžu byť veľmi citlivé informácie o koncových používateľoch zapojených do komunikácie. Podobne aj metaúdaje odvodené z elektronických komunikácií môžu obsahovať veľmi citlivé a osobné informácie, čo výslovne uznal aj Súdny dvor¹¹. Väčšina členských štátov zároveň uznáva potrebu chrániť komunikácie ako osobitné ústavné právo. Hoci členské štáty môžu prijímať politiky na zabezpečenie dodržiavania tohto práva, nebudú jednotné, pretože neexistujú pravidlá Únie, a tým vzniknú obmedzenia pri cezhraničných tokoch osobných aj iných ako osobných údajov súvisiacich s používaním

⁸ Nariadenie Európskeho parlamentu a Rady (ES) č. 45/2001 z 18. decembra 2000 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi Spoločenstva a o voľnom pohybe takýchto údajov (Ú. v. ES L 8, 12.1.2001, s. 1 – 22).

⁹ Pozri vec C-450/06 Varec SA, ECLI:EU:C:2008:91, § 48.

¹⁰ Pozri najmä rozsudky ESLP Niemietz/Nemecko, rozsudok zo 16. decembra 1992, séria A č. 251-B, § 29; Société Colas Est a i./Francúzsko, č. 37971/97, § 41; Zbierka rozsudkov a rozhodnutí 2002-III; Peck/Spojené kráľovstvo č. 44647/98, § 57, Zbierka rozsudkov a rozhodnutí 2003-I; ako aj Vinci Construction a GTM Génie Civil et Services/Francúzsko, č. 63629/10 a 60567/10, § 63, 2. apríla 2015.

¹¹ Pozri poznámku pod čiarou č. 7.

elektronických komunikačných služieb. A nakoniec, na zachovanie konzistentnosti so všeobecným nariadením o ochrane údajov je potrebné preskúmať smernicu o súkromí a elektronických komunikáciách a prijať opatrenia na zosúladenie oboch nástrojov.

Uskutočňovanie opatrení na úrovni Únie posilnili technologický vývoj a ambície stratégie DSM. Úspešnosť digitálneho jednotného trhu EÚ závisí od efektívnosti, s akou EÚ zruší vnútroštátne obmedzenia a prekážky a využije výhody a úspory európskeho digitálneho jednotného trhu. Navyše keďže internet a digitálne technológie nepoznajú hranice, táto problematika presahuje územie jedného členského štátu. Členské štáty nedokážu v súčasnej situácii problémy efektívne riešiť. Ak má digitálny jednotný trh fungovať správne, je potrebné zabezpečiť rovnaké podmienky pre hospodárske subjekty poskytujúce nahraditeľné služby, ako aj rovnakú ochranu koncových používateľov na úrovni Únie.

2.3. Proporcionalita

Ak sa má zabezpečiť efektívna právna ochrana rešpektovania súkromia a komunikácií, je potrebné rozšíriť rozsah pôsobnosti tak, aby zahŕňal aj poskytovateľov OTT. Hoci niekoľko známych poskytovateľov OTT už v plnom rozsahu alebo čiastočne dodržiava zásadu dôvernosti komunikácií, ochranu základných práv nemožno ponechať len na samoreguláciu v odvetví. Čoraz dôležitejšou sa stáva aj efektívna ochrana súkromia v koncových zariadeniach, ktorá je pri ukladaní citlivých informácií v osobnom aj pracovnom živote nenahraditeľná. Vykonávaním smernice o súkromí a elektronických komunikáciách sa nedosiahlo účinné posilnenie postavenia koncových používateľov. Na dosiahnutie cieľa je preto potrebné uplatňovať túto zásadu centralizovaním súhlasu v softvéri a zobrazovaním informácií používateľom o nastaveniach ochrany súkromia. Pokiaľ ide o presadzovanie tohto nariadenia, mali by ho zaručovať dozorné orgány a mechanizmus konzistentnosti zriadený v rámci všeobecného nariadenia o ochrane údajov. Okrem toho v návrhu sa členským štátom umožňuje prijímať vnútroštátne výnimky na osobitné legitímne účely. Návrh sa teda týka iba toho, čo je potrebné na dosiahnutie cieľov, a je v súlade so zásadou proporcionality stanovenou v článku 5 Zmluvy o Európskej únii. Služby, ktorých sa to týka, sú zaťažené povinnosťami v čo najmenšej miere, pričom na príslušné základné práva to nemá žiadny vplyv.

2.4. Výber nástroja

Komisia predkladá návrh nariadenia s cieľom zabezpečiť súlad so všeobecným nariadením o ochrane údajov a právnu istotu pre používateľov, ako aj podniky, aby sa zabránilo rozdielnemu výkladu v jednotlivých členských štátoch. Nariadenie môže na úrovni celej Únie zabezpečiť rovnaké podmienky ochrany používateľov a nižšie náklady na dodržiavanie predpisov pre podniky s cezhraničnou pôsobnosťou.

3. VÝSLEDKY HODNOTENÍ EX POST, KONZULTÁCIÍ SO ZAJINTERESOVANÝMI STRANAMI A POSÚDENÍ VPLYVU

3.1. Hodnotenia ex post/kontroly vhodnosti existujúcich právnych predpisov

Pri hodnotení REFIT sa skúmalo, do akej miery smernica o súkromí a elektronických komunikáciách efektívne prispieva k primeranej ochrane rešpektovania súkromného života a dôvernosti komunikácií v EÚ. Bolo zamerané aj na identifikovanie možných redundancií.

Z hodnotenia REFIT vyplynulo, že uvedené ciele smernice sú naďalej **relevantné**. Všeobecným nariadením o ochrane údajov sa zabezpečuje ochrana osobných údajov a smernicou o súkromí a elektronických komunikáciách dôvernosť komunikácií, ktoré môžu obsahovať aj iné ako osobné údaje a údaje súvisiace s právnickou osobou. Efektívnu ochranu článku 7 charty by mal preto zabezpečiť osobitný nástroj. Relevantnými sa ukázali aj ďalšie ustanovenia, ako napríklad pravidlá o odosielaní nevyžiadaných marketingových komunikácií.

Pokiaľ ide o **efektívnosť a účinnosť**, z hodnotenia REFIT vyplynulo, že smernica plne nedosahuje svoje ciele. Nejasné znenie niektorých ustanovení a nejednoznačnosť právnych koncepcií ohrozujú harmonizáciu a pre podniky s cezhraničnou pôsobnosťou predstavujú výzvy. Z hodnotenia ďalej vyplynulo, že niektoré ustanovenia predstavujú pre podniky a spotrebiteľov zbytočnú záťaž. Ciele sa nedosiahli napríklad v súvislosti s pravidlom súhlasu na ochranu dôvernosti v koncových zariadeniach, pretože koncovým používateľom sa zobrazujú žiadosti o povolenie trvalých súborov cookie bez toho, aby rozumeli ich významu, a v niektorých prípadoch sa dokonca súbory cookie nastavujú bez ich súhlasu. Pravidlo súhlasu je na jednej strane príliš inkluzívne, pretože sa vzťahuje aj na postupy nenarúšajúce súkromie, a zároveň nedostatočne inkluzívne, pretože sa jednoznačne nevzťahuje na niektoré sledovacie metódy (napr. odoberanie odtlačkov prstov na zariadení), ktorých súčasťou nemusí byť prístup k zariadeniu alebo ukladanie do zariadenia. A nakoniec, jej vykonávanie môže byť pre podniky nákladné.

Z hodnotenia vyplynulo, že pravidlá smernice o súkromí a elektronických komunikáciách majú stále **pridanú hodnotu EÚ**, vďaka ktorej je možné lepšie dosahovať ciele v oblasti zabezpečovania súkromia na internete na rozvíjajúcom sa nadnárodnom trhu elektronických komunikácií. Ukázalo sa aj to, že celkovo sú pravidlá **súdržné** s ďalšími relevantnými právnymi predpismi, aj keď bolo identifikovaných niekoľko redundancií v súvislosti s novým všeobecným nariadením o ochrane údajov (pozri v oddiele 1.2).

3.2. Konzultácie so zainteresovanými stranami

Komisia zorganizovala verejnú konzultáciu, ktorá sa uskutočnila od 12. apríla do 5. júla 2016, a dostala 421 odpovedí¹². Vyplynuli z nej tieto kľúčové zistenia¹³:

- **Potreba osobitných pravidiel pre sektor elektronických komunikácií v oblasti dôvernosti elektronických komunikácií:** Súhlas vyjadrilo 83,4 % respondentov z radov občanov, spotrebiteľských organizácií a organizácií občianskej spoločnosti a 88,9 % respondentov z radov orgánov verejnej moci a nesúhlas 63,4 % respondentov z radov subjektov odvetvia.
- **Rozšírenie rozsahu pôsobnosti na nové komunikačné služby (OTT):** Súhlas vyjadrilo 76 % respondentov z radov občanov a organizácií občianskej spoločnosti a 93,1 % respondentov z radov orgánov verejnej moci, zatiaľ čo z radov subjektov odvetvia s touto možnosťou súhlasí iba 36,2 % respondentov.

¹² 162 príspevkov pochádzalo od občanov, 33 od organizácií občianskej spoločnosti a spotrebiteľských organizácií, 186 od subjektov odvetvia a 40 od orgánov verejnej moci vrátane príslušných orgánov presadzujúcich smernicu o súkromí a elektronických komunikáciách.

¹³ Celá správa je dostupná na adrese: <https://ec.europa.eu/digital-single-market/news-redirect/37204>.

- **Zmena výnimiek zo súhlasu so spracovaním prevádzkových a lokalizačných údajov:** 49,1 % respondentov z radov občanov, spotrebiteľských organizácií a organizácií občianskej spoločnosti a 36 % respondentov z radov orgánov verejnej moci uprednostňuje možnosť nerozširovania výnimiek, zatiaľ čo 36 % respondentov z radov subjektov odvetvia súhlasí s rozšírením výnimiek a dve tretiny subjektov odvetvia sú za jednoduché zrušenie ustanovení.
- **Podpora riešení navrhovaných v oblasti odsúhlasovania súborov cookie:** Možnosť uloženia povinnosti výrobcov koncových zariadení uvádzať výrobky na trh s aktivovanými nastaveniami štandardnej ochrany súkromia podporuje 81,2 % respondentov z radov občanov a 63 % respondentov z radov orgánov verejnej moci, zatiaľ čo možnosť podpory samoregulácie alebo spoluregulácie schvaľuje 58,3 % respondentov z radov subjektov odvetvia.

Okrem toho Európska komisia v apríli 2016 zorganizovala dva semináre, pričom jeden bol prístupný pre všetky zainteresované strany a jeden pre príslušné vnútroštátne orgány, ktoré riešili najdôležitejšie otázky súvisiace s verejnými konzultáciami. Vo vystúpeniach na seminároch sa zohľadňovali výsledky verejnej konzultácie.

S cieľom získať názory občanov sa v celej EÚ uskutočnil prieskum Eurobarometer týkajúci sa súkromia a elektronických komunikácií¹⁴. Vyplývali z neho tieto kľúčové zistenia¹⁵:

- 78 % respondentov považuje za veľmi dôležité, aby sa prístup k osobným informáciám v ich počítači, smartfóne alebo tablete umožňoval len s ich súhlasom.
- 72 % respondentov považuje za veľmi dôležité, aby bola zaručená dôvernosť ich e-mailov a rýchlych správ na internete.
- 89 % respondentov súhlasí s navrhovanou možnosťou, aby zdieľaniu ich informácií zabráňovali štandardné nastavenia prehliadača.

3.3. Získavanie a využívanie odborných znalostí

Komisia vychádzala z tohto externého odborného poradenstva:

- Cílené konzultácie skupiny expertov EÚ: stanovisko pracovnej skupiny zriadenej podľa článku 29; stanovisko EDPS; stanovisko platformy REFIT; stanoviská orgánu BEREC; stanoviská agentúry ENISA a stanoviská členov siete na ochranu spotrebiteľov a spoluprácu.
- Externé odborné poznatky, najmä tieto dve štúdie:
 - štúdia *ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation* (Smernica o súkromí a elektronických komunikáciách: posúdenie transpozície, efektívnosti a súladu s navrhovaným nariadením o ochrane údajov) (SMART 2013/007116);
 - štúdia *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector* (Hodnotenie a preskúmanie smernice

¹⁴ Prieskum Eurobarometer (EB) 2016 443 týkajúci sa súkromia a elektronických komunikácií (SMART 2016/079).

¹⁵ Celá správa je dostupná na adrese: <https://ec.europa.eu/digital-single-market/news-redirect/37205>.

3.4. Posúdenie vplyvu

Vykonalo sa posúdenie vplyvu tohto návrhu a výbor pre kontrolu regulácie k nemu 28. septembra 2016 vydal kladné stanovisko¹⁶. S cieľom vykonať odporúčania výboru sa v posúdení vplyvu lepšie vysvetľuje rozsah pôsobnosti iniciatívy, jej súdržnosť s ostatnými právnymi nástrojmi (všeobecné nariadenie o ochrane údajov, EECC, RED) a potreba osobitného nástroja. Základný scenár sa ďalej prepracúva a objasňuje. Posilňuje a lepšie sa vyvažuje analýza vplyvov, aby sa dôkladnejšie objasnili a podrobnejšie uviedli očakávané náklady a prínosy.

Vzhľadom na kritériá efektívnosti, účinnosti a súdržnosti sa preskúmali tieto možnosti politik:

- **1. možnosť:** nelegislatívne opatrenia (právne nezáväzná);
- **2. možnosť:** obmedzené posilňovanie ochrany súkromia alebo dôvernosti a zjednodušenie;
- **3. možnosť:** premyslené posilňovanie ochrany súkromia alebo dôvernosti a zjednodušenie;
- **4. možnosť:** ďalekosiahle posilňovanie ochrany súkromia alebo dôvernosti a zjednodušenie;
- **5. možnosť:** zrušenie smernice o súkromí a elektronických komunikáciách.

Vo väčšine aspektov sa za **uprednostňovanú možnosť** na dosiahnutie cieľov považovala **3. možnosť**, a to pre svoju efektívnosť a súdržnosť. Jej hlavnými prínosmi sú:

- Posilnenie ochrany dôvernosti elektronických komunikácií prostredníctvom rozšírenia rozsahu pôsobnosti právneho nástroja tak, aby obsahoval nové, funkčne rovnocenné, elektronické komunikačné služby. Nariadením sa okrem toho umožňuje koncovým používateľom väčšia kontrola, pretože sa v ňom objasňuje, že súhlas možno vyjadriť vhodnými technickými nastaveniami.
- Posilnenie ochrany pred nevyžiadanými komunikáciami so zavedením povinnosti poskytnúť identifikáciu čísla volajúceho alebo povinnú predvoľbu pre reklamné volania a lepšie možnosti blokovania volaní z neželaných čísel.
- Zjednodušenie a objasnenie regulačného prostredia prostredníctvom zmenšenia manévrovacieho priestoru ponechaného členským štátom, zrušenia neaktuálnych ustanovení a rozšírenia výnimiek pri pravidlách súhlasu.

Hospodársky vplyv 3. možnosti má byť celkovo primeraný cieľom návrhu. Možnosti podnikania súvisiace so spracovaním údajov z komunikácií sú otvorené pre tradičné elektronické komunikačné služby, pričom na poskytovateľov OTT sa vzťahujú rovnaké pravidlá. To pre týchto prevádzkovateľov predstavuje určité dodatočné náklady na

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

dodržiavanie predpisov. Táto zmena však nebude mať podstatný vplyv na prevádzkovateľov OTT, ktorí už fungujú na základe súhlasu. A nakoniec, vplyv tejto možnosti nebudú pociťovať ani členské štáty, ktoré už tieto pravidlá rozšírili na OTT.

Tým, že sa súhlas centralizuje v softvéri, napríklad v internetovom prehliadači, a používatelia sú vyzvaní, aby si zvolili nastavenia ochrany súkromia, ako aj tým, že sa rozšíria výnimky z pravidiel odsúhlasovania súborov cookie, bude môcť veľká časť podnikov skončiť s bannermi a oznámeniami súvisiacimi so súbormi cookie, čo môže viesť k podstatným úsporám nákladov a zjednodušeniu. Inzerentom zameraným na internet to však môže sťažiť získavanie súhlasu v prípade, ak veľká časť používateľov vyberie nastavenie „zamietnutie súborov cookie tretích strán“. Zároveň však centralizovaný súhlas neberie prevádzkovateľom webových lokalít možnosť získať súhlas prostredníctvom individuálnych požiadaviek adresovaných koncovým používateľom, čím sa môže zachovať ich súčasný obchodný model. Dodatočné náklady vzniknú niektorým poskytovateľom prehliadačov alebo podobného softvéru, pretože budú musieť zabezpečiť nastavenia zohľadňujúce ochranu súkromia.

V externej štúdii boli identifikované tri rôzne scenáre realizácie 3. možnosti podľa toho, ktorý subjekt by zaviedol dialógové okno medzi používateľom, ktorý vybral nastavenie „zamietnutie súborov cookie tretích strán“ alebo „nesledovanie“, a navštívenými webovými lokalitami, ktoré si želajú, aby používateľ internetu prehodnotil svoje rozhodnutie. Touto technickou úlohou môžu byť poverené tieto subjekty: 1. softvér, ako sú internetové prehliadače; 2. sledovač tretej strany; 3. jednotlivé webové lokality (t. j. služba informačnej spoločnosti požadovaná používateľom). V prvom scenári (riešenie s prehliadačom), ktorý je uplatnený v tomto návrhu, by 3. možnosť viedla v porovnaní so základným scenárom k celkovým úsporám na nákladoch na dodržiavanie predpisov vo výške 70 % (úspory vo výške 948,8 milióna EUR). V ostatných scenároch by boli úspory nákladov nižšie. Keďže celkové úspory do veľkej miery vyplývajú z podstatného zníženia počtu podnikov, na ktoré to bude mať vplyv, individuálna výška nákladov na dodržiavanie predpisov pre jeden podnik bude v priemere vyššia než dnes.

3.5. Regulačná vhodnosť a zjednodušenie

Politické opatrenia navrhované v rámci uprednostňovanej možnosti sa týkajú cieľa zjednodušenia a zmiernenia administratívneho zaťaženia v súlade so zisteniami hodnotenia REFIT a stanoviskom platformy REFIT¹⁷.

Platforma REFIT vydala tri súbory odporúčaní pre Komisiu:

- ochrana súkromného života občanov by sa mala posilniť prostredníctvom zosúladenia smernice o súkromí a elektronických komunikáciách so všeobecným nariadením o ochrane údajov;
- efektívnosť ochrany občanov pred nevyžiadaným marketingom by sa mala posilniť pridaním výnimiek pri pravidle odsúhlasovania súborov cookie;
- Komisia rieši problémy vnútroštátneho vykonávania a uľahčuje výmenu najlepších postupov medzi členskými štátmi.

Návrh konkrétne obsahuje:

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

- využívanie technologicky neutrálneho vymedzenia pojmov na obsiahnutie nových služieb a technológií, čím sa zabezpečí odolnosť nariadenia voči budúcim zmenám;
- zrušenie pravidiel bezpečnosti na odstránenie regulačnej duplicity;
- objasnenie rozsahu pôsobnosti s cieľom pomôcť odstrániť alebo zmierniť riziko nejednotného vykonávania v členských štátoch (bod 3 stanoviska);
- objasnenie a zjednodušenie pravidla súhlasu na používanie súborov cookie a ďalších identifikátorov, ako sa vysvetľuje v oddieloch 3.1 a 3.4 (bod 2 stanoviska);
- zosúladenie dozorných orgánov s orgánmi zodpovednými za presadzovanie všeobecného nariadenia o ochrane údajov a uplatňovanie mechanizmu konzistentnosti zriadeného v rámci všeobecného nariadenia o ochrane údajov.

3.6. Vplyv na základné práva

Cieľom návrhu je zefektívniť a zvýšiť úroveň ochrany súkromia a osobných údajov spracúvaných v súvislosti s elektronickými komunikáciami v súlade s článkami 7 a 8 charty a zabezpečiť väčšiu právnu istotu. Návrh dopĺňa a špecifikuje všeobecné nariadenie o ochrane údajov. Na uplatňovanie slobody prejavu a práva na informácie, ako aj ďalších súvisiacich práv, ako je právo na ochranu osobných údajov alebo sloboda myslenia, svedomia a náboženského vyznania, je nevyhnutná efektívna ochrana dôvernosti komunikácií.

4. VPLYV NA ROZPOČET

Návrh nemá žiadny vplyv na rozpočet Únie.

5. INÉ PRVKY

5.1. Plány vykonávania, spôsob monitorovania, hodnotenia a podávania správ

Komisia bude monitorovať uplatňovanie nariadenia a každé tri roky predloží hodnotiacu správu Európskemu parlamentu, Rade a Európskemu hospodárskemu a sociálnemu výboru. Tieto správy budú verejné a budú sa týkať efektívneho uplatňovania a presadzovania tohto nariadenia.

5.2. Podrobné vysvetlenie konkrétnych ustanovení návrhu

Kapitola I obsahuje všeobecné ustanovenia: predmet úpravy (článok 1), rozsah pôsobnosti (články 2 a 3) a vymedzenie pojmov vrátane odkazov na príslušné pojmy z iných nástrojov EÚ, ako napríklad všeobecného nariadenia o ochrane údajov.

Kapitola II obsahuje kľúčové ustanovenia, ktorými sa zabezpečuje dôvernosť elektronických komunikácií (článok 5), obmedzené povolené účely a podmienky spracovania takýchto údajov o komunikáciách (články 6 a 7). Zaoberá sa tiež ochranou v koncových zariadeniach, a to i) zaručením integrity informácií, ktoré sú v nich uložené, a ii) ochranou informácií odosielaných z koncových zariadení, keďže môžu umožniť identifikáciu koncového používateľa (článok 8). A nakoniec, v článku 9 sa podrobne uvádza súhlas koncových používateľov, ktorý tvorí ústredný zákonný predpoklad tohto nariadenia, pričom sa výslovne odkazuje na jeho vymedzenie a podmienky zo všeobecného nariadenia o ochrane údajov,

zatiaľ čo článkom 10 sa poskytovateľom softvéru umožňujúceho elektronické komunikácie ukladá povinnosť pomôcť koncovým používateľom pri prijímaní efektívnych rozhodnutí v oblasti nastavení ochrany súkromia. Článok 11 sa podrobne venuje účelom a podmienkam, na základe ktorých môžu členské štáty obmedziť uvedené ustanovenia.

Kapitola III sa týka práv koncových používateľov na kontrolu odosielania a prijímania elektronických komunikácií s cieľom chrániť svoje súkromie: i) práva koncových používateľov zabrániť zobrazeniu čísla volajúceho, aby bola zaručená anonymita (článok 12), jeho obmedzení (článok 13) a ii) povinnosti poskytovateľov verejne dostupnej interpersonálnej komunikácie s číslovaním umožňovať obmedzenie prijímania neželaných volaní (článok 14). V tejto kapitole sa tiež upravujú podmienky, za ktorých môžu byť koncoví používatelia zaradení do verejne dostupných telefónnych zoznamov (článok 15), ako aj podmienky, za ktorých možno uskutočňovať nevyžiadané komunikácie na účely priameho marketingu (článok 17). Týka sa aj bezpečnostných rizík a stanovuje sa v nej povinnosť poskytovateľov elektronických komunikačných služieb upozorňovať koncových používateľov na konkrétne riziko, ktoré môže predstavovať hrozbu pre bezpečnosť sietí a služieb. Bezpečnostné požiadavky zo všeobecného nariadenia o ochrane údajov a kódexu EECC sa budú uplatňovať aj na poskytovateľov elektronických komunikačných služieb.

Kapitola IV sa týka dohľadu nad týmto nariadením a jeho presadzovania, ktorými sú vzhľadom na silné synergie medzi problematikou všeobecnej ochrany údajov a dôvernosti komunikácií poverené dozorné orgány zodpovedné za všeobecné nariadenie o ochrane údajov (článok 18). Právomoci Európskeho výboru pre ochranu údajov sa rozširujú (článok 19) a mechanizmus spolupráce a konzistentnosti predpokladaný vo všeobecnom nariadení o ochrane údajov sa bude uplatňovať v prípade cezhraničných otázok súvisiacich s týmto nariadením (článok 20).

V kapitole V sa podrobne opisujú rôzne prostriedky nápravy dostupné pre koncových používateľov (články 21 a 22) a sankcie, ktoré možno uložiť (článok 24), ako aj všeobecné podmienky ukladania správnych pokút (článok 23).

Kapitola VI sa zaoberá prijatím delegovaného a vykonávacieho aktu v súlade s článkami 290 a 291 zmluvy.

A nakoniec, kapitola VII obsahuje záverečné ustanovenia tohto nariadenia: zrušenie smernice o súkromí a elektronických komunikáciách, monitorovanie a preskúmanie, nadobudnutie účinnosti a uplatňovanie. Pokiaľ ide o preskúmanie, Komisia má okrem iného v úmysle vyhodnotiť, či je vzhľadom na právny, technický alebo hospodársky vývoj, ako aj s ohľadom na prvé hodnotenie nariadenia (EÚ) 2016/679, ktoré sa má vykonať do 25. mája 2020, aj naďalej potrebný samostatný právny akt.

Návrh

NARIADENIE EURÓPSKEHO PARLAMENTU A RADY

o rešpektovaní súkromného života a ochrane osobných údajov v elektronických komunikáciách a o zrušení smernice 2002/58/ES (smernica o súkromí a elektronických komunikáciách)

(Text s významom pre EHP)

EURÓPSKY PARLAMENT A RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o fungovaní Európskej únie, a najmä na jej články 16 a 114,

so zreteľom na návrh Európskej komisie,

po postúpení návrhu legislatívneho aktu národným parlamentom,

so zreteľom na stanovisko Európskeho hospodárskeho a sociálneho výboru¹,

so zreteľom na stanovisko Výboru regiónov²,

so zreteľom na stanovisko európskeho dozorného úradníka pre ochranu údajov³,

konajúc v súlade s riadnym legislatívnym postupom,

keďže:

- (1) Článkom 7 Charty základných práv Európskej únie (ďalej len „charta“) sa chráni základné právo každého človeka na rešpektovanie jeho súkromného a rodinného života, obdobia a komunikácie. Základným rozmerom tohto práva je rešpektovanie súkromia komunikácie človeka. Dôvernosť elektronických komunikácií znamená, že informácie, ktoré si strany medzi sebou vymieňajú, a externé prvky takejto komunikácie, vrátane údajov o tom, kedy bola informácia zaslaná, odkiaľ a komu, sa nemôžu sprístupniť nikomu okrem strán komunikácie. Zásada dôvernosti by sa mala uplatňovať na súčasné aj budúce komunikačné prostriedky vrátane volaní, prístupu na internet, aplikácií rýchlych správ, e-mailu, internetových volaní a osobných správ odosielaných cez sociálne médiá.
- (2) Elektronické komunikácie môžu obsahovať veľmi citlivé informácie o fyzických osobách zapojených do komunikácie, ako sú osobné skúsenosti a pocity, alebo aj

¹ Ú. v. EÚ C , , s. .

² Ú. v. EÚ C , , s. .

³ Ú. v. EÚ C , , s. .

zdravotný stav, sexuálna orientácia a politické názory, ktorých zverejnenie by mohlo viesť k osobnej alebo sociálnej ujme, hospodárskej strate alebo rozpakom. Veľmi citlivé a osobné informácie môžu obsahovať aj metaúdaje odvodené z elektronických komunikácií. Tieto metaúdaje obsahujú volané čísla, navštívené webové lokality, zemepisnú polohu, čas, dátum a trvanie volania atď., čím sa umožňuje dospieť k presným záverom o súkromnom živote človeka zapojeného do elektronickej komunikácie, pokiaľ ide o jeho spoločenské vzťahy, zvyky a činnosti každodenného života, záujmy, vkus a pod.

- (3) Údaje z elektronických komunikácií môžu obsahovať aj informácie týkajúce sa právnických osôb, napríklad obchodné tajomstvá alebo iné citlivé informácie, ktoré majú ekonomickú hodnotu. Ustanovenia tohto nariadenia by sa preto mali uplatňovať na fyzické aj právnické osoby. Týmto nariadením by sa ďalej malo zabezpečiť, aby sa ustanovenia nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679⁴ uplatňovali aj na koncových používateľov, ktorí sú právnickými osobami. V tejto súvislosti je dôležité aj vymedzenie súhlasu podľa nariadenia (EÚ) 2016/679. Vždy, keď sa hovorí o súhlase koncového používateľa, a to aj vtedy, ak je ním právnická osoba, malo by sa uplatniť toto vymedzenie. Okrem toho, právnické osoby by mali mať vo vzťahu k dozorným orgánom rovnaké práva ako koncoví používatelia, ktorí sú fyzickými osobami. Dozorné orgány by podľa tohto nariadenia mali byť zodpovedné aj za monitorovanie uplatňovania tohto nariadenia, pokiaľ ide o právnické osoby.
- (4) Podľa článku 8 ods. 1 charty a článku 16 ods. 1 Zmluvy o fungovaní Európskej únie má každý právo na ochranu svojich osobných údajov. Nariadením (EÚ) 2016/679 sa stanovujú pravidlá ochrany fyzických osôb pri spracúvaní osobných údajov a pravidlá týkajúce sa voľného pohybu osobných údajov. Údaje z elektronických komunikácií môžu obsahovať osobné údaje vymedzené v nariadení (EÚ) 2016/679.
- (5) Ustanovenia tohto nariadenia špecifikujú a dopĺňajú všeobecné pravidlá ochrany osobných údajov stanovené v nariadení (EÚ) 2016/679, pokiaľ ide o údaje z elektronických komunikácií, ktoré sa považujú za osobné údaje. Týmto nariadením sa teda neznižuje úroveň ochrany fyzických osôb podľa nariadenia (EÚ) 2016/679. Spracovanie údajov z elektronických komunikácií poskytovateľmi elektronických komunikačných služieb by sa malo umožniť iba v súlade s týmto nariadením.
- (6) Hoci zásady a hlavné ustanovenia smernice Európskeho parlamentu a Rady 2002/58/ES⁵ zostávajú vo všeobecnosti uspokojivé, daná smernica nedrží v plnej miere krok s technologickým vývojom a realitou na trhu, čo má za následok nejednotnú alebo nedostatočne efektívnu ochranu súkromia a dôvernosti vo vzťahu k elektronickým komunikáciám. K takémuto vývoju patrí vstup na trh elektronických komunikačných služieb, ktoré z pohľadu spotrebiteľa môžu nahrádzať tradičné služby, nemusia však vyhovovať rovnakému súboru pravidiel. Ďalší vývoj predstavujú nové metódy sledovania správania koncových používateľov na internete, ktorých sa netýka

⁴ Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1 – 88).

⁵ Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002, týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) (Ú. v. ES L 201, 31.7.2002, s. 37).

smernica 2002/58/ES. Smernica 2002/58/ES by mala byť preto zrušená a nahradená týmto nariadením.

- (7) Členským štátom by sa malo v rozsahu tohto nariadenia umožniť zachovanie alebo zavedenie vnútroštátnych ustanovení na podrobnejšiu špecifikáciu alebo objasnenie uplatňovania pravidiel tohto nariadenia, aby sa zabezpečilo efektívne uplatňovanie a výklad týchto pravidiel. Priestor na voľné uváženie, ktorý členské štáty v tomto zmysle majú, by mal slúžiť na zachovanie rovnováhy medzi ochranou súkromného života a osobných údajov a voľným pohybom údajov z elektronických komunikácií.
- (8) Toto nariadenie by sa malo uplatňovať na poskytovateľov elektronických komunikačných služieb, poskytovateľov verejne dostupných zoznamov a poskytovateľov softvéru umožňujúceho elektronické komunikácie vrátane vyhľadávania a prezentácie informácií na internete. Toto nariadenie by sa malo uplatňovať aj na fyzické a právnické osoby, ktoré používajú elektronické komunikačné služby na odosielanie priamych marketingových obchodných komunikácií alebo získavanie informácií súvisiacich s koncovými zariadeniami koncových používateľov alebo uložených v týchto zariadeniach.
- (9) Toto nariadenie by sa malo uplatňovať na údaje z elektronických komunikácií spracúvané v súvislosti s poskytovaním a používaním elektronických komunikačných služieb v Únii, a to bez ohľadu na to, či sa spracovanie vykonáva v Únii. S cieľom nepripraviť koncových používateľov v Únii o efektívnu ochranu by sa toto nariadenie malo okrem toho uplatňovať aj na údaje z elektronických komunikácií v súvislosti s poskytovaním elektronických komunikačných služieb z krajín mimo Únie koncovým používateľom v Únii.
- (10) Rádiové zariadenia a ich softvér, ktoré sú uvádzané na vnútorný trh Únie, musia byť v súlade so smernicou Európskeho parlamentu a Rady 2014/53/EÚ⁶. Toto nariadenie by nemalo ovplyvniť uplatniteľnosť akejkoľvek požiadavky smernice 2014/53/EÚ, ani právomoc Komisie prijímať delegované akty podľa smernice 2014/53/EÚ, podľa ktorej sa vyžaduje, aby osobitné kategórie alebo triedy rádiových zariadení obsahovali prostriedky na zabezpečenie ochrany osobných údajov a súkromia koncových používateľov.
- (11) Služby používané na komunikačné účely a technické prostriedky ich poskytovania sa podstatne zmenili. Koncoví používatelia čoraz viac nahrádzajú tradičné služby hlasového telefonovania, SMS správ a prenosu elektronickej pošty funkčne rovnocennými elektronickými službami, ako sú internetová telefónia, služby odosielania správ a e-mailové služby založené na webe. S cieľom zabezpečiť efektívnu a rovnakú ochranu koncových používateľov pri používaní funkčne rovnocenných služieb sa v tomto nariadení používa vymedzenie elektronických komunikačných služieb uvedené v [smernici Európskeho parlamentu a Rady, ktorou sa stanovuje európsky kódex elektronickej komunikácie⁷]. Do tohto vymedzenia nie sú zahrnuté len služby prístupu na internet a služby pozostávajúce úplne alebo čiastočne z

⁶ Smernica Európskeho parlamentu a Rady 2014/53/EÚ zo 16. apríla 2014 o harmonizácii právnych predpisov členských štátov týkajúcich sa sprístupňovania rádiových zariadení na trhu, ktorou sa zrušuje smernica 1999/5/ES (Ú. v. EÚ L 153, 22.5.2014, s. 62).

⁷ Návrh smernice Európskeho parlamentu a Rady, ktorou sa stanovuje európsky kódex elektronickej komunikácie (Prepracované znenie) [COM/2016/0590 final – 2016/0288 (COD)].

prenosu signálov, ale aj interpersonálne komunikačné služby, v prípade ktorých môže, ale nemusí ísť o služby s číslovaním, ako napríklad internetová telefónia, služby odosielania správ a e-mailové služby založené na webe. Ochrana dôvernosti komunikácií je kľúčová aj pri interpersonálnych komunikačných službách, ktoré sú doplnkom k inej službe; preto by sa malo toto nariadenie vzťahovať aj na tieto služby, ktoré tiež obsahujú funkciu komunikácie.

- (12) Hybridné zariadenia a prístroje čoraz častejšie navzájom komunikujú pomocou elektronických komunikačných sietí (internet vecí). Pri prenose komunikácií medzi prístrojmi dochádza k prenosu signálov v sieti, čím sa zvyčajne vytvára elektronická komunikačná služba. Ak sa má zabezpečiť úplná ochrana práva na súkromie a dôvernosť komunikácií a podporiť dôveryhodný a bezpečný internet vecí na jednotnom digitálnom trhu, je potrebné objasniť, že toto nariadenie by sa malo uplatňovať na prenos komunikácií medzi prístrojmi. Zásada dôvernosti zakotvená v tomto nariadení by sa preto mala uplatňovať aj na prenos komunikácií medzi prístrojmi. Osobitné prostriedky na zabezpečenie ochrany by sa mohli prijať aj podľa odvetvových právnych predpisov, ako napríklad smernice 2014/53/EÚ.
- (13) Vývoj rýchlych a účinných bezdrôtových technológií priniesol lepšiu dostupnosť verejného prístupu na internet prostredníctvom bezdrôtových sietí, ktoré sú k dispozícii každému, kto sa nachádza vo verejných alebo čiastočne súkromných priestoroch, ako sú napr. takzvané hotspots, umiestnené na rôznych miestach v meste, obchodných domoch, nákupných strediskách a nemocniciach. Dôvernosť komunikácií prenášaných cez takéto siete by sa mala chrániť v rozsahu, v akom sa tieto komunikačné siete poskytujú nevymedzenej skupine koncových používateľov. Zabezpečeniu ochrany dôvernosti údajov komunikácie a uplatňovaniu tohto nariadenia by nemala brániť ani skutočnosť, že bezdrôtové elektronické komunikačné služby môžu byť doplnkom k iným službám. Preto by sa toto nariadenie malo uplatňovať na údaje z elektronických komunikácií využívajúce elektronické komunikačné služby a verejné komunikačné siete. Naopak, toto nariadenie by sa nemalo uplatňovať na uzavreté skupiny koncových používateľov, napríklad na podnikové siete, do ktorých majú prístup iba zamestnanci podniku.
- (14) Údaje z elektronických komunikácií by sa mali vymedziť dostatočne široko a technologicky neutrálne, aby zahŕňali všetky informácie týkajúce sa prenášaného alebo vymieňaného obsahu (obsah elektronických komunikácií) a informácie týkajúce sa koncového používateľa elektronických komunikačných služieb spracúvané na účely prenosu, distribúcie alebo umožnenia výmeny obsahu elektronických komunikácií. Patria sem údaje slúžiace na sledovanie a identifikáciu zdroja a cieľa komunikácie, zemepisnej polohy a dátumu, času, trvania a druhu komunikácie. Bez ohľadu na to, či sa tieto signály a súvisiace údaje prenášajú po drôte, rádiovými, optickými alebo elektromagnetickými prostriedkami, a to aj vrátane družicových sietí, káblových sietí, pevných (s prepínaním okruhov a paketov vrátane internetu) a mobilných pozemských sietí, elektrických káblových systémov, údaje súvisiace s takýmito signálmi by sa mali považovať za metaúdaje z elektronických komunikácií, a preto by sa na ne mali vzťahovať ustanovenia tohto nariadenia. Metaúdaje z elektronických komunikácií môžu zahŕňať informácie, ktoré sú súčasťou prihlásenia sa k službe, ak sa takéto informácie spracúvajú na účely prenosu, distribúcie alebo výmeny obsahu elektronických komunikácií.

- (15) Údaje z elektronických komunikácií by sa mali považovať za dôverné. Znamená to, že každý zásah do prenosu údajov z elektronických komunikácií, či už priamo človekom alebo prostredníctvom automatizovaného spracovania prístrojmi, ku ktorému dôjde bez súhlasu všetkých strán komunikácie, by mal byť zakázaný. Zákaz zachytávania údajov z komunikácií by sa mal uplatňovať počas prenosu údajov, t. j. až do prijatia obsahu elektronickej komunikácie určeným adresátom. Zachytávanie údajov z elektronických komunikácií sa môže vyskytnúť napríklad vtedy, keď iná osoba, ktorá nie je stranou komunikácie, odpočúva volania, číta, skenuje alebo ukladá obsah elektronických komunikácií alebo s nimi súvisiace metaúdaje na iné účely, než je výmena komunikácií. K zachytávaniu údajov dochádza aj vtedy, keď tretie strany monitorujú navštívené webové lokality, načasovanie návštev, interakciu s inými osobami atď. bez súhlasu príslušného koncového používateľa. S technologickým vývojom sa zlepšujú aj technické možnosti zachytávania údajov. Môže ísť o inštaláciu zariadení, ktoré zhromažďujú údaje z koncového zariadenia v cieľových oblastiach, ako sú takzvané IMSI (medzinárodná identifikácia mobilného účastníka) catchery, programy a metódy, ktoré dokážu napríklad tajne monitorovať zvyky pri prehľadávaní webu na účely vytvárania profilov koncových používateľov. Medzi ďalšie príklady zachytávania údajov patrí zachytávanie údajov informačného poľa alebo údajov o obsahu z nezašifrovaných bezdrôtových sietí a smerovačov vrátane zvykov pri prehľadávaní webu, bez súhlasu koncového používateľa.
- (16) Zákaz ukladania komunikácií nemá za cieľ zakázať každé automatické, dočasné a prechodné uloženie týchto informácií, pokiaľ sa uskutočňuje výlučne na účel vykonania prenosu v elektronickej komunikačnej sieti. Nemalo by sa zakazovať ani spracovanie údajov z elektronických komunikácií na účely zaistenia bezpečnosti a pokračovania činnosti elektronických komunikačných služieb, a to vrátane vyhľadávania bezpečnostných hrozieb, ako je prítomnosť malvéru, alebo spracovania metaúdajov na splnenie potrebných požiadaviek kvality na služby ako oneskorenie, džiter atď.
- (17) Spracovanie údajov z elektronických komunikácií môže byť užitočné pre podniky, spotrebiteľov aj celú spoločnosť. V porovnaní so smernicou 2002/58/ES sa v tomto nariadení poskytujú poskytovateľom elektronických komunikačných služieb širšie možnosti spracovania metaúdajov z elektronických komunikácií na základe súhlasu koncových používateľov. Koncoví používatelia však pripisujú dôvernosti svojich komunikácií, ako aj činností na internete, veľkú dôležitosť a chcú mať kontrolu nad použitím údajov z elektronických komunikácií na iné účely, než je prenos komunikácie. V tomto nariadení by sa preto od poskytovateľov elektronických komunikačných služieb malo vyžadovať, aby získali súhlas koncových používateľov so spracovaním metaúdajov z elektronických komunikácií, ktoré by mali zahŕňať údaje o umiestnení zariadenia vygenerované na účely udelenia alebo zachovania prístupu a pripojenia k službe. Za metaúdaje by sa nemali považovať lokalizačné údaje vygenerované v inom kontexte, než je kontext poskytovania elektronických komunikačných služieb. K príkladom komerčného využitia metaúdajov z elektronických komunikácií poskytovateľmi elektronických komunikačných služieb môže patriť napríklad poskytovanie teplotných máp, čiže grafické zobrazenie údajov o prítomnosti osôb pomocou farieb. Na zobrazenie pohybov toku v určitých smeroch počas daného časového obdobia je potrebný identifikátor na prepojenie polôh osoby v určitých časových intervaloch. Ak sa použijú anonymné údaje, tento identifikátor bude chýbať, preto sa pohyb nebude dať zobrazit'. Z takéhoto využívania metaúdajov z elektronických komunikácií môžu mať prospech napríklad orgány verejnej moci

a verejné dopravné podniky, ktoré tak môžu na základe využívania existujúcej štruktúry a tlaku na ňu vymedziť oblasti vývoja novej infraštruktúry. Ak by druh spracovania metaúdajov z elektronických komunikácií, konkrétne pomocou nových technológií, a vzhľadom na povahu, rozsah pôsobnosti, kontext a účely spracovania predstavoval veľké riziko pre práva a slobody fyzických osôb, pred spracovaním by sa malo podľa článkov 35 a 36 nariadenia (EÚ) 2016/679 uskutočniť posúdenie vplyvu na ochranu údajov a v prípade potreby aj konzultácia s dozorným orgánom.

- (18) Koncoví používatelia môžu súhlasiť so spracovaním svojich metaúdajov, ak chcú využívať osobitné služby, ako napríklad služby ochrany pred podvodnými činnosťami (pomocou analýzy údajov o používaní, lokalizácii a zákazníckom účte v reálnom čase). V digitálnej ekonomike sa služby často dodávajú za protislužbu inú než peniaze, napríklad za to, že koncový používateľ je vystavený reklame. Na účely tohto nariadenia by mal mať súhlas koncového používateľa, bez ohľadu na to, či ide o fyzickú alebo právnickú osobu, rovnaký význam a mali by sa naň vzťahovať rovnaké podmienky ako na súhlas dotknutej osoby podľa nariadenia (EÚ) 2016/679. Služby základného širokopásmového prístupu na internet a hlasovej komunikácie sa považujú za základné služby, vďaka ktorým môžu osoby komunikovať a mať prínos z digitálnej ekonomiky. Súhlas so spracovaním údajov z internetovej alebo hlasovej komunikácie nebude platný, ak dotknutá osoba nemá možnosť skutočnej a slobodnej voľby alebo nemôže bez negatívnych dôsledkov odmietnuť či stiahnuť súhlas.
- (19) Obsah elektronických komunikácií sa týka podstaty základného práva na rešpektovanie súkromného a rodinného života, obydľia a komunikácie, ktoré je chránené článkom 7 charty. Zásah do obsahu elektronických komunikácií by sa mal povoliť iba za veľmi jasne vymedzených podmienok a na osobitné účely a mal by podliehať primeraným prostriedkom na zabezpečenie ochrany proti zneužitiu. V tomto nariadení sa poskytovateľom elektronických komunikačných služieb umožňuje spracovanie prenášaných údajov z elektronických komunikácií na základe informovaného súhlasu všetkých príslušných koncových používateľov. Poskytovatelia môžu napríklad ponúkať služby, ktoré obsahujú skenovanie e-mailov, aby bolo možné odstrániť určitý vopred vymedzený materiál. Vzhľadom na citlivosť obsahu komunikácií sa v tomto nariadení stanovuje predpoklad, že spracovanie takýchto údajov o obsahu bude mať za následok vysoké riziko pre práva a slobody fyzických osôb. Pri spracúvaní takéhoto druhu údajov by mal poskytovateľ elektronických komunikačných služieb pred spracovaním vždy konzultovať s dozorným orgánom. Táto konzultácia by mala byť v súlade s článkom 36 ods. 2 a 3 nariadenia (EÚ) 2016/679. Tento predpoklad sa netýka spracovania údajov obsahu na poskytovanie služby, o ktorú požiadal koncový používateľ, ak koncový používateľ súhlasil s takýmto spracovaním a služba sa vykonáva na účely a v trvaní, ktoré sú pre danú službu nevyhnutné a primerané. Keď koncový používateľ odošle obsah elektronických komunikácií a určený koncový používateľ alebo určení koncoví používatelia ho prijímú, koncový používateľ, koncoví používatelia alebo tretia strana poverená zaznamenaním alebo uložením údajov ho môžu zaznamenať alebo uložiť. Každé spracovanie takýchto údajov musí byť v súlade s nariadením (EÚ) 2016/679.
- (20) Koncové zariadenia koncových používateľov elektronických komunikačných sietí a všetky informácie týkajúce sa používania takýchto koncových zariadení, bez ohľadu na to, či sú v takomto zariadení uložené alebo ich takéto zariadenie odosiela, vyžaduje alebo spracúva s cieľom umožniť pripojenie k inému zariadeniu alebo sieťovému zariadeniu, sú súčasťou súkromia koncových používateľov, ktoré sa musí chrániť

podľa Charty základných práv Európskej únie a Európskeho dohovoru o ochrane ľudských práv a základných slobôd. Vzhľadom na to, že takéto zariadenia obsahujú alebo spracúvajú informácie, ktoré môžu obsahovať podrobnosti o citovom, politickom a spoločenskom živote človeka, ako aj obsah komunikácií, obrázky, lokalizáciu osôb po získaní prístupu k funkciám GPS zariadenia, zoznam kontaktov a ďalšie informácie, ktoré sú v zariadení uložené, vyžadujú informácie týkajúce sa takéhoto zariadenia lepšiu ochranu súkromia. Do koncového zariadenia koncového používateľa môže okrem toho bez jeho vedomia vniknúť takzvaný špiónsky program (spyware), sledovacie objekty (web bugs), skryté identifikátory, trvalé súbory cookie a ďalšie podobné neželané sledovacie nástroje, ktorých cieľom je získať prístup k informáciám, uložiť skryté informácie a sledovať činnosti. Informácie týkajúce sa zariadenia koncového používateľa sa môžu zbierať, často bez vedomia koncového používateľa, aj vzdialene na účely identifikácie a sledovania, a to pomocou metód, ako napríklad zariadenie na odobratie odtlačkov prstov, pričom môžu vážne ohroziť súkromie koncového používateľa. Metódy, ktoré tajne monitorujú činnosti koncových používateľov, napríklad pomocou sledovania ich činností na internete alebo lokalizácie koncového zariadenia, alebo zhoršujú funkčnosť koncového zariadenia koncových používateľov, predstavujú závažnú hrozbu pre súkromie koncových používateľov. Preto by sa mal takýto zásah do koncového zariadenia koncového používateľa povoliť iba so súhlasom koncového používateľa a na osobitné a transparentné účely.

- (21) Výnimky z povinnosti získať súhlas, aby bolo možné využiť funkcie spracovania a ukladania koncového zariadenia alebo získať prístup k informáciám uloženým v koncovom zariadení, by sa mali obmedziť na situácie, v ktorých nedochádza vôbec, alebo len vo veľmi obmedzenom rozsahu, k narušeniu súkromia. Súhlas by napríklad nemal byť potrebný pri povoľovaní technického uloženia alebo prístupu, ktorý je nevyhnutne potrebný a primeraný na zákonné účely umožnenia využitia osobitnej služby, o ktorú výslovne požiadal koncový používateľ. Môže sem patriť aj ukladanie súborov cookie počas jednej relácie na webovej lokalite s cieľom sledovať vstup koncového používateľa pri vyplňaní elektronických formulárov na niekoľkých stranách. Súbory cookie môžu predstavovať zákonný a užitočný nástroj, napríklad pri meraní webového prenosu údajov na webovej lokalite. Poskytovatelia služieb informačnej spoločnosti zapojení do kontroly konfigurácie pri poskytovaní služieb v súlade s nastaveniami koncového používateľa, a to ani v prípade, ak zariadenie koncového používateľa nedokáže prijímať obsah vyžiadaný koncovým používateľom, by nemali získavať prístup k takémuto zariadeniu, ani používať funkcie spracovania takéhoto zariadenia.
- (22) Metódy použité na poskytnutie informácií a získanie súhlasu koncového používateľa by mali byť voči používateľovi čo najústretivejšie. Vzhľadom na všadeprítomné používanie trvalých súborov cookie a ďalších sledovacích metód sa od koncových používateľov čoraz častejšie požaduje odsúhlasenie uloženia týchto trvalých súborov cookie v koncovom zariadení. V dôsledku toho sú koncoví používatelia zaplavení žiadosťami o poskytnutie súhlasu. Tento problém možno vyriešiť pomocou technických prostriedkov na poskytnutie súhlasu, napríklad prostredníctvom prehľadných a voči používateľom ústretivejších nastavení. V tomto nariadení sa preto umožňuje vyjadrenie súhlasu pomocou vhodných nastavení prehliadača alebo inej aplikácie. Nastavenia koncových používateľov zadane vo všeobecných nastaveniach súkromia prehliadača alebo inej aplikácie by mali byť pre všetky tretie strany záväzné a vymáhateľné. Webové prehliadače predstavujú druh softvérovej aplikácie, ktorá

umožňuje získavanie a prezentáciu informácií na internete. Tie isté možnosti poskytujú aj ďalšie druhy aplikácií, napríklad také, ktoré umožňujú volanie a odosielanie správ alebo navádzanie po trase. Webové prehliadače sprostredkujú väčšinu činností, ktoré sa uskutočňujú medzi koncovým používateľom a webovou lokalitou. Z tohto pohľadu majú výsadné postavenie a koncovému používateľovi aktívne pomáhajú v oblasti riadenia toku informácií z koncového zariadenia a do neho. Konkrétnejšie sa môžu webové prehliadače použiť ako riadiace jednotky sieťového prostriedku, a tým pomôcť koncovým používateľom zabrániť získaniu prístupu k informáciám z koncového zariadenia (napríklad smartfónu, tabletu alebo počítača) alebo ich uloženiu.

- (23) Zásady špecificky navrhutej ochrany údajov a štandardnej ochrany údajov boli kodifikované v článku 25 nariadenia (EÚ) 2016/679. V súčasnosti sú štandardné nastavenia pre súbory cookie vo väčšine súčasných prehliadačov nastavené na možnosť prijatia všetkých súborov cookie. Poskytovatelia softvéru umožňujúceho získavanie a prezentáciu informácií na internete by preto mali byť povinní nakonfigurovať softvér tak, aby ponúkal možnosť zabrániť tretím stranám v uchovávaní informácií na koncovom zariadení; zvyčajne ide o zamietnutie súborov cookie tretích strán. Koncoví používatelia by mali mať k dispozícii možnosti nastavenia ochrany súkromia v rozsahu od najprísnejšej (napríklad nikdy nepovoliť súbory cookie) k najmenej prísnej (napríklad vždy povoliť súbory cookie) a strednej úrovni (napríklad zamietnuť súbory cookie tretích strán alebo povoliť iba súbory cookie prvých strán). Tieto nastavenia ochrany súkromia by mali byť jednoducho viditeľné a čitateľné.
- (24) Webové prehliadače, v ktorých môžu koncoví používatelia vyjadrovať súhlas podľa vymedzenia v nariadení (EÚ) 2016/679, napríklad s uložením trvalých súborov cookie tretích strán, by mali okrem iného od koncového zariadenia koncových používateľov vyžadovať jednoznačný potvrdzujúci úkon na vyjadrenie slobodného, osobitne informovaného a jednoznačného súhlasu s uložením takýchto súborov cookie do koncového zariadenia a prístupom k nemu a z neho. Takýto úkon sa považuje za potvrdzujúci, ak sa napríklad od koncových používateľov vyžaduje aktívny výber možnosti povolenia súborov cookie tretích strán na potvrdenie súhlasu, pričom majú k dispozícii potrebné informácie na to, aby sa mohli rozhodnúť. Na tento účel je potrebné vyžadovať od poskytovateľov softvéru umožňujúceho prístup na internet, aby koncových používateľov počas inštalácie informovali o možnosti výberu nastavení ochrany súkromia spomedzi rôznych možností a požiadali ich o výber konkrétnej možnosti. Poskytnuté informácie by nemali koncových používateľov odrádzať od výberu prísnejších nastavení ochrany súkromia a mali by relevantne uvádzať riziká súvisiace s povolením uloženia súborov cookie tretích strán do počítača vrátane zhromažďovania dlhodobých záznamov histórie prehľadávania jednotlivcov a používania týchto záznamov na odosielanie cielennej reklamy. Od webových prehliadačov sa víta poskytovanie jednoduchého spôsobu, ktorým koncoví používatelia môžu kedykoľvek počas používania zmeniť nastavenia ochrany súkromia a ktorý používateľom umožňuje nastaviť výnimky v prípade určitých webových lokalít, zaradiť určité webové lokality do zoznamov povolených lokalít alebo určiť webové lokality, na ktorých sú súbory cookie (tretích) strán povolené vždy alebo nie sú povolené nikdy.
- (25) Prístup k elektronickým komunikačným sieťam vyžaduje pravidelné odosielanie určitých dátových paketov s cieľom nadviazať alebo zachovať spojenie so sieťou

alebo inými zariadeniami v sieti. Zariadenia musia mať okrem toho priradenú jedinečnú adresu, aby boli v sieti identifikovateľné. Bezdrôtové a mobilné telefonické normy tiež obsahujú odosielanie aktívnych signálov, ktorých súčasťou sú jedinečné identifikátory ako adresa MAC, IMEI (medzinárodné označenie mobilného zariadenia), IMSI atď. Každá bezdrôtová základňová stanica (t. j. vysielateľ a prijímač), ako napríklad bezdrôtový prístupový bod, má osobitný rozsah, v rámci ktorého sa môžu takéto informácie zachytiť. Objavili sa poskytovatelia služieb, ktorí ponúkajú sledovacie služby na základe skenovania informácií súvisiacich so zariadeniami, pričom tieto služby majú rôzne funkcie, napríklad počítanie ľudí, poskytovanie údajov o počte ľudí čakajúcich v rade, zisťovanie počtu ľudí v konkrétnej oblasti atď. Tieto informácie možno využiť na intenzívnejšie narušanie súkromia, napríklad na odosielanie reklamných správ s prispôbenými ponukami koncovým používateľom, keď navštívia obchod. Hoci niektoré z týchto funkcií nepredstavujú veľké riziko pre súkromie, iné áno, napríklad tie, ktoré obsahujú sledovanie jednotlivcov v čase vrátane opakovaných návštev konkrétnych miest. Poskytovatelia vykonávajúci takéto postupy by mali zobrazovať výrazné oznamy umiestnené na okraji príslušnej plochy, v ktorých sú koncoví používatelia pred zadaním vymedzenej oblasti informovaní o tom, že technológia sa prevádzkuje v určitom ohraničení, ako aj o účele sledovania, osobe zodpovednej za sledovanie a o existencii opatrení, ktoré sa môžu vykonať v koncovom zariadení koncového používateľa na minimalizáciu alebo zastavenie získavania údajov. Ak sa osobné údaje získavajú podľa článku 13 nariadenia (EÚ) 2016/679, mali by sa poskytnúť dodatočné informácie.

- (26) Ak spracúvanie údajov z elektronických komunikácií poskytovateľmi elektronických komunikačných služieb patrí do rozsahu pôsobnosti tohto nariadenia, Únii alebo členským štátom by sa mala v nariadení poskytnúť možnosť, aby za určitých podmienok mohli na základe právnych predpisov obmedziť určité povinnosti a práva, ak takéto obmedzenie predstavuje potrebné a primerané opatrenie v demokratickej spoločnosti na ochranu konkrétnych verejných záujmov, ku ktorým patrí národná bezpečnosť, obrana, verejná bezpečnosť, predchádzanie trestným činom, ich vyšetrovanie, odhaľovanie alebo stíhanie, ako aj výkon trestných sankcií, vrátane ochrany pred ohrozením verejnej bezpečnosti a predchádzania takémuto ohrozeniu a ďalších dôležitých cieľov všeobecného verejného záujmu Únie alebo členského štátu, a to najmä dôležitého hospodárskeho alebo finančného záujmu Únie alebo členského štátu alebo monitorovacej, kontrolnej alebo regulačnej funkcie spojenej s výkonom verejnej moci v súvislosti s takýmito záujmami. Toto nariadenie by preto nemalo mať vplyv na možnosť členských štátov zákonne zachytávať elektronické komunikácie alebo prijímať iné opatrenia, ak je to nevyhnutné a primerané na účely ochrany uvedených verejných záujmov, v súlade s Chartou základných práv Európskej únie a Európskym dohovorom o ochrane ľudských práv a základných slobôd podľa výkladu rozhodnutí Súdneho dvora Európskej únie a Európskeho súdu pre ľudské práva. Poskytovatelia elektronických komunikačných služieb by mali poskytnúť vhodné postupy na uľahčenie legitímnych požiadaviek príslušných orgánov a v prípade potreby aj zohľadniť úlohu zástupcu povereného podľa článku 3 ods. 3.
- (27) Pokiaľ ide o identifikáciu čísla volajúceho, je potrebné chrániť právo volajúcej strany na odopretie zobrazenia čísla, z ktorého sa uskutočňuje volanie, a právo volanej strany odmietnuť volanie z neidentifikovaného čísla. Niektorí koncoví používatelia, najmä telefónne poradenské služby alebo podobné organizácie, majú záujem na zaručení anonymity volajúcich. Pokiaľ ide o identifikáciu čísla volaného účastníka, je potrebné

chrániť právo a oprávnený záujem volanej strany na odopretie zobrazenia čísla volaného, s ktorým je volajúca strana skutočne spojená.

- (28) V osobitných prípadoch je oprávnené zrušiť možnosť odopretia zobrazenia čísla volajúceho. Práva koncových používateľov na súkromie vo vzťahu k číslu volajúceho by sa mali obmedziť, ak je to potrebné na zistenie obťažujúcich volaní, a vo vzťahu k číslu volajúceho a lokalizačným údajom, ak je to potrebné preto, aby mohli záchranné služby, ako napríklad eCall, vykonávať svoje úlohy čo možno najefektívnejšie.
- (29) Existuje technológia, ktorá poskytovateľom elektronických komunikačných služieb umožňuje rôznymi spôsobmi obmedziť prijímanie neželaných volaní koncovým používateľom, ako napríklad blokovaním prezvonení a iných podvodných a obťažujúcich volaní. Poskytovatelia verejne dostupných interpersonálnych komunikačných služieb s číslovaním by mali túto technológiu použiť a chrániť koncových používateľov pred obťažujúcimi volaniami, a to bezplatne. Poskytovatelia by mali zabezpečiť, aby si koncoví používatelia boli vedomí existencie takýchto funkcií, napríklad publikovaním tejto skutočnosti na svojich webových stránkach.
- (30) Verejne dostupné telefónne zoznamy koncových používateľov elektronických komunikačných služieb sú značne rozšírené. Verejne dostupné telefónne zoznamy sú telefónne zoznamy alebo služby obsahujúce informácie o koncových používateľoch, ako napríklad ich telefónne čísla (vrátane mobilných telefónnych čísel), e-mailové adresy a kontaktné informácie, a patria k nim aj informačné služby. Právo na súkromie a ochranu osobných údajov fyzickej osoby vyžaduje, aby sa od koncových používateľov, ktorí sú fyzickými osobami, vyžadoval súhlas so zaradením ich osobných údajov do telefónneho zoznamu. Oprávnený záujem právnických osôb vyžaduje, aby mali koncoví používatelia, ktorí sú právnickými osobami, právo namietat proti zaradeniu s nimi súvisiacich údajov do telefónneho zoznamu.
- (31) Ak koncoví používatelia, ktorí sú fyzickými osobami, vyjadria súhlas so zaradením svojich údajov do takýchto telefónnych zoznamov, mali by mať možnosť vyjadriť súhlas s jednotlivými kategóriami osobných údajov, ktoré budú do telefónneho zoznamu zaradené (napríklad meno, e-mailová adresa, adresa domov, používateľské meno, telefónne číslo). Poskytovatelia verejne dostupných telefónnych zoznamov by mali okrem toho pred ich zaradením do daného telefónneho zoznamu informovať koncových používateľov o jeho účele a vyhľadávacích funkciách. Koncoví používatelia by mali mať možnosť vyjadriť súhlas s jednotlivými kategóriami osobných údajov (kontaktných informácií), ktoré sa budú dať vyhľadávať. Kategórie osobných údajov zaradených do telefónneho zoznamu a kategórie osobných údajov, na základe ktorých sa budú dať vyhľadávať kontaktné informácie koncového používateľa, nemusia byť to isté.
- (32) V tomto nariadení znamená priamy marketing každú formu reklamy, ktorou fyzická alebo právnická osoba odosiela priame marketingové komunikácie priamo jednému alebo viacerým identifikovaným alebo identifikovateľným koncovým používateľom prostredníctvom elektronických komunikačných služieb. Okrem ponuky produktov a služieb na komerčné účely by sem mali patriť aj správy, ktoré odosielajú politické strany kontaktujúce fyzické osoby prostredníctvom elektronických komunikačných služieb s cieľom vlastnej propagácie. To isté by sa malo vzťahovať aj na správy odosielané inými neziskovými organizáciami a slúžiace na propagáciu ich účelu.

- (33) Na ochranu koncových používateľov pred nevyžiadanými priamymi komunikáciami na účely priameho marketingu, ktoré narúšajú ich súkromný život, by sa mali poskytovať prostriedky na zabezpečenie ochrany. Miera narušenia súkromia a obťažovania sa považuje za relatívne podobnú bez ohľadu na široký rozsah technológií a kanálov, ktoré sa používajú na uskutočňovanie takýchto elektronických komunikácií, či už ide o automatické volacie a komunikačné systémy, aplikácie rýchlych správ, e-maily, SMS správy, MMS správy, Bluetooth atď. Preto je opodstatnené požadovať pred odoslaním obchodných elektronických komunikácií na účely priameho marketingu koncovým používateľom získanie súhlasu koncových používateľov, aby bolo možné efektívne chrániť jednotlivcov pred narúšaním ich súkromného života a oprávnený záujem právnických osôb. Právna istota a potreba zabezpečiť neustálu odolnosť pravidiel ochrany pred nevyžiadanými elektronickými komunikáciami voči budúcim zmenám opodstatňuje nevyhnutnosť vymedzenia súboru pravidiel, ktoré budú spoločné pre všetky technológie slúžiace na prenášanie týchto nevyžiadaných komunikácií a zároveň budú zabezpečovať rovnakú úroveň ochrany všetkým občanom Únie. Je však rozumné povoliť používanie e-mailových kontaktných informácií na ponúkanie podobných produktov a služieb, pokiaľ ide o existujúci vzťah s klientom. Takáto možnosť by sa vzťahovala iba na tú spoločnosť, ktorá získala elektronické kontaktné informácie v súlade s nariadením (EÚ) 2016/679.
- (34) Aj v prípade poskytnutia súhlasu s prijímaním nevyžiadaných komunikácií na účely priameho marketingu by mali mať koncoví používatelia možnosť kedykoľvek a jednoducho svoj súhlas stiahnuť. Na uľahčenie efektívneho presadzovania pravidiel Únie o nevyžiadaných správach na účely priameho marketingu je nevyhnutné zakázať maskovanie identity a používanie falošnej identity, falošných spiatočných adries alebo čísel pri odosielaní nevyžiadaných obchodných komunikácií na účely priameho marketingu. Nevyžiadané marketingové komunikácie by preto mali byť ako také jednoznačne rozpoznateľné a mali by obsahovať identitu právnickej alebo fyzickej osoby odosielajúcej komunikáciu alebo identitu osoby, v menej ktorej sa komunikácia odosiela, ako aj potrebné informácie, ktoré príjemcom umožnia výkon práva na odmietnutie prijímania ďalších písomných a/alebo ústnych marketingových správ.
- (35) S cieľom umožniť jednoduché stiahnutie súhlasu by mali právnické alebo fyzické osoby odosielajúce priame marketingové komunikácie e-mailom uviesť hypertextový odkaz alebo platnú adresu elektronickej pošty, ktorú budú môcť koncoví používatelia jednoducho použiť na stiahnutie súhlasu. Právnické alebo fyzické osoby odosielajúce priame marketingové komunikácie prostredníctvom hlasových volaní a automatických volacích a komunikačných systémov by mali zobraziť číslo, na ktoré možno spoločnosti zavolať, alebo osobitný kód identifikujúci skutočnosť, že ide o marketingové volanie.
- (36) Pri priamych marketingových hlasových volaniach sa nepoužívajú automatické volacie a komunikačné systémy vzhľadom na to, že sú pre odosielaťľa nákladnejšie a pre koncových používateľov nepredstavujú žiadne finančné náklady. Členské štáty by mali preto zaviesť a/alebo zachovať vnútroštátne systémy, ktoré umožňujú takéto volania iba koncovým používateľom, ktorí proti nim nenamietajú.
- (37) Poskytovatelia služieb, ktorí ponúkajú elektronické komunikačné služby, by mali koncových používateľov informovať o opatreniach, ktoré môžu prijať na ochranu bezpečnosti svojich komunikácií, napríklad použitím osobitných druhov softvéru alebo šifrovacích technológií. Požiadavka informovať koncových používateľov o

konkrétnych bezpečnostných rizikách nezavahuje poskytovateľa služby povinnosti vykonať na svoje vlastné náklady vhodné a okamžité opatrenia na nápravu akýchkoľvek nových, nepredvídaných bezpečnostných rizík a znovu obnoviť úroveň bezpečnosti služby. Poskytovanie informácií o bezpečnostných rizikách účastníkovi by malo byť bezplatné. Hodnotenie bezpečnosti sa vykonáva na základe článku 32 nariadenia (EÚ) 2016/679.

- (38) Aby sa zabezpečil úplný súlad s nariadením (EÚ) 2016/679, presadzovaním ustanovení tohto nariadenia by mali byť poverené tie isté orgány, ktoré sú zodpovedné za presadzovanie nariadenia (EÚ) 2016/679, pričom aj toto nariadenie sa opiera o mechanizmus konzistentnosti zriadený v rámci nariadenia (EÚ) 2016/679. Členské štáty by mali mať možnosť mať viac ako jeden dozorný orgán tak, aby to zodpovedalo ich ústavnej, organizačnej a správnej štruktúre. Dozorné orgány by mali byť zodpovedné aj za monitorovanie uplatňovania tohto nariadenia, pokiaľ ide o údaje z elektronických komunikácií týkajúce sa právnických osôb. Takéto dodatočné úlohy by nemali ohroziť schopnosť dozorného orgánu vykonávať svoje úlohy v oblasti ochrany osobných údajov podľa nariadenia (EÚ) 2016/679 a tohto nariadenia. Každému dozornému orgánu by mali byť poskytnuté dodatočné finančné a ľudské zdroje, priestory a infraštruktúra potrebné na efektívny výkon úloh podľa tohto nariadenia.
- (39) Každý dozorný orgán by mal byť na území svojho členského štátu príslušný vykonávať právomoci a úlohy stanovené v tomto nariadení. S cieľom zabezpečiť konzistentné monitorovanie a presadzovanie tohto nariadenia v celej únii by mali mať dozorné orgány v každom členskom štáte rovnaké úlohy a účinné právomoci, a to bez toho, aby boli dotknuté právomoci orgánov zodpovedných za stíhanie podľa práva členských štátov v oblasti upozorňovania justičných orgánov na porušovanie tohto nariadenia a obracania sa na súdy. Členské štáty a ich dozorné orgány sa vyzývajú, aby pri uplatňovaní tohto nariadenia zohľadnili osobitné potreby mikropodnikov, ako aj malých a stredných podnikov.
- (40) S cieľom posilniť presadzovanie pravidiel tohto nariadenia by mal mať každý dozorný orgán právomoc ukladať za každé porušenie tohto nariadenia okrem iných vhodných opatrení podľa tohto nariadenia alebo namiesto nich aj sankcie vrátane správnych pokút. V tomto nariadení by sa mali uviesť porušenia a horná hranica príslušných správnych pokút, ako aj kritériá ich stanovenia, ktoré by mal určiť príslušný dozorný orgán v každom jednotlivom prípade, pričom zohľadní všetky relevantné okolnosti konkrétnej situácie s náležitým zreteľom najmä na povahu, závažnosť a trvanie porušenia a jeho následkov, ako aj opatrenia, ktoré sa prijali na zabezpečenie súladu s povinnosťami podľa tohto nariadenia a na predchádzanie následkom porušenia alebo ich zmiernenie. Na účely stanovenia pokuty podľa tohto nariadenia sa za podnik považuje podnik podľa článkov 101 a 102 zmluvy.
- (41) S cieľom splniť ciele tohto nariadenia, a to ochranu základných práv a slobôd fyzických osôb, a najmä ich právo na ochranu osobných údajov a zabezpečenie voľného pohybu osobných údajov v rámci únie, by sa mala na Komisiu delegovať právomoc prijímať akty v súlade s článkom 290 zmluvy, aby sa toto nariadenie doplnilo. Konkrétne by sa mali delegované akty prijímať, pokiaľ ide o prezentované informácie, a to aj prostredníctvom štandardizovaných ikon, aby sa zabezpečil jednoducho viditeľný a čitateľný prehľad o získavaní informácií odosielaných koncovým zariadením, ich účele, osobe, ktorá je za ne zodpovedná, ako aj o každom opatrení, ktoré môže koncový používateľ koncového zariadenia prijať na

minimalizovanie tohto získavania. Delegované akty sú potrebné aj na špecifikovanie kódu, ktorým sa identifikujú priame marketingové volania vrátane tých, ktoré sa uskutočňujú prostredníctvom automatických volacích a komunikačných systémov. Je osobitne dôležité, aby Komisia uskutočnila príslušné konzultácie a aby tieto konzultácie vykonala v súlade so zásadami stanovenými v Medziinštitucionálnej dohode o lepšej tvorbe práva z 13. apríla 2016⁸. Predovšetkým v záujme rovnakého zastúpenia pri príprave delegovaných aktov sa všetky dokumenty doručujú Európskemu parlamentu a Rade v rovnakom čase ako odborníkom z členských štátov a odborníci Európskeho parlamentu a Rady majú systematicky prístup na zasadnutia expertných skupín Komisie, ktoré sa zaoberajú prípravou delegovaných aktov. Okrem toho, s cieľom zabezpečiť jednotné podmienky vykonávania tohto nariadenia by sa v prípadoch stanovených v tomto nariadení mali na Komisiu preniesť vykonávacie právomoci. Uvedené právomoci by sa mali vykonávať v súlade s nariadením (EÚ) č. 182/2011.

- (42) Keďže cieľ tohto nariadenia, a to zabezpečiť rovnocennú úroveň ochrany fyzických a právnických osôb a voľný tok údajov z elektronických komunikácií v rámci celej Únie, nie je možné uspokojivo dosiahnuť na úrovni samotných členských štátov, ale z dôvodov rozsahu a dôsledkov činnosti ich možno lepšie dosiahnuť na úrovni Únie, môže Únia prijať opatrenia v súlade so zásadou subsidiarity podľa článku 5 Zmluvy o Európskej únii. V súlade so zásadou proporcionality podľa uvedeného článku toto nariadenie neprekračuje rámec nevyhnutný na dosiahnutie tohto cieľa.
- (43) Smernica 2002/58/ES by sa mala zrušiť.

PRIJALI TOTO NARIADENIE:

⁸

Medziinštitucionálna dohoda medzi Európskym parlamentom, Radou Európskej únie a Európskou komisiou o lepšej tvorbe práva z 13. apríla 2016 (Ú. v. EÚ L 123, 12.5.2016, s. 1 – 14).

KAPITOLA I

VŠEOBECNÉ USTANOVENIA

Článok 1 *Predmet úpravy*

1. V tomto nariadení sa stanovujú pravidlá týkajúce sa ochrany základných práv a slobôd fyzických a právnických osôb pri poskytovaní a využívaní elektronických komunikačných služieb, a to predovšetkým práva na rešpektovanie súkromného života a komunikácií a ochranu fyzických osôb v oblasti spracovania osobných údajov.
2. Týmto nariadením sa zabezpečuje voľný pohyb údajov z elektronických komunikácií a elektronických komunikačných služieb v rámci Únie, ktoré nesmie byť obmedzený ani zakázaný z dôvodov súvisiacich s rešpektovaním súkromného života a komunikácií fyzických a právnických osôb a s ochranou fyzických osôb v súvislosti s spracovávaním osobných údajov.
3. Ustanovenia tohto nariadenia spresňujú a dopĺňajú nariadenie (EÚ) 2016/679 tým, že sa v nich stanovujú osobitné pravidlá na účely uvedené v odsekoch 1 a 2.

Článok 2 *Vecná pôsobnosť*

1. Toto nariadenie sa uplatňuje na spracovávanie údajov z elektronických komunikácií uskutočňované v spojitosti s poskytovaním a využívaním elektronických komunikačných služieb a na informácie súvisiace s koncovými zariadeniami koncových používateľov.
2. Toto nariadenie sa neuplatňuje na:
 - a) činnosti, ktoré nepatria do pôsobnosti práva Únie;
 - b) činnosti členských štátov, ktoré patria do rozsahu pôsobnosti kapitoly 2 hlavy V Zmluvy o Európskej únii;
 - c) elektronické komunikačné služby, ktoré nie sú verejne dostupné;
 - d) činnosti príslušných orgánov na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo výkonu trestných sankcií vrátane ochrany pred ohrozením verejnej bezpečnosti a jeho predchádzania;
3. Spracovávanie údajov z elektronických komunikácií inštitúciami, orgánmi, úradmi a agentúrami Únie sa riadi nariadením (EÚ) 00/0000 [nové nariadenie, ktorým sa nahrádza nariadenie 45/2001].

4. Týmto nariadením nie je dotknuté uplatňovanie smernice 2000/31/ES⁹, a to predovšetkým pravidiel týkajúcich sa zodpovednosti poskytovateľov sprostredkovateľských služieb uvedených v článkoch 12 až 15 danej smernice.
5. Týmto nariadením nie sú dotknuté ustanovenia smernice 2014/53/EÚ.

Článok 3 *Územná pôsobnosť a zástupca*

1. Toto nariadenie sa uplatňuje na:
 - a) poskytovanie elektronických komunikačných služieb koncovým používateľom v Únii, bez ohľadu na to, či sa od koncového používateľa vyžaduje platba;
 - b) využívanie takýchto služieb;
 - c) ochranu informácií súvisiacich s koncovými zariadeniami koncových používateľov, ktoré sa nachádzajú v Únii.
2. Ak poskytovateľ elektronických komunikačných služieb nie je usadený v Únii, písomne určí svojho zástupcu v Únii.
3. Tento zástupca musí byť usadený v jednom z členských štátov, v ktorom sa nachádzajú koncoví používatelia takýchto elektronických komunikačných služieb.
4. Na účely zabezpečenia zhody s týmto nariadením má zástupca právomoc odpovedať na otázky a poskytovať informácie najmä dozorným orgánom a koncovým používateľom v súvislosti so všetkými záležitosťami týkajúcimi sa spracovávania údajov z elektronických komunikácií, a to popri poskytovateľovi, ktorého zastupuje, alebo namiesto neho.
5. Vymenovaním zástupcu podľa odseku 2 nie je dotknutá možnosť podniknúť právne kroky voči fyzickej alebo právnickej osobe, ktorá spracúva údaje z elektronických komunikácií v súvislosti s poskytovaním elektronických komunikačných služieb z krajín mimo Únie koncovým používateľom v Únii.

Článok 4 *Vymedzenie pojmov*

1. Na účely tohto nariadenia sa uplatňuje toto vymedzenie pojmov:
 - a) vymedzenie pojmov z nariadenia (EÚ) 2016/679;
 - b) vymedzenie pojmov „elektronická komunikačná sieť“, „elektronická komunikačná služba“, „interpersonálna komunikačná služba“, „interpersonálna komunikačná služba s číslovaním“, „interpersonálna komunikačná služba bez číslovania“,

⁹ Smernica Európskeho parlamentu a Rady 2000/31/ES z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode (smernica o elektronickom obchode) (Ú. v. ES L 178, 17.7.2000, s. 1 – 16).

„koncový používateľ“ a „volanie“ z článku 2 ods. 1, 4, 5, 6, 7, 14 a 21 [smernice, ktorou sa stanovuje európsky kódex elektronickej komunikácie];

- c) vymedzenie pojmu „koncové zariadenie“ z článku 1 ods. 1 smernice Komisie 2008/63/ES¹⁰.
- 2. Na účely odseku 1 písm. b) zahŕňa vymedzenie pojmu „interpersonálna komunikačná služba“ aj služby, ktoré umožňujú interpersonálnu a interaktívnu komunikáciu len ako drobnú doplnkovú funkciu prepojenú s inou službou.
- 3. Na účely tohto nariadenia sa okrem toho uplatňuje toto vymedzenie pojmov:
 - a) „údaje z elektronických komunikácií“ sú obsah elektronických komunikácií a metaúdaje z elektronických komunikácií;
 - b) „obsah elektronických komunikácií“ je obsah vymieňaný prostredníctvom elektronických komunikačných služieb, ako napríklad textový, hlasový, obrazový, obrázkový a zvukový obsah;
 - c) „metaúdaje z elektronických komunikácií“ sú údaje spracúvané v elektronickej komunikačnej sieti na účely prenosu, distribúcie alebo výmeny obsahu elektronických komunikácií vrátane údajov slúžiacich na sledovanie a identifikovanie zdroja a cieľa komunikácie, údajov o polohe zariadenia vygenerovaných v kontexte poskytovania elektronických komunikačných služieb, ako aj údajov o dátume, čase, trvaní a druhu komunikácie;
 - d) „verejne dostupný informačný zoznam“ je zoznam koncových používateľov elektronických komunikačných služieb v tlačenej alebo elektronickej podobe, ktorý sa zverejňuje alebo sprístupňuje verejnosti alebo časti verejnosti, a to aj prostredníctvom informačnej služby;
 - e) „elektronická pošta“ je každá elektronická správa obsahujúca informácie, napríklad textové, hlasové, obrazové, zvukové alebo obrázkové, odosielané cez elektronickú komunikačnú sieť, ktoré môžu byť uložené v sieti alebo súvisiacich počítačových zariadeniach, ako aj v koncovom zariadení príjemcu;
 - f) „priame marketingové komunikácie“ sú formou písomnej alebo ústnej reklamy, ktorá sa odosiela jednému alebo viacerým identifikovaným alebo identifikovateľným koncovým používateľom elektronických komunikačných služieb, a to aj prostredníctvom automatických volacích a komunikačných systémov s ľudskou interakciou aj bez nej, elektronickej pošty, SMS správ atď.;
 - g) „priame marketingové hlasové volania“ sú volania v reálnom čase, pri ktorých sa nepoužívajú automatické volacie a komunikačné systémy;
 - h) „automatické volacie a komunikačné systémy“ sú systémy, ktoré dokážu automaticky spájať volania s jedným alebo viacerými príjemcami podľa pokynov stanovených pre daný systém a prenášať zvuky zo záznamu, a to vrátane volaní

¹⁰

Smernica Komisie 2008/63/ES z 20. júna 2008 o hospodárskej súťaži na trhoch s koncovými telekomunikačnými zariadeniami (Ú. v. EÚ L 162, 21.6.2008, s. 20 – 26).

uskutočňovaných pomocou automatických volacích a komunikačných systémov, pri ktorých sa spája volaná osoba s inou osobou.

KAPITOLA II

OCHRANA ELEKTRONICKÝCH KOMUNIKÁCIÍ FYZICKÝCH A PRÁVNICKÝCH OSÔB A INFORMÁCIÍ ULOŽENÝCH V ICH KONCOVÝCH ZARIADENIACH

Článok 5

Dôvernosť údajov z elektronických komunikácií

Údaje z elektronických komunikácií sú dôverné. S výnimkou prípadov povolených v tomto nariadení sa zakazuje každý zásah do údajov z elektronických komunikácií, ako napríklad počúvanie, odpočúvanie, uchovávanie, monitorovanie, skenovanie alebo iné druhy zachytávania, sledovania alebo spracovávania údajov z elektronických komunikácií osobami inými než koncoví používatelia.

Článok 6

Povolené spracovanie údajov z elektronických komunikácií

1. Poskytovatelia elektronických komunikačných sietí a služieb môžu spracúvať údaje z elektronických komunikácií, ak:
 - a) je to potrebné na zabezpečenie prenosu komunikácie, a to v trvaní nevyhnutom na tento účel; alebo
 - b) je to potrebné na zachovanie alebo obnovenie bezpečnosti elektronických komunikačných sietí a služieb alebo na zistenie technických porúch a/alebo chýb pri prenose elektronických komunikácií, a to v trvaní nevyhnutnom na tento účel.
2. Poskytovatelia elektronických komunikačných služieb môžu spracúvať metaúdaje z elektronických komunikácií, ak:
 - a) je to potrebné na splnenie povinných požiadaviek na kvalitu služieb podľa [smernice, ktorou sa stanovuje európsky kódex elektronickej komunikácie] alebo nariadenia (EÚ) 2015/2120¹¹, a to v trvaní nevyhnutnom na tento účel; alebo
 - b) je to potrebné z dôvodu fakturácie, výpočtu prepojovacích poplatkov, odhaľovania podvodného využívania alebo zneužívania elektronických komunikačných služieb alebo ich predplatného, alebo z dôvodu zabraňovania takýmto činom; alebo

¹¹ Nariadenie Európskeho parlamentu a Rady (EÚ) 2015/2120 z 25. novembra 2015, ktorým sa ustanovujú opatrenia týkajúce sa prístupu k otvorenému internetu a ktorým sa mení smernica 2002/22/ES o univerzálnej službe a právach užívateľov týkajúcich sa elektronických komunikačných sietí a služieb a nariadenie (EÚ) č. 531/2012 o roamingu vo verejných mobilných komunikačných sieťach v rámci Únie (Ú. v. EÚ L 310, 26.11.2015, s. 1 – 18).

- c) dotknutý koncový používateľ vyjadril súhlas so spracovaním metaúdajov zo svojich komunikácií na jeden alebo viacero konkrétnych účelov vrátane poskytovania osobitných služieb takýmto koncovým používateľom, za predpokladu, že tento účel alebo účely nemožno dosiahnuť spracovaním anonymizovaných informácií.
3. Poskytovatelia elektronických komunikačných služieb môžu spracúvať obsah elektronických komunikácií iba vtedy, ak:
- a) ide výlučne o účel poskytnutia osobitnej služby koncovému používateľovi a ak dotknutý koncový používateľ alebo dotknutí koncoví používatelia vyjadrili súhlas so spracovaním obsahu ich elektronických komunikácií a takú službu nemožno poskytnúť bez spracovania takéhoto obsahu; alebo
 - b) ak všetci dotknutí koncoví používatelia vyjadrili súhlas so spracovaním obsahu ich elektronických komunikácií na jeden alebo viaceré konkrétne účely, ktoré nemožno dosiahnuť spracovaním anonymizovaných informácií, a poskytovateľ konzultoval s dozorným orgánom. V prípade konzultácie s dozorným orgánom sa uplatňuje 36 ods. 2 a 3 nariadenia (EÚ) 2016/679.

Článok 7

Uloženie a vymazanie údajov z elektronických komunikácií

1. Bez toho, aby bol dotknutý článok 6 ods. 1 písm. b) a článok 6 ods. 3 písm. a) a b), poskytovateľ elektronických komunikačných služieb po prijatí obsahu elektronickej komunikácie určeným príjemcom alebo príjemcami vymaže obsah elektronickej komunikácie alebo tieto údaje anonymizuje. V súlade s nariadením (EÚ) 2016/679 môžu tieto údaje zaznamenať alebo uložiť koncoví používatelia alebo tretia strana, ktorú koncoví používatelia poverili zaznamenaním, uložením alebo iným spracovaním takýchto údajov.
2. Bez toho, aby bol dotknutý článok 6 ods. 1 písm. b) a článok 6 ods. 2 písm. a) a c), poskytovateľ elektronických komunikačných služieb vymaže metaúdaje z elektronických komunikácií alebo tieto údaje anonymizuje, ak už nie sú potrebné na účely prenosu komunikácie.
3. Ak sa spracovanie metaúdajov z elektronických komunikácií uskutočňuje na účely fakturácie v súlade s článkom 6 ods. 2 písm. b), príslušné metaúdaje sa môžu uchovávať do konca obdobia, počas ktorého môže byť faktúra zákonne napadnutá alebo počas ktorého sa môže uplatniť nárok na platbu v súlade s vnútroštátnym právom.

Článok 8

Ochrana informácií uložených v koncových zariadeniach koncových používateľov a súvisiacich s koncovými zariadeniami koncových používateľov

1. Využívanie funkcií koncových zariadení pre spracovávanie a uchovávanie údajov a získavanie informácií z koncových zariadení koncových používateľov vrátane informácií o ich softvéri a hardvéri, inými subjektmi, ako sú koncoví používatelia, sa zakazuje s výnimkou týchto dôvodov:

- a) je to potrebné výlučne na účely uskutočnenia prenosu elektronickej komunikácie cez elektronickú komunikačnú sieť; alebo
 - b) koncový používateľ vyjadril svoj súhlas; alebo
 - c) je to potrebné na poskytnutie služby informačnej spoločnosti, o ktorú požiadal koncový používateľ; alebo
 - d) je to potrebné na meranie využívania webu, za predpokladu, že toto meranie vykonáva poskytovateľ služby informačnej spoločnosti, o ktorú požiadal koncový používateľ.
2. Získavanie informácií vysielaných koncovým zariadením s cieľom umožniť jeho pripojenie k inému zariadeniu a/alebo k sieťovému zariadeniu, sa zakazuje s výnimkou prípadov:
- a) keď sa to uskutočňuje výlučne s cieľom a na účely vytvorenia prepojenia a výlučne počas nevyhnutného času na vytvorenie prepojenia; alebo
 - b) keď sa zobrazí jasný a výrazný oznam poskytujúci informácie prinajmenšom o postupoch získavania informácií, jeho účele, osobe, ktorá je zaň zodpovedná, a ďalšie informácie, ktoré sa vyžadujú podľa článku 13 nariadenia (EÚ) 2016/679 v prípade, že sa zbierajú osobné údaje, ako aj informácie o každom opatrení, ktoré môže koncový používateľ koncového zariadenia prijať na zastavenie alebo minimalizovanie získavania informácií.
- Získavanie takýchto informácií je podmienené uplatnením primeraných technických a organizačných opatrení na zaistenie takej úrovne bezpečnosti, ktorá je primeraná rizikám, ako sa to stanovuje v článku 32 nariadenia (EÚ) 2016/679.
3. Informácie, ktoré sa majú poskytnúť podľa odseku 2 písm. b), môžu byť doplnené o štandardizované ikony s cieľom poskytnúť zmysluplný prehľad o získavaní údajov ľahko viditeľným, čitateľným a jednoznačným spôsobom.
4. Komisia je splnomocnená prijímať v súlade s článkom 27 delegované akty s cieľom určiť informácie, ktoré sa majú prezentovať vo forme štandardizovaných ikon, a postupy poskytovania štandardizovaných ikon.

Článok 9 *Súhlas*

- 1. Uplatňuje sa vymedzenie pojmu a podmienky súhlasu uvedené v článku 4 ods. 11 a článku 7 nariadenia (EÚ) 2016/679/EÚ.
- 2. Bez toho, aby bol dotknutý odsek 1, a ak je to technicky možné a uskutočniteľné, môže sa súhlas na účely článku 8 ods. 1 písm. b) vyjadriť aj pomocou vhodných technických nastavení softvérovej aplikácie umožňujúcej prístup na internet.
- 3. Koncoví používatelia, ktorí vyjadrili súhlas so spracovaním údajov z elektronických komunikácií, ako sa stanovuje v článku 6 ods. 2 písm. c) a článku 6 ods. 3 písm. a) a b), majú možnosť kedykoľvek stiahnuť svoj súhlas, ako sa stanovuje v článku 7

ods. 3 nariadenia (EÚ) 2016/679, pričom táto možnosť sa im pripomína v pravidelných šesťmesačných intervaloch počas celého obdobia trvania spracovávaní údajov.

Článok 10

Poskytované informácie a možnosti nastavení ochrany súkromia

1. Softvér, ktorý sa uvádza na trh a umožňuje elektronické komunikácie vrátane vyhľadávania a prezentácie informácií na internete, musí ponúkať možnosť zabrániť tretím stranám v uchovávaní informácií o koncovom zariadení koncového používateľa alebo v spracovávaní informácií, ktoré sú už v danom zariadení uložené.
2. Počas inštalácie musí softvér informovať koncového používateľa o možnostiach nastavení ochrany súkromia a inštalácia môže pokračovať až po vyjadrení súhlasu koncového používateľa s nastaveniami.
3. V prípade softvéru, ktorý bol nainštalovaný do 25. mája 2018, musia byť požiadavky odsekov 1 a 2 splnené v čase prvej aktualizácie softvéru, najneskôr však do 25. augusta 2018.

Článok 11

Obmedzenia

1. Únia alebo členské štáty môžu prostredníctvom legislatívneho opatrenia obmedziť rozsah povinností a práv uvedených v článkoch 5 až 8, ak sa pri takýchto obmedzeniach dodrží podstata základných práv a slobôd a tieto obmedzenia predstavujú potrebné, vhodné a primerané opatrenia v demokratickej spoločnosti na ochranu všeobecných verejných záujmov, ako je to uvedené v článku 23 ods. 1 písm. a) až e) nariadenia (EÚ) 2016/679, alebo na zabezpečenie monitorovania, kontroly a regulácie spojených s výkonom verejnej moci v súvislosti s takýmito záujmami.
2. Poskytovatelia elektronických komunikačných služieb stanovujú na základe legislatívneho opatrenia prijatého podľa odseku 1 vnútorné postupy na poskytovanie odpovedí na žiadosti o prístup k údajom z elektronických komunikácií koncových používateľov. Príslušnému orgánu dohľadu poskytujú na požiadanie informácie o týchto postupoch, počte prijatých žiadostí, právnych dôvodoch, na ktoré sa žiadosti odvolávajú, a o odpovediach poskytovateľa.

KAPITOLA III

PRÁVO FYZICKÝCH A PRÁVNICKÝCH OSÔB NA KONTROLU ELEKTRONICKÝCH KOMUNIKÁCIÍ

Článok 12

Identifikácia volajúceho a volaného účastníka a zamedzenie identifikácie

1. Ak sa v súlade s článkom [107] [smernice, ktorou sa stanovuje európsky kódex elektronickej komunikácie] ponúka identifikácia volajúceho a volaného účastníka,

poskytovatelia verejne dostupných interpersonálnych komunikačných služieb s číslom poskytujú:

- a) volajúcemu koncovému používateľovi možnosť nezobraziť identifikáciu volajúceho pri konkrétnom volaní, spojení alebo nikdy;
 - b) volanému koncovému používateľovi možnosť nezobraziť identifikáciu volajúceho pri prichádzajúcich volaniach;
 - c) volanému koncovému používateľovi možnosť odmietnuť prichádzajúce volania, ak volajúci koncový používateľ odmietol zobrazenie identifikácie volajúceho;
 - d) volanému koncovému používateľovi možnosť nezobraziť volajúcemu koncovému používateľovi identifikáciu volaného účastníka.
2. Možnosti uvedené v odseku 1 písm. a), b), c) a d) sa koncovým používateľom poskytujú jednoducho a bezplatne.
 3. Odsek 1 písm. a) sa uplatňuje aj na volania do tretích krajín s pôvodom v Únii. Odsek 1 písm. b), c) a d) sa uplatňujú aj na prichádzajúce volania s pôvodom v tretích krajinách.
 4. Ak sa ponúka identifikácia volajúceho a volaného účastníka, poskytovatelia verejne dostupných interpersonálnych komunikačných služieb s číslom poskytujú verejnosti informácie o možnostiach stanovených v odseku 1 písm. a), b), c) a d).

Článok 13

Výnimky z identifikácie volajúceho a volaného účastníka a zo zamedzenia identifikácie

1. Bez ohľadu na to, či si volajúci koncový používateľ zvolil možnosť nezobraziť identifikáciu volajúceho, poskytovatelia verejne dostupných interpersonálnych komunikačných služieb s číslom povoľujú v prípade volaní na čísla záchranných služieb zobrazenie identifikácie volajúceho a neprihliadajú na odopretie alebo absenciu súhlasu koncového používateľa na účely spracovania metaúdajov, a to jednotlivo pre každú linku v prípade organizácií, ktoré majú na starosti tiesňovú komunikáciu vrátane stredísk tiesňového volania, aby mohli reagovať na takúto komunikáciu.
2. Členské štáty zavedú konkrétnejšie ustanovenia, pokiaľ ide o zavádzanie postupov a okolností, za ktorých poskytovatelia verejne dostupných interpersonálnych komunikačných služieb s číslom dočasne povoľujú zobrazenie identifikácie volajúceho, ak koncoví používatelia požadujú sledovanie zlomyseľných alebo obťažujúcich volaní.

Článok 14

Blokovanie prichádzajúcich volaní

Poskytovatelia verejne dostupných interpersonálnych komunikačných služieb s číslom uplatňujú najmodernejšie opatrenia na obmedzenie prijímania neželaných volaní koncovými používateľmi a volanému koncovému používateľovi bezplatne poskytujú tieto možnosti:

- a) zablokovanie prichádzajúcich volaní z konkrétnych čísel alebo z anonymných zdrojov;
- b) vypnutie automatického presmerovania volaní treťou stranou na koncové zariadenie koncového používateľa.

Článok 15

Verejne dostupné informačné zoznamy

1. Poskytovatelia verejne dostupných informačných zoznamov získajú súhlas koncových používateľov, ktorí sú fyzickými osobami, so zaradením ich osobných údajov do informačného zoznamu a tým zároveň aj ich súhlas so začlenením údajov do jednotlivých kategórií osobných údajov, a to v miere, v akej sú tieto údaje relevantné na účely informačného zoznamu stanovené poskytovateľom informačného zoznamu. Poskytovatelia poskytujú koncovým používateľom, ktorí sú fyzickými osobami, možnosť overiť, opraviť a vymazať tieto údaje.
2. Poskytovatelia verejne dostupného informačného zoznamu informujú koncových používateľov, ktorí sú fyzickými osobami a ktorých osobné údaje sa nachádzajúci v informačnom zozname, o dostupných funkciách vyhľadávania v informačnom zozname a pred povolením funkcií vyhľadávania v súvislosti s ich údajmi získajú súhlas týchto koncových používateľov.
3. Poskytovatelia verejne dostupných informačných zoznamov poskytujú koncovým používateľom, ktorí sú právnickými osobami, možnosť namietat' voči začleneniu svojich údajov do informačného zoznamu. Poskytovatelia poskytujú koncovým používateľom, ktorí sú právnickými osobami, možnosť overiť, opraviť a vymazať tieto údaje.
4. Možnosť koncových používateľov, aby neboli zaradení do verejne dostupného informačného zoznamu alebo mohli overiť, opraviť a vymazať svoje údaje, sa poskytuje bezplatne.

Článok 16

Nevyžiadané komunikácie

1. Fyzické alebo právnické osoby môžu používať elektronické komunikačné služby na účely odosielania priamych marketingových komunikácií koncovým používateľom, ktorí sú fyzickými osobami a vyjadrili svoj súhlas.
2. Ak fyzická alebo právnická osoba získa od svojho zákazníka elektronické kontaktné informácie na účely elektronickej pošty v súvislosti s predajom výrobku alebo služby podľa nariadenia (EÚ) 2016/679, táto fyzická alebo právnická osoba môže tieto elektronické kontaktné informácie použiť na priamy marketing vlastných podobných výrobkov alebo služieb iba vtedy, ak je zákazníkom jasne a jednoznačne poskytnutá možnosť bezplatne a jednoduchým spôsobom proti takémuto použitiu namietat'. Právo namietat' sa poskytne v čase získavania informácií a pri každom odoslaní správy.

3. Bez toho, aby boli dotknuté odseky 1 a 2, fyzické alebo právnické osoby využívajúce elektronické komunikačné služby na účely priamych marketingových volaní:
 - a) uvedú číslo, na ktorom je možné ich kontaktovať; alebo
 - b) uvedú osobitný kód alebo predvoľbu, z ktorej vyplýva, že volanie je marketingovým volaním.
4. Bez ohľadu na odsek 1 môžu členské štáty zákonne rozhodnúť o tom, že priame marketingové hlasové volania koncovým používateľom, ktorí sú fyzickými osobami, sa umožňujú iba v prípade koncových používateľov, ktorí sú fyzickými osobami a nenamietali proti prijímaniu takýchto komunikácií.
5. Členské štáty tiež v rámci práva Únie a platného vnútroštátneho práva zabezpečujú dostatočnú ochranu oprávnených záujmov koncových používateľov, ktorí sú právnickými osobami, pokiaľ ide o nevyžiadané komunikácie odosielané prostriedkami uvedenými v odseku 1.
6. Každá fyzická alebo právnická osoba, ktorá využíva elektronické komunikačné služby na prenos priamych marketingových komunikácií, informuje koncových používateľov o marketingovej povahe komunikácie a totožnosti právnickej alebo fyzickej osoby, v mene ktorej sa komunikácia prenáša, a príjemcom poskytuje potrebné informácie, aby mohli jednoduchým spôsobom uplatniť svoje právo vziať späť svoj súhlas s prijímaním ďalších marketingových komunikácií.
7. Komisia je splnomocnená prijímať v súlade s článkom 26 ods. 2 vykonávacie opatrenia, ktorými sa stanovuje kód alebo predvoľba na identifikáciu marketingových volaní podľa odseku 3 písm. b).

Článok 17

Informácie o zistených bezpečnostných rizikách

V prípade osobitného rizika, ktoré by mohlo ohroziť bezpečnosť sietí a elektronických komunikačných služieb, poskytovateľ elektronickej komunikačnej služby informuje dotknutých koncových používateľov o takom riziku a ak je riziko mimo rozsahu pôsobnosti opatrení, ktoré má prijať poskytovateľ služby, informuje koncových používateľov o všetkých možných prostriedkoch nápravy vrátane uvedenia pravdepodobnej výšky príslušných nákladov.

KAPITOLA IV NEZÁVISLÉ DOZORNÉ ORGÁNY A PRESADZOVANIE PREDPISOV

Článok 18

Nezávislé dozorné orgány

1. Nezávislé dozorné orgány alebo orgány zodpovedné za monitorovanie uplatňovania nariadenia (EÚ) 2016/679 sú zodpovedné aj za monitorovanie uplatňovania tohto

nariadenia. Kapitoly VI a VII nariadenia (ES) 2016/679 sa uplatňujú primerane. Dozorné orgány vykonávajú svoje úlohy a právomoci s prihliadnutím na koncových používateľov.

2. Dozorný orgán, resp. orgány uvedené v odseku 1 spolupracujú vždy, keď je to vhodné, s vnútroštátnymi regulačnými orgánmi zriadenými podľa [smernice, ktorou sa stanovuje európsky kódex elektronickej komunikácie].

Článok 19

Európsky výbor pre ochranu údajov

Európsky výbor pre ochranu údajov zriadený podľa článku 68 nariadenia (EÚ) 2016/679 má právomoc zabezpečovať jednotné uplatňovanie tohto nariadenia. Na tento účel vykonáva Európsky výbor pre ochranu údajov úlohy stanovené v článku 70 nariadenia (EÚ) 2016/679. Výbor plní aj tieto úlohy:

- a) radí Komisii v prípade každej navrhovanej zmeny tohto nariadenia;
- b) preskúmava z vlastnej iniciatívy, na žiadosť jedného zo svojich členov alebo na žiadosť Komisie každú otázku týkajúcu sa uplatňovania tohto nariadenia a vydáva usmernenia, odporúčania a najlepšie postupy s cieľom podporiť jednotné uplatňovanie tohto nariadenia.

Článok 20

Postupy spolupráce a konzistentnosti

Každý dozorný orgán prispieva k jednotnému uplatňovaniu tohto nariadenia v celej Únii. V súlade s kapitolou VII nariadenia (EÚ) 2016/679 dozorné orgány spolupracujú na tento účel v otázkach spadajúcich do rozsahu pôsobnosti tohto nariadenia medzi sebou, ako aj s Komisiou.

KAPITOLA V PROSTRIEDKY NÁPRAVY, ZODPOVEDNOSŤ A SANKCIE

Článok 21

Prostriedky nápravy

1. Bez toho, aby boli dotknuté iné správne alebo súdne prostriedky nápravy, má každý koncový používateľ elektronických komunikačných služieb k dispozícii rovnaké prostriedky nápravy, ktoré sú uvedené v článkoch 77, 78 a 79 nariadenia (EÚ) 2016/679.
2. Každá fyzická alebo právnická osoba iná ako koncový používateľ, ktorá e nepriaznivo ovplyvnená porušením ustanovení tohto nariadenia a ktorá má oprávnený záujem na zastavení alebo zákaze údajného porušenia ustanovení, vrátane poskytovateľa elektronických komunikačných služieb, ktorý chráni svoje oprávnené obchodné záujmy, má právo začať súdne konanie vo veci takéhoto porušenia.

Článok 22
Právo na náhradu škody a zodpovednosť

Každý koncový používateľ elektronických komunikačných služieb, ktorý v dôsledku porušenia tohto nariadenia utrpel majetkovú alebo nemajetkovú ujmu, má právo na náhradu vzniknutej škody od osoby, ktorá sa dopustila porušenia, ak táto osoba nedokáže, že nie je v súlade s článkom 82 nariadenia (EÚ) 2016/679 v žiadnom prípade zodpovedná za udalosť, v dôsledku ktorej vznikla škoda.

Článok 23
Všeobecné podmienky ukladania správnych pokút

1. Na účely tohto článku sa na porušenia tohto nariadenia uplatňuje kapitola VII nariadenia (EÚ) 2016/679.
2. Za porušenie nasledujúcich ustanovení tohto nariadenia sa podľa odseku 1 uloží správna pokuta až do výšky 10 000 000 EUR alebo v prípade podniku až do výšky 2 % celkového svetového ročného obratu za predchádzajúci účtovný rok, podľa toho, ktorá suma je vyššia:
 - a) povinnosti akejkoľvek právnickej alebo fyzickej osoby, ktorá spracúva údaje z elektronických komunikácií, podľa článku 8;
 - b) povinnosti poskytovateľa softvéru umožňujúceho elektronické komunikácie podľa článku 10;
 - c) povinnosti poskytovateľov verejne dostupných informačných zoznamov podľa článku 15;
 - d) povinnosti akejkoľvek právnickej alebo fyzickej osoby, ktorá využíva elektronické komunikačné služby, podľa článku 16.
3. Za porušenie zásady dôvernosti komunikácií, povoleného spracovania údajov z elektronických komunikácií, časových lehôt na vymazanie údajov podľa článkov 5, 6 a 7 sa podľa odseku 1 tohto článku uloží správna pokuta až do výšky 20 000 000 EUR alebo v prípade podniku až do výšky 4 % celkového svetového ročného obratu za predchádzajúci účtovný rok, podľa toho, ktorá suma je vyššia.
4. Členské štáty stanovujú pravidlá týkajúce sa sankcií za porušenia článkov 12, 13, 14 a 17.
5. Za nesplnenie príkazu dozorného orgánu podľa článku 18 sa uloží správna pokuta až do výšky 20 000 000 EUR alebo v prípade podniku až do výšky 4 % celkového svetového ročného obratu za predchádzajúci účtovný rok, podľa toho, ktorá suma je vyššia.
6. Bez toho, aby boli dotknuté nápravné právomoci dozorných orgánov podľa článku 18, každý členský štát môže stanoviť, či a v akom rozsahu sa môžu správne pokuty ukladať orgánom verejnej moci a verejnoprávnym subjektom usadeným v danom členskom štáte.

7. Výkon právomocí dozorného orgánu podľa tohto článku podlieha primeraným procesným zárukám v súlade s právom Únie a právom členského štátu vrátane účinného súdneho prostriedku nápravy a riadneho procesu.
8. Ak sa v právnom systéme členského štátu nestanovujú správne pokuty, tento článok sa môže uplatňovať tak, že uloženie pokuty iniciuje príslušný dozorný orgán a uloží ju príslušný vnútroštátny súd, pričom sa zabezpečí, aby tieto právne prostriedky nápravy boli účinné a mali rovnocenný účinok ako správne pokuty ukladané dozornými orgánmi. Ukladané pokuty sú v každom prípade účinné, primerané a odrádzajúce. Tieto členské štáty oznámi Komisii ustanovenia svojich právnych predpisov, ktoré prijímú podľa tohto odseku, do [xxx] a bezodkladne oznámia aj všetky následné pozmeňujúce právne predpisy či zmeny, ktoré sa ich týkajú.

Článok 24 *Sankcie*

1. Členské štáty stanovujú pravidlá týkajúce sa iných sankcií za porušovanie ustanovení tohto nariadenia, a to predovšetkým za tie porušenia, na ktoré sa nevzťahujú správne pokuty podľa článku 23, a prijímajú všetky opatrenia potrebné na zabezpečenie ich vykonania. Takéto sankcie sú účinné, primerané a odrádzajúce.
2. Každý členský štát oznámi Komisii ustanovenia svojich právnych predpisov, ktoré prijme podľa odseku 1, najneskôr 18 mesiacov od dátumu stanoveného v článku 29 ods. 2 a bezodkladne oznámi aj všetky následné zmeny, ktoré sa ich týkajú.

KAPITOLA VI **DELEGOVANÉ AKTY A VYKONÁVACIE AKTY**

Článok 25 *Vykonávanie delegovania právomoci*

1. Komisii sa udeľuje právomoc prijímať delegované akty za podmienok stanovených v tomto článku.
2. Právomoc prijímať delegované akty uvedené v článku 8 ods. 4 sa Komisii udeľuje na neurčité obdobie odo [dňa nadobudnutia účinnosti tohto nariadenia].
3. Delegovanie právomoci uvedené v článku 8 ods. 4 môže Európsky parlament alebo Rada kedykoľvek odvolať. Rozhodnutím o odvolaní sa ukončuje delegovanie právomoci, ktoré sa v ňom uvádza. Rozhodnutie nadobúda účinnosť dňom nasledujúcim po jeho uverejnení v *Úradnom vestníku Európskej únie* alebo k neskoršiemu dátumu, ktorý je v ňom určený. Nie je ním dotknutá platnosť delegovaných aktov, ktoré už nadobudli účinnosť.
4. Pred prijatím delegovaného aktu bude Komisia viesť konzultácie s expertmi určenými každým členským štátom v súlade so zásadami stanovenými v Medziinštitucionálnej dohode o lepšej tvorbe práva z 13. apríla 2016.

5. Komisia oznamuje delegovaný akt hneď po jeho prijatí súčasne Európskemu parlamentu a Rade.
6. Delegovaný akt prijatý podľa článku 8 ods. 4 nadobudne účinnosť, len ak Európsky parlament alebo Rada voči nemu nevzniesli námietku v lehote dvoch mesiacov odo dňa oznámenia uvedeného aktu Európskemu parlamentu a Rade alebo ak pred uplynutím uvedenej lehoty Európsky parlament a Rada informovali Komisiu o svojom rozhodnutí nevzniesť námietku. Na podnet Európskeho parlamentu alebo Rady sa táto lehota predĺži o dva mesiace.

Článok 26 *Výbor*

1. Komisii pomáha Komunikačný výbor zriadený podľa článku 110 [smernice, ktorou sa stanovuje európsky kódex elektronickej komunikácie]. Tento výbor je výborom v zmysle nariadenia (EÚ) č. 182/2011¹².
2. Ak sa odkazuje na tento odsek, uplatňuje sa článok 5 nariadenia (EÚ) č. 182/2011.

KAPITOLA VII **ZÁVEREČNÉ USTANOVENIA**

Článok 27 *Zrušenie*

1. Smernica 2002/58/ES sa zrušuje s účinnosťou od 25. mája 2018.
2. Odkazy na zrušenú smernicu sa považujú za odkazy na toto nariadenie.

Článok 28 *Monitorovanie a hodnotenie*

Najneskôr do 1. januára 2018 stanoví Komisia podrobný program monitorovania účinnosti tohto nariadenia.

Najneskôr tri roky odo dňa začatia uplatňovania tohto nariadenia a následne každé tri roky Komisia vykoná hodnotenie tohto nariadenia a hlavné zistenia predloží Európskemu parlamentu, Rade a Európskemu hospodárskemu a sociálnemu výboru. V prípade, že to bude potrebné vzhľadom na právny, technický alebo hospodársky vývoj, toto hodnotenie poslúži ako základ pre návrh na zmenu alebo zrušenie tohto nariadenia.

¹² Nariadenie Európskeho parlamentu a Rady (EÚ) č. 182/2011 zo 16. februára 2011, ktorým sa ustanovujú pravidlá a všeobecné zásady mechanizmu, na základe ktorého členské štáty kontrolujú vykonávanie vykonávacích právomocí Komisie (Ú. v. EÚ L 55, 28.2.2011, s. 13 – 18).

Článok 29
Nadobudnutie účinnosti a uplatňovanie

1. Toto nariadenie nadobúda účinnosť dvadsiatym dňom po jeho uverejnení v *Úradnom vestníku Európskej únie*.
2. Uplatňuje sa od 25. mája 2018.

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli

za Európsky parlament
predseda

za Radu
predseda