EUROPA-
KOMMISSIONEN

Bruxelles, den 10.1.2017
COM(2017) 10 final

2017/0003 (COD)

Forslag til

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING

om respekt for privatliv og beskyttelse af personoplysninger i forbindelse med elektroniske kommunikation og om ophævelse af direktiv 2002/58/EF (forordning om databeskyttelse inden for elektronisk kommunikation)

(EØS-relevant tekst)

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

BEGRUNDELSE

1. BAGGRUND FOR FORSLAGET

1.1. Forslagets begrundelse og formål

Strategien for et digitalt indre marked[1] har til formål at øge tilliden til og sikkerheden ved digitale tjenester. Reformen af databeskyttelsesrammen og især vedtagelsen af forordning (EU) 2016/679, **den generelle forordning om databeskyttelse**[2], var et vigtigt skridt i denne henseende. Strategien for et digitalt indre marked varslede også en revision af direktiv 2002/58/EF ("**e-databeskyttelsesdirektivet**")[3] med henblik på at sikre et højt niveau af beskyttelse af privatlivets fred for brugerne af elektroniske kommunikationstjenester samt lige vilkår for alle markedsaktører. Nærværende forslag vedrører den planlagte revision, der bygger på målene i strategien for et digitalt indre marked og sikrer overensstemmelse med den generelle forordning om databeskyttelse.

E-databeskyttelsesdirektivet sikrer beskyttelsen af grundlæggende rettigheder og friheder, navnlig retten til privatlivets fred, kommunikationshemmelighed og beskyttelse af personoplysninger i sektoren for elektronisk kommunikation. Desuden garanterer det fri udveksling af elektronisk kommunikation, udstyr og tjenesteydelser i Unionen. Det gennemfører den grundlæggende ret til respekt for privatlivets fred i den afledte EU-ret, for så vidt angår kommunikation, som fastsat i artikel 7 chartret om Den Europæiske Unions grundlæggende rettigheder ("**chartret**").

I overensstemmelse med kravet om bedre regulering har Kommissionen foretaget en efterfølgende evaluering af e-databeskyttelsesdirektivet som led i programmet for målrettet og effektiv regulering ("**Refit**") . Det fremgår af evalueringen, at målsætningerne og principperne bag den nuværende ramme stadig er gyldige. Imidlertid er der sket en betydelig teknologisk og økonomisk udvikling på markedet siden sidste revision af direktivet i 2009. Forbrugere og virksomheder er i stigende grad afhængige af nye internetbaserede tjenester, der muliggør interpersonel kommunikation, såsom internettelefoni, instant messaging og webbaserede e-mailtjenester i stedet for traditionelle kommunikationstjenester. Disse "over-the-top"-kommunikationstjenester ("**OTT-tjenester**") er generelt ikke omfattet af Unionens nuværende rammebestemmelser for elektronisk kommunikation, herunder e-databeskyttelsesdirektivet. Følgelig har direktivet ikke holdt trit med den teknologiske udvikling, hvilket har resulteret i et tomrum, for så vidt angår beskyttelsen af kommunikation, der formidles gennem nye tjenester.

1.2. Sammenhæng med de gældende regler på samme område

Dette forslag udgør særlovgivning i forhold til den generelle forordning om databeskyttelse og vil præcisere og supplere denne for så vidt angår elektronisk kommunikation, der betragtes som personoplysninger. Alle spørgsmål vedrørende behandling af personoplysninger, der ikke specifikt er behandlet i forslaget, er omfattet af den generelle forordning om databeskyttelse.

---

1 Meddelelse fra Kommissionen til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget: En strategi for et digitalt indre marked i EU, COM(2015) 192 final.

2 Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1-88).

3 Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktivet om databeskyttelse inden for elektronisk kommunikation) (EFT L 201 af 31.7.2002, s. 37).

Den styrkede sammenhæng med den generelle forordning om databeskyttelse har medført, at visse bestemmelser, såsom sikkerhedsforpligtelserne i artikel 4 e-databeskyttelsesdirektivet, ophæves.

1.3. Sammenhæng med Unionens politik på andre områder

E-databeskyttelsesdirektivet er en del af regelsættet for elektronisk kommunikation. I 2016 forelagde Kommissionen et direktivforslag om en **europæisk kodeks for elektronisk kommunikation**[4], der udgør en revision af regelsættet. Selv om nærværende forslag ikke er en integrerende del af kodeksen for elektronisk kommunikation, bygger det delvis på definitionerne deri, herunder begrebet "elektroniske kommunikationstjenester". Ligesom kodeksen omfatter nærværende forslag også udbydere af OTT-tjenester for at afspejle virkeligheden på markedet. Desuden supplerer forslaget kodeksen ved at garantere sikkerheden i forbindelse med elektroniske kommunikationstjenester.

Direktiv 2014/53/EU om **radioudstyr**[5] danner grundlaget for et indre marked for radioudstyr. Det fastsætter navnlig, at radioudstyr for at kunne markedsføres skal være forsynet med sikkerhedsforanstaltninger til beskyttelse af brugerens personoplysninger og privatliv. I henhold til direktivet om radioudstyr og forordning (EU) nr. 1025/2012 om europæisk standardisering[6] tillægges Kommissionen beføjelser til at vedtage foranstaltninger. Dette forslag berører ikke direktivet om radioudstyr.

Forslaget indeholder ingen særlige bestemmelser om opbevaring af data. Det fastholder substansen i artikel 15 i e-databeskyttelsesdirektivet og bringer den i overensstemmelse med en specifik formulering af artikel 23 i den generelle forordning om databeskyttelse, der giver grundlag for, at medlemsstaterne kan begrænse rækkevidden af de rettigheder og forpligtelser, der følger af bestemte artikler i e-databeskyttelsesdirektivet. Derfor kan medlemsstaterne frit bevare eller etablere nationale rammer for dataopbevaring, der bl.a. indeholder bestemmelser om målrettet dataopbevaring, for så vidt som disse rammer – under hensyntagen til Domstolens praksis vedrørende fortolkningen af e-databeskyttelsesdirektivet og chartret om grundlæggende rettigheder[7] – er i overensstemmelse med EU-retten.

Endelig finder forslaget ikke anvendelse på Unionens institutioners, organers og agenturers handlinger. Imidlertid er dets principper og relevante forpligtelser vedrørende retten til respekt for privatliv og kommunikationshemmelighed i forbindelse med behandling af elektronisk kommunikation indarbejdet i forslaget til forordning om ophævelse af forordning (EF) nr. 45/2001[8].

---

4 Kommissionens forslag til Europa-Parlamentets og Rådets direktiv om en europæisk kodeks for elektronisk kommunikation (omarbejdning) (COM/2016/0590 final - 2016/0288 (COD)).

5 Europa-Parlamentets og Rådets direktiv 2014/53/EU af 16. april 2014 om harmonisering af medlemsstaternes love om tilgængeliggørelse af radioudstyr på markedet og om ophævelse af direktiv 1999/5/EF (EUT L 153 af 22.5.2014, s. 62-106).

6 Europa-Parlamentets og Rådets forordning (EU) nr. 1025/2012 af 25. oktober 2012 om europæisk standardisering, om ændring af Rådets direktiv 89/686/EØF og 93/15/EØF og Europa-Parlamentets og Rådets direktiv 94/9/EF, 94/25/EF, 95/16/EF, 97/23/EF, 98/34/EF, 2004/22/EF, 2007/23/EF, 2009/23/EF og 2009/105/EF og om ophævelse af Rådets beslutning 87/95/EØF og Europa-Parlamentets og Rådets afgørelse nr. 1673/2006/EF (EUT L 316 af 14.11.2012, s. 12-33).

7 Se forenede sager C-293/12 og C-594/12 *Digital Rights Ireland og Seitlinger m.fl.*, ECLI:EU:C:2014:238; Forenede sager C-203/15 og C-698/15, *Tele2 Sverige AB og Secretary of State for the Home Department*, ECLI:EU:C:2016:970.

8 Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger (EFT L 8 af 12.1.2001, s. 1).

2. RETSGRUNDLAG, NÆRHEDSPRINCIPPET OG PROPORTIONALITETSPRINCIPPET

2.1. Retsgrundlag

Retsgrundlaget for forslaget er artikel 16 og artikel 114 i traktaten om Den Europæiske Unions funktionsmåde ("**TEUF**").

Med artikel 16 i TEUF er der indført et specifikt retsgrundlag for vedtagelsen af regler for beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger foretaget af Unionens institutioner samt af medlemsstaterne under udøvelse af aktiviteter, der er omfattet af EU-retten, og regler for den frie udveksling af personoplysninger. Da elektronisk kommunikation, der involverer en fysisk person, normalt kan betragtes som personoplysninger, bør beskyttelsen af fysiske personer, for så vidt angår privatlivets fred i forbindelse med kommunikation og behandling af sådanne oplysninger, være baseret på artikel 16.

Desuden har forslaget til formål at beskytte kommunikation og juridiske personers legitime interesser i forbindelse hermed. Betydningen og rækkevidden af de rettigheder, der er omhandlet i chartrets artikel 7, skal i overensstemmelse med chartrets artikel 52, stk. 3, være de samme som dem, der er fastsat i artikel 8, stk. 1, i den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder ("**EMRK**"). Hvad angår anvendelsesområdet for chartrets artikel 7, bekræfter **EU-Domstolen**s og Den Europæiske Menneskerettighedsdomstols[9] retspraksis[10], at juridiske personers aktiviteter af erhvervsmæssig karakter ikke kan udelukkes fra beskyttelsen af den rettighed, der er sikret ved chartrets artikel 7 og menneskerettighedskonventionens artikel 8.

Da initiativet har et dobbelt formål, og da aspekter vedrørende beskyttelse af juridiske personers kommunikation og målet om at virkeliggøre et indre marked for denne type elektronisk kommunikation og sikre, at det fungerer tilfredsstillende i denne henseende, ikke kan anses for at være af underordnet betydning, bør initiativet derfor også baseres på artikel 114 i TEUF.

2.2. Nærhedsprincippet

Respekt for kommunikation er en grundlæggende rettighed, der er anerkendt i chartret. Indholdet af elektronisk kommunikation kan afsløre meget følsomme oplysninger om de slutbrugere, der er involveret i kommunikationen. Ligeledes kan metadata, der afledes af elektronisk kommunikation, også afsløre meget følsomme og personlige oplysninger, hvilket EU-Domstolen udtrykkelig har anerkendt[11]. De fleste medlemsstater anerkender også behovet for at beskytte kommunikation som en særskilt forfatningsmæssig rettighed. Selv om det er muligt for medlemsstaterne at vedtage politikker, der sikrer, at denne ret ikke tilsidesættes, ville dette ikke kunne opnås på en ensartet måde i mangel af EU-regler, og det ville skabe begrænsninger for grænseoverskridende strømme af personoplysninger og ikke-personoplysninger i forbindelse med brug af elektroniske kommunikationstjenester. Endelig er det – for at sikre overensstemmelse med den generelle forordning om databeskyttelse –

---

9 Se bl.a. Menneskerettighedsdomstolens domme *Niemietz v Germany*, dom af 16. december 1992, serie A nr. 251-B, § 29; *Société Colas Est m.fl. mod Frankrig*, nr. 37971/97, § 41; ECHR 2002-III. *Peck mod Det Forenede Kongerige* nr. 44647/98, § 57, ECHR 2003-I; samt *Vinci Construction og GTM Génie Civil et Services mod Frankrig*, nr. 63629/10 og 60567/10, § 63, 2. april 2015.

10 Se C-450/06 *Varec SA*, ECLI:EU:C:2008:91, § 48.

11 Se fodnote 7.

nødvendigt at revidere e-databeskyttelsesdirektivet og vedtage foranstaltninger for at bringe disse to retsakter i overensstemmelse med hinanden.

Den teknologiske udvikling og ambitionerne for strategien for et digitalt indre marked har styrket begrundelsen for handling på EU-plan. Hvorvidt EU's digitale indre marked bliver en succes afhænger af, hvor effektivt EU nedbringer nationale barrierer og udnytter fordelene og mulighederne ved et europæisk digitalt indre marked. Og eftersom internettet og digitale teknologier ikke kender nogen grænser, rækker problemets omfang ud over den enkelte medlemsstats område. Medlemsstaterne kan ikke effektivt løse problemerne i den nuværende situation. Lige vilkår for økonomiske operatører, der leverer substituerbare tjenester, og lige beskyttelse af slutbrugerne på EU-plan er en forudsætning for, at det digitale indre marked kan fungere ordentligt.

2.3. Proportionalitetsprincippet

For at sikre en effektiv retlig beskyttelse af retten til respekt for privatlivet og kommunikationshemmelighed er det nødvendigt at udvide anvendelsesområdet til også at omfatte OTT-udbydere. Selv om en række populære OTT-udbydere allerede overholder, eller delvis overholder, princippet om kommunikationshemmelighed, kan beskyttelsen af de grundlæggende rettigheder ikke overlades til selvregulering i branchen. Desuden bliver det mere og mere nødvendigt at sikre en effektiv beskyttelse af privatlivets fred i forbindelse med terminaludstyr, der er blevet et uundværligt værktøj i privat- og arbejdslivet til opbevaring af følsomme oplysninger. Gennemførelsen af e-databeskyttelsesdirektivet har ikke reelt styrket brugernes indflydelse. For at nå målet er det derfor nødvendigt at gennemføre dette princip ved at centralisere indhentningen af samtykke i softwaren og få brugerne til at handle ved at forsyne dem med oplysninger om privatlivsindstillinger. Håndhævelsen af denne forordning påhviler tilsynsmyndighederne og er underlagt sammenhængsmekanismen i den generelle forordning om databeskyttelse. Derudover giver forslaget medlemsstaterne mulighed for at træffe nationale undtagelsesforanstaltninger til bestemte legitime formål. Forslaget går således ikke videre, end hvad der er nødvendigt for at nå målet, og er i overensstemmelse med proportionalitetsprincippet, som fastsat i artikel 5 traktaten om Den Europæiske Union. De forpligtelser, der pålægges de berørte tjenester, holdes på det lavest mulige niveau, uden at de pågældende grundlæggende rettigheder derved indskrænkes.

2.4. Valg af retsakt

Kommissionen fremsætter et forslag til forordning for at sikre overensstemmelse med den generelle forordning om databeskyttelse og retssikkerhed for brugerne og erhvervslivet ved at undgå forskellige fortolkninger i medlemsstaterne. En forordning kan sikre et ensartet beskyttelsesniveau i hele EU for brugerne og nedbringe efterlevelsesomkostningerne for virksomheder, der opererer på tværs af grænserne.

3. RESULTATER AF EFTERFØLGENDE EVALUERINGER, HØRINGER AF INTERESSEREDE PARTER OG KONSEKVENSANALYSER

3.1. Efterfølgende evalueringer/kvalitetskontrol af gældende lovgivning

Som led i Refit-evalueringen er det blevet undersøgt, hvor effektivt e-databeskyttelsesdirektivet har bidraget til en tilstrækkelig beskyttelse af retten til respekt for privatliv og kommunikationshemmelighed i EU. Det har også været målet at påpege mulige overlapninger.

Konklusionen på Refit-evalueringen er, at de ovennævnte mål for direktivet fortsat er **relevante**. Den generelle forordning om databeskyttelse sikrer beskyttelse af

personoplysninger, og e-databeskyttelsesdirektivet sikrer kommunikationshemmeligheden, der også kan omfatte ikke-personoplysninger og oplysninger vedrørende juridiske personer. Derfor bør et særskilt instrument sikre en effektiv beskyttelse af rettighederne i chartrets artikel 7. Andre bestemmelser, såsom reglerne vedrørende uanmodede markedsføringsmeddelelser, har også vist sig fortsat at være relevante.

For så vidt angår **virkning og effektivitet**, er konklusionen af Refit-evalueringen, at direktivet ikke fuldt ud har opfyldt sine mål. Den uklare formulering af visse bestemmelser og tvetydighed i retlige begreber har været til hinder for en harmonisering, hvilket har skabt problemer for foretagender, der vil drive virksomhed på tværs af grænserne. Evalueringen har desuden vist, at visse bestemmelser har skabt en unødvendig byrde for både virksomheder og forbrugere. F.eks. har samtykkereglen, der skal beskytte fortroligheden i forbindelse med terminaludstyr, ikke opfyldt sit mål, eftersom slutbrugerne stilles over for opfordringer til at acceptere sporingscookies uden at forstå deres betydning og i visse tilfælde endda udsættes for, at der anbringes cookies uden deres samtykke. Samtykkereglen er på den ene side for omfattende, da den også dækker fremgangsmåder, der ikke griber ind i privatlivets fred, og på den anden ikke omfattende nok, da den ikke klart dækker visse sporingsteknologier (f.eks. "device fingerprinting"), der muligvis ikke indebærer adgang/opbevaring i udstyret. Endelig kan det være dyrt for virksomhederne at efterleve reglen.

Evalueringen har vist, at e-databeskyttelsesreglerne stadig har en **merværdi på EU-plan** med henblik på at nå målet om at beskytte privatlivets fred online på et stadig mere grænseoverskridende marked for elektronisk kommunikation. Den viste også, at der i det store hele er **sammenhæng** mellem reglerne og den øvrige relevante lovgivning, selv om der er påpeget enkelte overlapninger i forhold til den nye generelle forordning om databeskyttelse (jf. afsnit 1.2).

3.2. Høringer af interesserede parter

Kommissionen gennemførte en offentlig høring mellem den 12. april og den 5. juli 2016 og modtog 421 svar[12]. De vigtigste resultater er følgende[13]:

– **Om behovet for særlige regler for den elektroniske kommunikationssektor vedrørende kommunikationshemmelighed**: 83,4 % af de borgere, forbrugere og civilsamfundsorganisationer, der har reageret på høringen, og 88,9 % af de offentlige myndigheder mener, at der er behov for særlige regler, mens 63,4 % af respondenterne fra erhvervslivet er uenige i dette.

– **Om udvidelse af anvendelsesområdet til at omfatte nye kommunikationstjenester ("OTT-tjenester)**: 76 % af borgerne og civilsamfundet og 93,1 % af de offentlige myndigheder er enige i, at anvendelsesområdet bør udvides, mens kun 36,2 % af respondenterne fra erhvervslivet går ind for en sådan udvidelse.

– **Om ændring af undtagelserne fra reglen om samtykke til behandling af trafikdata og lokaliseringsdata**: 49,1 % af borgerne, forbrugerne og civilsamfundsorganisationerne og 36 % af de offentlige myndigheder foretrækker ikke at udvide undtagelserne, mens 36 % af virksomhederne går ind for udvidede

[12] 162 bidrag fra borgere, 33 fra civilsamfundet og forbrugerorganisationerne; 186 fra erhvervslivet og 40 fra offentlige myndigheder, herunder de kompetente myndigheder, der håndhæver e-databeskyttelsesdirektivet.

[13] Den fuldstændige rapport findes på: https://ec.europa.eu/digital-single-market/news-redirect/37204.

undtagelser, og to tredjedele af virksomhederne taler for helt at ophæve bestemmelserne.

– **Om støtte til løsninger, der foreslås på cookiesamtykkeproblemet**: 81,2 % af borgerne og 63 % af de offentlige myndigheder går ind for at pålægge fabrikanter af terminaludstyr forpligtelser til at markedsføre produkter med indbygget privatlivsbeskyttelse, der er aktiveret, mens 58,3 % af virksomhederne foretrækker selv- eller samregulering.

Desuden har Europa-Kommissionen afholdt to workshopper i april 2016 – én for de nationale kompetente myndigheder og én, som alle interesserede parter kunne deltage i – hvor de vigtigste spørgsmål i den offentlige høring blev drøftet. De synspunkter, der kom til udtryk under workshopperne, afspejler resultatet af den offentlige høring.

For at indhente synspunkter fra borgerne blev der gennemført en Eurobarometerundersøgelse om e-databeskyttelse[14] i hele EU. De vigtigste resultater er følgende[15]:

– 78 % mener, at det er meget vigtigt, at personlige oplysninger på deres computer, smartphone eller tablet kun kan tilgås med deres tilladelse.

– 72 % siger, at det er meget vigtigt, at fortroligheden af deres e-mails og instant messaging er garanteret.

– 89 % tilslutter sig forslaget om, at standardindstillingerne i browsere bør forhindre, at brugernes oplysninger videregives.

3.3. Indhentning og brug af ekspertbistand

Kommissionen har benyttet sig af følgende eksterne ekspertbistand:

– Målrettede høringer af EU-ekspertgrupper: Udtalelse fra Artikel 29-Gruppen, Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse, Udtalelse fra Refit-platformen, BEREC's synspunkter, ENISA's synspunkter samt synspunkter blandt medlemmerne af Samarbejdsnetværket for Håndhævelse af Forbrugerbeskyttelse.

– Ekstern ekspertbistand, navnlig følgende to undersøgelser:

  – "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation" (SMART 2013/007116).

  – "Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector" (SMART 2016/0080).

3.4. Konsekvensanalyse

Der er gennemført en konsekvensanalyse af dette forslag, som Udvalget for Forskriftskontrol afgav en positiv udtalelse[16] om den 28. september 2016. Som reaktion på udvalgets anbefalinger indeholder konsekvensanalysen en mere udførlig redegørelse for initiativets anvendelsesområde, dets sammenhæng med andre retlige instrumenter (den generelle databeskyttelsesforordning, forslaget om en europæisk kodeks for elektronisk kommunikation, direktivet om radioudstyr) og behovet for en særskilt retsakt. Beskrivelsen af

14 2016-Eurobarometerundersøgelse (EB) 443 om e-databeskyttelse (SMART 2016/079).

15 Den fuldstændige rapport findes på: https://ec.europa.eu/digital-single-market/news-redirect/37205.

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

referencescenariet er uddybet og præciseret. Analysen af virkningerne er styrket og fremstilles mere afbalanceret, så beskrivelsen af de forventede udgifter og fordele bliver klarere og mere udførlig.

Følgende politiske løsningsmodeller er blevet vurderet ud fra kriterierne om effektivitet, omkostningseffektivitet og sammenhæng:

– **Løsningsmodel 1:** Ikkelovgivningsmæssige foranstaltninger ("blød lovgivning")

– **Løsningsmodel 2:** Begrænset styrkelse af privatlivets fred/kommunikationshemmeligheden samt forenkling

– **Løsningsmodel 3:** Moderat styrkelse af privatlivets fred/kommunikationshemmeligheden samt forenkling

– **Løsningsmodel 4:** Vidtgående styrkelse af privatlivets fred/kommunikationshemmeligheden samt forenkling

– **Løsningsmodel 5:** Ophævelse af e-databeskyttelsesdirektivet.

Løsningsmodel 3 blev i forbindelse med de fleste aspekter fremhævet som den **foretrukne løsning** med henblik på at nå målene og samtidig tage hensyn til løsningens effektivitet og sammenhæng med andre tiltag. De vigtigste fordele er:

– Beskyttelsen af kommunikationshemmeligheden i forbindelse med elektronisk kommunikation styrkes, ved at anvendelsesområdet for det retlige instrument udvides til at omfatte nye funktionelt tilsvarende elektroniske kommunikationstjenester. Desuden styrker forordningen slutbrugerens kontrol ved at præcisere, at samtykke kan udtrykkes ved hjælp af passende tekniske indstillinger.

– Beskyttelsen mod uanmodet kommunikation styrkes med indførelsen af et krav om visning af opkaldende nummer eller et obligatorisk præfiks for marketingshenvendelser og de øgede muligheder for at blokere for opkald fra uønskede numre.

– Lovrammerne forenkles og præciseres, idet medlemsstaternes råderum begrænses, forældede bestemmelser ophæves, og undtagelserne fra samtykkereglerne udvides.

De økonomiske konsekvenser af løsningsmodel 3 forventes generelt at stå i et rimeligt forhold til formålet med forslaget. Der skabes nye forretningsmuligheder i forbindelse med behandling af kommunikationsdata for de traditionelle elektroniske kommunikationstjenester, mens OTT-udbydere underkastes de samme regler. Dette indebærer yderligere omkostninger for disse udbydere. Ændringen vil dog ikke få nogen væsentlig betydning for de OTT-udbydere, der allerede arbejder på grundlag af samtykke. Endelig vil virkningen af denne løsningsmodel ikke kunne mærkes i de medlemsstater, der allerede har udvidet anvendelsesområdet for samtykkereglerne til at omfatte OTT-udbydere.

Ved at centralisere indhentningen af samtykke i softwaren, såsom internetbrowsere, og tilskynde brugerne til at vælge deres privatlivsindstillinger, og ved at udvide undtagelserne fra reglen om samtykke til cookies vil en betydelig del af virksomhederne kunne fjerne cookiebannere og meddelelser, hvilket kan medføre store besparelser og forenkling. Imidlertid kan det blive vanskeligere for annoncører, der udsender målrettede onlinereklamer, at indhente samtykke, hvis en stor del af brugerne vælger indstillingen "afvis tredjepartscookies". Samtidig fratager den centraliserede indhentning af samtykke ikke webstedsoperatører muligheden for at opnå godkendelse ved hjælp af individuelle anmodninger til slutbrugerne og således bevare deres nuværende forretningsmodel. Der vil

opstå yderligere omkostninger for nogle udbydere af browsere eller lignende software, da de vil være nødt til at sørge for privatlivsbeskyttende indstillinger.

Den eksterne undersøgelse har opstillet tre forskellige gennemførelsesscenarier for løsningsmodel 3, alt afhængigt af hvem der etablerer dialogboksen mellem en bruger, der har valgt indstillingen "afvis tredjepartscookies" eller "ingen sporing", og de websteder, som denne bruger besøger, og som gerne vil have brugeren til at genoverveje sit valg. Denne tekniske opgave kan varetages af følgende parter: 1) software såsom internetbrowsere, 2) den tredjepart, der foretager sporingen, 3) de enkelte websteder (dvs. de informationssamfundstjenester, som brugeren har opsøgt). Løsningsmodel 3 vil føre til samlede besparelser i efterlevelsesomkostningerne set i forhold til referencescenariet på 70 % (948,8 mio. EUR) i det første gennemførelsesscenarie (browserløsningen), der er implementeret i nærværende forslag. Omkostningsbesparelserne ville være lavere i de andre scenarier. Da de samlede besparelser overvejende skyldes et meget betydeligt fald i antallet af berørte virksomheder, vil de forventede efterlevelsesomkostninger for den enkelte virksomhed – i gennemsnit – være højere end i dag.

3.5. Målrettet regulering og forenkling

De politiske tiltag, der foreslås i den foretrukne løsningsmodel, opfylder målet om forenkling og begrænsning af den administrative byrde i overensstemmelse med resultaterne af Refit-evalueringen og udtalelsen fra Refit-platformen[17].

Refit-platformen har fremsat tre sæt anbefalinger for Kommissionen:

– Beskyttelsen af borgernes privatliv bør styrkes, ved at e-databeskyttelsesdirektivet bringes i overensstemmelse med den generelle forordning om databeskyttelse.

– Beskyttelsen af borgerne mod uanmodet markedsføring bør gøres mere effektiv ved at udvide undtagelserne fra samtykkereglen vedrørende cookies.

– Kommissionen bør gribe ind over for problemer med gennemførelsen på nationalt plan og fremme udvekslingen af bedste praksis blandt medlemsstaterne.

Hovedpunkterne i forslaget er:

– Teknologineutrale definitioner, der vil kunne dække nye tjenester og teknologier for at sikre, at forordningen er fremtidssikret.

– Bestemmelserne om sikkerhed ophæves for at undgå overlapning i lovgivningen.

– Anvendelsesområdet præciseres for at bidrage til at udrydde/begrænse risikoen for, at reglerne gennemføres forskelligt i medlemsstaterne (punkt 3 i udtalelsen).

– Samtykkereglen om brug af cookies og andre identifikatorer præciseres og forenkles som forklaret i afsnit 3.1 og 3.4 (punkt 2 i udtalelsen).

– Tilsynsmyndighederne er de samme som de myndigheder, der skal håndhæve den generelle forordning om databeskyttelse, og sammenhængsmekanismen i den generelle forordning om databeskyttelse finder anvendelse.

3.6. Indvirkning på de grundlæggende rettigheder

Forslaget har til formål at styrke beskyttelsen af privatlivets fred og personoplysninger, der behandles i forbindelse med elektronisk kommunikation, i overensstemmelse med artikel 7 og 8 i chartret om Den Europæiske Unions grundlæggende rettigheder, samt at øge

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

retssikkerheden. Forslaget supplerer og præciserer den generelle forordning om databeskyttelse. En effektiv beskyttelse af kommunikationshemmeligheden er afgørende for udøvelsen af ytrings- og informationsfriheden og andre beslægtede rettigheder, såsom retten til beskyttelse af personoplysninger og retten til tanke-, samvittigheds- og religionsfrihed.

4. VIRKNINGER FOR BUDGETTET

Forslaget har ingen virkninger for Unionens budget.

5. ANDRE FORHOLD

5.1. Planer for gennemførelsen og foranstaltninger til overvågning, evaluering og rapportering

Kommissionen vil overvåge anvendelsen af forordningen og forelægge en rapport om evalueringen for Europa-Parlamentet og Rådet og Det Europæiske Økonomiske og Sociale Udvalg hvert tredje år. I disse rapporter, der vil blive offentliggjort, vil der blive gjort rede for, hvordan forordningen anvendes og håndhæves i praksis.

5.2. Nærmere redegørelse for de enkelte bestemmelser i forslaget

Kapitel I indeholder de generelle bestemmelser: Genstand (artikel 1), anvendelsesområde (artikel 2 og 3) og definitioner, herunder henvisninger til relevante definitioner fra andre EU-instrumenter, herunder den generelle forordning om databeskyttelse.

Kapitel II indeholder de centrale bestemmelser, som sikrer fortroligheden af elektronisk kommunikation (artikel 5), og fastsætter, til hvilke begrænsede formål elektroniske kommunikationsoplysninger må behandles, samt betingelserne for en sådan behandling (artikel 6 og 7). Kapitlet indeholder også bestemmelser, der har til formål at beskytte terminaludstyr ved i) at sikre integriteten af de oplysninger, der opbevares i det, og ii) at beskytte oplysninger, der udsendes af terminaludstyr, da disse kan muliggøre identifikation af slutbrugeren (artikel 8). Endelig fastsætter artikel 9 nærmere bestemmelser om indhentning af samtykke fra slutbrugerne, der udgør et centralt retligt grundlag i denne forordning, idet der udtrykkeligt henvises til definitionen af samtykke og betingelserne herfor i den generelle forordning om databeskyttelse, mens artikel 10 indfører en forpligtelse for udbydere af software, der muliggør elektronisk kommunikation, til at hjælpe slutbrugerne til at træffe formålstjenlige valg om privatlivsindstillingerne. Artikel 11 indeholder nærmere bestemmelser om, til hvilke formål og under hvilke betingelser medlemsstaterne kan indskrænke de ovennævnte bestemmelser.

Kapitel III omhandler slutbrugernes ret til at have kontrol med afsendelse og modtagelse af elektronisk kommunikation med henblik på at beskytte deres privatliv: i) slutbrugernes ret til at forhindre visning af opkaldende nummer for at sikre anonymitet (artikel 12), samt begrænsningerne i denne ret (artikel 13); og ii) en forpligtelse for udbydere af offentligt tilgængelig nummerbaseret interpersonel kommunikation til at give mulighed for at begrænse modtagelsen af uønskede opkald (artikel 14). Dette kapitel fastsætter også betingelserne for opførelse af slutbrugere i offentligt tilgængelige fortegnelser (artikel 15) og de betingelser, hvorunder der kan foretages uanmodede henvendelser med henblik på direkte markedsføring (artikel 17). Det vedrører desuden sikkerhedsrisici og fastsætter krav om, at udbydere af elektroniske kommunikationstjenester advarer brugerne i tilfælde af en særlig risiko, der kan bringe sikkerheden i deres net og tjenester i fare. Kravene vedrørende sikkerhed i den generelle forordning om databeskyttelse og i den europæiske kodeks for elektronisk kommunikation finder anvendelse på udbydere af elektroniske kommunikationstjenester.

Kapitel IV indeholder bestemmelser om tilsyn og håndhævelse af denne forordning, som overlades til de tilsynsmyndigheder, der har ansvar for håndhævelsen af den generelle forordning om databeskyttelse, i betragtning af den tætte forbindelse mellem de generelle spørgsmål om databeskyttelse og kommunikationshemmeligheden (artikel 18). Det Europæiske Databeskyttelsesråds beføjelser udvides (artikel 19), og samarbejds- og sammenhængsmekanismen i den generelle forordning om databeskyttelse finder anvendelse i tilfælde af grænseoverskridende spørgsmål vedrørende denne forordning (artikel 20).

Kapitel V indeholder bestemmelser om de forskellige retsmidler, der er til rådighed for slutbrugerne (artiklerne 21 og 22), og de sanktioner, der kan pålægges (artikel 24), herunder de generelle betingelser for pålæggelse af administrative bøder (artikel 23).

Kapitel VI vedrører vedtagelsen af delegerede retsakter og gennemførelsesretsakter i overensstemmelse med traktatens artikel 290 og 291.

Endelig indeholder kapitel VII de afsluttende bestemmelser i forordningen: ophævelse af e-databeskyttelsesdirektivet, tilsyn og evaluering, ikrafttræden og anvendelse. I forbindelse med revisionen vil Kommissionen bl.a. vurdere, om en særskilt retsakt er fortsat nødvendig set i lyset af den retlige, tekniske og økonomiske udvikling og under hensyntagen til den første evaluering af forordning (EU) 2016/679, som skal foreligge senest den 25. maj 2020.

2017/0003 (COD)

Forslag til

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING

om respekt for privatliv og beskyttelse af personoplysninger i forbindelse med elektroniske kommunikation og om ophævelse af direktiv 2002/58/EF (forordning om databeskyttelse inden for elektronisk kommunikation)

(EØS-relevant tekst)

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 16 og 114,

under henvisning til forslag fra Europa-Kommissionen,

efter fremsendelse af udkast til lovgivningsmæssig retsakt til de nationale parlamenter,

under henvisning til udtalelse fra Det Europæiske Økonomiske og Sociale Udvalg[1],

under henvisning til udtalelse fra Regionsudvalget[2],

under henvisning til udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse[3],

efter den almindelige lovgivningsprocedure, og

ud fra følgende betragtninger:

(1) I artikel 7 af Den Europæiske Unions charter om grundlæggende rettigheder ("chartret") beskyttes enhvers ret til respekt for sit privatliv og familieliv, sit hjem og sin kommunikation. Respekt for ens private kommunikation er en væsentlig del af denne rettighed. Fortroligheden af elektronisk kommunikation sikrer, at udvekslingen af oplysninger mellem parter og det eksterne element af denne type kommunikation, herunder hvornår oplysningerne er sendt, hvorfra, og til hvem, ikke åbenbares for andre end de parter, der er involveret i kommunikationen. Fortrolighedsprincippet bør omfatte alle nuværende og fremtidige kommunikationsmidler, herunder telefonopkald, internetadgang, instant messaging-applikationer, e-mail, internettelefonopkald og private beskeder sendt gennem sociale medier.

(2) Indholdet af elektronisk kommunikation kan åbenbare yderst følsomme oplysninger om de fysiske personer, der er involveret i kommunikationen, fra personlige oplevelser og følelser til sygdomstilstande, seksuel orientering og politiske synspunkter, som hvis de åbenbares, vil kunne medføre personlig og social skade, økonomiske tab eller forlegenhed. Ydermere kan metadata afledt fra elektronisk kommunikation også videregive meget følsomme og personlige oplysninger. Disse metadata omfatter, hvilke numre der er ringet til, hvilke websteder der er besøgt, geografisk placering,

[1] EUT C […] af […], s. […].
[2] EUT C […] af […], s. […].
[3] EUT C […] af […], s. […].

tidspunkt, dato og varighed af et foretaget opkald osv., og gør det muligt at drage nøjagtige konklusioner vedrørende privatlivet for de personer, der har været involveret i den elektroniske kommunikation, som f.eks. deres social forhold, deres vaner og hverdagsaktiviteter, deres interesser, deres smag osv.

(3) Elektroniske kommunikationsdata kan også videregive oplysninger om juridiske personer, som f.eks. forretningshemmeligheder eller andre følsomme oplysninger, som har økonomisk værdi. Derfor bør bestemmelserne i denne forordning finde anvendelse på både fysiske og juridiske personer. Endvidere bør denne forordning sikre, at bestemmelserne i Europa-Parlamentets og Rådets forordning (EU) 2016/679[4] også finder anvendelse for slutbrugere, som er juridiske personer. De omfatter bl.a. definitionen af samtykke i forordning (EU) 2016/679. Når der henvises til samtykke fra en slutbruger, herunder juridiske personer, bør denne definition finde anvendelse. Ydermere bør juridiske personer have samme rettigheder som slutbrugere, der er fysiske personer, for så vidt angår tilsynsmyndighederne, og endvidere bør tilsynsmyndighederne i henhold til denne forordning også være ansvarlige for overvågningen af forordningens anvendelse på juridiske personer.

(4) I henhold til artikel 8, stk. 1, i chartret og artikel 16, stk. 1, i traktaten om Den Europæiske Unions funktionsmåde har enhver ret til beskyttelse af personoplysninger, der vedrører den pågældende. I forordning (EU) 216/679 fastsættes regler om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og regler om fri udveksling af personoplysninger. Elektroniske kommunikationsdata kan omfatte personoplysninger som defineret i forordning (EU) 2016/679.

(5) Bestemmelserne i denne forordning præciserer og komplementerer de generelle regler om beskyttelse af personoplysninger, som er fastsat i forordning (EU) 2016/679, for så vidt angår elektroniske kommunikationsdata, der kan betegnes som personoplysninger. Denne forordning sænker derfor ikke beskyttelsesniveauet for fysiske personer i henhold til forordning (EU) 2016/679. Behandling af elektroniske kommunikationsdata foretaget af leverandører af elektroniske kommunikationstjenester bør kun være tilladt i overensstemmelse med denne forordning.

(6) Selv om principperne og de vigtigste bestemmelser i Europa-Parlamentets og Rådets direktiv 2002/58/EF[5] fortsat er fornuftige, har direktivet ikke helt fulgt med den teknologiske og markedsmæssige udvikling, hvilket fører til en usammenhængende eller utilstrækkelig beskyttelse af privatlivets fred og fortrolighed i forbindelse med elektronisk kommunikation. Denne udvikling omfatter indtræden på markedet af elektroniske kommunikationstjenester, som set fra et forbrugerperspektiv kan erstatte traditionelle tjenester, men som ikke skal overholde de samme regler. En anden udvikling vedrører nye teknikker, som gør det muligt at overvåge slutbrugernes onlineadfærd, hvilket ikke er omfattet af direktiv 2002/58/EF. Direktiv 2002/58/EF bør derfor ophæves og erstattes af nærværende forordning.

---

[4] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1-88).

[5] Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktivet om databeskyttelse inden for elektronisk kommunikation) (EFT L 201 af 31.7.2002, s. 37).

(7) Det bør være tilladt for medlemsstaterne inden for rammerne af nærværende forordning at bevare eller indføre nationale bestemmelser, som yderligere præciserer og tydeliggør anvendelsen af reglerne i nærværende forordning med henblik på at sikre effektiv anvendelse og fortolkning af disse regler. Derfor bør den skønsmargin, som medlemsstaterne har i den forbindelse, tage hensyn til balancen mellem beskyttelse af privatlivets fred og personoplysninger og elektroniske kommunikationsdatas fri bevægelighed.

(8) Nærværende forordning bør finde anvendelse på leverandører af elektroniske kommunikationstjenester, på leverandører af offentligt tilgængelige fortegnelser og på leverandører af software, som muliggør elektronisk kommunikation, herunder søgning og fremvisning af oplysninger på internettet. Denne forordning bør også finde anvendelse på fysiske og juridiske personer, der anvender elektroniske kommunikationstjenester til at sende kommercielle direkte markedsføringsmeddelelser eller til at indsamle oplysninger om eller lagret på slutbrugerens terminaludstyr.

(9) Denne forordning bør finde anvendelse på elektroniske kommunikationsdata, der behandles i forbindelse med levering og anvendelse af elektroniske kommunikationstjenester i Unionen, uanset om behandlingen finder sted i Unionen eller ej. For ikke at snyde slutbrugerne i Unionen for effektiv beskyttelse, bør forordningen også finde anvendelse på elektroniske kommunikationsdata, der behandles i forbindelse med levering af elektroniske kommunikationstjenester uden for Unionen til slutbrugere i Unionen.

(10) Radioudstyr og tilhørende software der bringes i omsætning på Unionens indre marked, skal overholde Europa-Parlamentets og Rådets direktiv 2014/53/EU[6]. Denne forordning bør ikke påvirke anvendelsen af eventuelle andre krav i direktiv 2014/53/EU eller Kommissionens beføjelser til at vedtage delegerede retsakter i henhold til direktiv 2014/53/EU, hvoraf det kræves, at specifikke radioudstyrskategorier eller -klasser sikrer, at slutbrugerens personoplysninger og privatliv er beskyttet.

(11) Tjenester der bruges til at kommunikere, og de tekniske metoder til at sikre dette, har udviklet sig meget. I stedet for traditionelle taletelefonitjenester, tekstbeskeder (sms) og e-mailtjenester anvender slutbrugerne i stigende grad funktionelt tilsvarende onlinetjenester som f.eks. internettelefoni, beskedtjenester og webbaserede e-mailtjenester. For at sikre en effektiv og ens beskyttelse af slutbrugere, når de anvender funktionelt tilsvarende tjenester, anvendes den definitionen af elektroniske kommunikationstjenester, som er fastsat i [Europa-Parlamentets og Rådets direktiv om en europæiske kodeks for elektronisk kommunikation[7]] i denne forordning. Denne definition omfatter ikke kun internetadgangstjenester og tjenester, som helt eller delvis består i overføring af signaler, men også interpersonelle kommunikationstjenester, som kan være nummerbaserede, som f.eks. internettelefoni, beskedtjenester og webbaserede e-mailtjenester. Beskyttelse af kommunikationshemmeligheden er også væsentlig for interpersonelle kommunikationstjenester, som understøtter andre tjenester, og derfor bør denne type tjenester, der også har til formål at kommunikere, være omfattet af denne forordning.

---

6 Europa-Parlamentets og Rådets direktiv 2014/53/EU af 16. april 2014 om harmonisering af medlemsstaternes love om tilgængeliggørelse af radioudstyr på markedet og om ophævelse af direktiv 1999/5/EF (EUT L 153 af 22.5.2014, s. 62).

7 Kommissionens forslag til Europa-Parlamentets og Rådets direktiv om en europæisk kodeks for elektronisk kommunikation (omarbejdning) (COM/2016/0590 final - 2016/0288 (COD)).

(12) Netforbundne apparater og maskiner kommunikerer i stadig større grad med hverandre ved hjælp af elektroniske kommunikationsnet (tingenes internet). Transmission af kommunikation mellem maskiner omfatter overføring af signaler via et net, og det udgør derfor sædvanligvis en elektronisk kommunikationstjeneste. For at sikre fuld beskyttelse af retten til privatlivets fred og kommunikationshemmelighed samt for at fremme et sikkert tingenes internet, som man kan have tillid til, på det digitale indre marked, er der behov for at præcisere, at denne forordning finder anvendelse på videregivelse af kommunikation mellem maskiner. Derfor bør princippet om kommunikationshemmelighed, som er bevaret i denne forordning, finde anvendelse på transmission af kommunikation mellem maskiner. Der kan også vedtages specifikke sikkerhedsmekanismer i henhold til sektorspecifik lovgivning, som f.eks. direktiv 2014/53/EU.

(13) Udviklingen af hurtige og effektive trådløse teknologier har bidraget til øget adgang til offentlig internetadgang gennem trådløse net, som kan tilgås af alle i offentlige og halvprivate områder, som f.eks. "hotspots" forskellige steder i byer, stormagasiner, indkøbscentre og på hospitaler. I det omfang disse kommunikationsnet tilbydes til en udefineret gruppe af slutbrugere bør fortroligheden af den kommunikation, der sendes gennem sådanne net, beskyttes. Det forhold, at trådløse elektroniske kommunikationstjenester kan understøtte andre tjenester, bør ikke være til hinder for, at kommunikationsdata beskyttes eller at denne forordning finder anvendelse. Forordningen bør derfor finde anvendelse på elektroniske kommunikationsdata, der anvender elektroniske kommunikationstjenester og offentlige kommunikationsnet. Forordningen bør derimod ikke finde anvendelse på lukkede grupper af slutbrugere, som f.eks. virksomhedsnet, hvor adgangen er begrænset til personer, som er tilknyttet virksomheden.

(14) Elektroniske kommunikationsdata bør defineres på en så tilstrækkeligt omfattende og teknologineutral måde, at enhver oplysning om sendt eller udvekslet indhold (elektronisk kommunikationsindhold) og oplysninger om slutbrugeren af de elektroniske kommunikationstjenester kan behandles med henblik på at videresende, distribuere eller muliggøre udveksling af elektronisk kommunikationsindhold, herunder data til at spore og identificere kilden til og modtageren af en kommunikation, geografisk placering og dato, tid, varighed og kommunikationstypen. Uanset om signaler eller tilhørende data overføres ved hjælp af trådforbindelse, radiobølger, lyslederteknik eller elektromagnetiske midler, herunder satellitnet, kabelnet, jordbaserede fastnet (kredsløbs- og pakkekoblede, herunder i internettet) og mobilnet, samt elkabelsystemer, bør de data, der har at gøre med sådanne signaler, betragtes som elektroniske kommunikationsmetadata og følgelig være omfattet af bestemmelserne i denne forordning. Elektroniske kommunikationsmetadata kan omfatte oplysninger, som er en del af abonnementet på en tjeneste, hvis disse oplysninger behandles med henblik på at videresende, distribuere eller muliggøre udveksling af elektronisk kommunikationsindhold.

(15) Elektroniske kommunikationsdata bør behandles fortroligt. Det betyder, at indblanding i videresendelsen af elektroniske kommunkationsdata, uanset om dette sker ved menneskelig indgriben eller ved maskiners automatiske behandling, er forbudt uden samtykke fra alle de kommunikerende parter. Forbuddet mod at opfange kommunikationsdata bør finde anvendelse under overføringen af disse, dvs. indtil den modtager, som den elektroniske kommunikation er rettet til, har modtaget den. Opfangning af elektroniske kommunikationsdata kan f.eks. finde sted, hvis andre end de kommunikerende parter aflytter opkald, læser, skanner eller opbevarer indhold fra

elektronisk kommunikation eller tilhørende metadata med andre formål end at gennemføre kommunikationen. Opfangning finder også sted, når tredjeparter overvåger, hvilke websteder der er besøgt, hvornår besøgene har fundet sted, interaktion med andre osv. uden den pågældende slutbrugers samtykke. Efterhånden som teknologien har udviklet sig, er de tekniske muligheder for at opfange data blevet flere. Mulighederne strækker sig fra installation af udstyr, der indsamler data fra terminaludstyr i udvalgte områder, som f.eks. de såkaldte IMSI-catchere (Internationale Mobile Subscriber Identity), til programmer og teknikker, der i al hemmelighed overvåger internetvaner med henblik på at skabe profiler for slutbrugere. Andre eksempler på dataopfangning omfatter nyttelastdata eller indholdsdata fra ukrypterede trådløse net og routere, herunder internetvaner, uden slutbrugerens samtykke.

(16) Det er ikke hensigten, at forbuddet mod at lagre oplysninger skal forbyde nogen automatisk, mellemliggende og kortvarig lagring af disse oplysninger, når blot lagringen udelukkende sker med henblik på at gennemføre transmissionen i de elektroniske kommunikationsnet. Det bør ikke forhindre hverken behandlingen af elektroniske kommunikationsdata, som sikrer elektroniske kommunikationstjenesters sikkerhed og kontinuitet, herunder kontrol af sikkerhedstrusler som forekomsten af malware, eller behandlingen af metadata til at opfylde de nødvendige krav til tjenestekvalitet, som f.eks. latency, jitter osv.

(17) Behandlingen af elektroniske kommunikationsdata kan være til gavn for virksomheder, forbrugere og samfundet som helhed. I forhold til direktiv 20002/58/EF udvider denne forordning leverandører af elektroniske kommunikationstjenesters mulighed for at behandle elektroniske kommunikationsmetadata med baggrund i slutbrugernes samtykke. Slutbrugere finder det imidlertid meget vigtigt, at deres kommunikation er fortrolig, herunder deres onlineaktiviteter, og de vil kontrollere brug af elektroniske kommunikationsdata til andre formål end til at gennemføre kommunikationen. Derfor bør denne forordning kræve, at leverandører af elektroniske kommunikationstjenester indhenter slutbrugernes samtykke til at behandle elektroniske kommunikationsmetadata, som bør omfatte data om apparaters placering, der genereres med henblik på at give og bevare adgang og forbindelse til en tjeneste. Lokaliseringsdata, der generes i forbindelse med andet end levering af elektroniske kommunikationstjenester, bør ikke betragtes som metadata. Eksempler på kommerciel anvendelse af elektroniske kommunikationsmetadata hos leverandører af elektroniske kommunikationstjenester kan omfatte levering af "heatmaps", en geografisk fremstilling af data, hvor farver bruges til at angive, at der findes personer i området. For at kunne vise trafikbevægelserne i visse retninger i løbet af en bestemt periode, er det nødvendigt med en identifikator, der kan forbinde personers positioner i bestemte intervaller. Denne identifikator ville mangle, hvis der blev indsamlet anonyme data, og derfor ville disse bevægelser ikke kunne vises. Denne type brug af elektroniske kommunikationsmetadata kunne f.eks. være til gavn for offentlige myndigheder og offentlige transportvirksomheder i forbindelse med beslutninger om, hvor ny infrastruktur skal opføres baseret på brugen af og presset på eksisterende infrastruktur. Hvis det er sandsynligt, at en type behandling af elektroniske kommunikationsmetadata, navnlig i form af brug af nye teknologier og under hensyntagen til behandlingens karakter, omfang, sammenhæng og formål, vil medføre en højere risiko for fysiske personers rettigheder og frihedsrettigheder, bør der gennemføres en konsekvensanalyse vedrørende databeskyttelse, og eventuelt en høring ved tilsynsmyndigheden forud for behandlingen, jf. artikel 45 og 36 i forordning (EU) 2016/679.

(18) Slutbrugere kan give samtykke til behandling af deres metadata med henblik på at modtage specifikke tjenester som f.eks. beskyttelse mod bedrageri (gennem analyse i realtid af forbrugsdata, placering og kundekonti). I den digitale økonomi leveres tjenester ofte til gengæld for andre modydelser end penge, f.eks. ved at brugerne bliver udsat for reklamer. I denne forordning bør en slutbrugers samtykke, uanset om denne er en fysisk eller en juridisk person, have samme betydning og være underlagt samme betingelser som den registreredes samtykke i henhold til forordning (EU) 2016/679. Basal bredbåndadgang til internettjenester og talekommunikationstjenester bør anses for at være grundlæggende tjenester, som gør individer i stand til at kommunikere og få gavn af fordelene ved den digitale økonomi. Samtykke til behandling af data fra internettet eller brug af talekommunikation er ugyldigt, hvis den registrerede ikke har et reelt og frit valg eller ikke kan afvise eller tilbagetrække sit samtykke, uden at det er til skade for den pågældende.

(19) Indholdet af elektronisk kommunikation vedrører kernen i den grundlæggende ret til respekt for privatliv og familieliv, hjem og kommunikation, som er beskyttet i medfør af chartrets artikel 7. Indblanding i indholdet af elektronisk kommunikation bør kun være tilladt på meget klart definerede betingelser, af hensyn til specifikke formål og den tilstrækkeligt beskyttet mod misbrug. Denne forordning giver leverandører af elektroniske kommunikationstjenester mulighed for at behandle elektroniske kommunikationsdata i transit med informeret samtykke fra alle de pågældende slutbrugere. Leverandører må f.eks. tilbyde tjenester, som medfører skanning af e-mails med henblik på at fjerne foruddefineret materiale. På grund af følsomheden af kommunikationernes indhold antages det i denne forordning, at behandling af indholdsdata vil medføre højere risiko for fysiske personers rettigheder og frihedsrettigheder. Når denne type data behandles, bør leverandøren af den elektroniske kommunikationstjeneste altid høre tilsynsmyndigheden inden behandlingen. Denne høring bør ske i overensstemmelse med artikel 36, stk. 2 og 3, i forordning (EU) 2016/679. Denne antagelse omfatter ikke behandling af indholdsdata med henblik på at levere en tjeneste til slutbrugeren, som denne har bedt om, hvis slutbrugeren har givet samtykke til behandlingen, og den udføres med henblik på de formål og den varighed, der er strengt nødvendig og hensigtsmæssig til levering af en sådan tjeneste. Efter det elektroniske kommunikationsindhold er blevet sendt af slutbrugeren og modtaget af den eller de tiltænkte slutbruger eller slutbrugere, må det lagres eller opbevares af slutbrugeren, slutbrugerne eller en tredjepart, der er betroet af dem til at lagre eller opbevare sådanne data. Enhver behandling af dataene skal leve op til forordning (EU) 2016/679.

(20) Terminaludstyr tilhørende slutbrugere af elektroniske kommunikationsnet og eventuelle oplysninger vedrørende brugen af dette terminaludstyr er, uanset om det opbevares på eller udsendes af udstyret, om oplysninger udbedes af eller behandles med henblik på at gøre udstyret i stand til at opnå forbindelse til et andet apparat og eller andet netværksudstyr, en del af slutbrugernes privatsfære, som skal beskyttelse i henhold til Den Europæiske Unions charter om grundlæggende rettigheder og den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder. Eftersom dette udstyr indeholder eller behandler oplysninger, som kan afsløre detaljer om en persons følelsesmæssige, politiske og sociale indstilling, herunder meddelelsers indhold, billeder, fysiske personers placering ved brug af apparatets GPS-funktioner, kontaktlister og andre oplysninger, som allerede er lagret på apparatet, kræver oplysninger vedrørende dette udstyr øget beskyttelse af privatlivets fred. Endvidere kan såkaldt spionsoftware, såkaldte web bugs, skjulte identifikatorer, sporingscookies og andre tilsvarende uønskede sporingsværktøjer

komme ind i slutbrugerens terminaludstyr uden dennes viden for at skaffe adgang til oplysninger, for at lagre skjulte oplysninger eller for at spore brugerens aktiviteter. Der kan også fjernindsamles oplysninger vedrørende slutbrugerens apparat med henblik på identificering og sporing ved hjælp af teknikker som det såkaldte "device fingerprinting", hvilket ofte sker uden slutbrugerens viden, og det kan alvorligt krænke disse slutbrugeres privatliv. Teknikker som i det skjulte overvåger slutbrugeres handlinger, f.eks. ved at spore deres aktiviteter på internettet eller placeringen af deres terminaludstyr, eller som undergraver funktionsevnen af slutbrugerens terminaludstyr, udgør en alvorlig trussel for slutbrugeres privatliv. Derfor bør indblanding i slutbrugerens terminaludstyr kun være tilladt med slutbrugerens samtykke og med specifikke gennemsigtige mål for øje.

(21) Undtagelser fra forpligtelsen til at indhente samtykke med henblik på at gøre brug af behandlings- og lagringsfunktionerne i terminaludstyr eller på at tilgå oplysninger, som er lagret på terminaludstyr, bør være begrænset til situationer, der ikke omfatter nogen eller kun en meget begrænset krænkelse af privatlivets fred. Der bør f.eks. ikke kræves samtykke til at foretage teknisk lagring eller til at give adgang, som er strengt nødvendig og hensigtsmæssig med det legitime formål at muliggøre brugen af en specifik tjeneste, som slutbrugeren udtrykkeligt har bedt om. Dette kan f.eks. gælde lagring af cookies af en sessions varighed fra et websted for at holde styr på slutbrugerens input ved udfyldelse af onlineformularer over flere sider. Cookies kan også være et legitimt og brugbart værktøj til f.eks. at måle trafikken på et websted. Udbydere i informationssamfundet, der beskæftiger sig med kontrol af konfigurationer med henblik på at levere en tjeneste i overensstemmelse med slutbrugerens indstillinger og logning af det forhold, at slutbrugerens apparat ikke er i stand til at modtage det indhold, som slutbrugeren har bedt om, bør ikke forstås som adgang til et apparat eller brug af apparatets behandlingskapacitet.

(22) Metoderne til at oplyse slutbrugerne og indhente deres samtykke bør være så brugervenlige som muligt. På grund af den allestedsnærværende brug af sporingscookies og andre sporingsteknikker anmodes slutbrugerne i stadigt større omfang om at give samtykke til at lagre sådanne cookies på deres terminaludstyr. Som følge heraf bliver slutbrugerne overbebyrdet med anmodninger om samtykke. Brugen af tekniske midler til at indhente samtykke, f.eks. gennem gennemsigtige og brugervenlige indstillinger, kan hjælpe med at løse dette problem. Forordningen bør derfor give mulighed for at give samtykke ved hjælp af hensigtsmæssig indstilling af en browser eller en anden applikation. De valg, som slutbrugerne træffer, når de foretager deres generelle privatlivsindstillinger i en browser eller en anden applikation, bør være bindende og kunne gøres gældende over for eventuelle tredjeparter. Internetbrowsere er en type softwareprogram, der giver mulighed for at hente og fremvise oplysninger fra internettet. Andre typer applikationer, som f.eks. applikationer, der giver mulighed for at ringe og sende beskeder eller for GPS-navigation, har samme funktionalitet. Internetbrowsere formidler meget af, hvad der sker mellem slutbrugeren og et websted. Set ud fra dette perspektiv har internetbrowsere en god mulighed for at spille en aktiv rolle i at hjælpe slutbrugeren med at kontrollere flowet af oplysninger til og fra terminaludstyret. Internetbrowsere kan bruges som dørvogtere og hjælpe slutbrugerne med at forhindre, at oplysninger fra deres terminaludstyr (f.eks. smartphones, tablets eller computere) tilgås eller lagres.

(23) Principperne om databeskyttelse gennem design og gennem standardindstillinger blev kodificeret i artikel 25 i forordning (EU) 2016/679. Standardindstillingerne for cookies er på nuværende tidspunkt i de fleste browsere angivet til "accepter alle cookies".

Derfor bør leverandører af software, som gør det muligt at hente og fremvise oplysninger fra internettet, være forpligtet til at konfigurere softwaren således, at den giver mulighed for at forhindre tredjeparter i at lagre oplysninger på terminaludstyret, hvilket ofte gengives som "afvis cookies fra tredjeparter". Slutbrugere bør have adgang til et sæt privatlivsindstillinger, der strækker sig fra højere sikkerhed (f.eks. "accepter aldrig cookies") til lavere (f.eks. "accepter altid cookies"), men også har et mellemniveau (f.eks. "afvis cookies fra tredjeparter" eller "accepter kun førstepartscookies"). Disse privatlivsindstillinger bør præsenteres på en let synlig og forståelig måde.

(24) For at internetbrowsere skal kunne indhente slutbrugerens samtykke som defineret i forordning (EU) 2016/679 til f.eks. lagring af sporingscookies fra tredjeparter, bør de bl.a. kræve en klar bekræftelse fra terminaludstyrets slutbruger, som betyder, at slutbrugeren udtrykker sin frivillige, specifikke, informerede og utvetydige enighed i, at sådanne cookies lagres og kan tilgås på terminaludstyret. En sådan handling kan betragtes som bekræftende, hvis slutbrugeren f.eks. aktivt skal vælge "accepter cookies fra tredjeparter" for at bekræfte deres enighed i valget, og denne gives de nødvendige oplysninger til at kunne træffe valget. Med henblik herpå er det nødvendigt at kræve af softwareleverandører, der muliggør adgang til internettet, at slutbrugerne i installationsøjeblikket informeres om muligheden for at vælge mellem de forskellige privatlivsindstillinger, og at de foretager et valg. Oplysningerne bør ikke afskrække slutbrugerne fra at vælge strengere privatlivsindstillinger, og de bør omfatte relevant information om de risici, der er forbundet med at tillade lagring af tredjepartscookies på computeren, herunder indsamling af registreringer over tid af en persons browsinghistorik og anvendelsen af sådanne registreringer til at målrette reklamer. Internetbrowsere opfordres til at gøre det let for slutbrugere at ændre privatlivsindstillingerne når som helst under brug og give brugeren mulighed for at gøre undtagelser eller lave en positivliste over visse websteder eller specificere, for hvilke websteder tredjepartscookies altid eller aldrig er tilladt.

(25) Adgang til elektroniske kommunikationsnet kræver, at der jævnligt udsendes bestemte datapakker for at opdage eller bevare en forbindelse til netværket eller til andre apparater på netværket. Endvidere skal apparater have tildelt en unik adresse, så de kan identificeres på netværket. Trådløse standarder og mobiltelefonstandarder involverer ligeledes udsendelse af aktive signaler, som indeholder unikke identifikatorer som f.eks. MAC-adresse, IMEI-nummer (international identitet for mobilstationsudstyr), IMSI-nummer osv. En enkelt trådløs basisstation (dvs. en sender og modtager) som f.eks. et trådløst adgangspunkt, har et specifikt område, inden for hvilket sådanne oplysninger kan opfanges. Der er opstået tjenesteudbydere, som tilbyder sporingstjenester baseret på skanning af oplysninger vedrørende udstyr med diverse funktioner, herunder optælling af personer, indsamling af oplysninger om, hvor mange der venter i kø, registrering af antallet af personer i et specifikt område, osv. Disse oplysninger kan bruges til andre mere nærgående formål, som f.eks. at sende reklamer med individualiserede tilbud til slutbrugere, når de går ind i butikker. Selv om nogle af funktionerne ikke medfører store private risici, er der andre, der gør, f.eks. dem som omfatter sporing af personer over tid, herunder gentagne besøg til specifikke steder. Leverandører, der anvender en sådan praksis, bør på fremtrædende steder i udkanten af det pågældende område informere slutbrugerne herom, inden de går ind i det afgrænsede område, hvor denne teknologi anvendes, om formålet med indsamlingen af oplysninger, om hvem der er ansvarlig for den og om eventuelle foranstaltninger, slutbrugeren af terminaludstyret kan træffe med henblik på at minimere eller standse indsamlingen af oplysninger. Der bør gives yderligere

oplysninger, hvis der indsamles personoplysninger i henhold til artikel 13 i forordning (EU) 2016/679.

(26) Når behandling af elektroniske kommunikationsdata på vegne af leverandører af elektroniske kommunikationstjenester omfattet af denne forordnings anvendelsesområde, bør forordningen give Unionen og medlemsstaterne mulighed for på særlige betingelser ved lov at begrænse visse forpligtelser og rettigheder, når en sådan begrænsning udgør en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund for at sikre bestemte offentlige interesser, herunder den nationale sikkerhed, forsvaret, den offentlige sikkerhed og forebyggelse, efterforskning, afsløring eller retsforfølgning af strafbare handlinger eller fuldbyrdelse af strafferetlige sanktioner, herunder beskyttelse mod og forebyggelse af trusler mod den offentlige sikkerhed og andre af Unionens eller en medlemsstats samfundsinteresser, navnlig Unionens eller en medlemsstats væsentlige økonomiske eller finansielle interesser, eller kontrol-, tilsyns- eller reguleringsfunktioner, der er forbundet med offentlig myndighedsudøvelse for sådanne interesser. Dette direktiv bør derfor ikke berøre medlemsstaternes mulighed for lovligt at opfange elektronisk kommunikation eller træffe andre foranstaltninger, hvis de er nødvendige og forholdsmæssige for at sikre ovennævnte offentlige interesser i overensstemmelse med Den Europæiske Unions charter om grundlæggende rettigheder og den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder som fortolket af Den Europæiske Unions Domstol og Den Europæiske Menneskerettighedsdomstol. Leverandører af elektroniske kommunikationstjenester bør sørge for hensigtsmæssige procedurer, der letter legitime anmodninger fra de kompetente myndigheder, og hvor det er relevant også under hensyntagen til den rolle, den i artikel 3, stk. 3, udpegede repræsentant spiller.

(27) For så vidt angår nummervisningsfunktionen er det nødvendigt at beskytte den opkaldende parts ret til at forhindre, at det nummer, hvorfra opkaldet foretages, identificeres, og den opkaldte parts ret til at afvise opkald fra uidentificerede numre. Visse slutbrugere, herunder særligt hjælpetjenester og lignende, har en interesse i at sikre deres opkald fuld anonymitet. For så vidt angår identifikation af opkaldte numre er det nødvendigt at beskytte den opkaldte parts ret til og legitime interesse i at suspendere identifikationen af det nummer, som den opkaldende part faktisk er tilsluttet.

(28) Det er i særlige tilfælde berettiget at suspendere en blokering af denne funktion. Slutbrugernes ret til beskyttelse af privatlivets fred med hensyn til nummervisningsfunktionen bør begrænses, når dette er nødvendigt for at spore generende opkald, og med hensyn til nummervisningsfunktionen og lokaliseringsdata, når dette er nødvendigt, for at nødtjenester, som f.eks. eCall, kan udføre deres opgaver så effektivt som muligt.

(29) Der findes teknologi, som på forskellig vis gør leverandører af elektroniske kommunikationstjenester i stand til at begrænse slutbrugeres modtagelse af uønskede opkald, herunder "tavse opkald" og andre bedrageriske og generende opkald. Leverandører af offentligt tilgængelige nummerbaserede interpersonelle kommunikationstjenester bør anvende denne teknologi og gratis beskytte slutbrugere mod generende opkald. Leverandørerne bør sikre, at slutbrugerne er klar over, at sådanne funktioner findes, f.eks. ved at meddele det på deres websted.

(30) Offentligt tilgængelige fortegnelser over slutbrugere af elektroniske kommunikationstjenester distribueres i vidt omfang. En offentligt tilgængelig

fortegnelse betyder enhver fortegnelse eller tjeneste, der indeholder oplysninger om slutbrugere, som f.eks. telefonnumre (herunder mobiltelefonnumre), e-mailadresser og kontaktoplysninger, og som giver mulighed for at søge i disse. Retten til privatlivets fred og til beskyttelse af fysiske personers personlige oplysninger nødvendiggør, at slutbrugere, som er fysiske personer, anmodes om samtykke før deres personoplysninger opføres i en fortegnelse. Juridiske personers legitime interesser nødvendiggør, at slutbrugere, som er juridiske personer, har ret til, at de data, som vedrører dem, bliver inkluderet i en fortegnelse.

(31) Hvis slutbrugere, som er fysiske personer, samtykker i, at deres data opføres i sådanne fortegnelser, bør de være i stand til på grundlag af deres samtykkeerklæring at bestemme, hvilke personoplysninger der inkluderes i fortegnelsen (f.eks. navn, e-mailadresse, fysisk adresse, brugernavn, telefonnummer). Leverandører af offentligt tilgængelige fortegnelser bør ydermere informere slutbrugerne om formålet med fortegnelsen eller dennes søgefunktion, inden de opføres i fortegnelsen. Slutbrugere bør i samtykkeerklæringen være i stand til at vælge, hvilke kategorier af personoplysninger der kan søges på. De kategorier af personoplysninger, der inkluderes i fortegnelsen, og de kategorier af personoplysninger, hvori der kan søges efter slutbrugerens kontaktoplysninger, bør ikke nødvendigvis være de samme.

(32) I denne forordning menes der med direkte markedsføring enhver form for markedsføring, hvor en fysisk eller juridisk person sender direkte markedsføringsmeddelelser til en eller flere identificerede eller identificerbare slutbrugere ved hjælp af elektroniske kommunikationstjenester. Ud over at tilbyde et produkt eller en tjeneste af kommercielle årsager bør begrebet også omfatte meddelelser afsendt af politiske partier, som kontakter fysiske personer via elektroniske kommunikationstjenester for at fremme deres partier. Det samme bør gælde for meddelelser afsendt af andre nonprofitorganisationer for at hente støtte til organisationens formål.

(33) Der bør indføres sikkerhedsmekanismer til at beskytte slutbrugere mod uanmodede direkte markedsføringsmeddelelser, som krænker slutbrugernes privatliv. Graden af privatlivskrænkelse og gene anses for at være rimelig ens, uanset hvilke af den brede vifte af teknologier og kanaler, der anvendes til at sende disse elektroniske meddelelser, uanset om der anvendes automatiserede opkalds- og kommunikationssystemer, instant messaging-applikationer, e-mails, sms, mms, bluetooth osv. Det er derfor berettiget at kræve, at slutbrugerens samtykke indhentes, før der må sendes kommercielle elektroniske direkte markedsføringsmeddelelser til slutbrugere, således at personer beskyttes effektivt mod krænkelse af deres privatliv, samt at juridiske personers legitime interesser beskyttes. Retssikkerhed og behovet for at sikre, at reglerne beskytter mod uanmodede elektroniske meddelelser i fremtiden retfærdiggør, at der er behov for at definere et enkelt regelsæt, som ikke ændrer sig afhængigt af, hvilken teknologi der anvendes til at aflevere uanmodede meddelelser, men som samtidig garanterer et ens beskyttelsesniveau for alle borgere på tværs af Unionen. Det er imidlertid rimeligt at tillade brugen af e-mailoplysninger i forbindelse med et eksisterende kundeforhold med henblik på at tilbyde lignende produkter eller tjenester. Denne mulighed bør kun gælde for den virksomhed, som har modtaget e-mailoplysningerne i henhold til forordning (EU) 2016/679.

(34) Når slutbrugere har givet deres samtykke til at modtage uanmodede direkte markedsføringsmeddelelser, bør de til enhver tid have mulighed for at trække deres samtykke tilbage på en let måde. For at lette en effektiv håndhævelse af Unionens regler om uanmodede direkte markedføringsmeddelelser er det nødvendigt at forbyde

maskering af identiteter og brug af falske identiteter, falske afsenderadresser eller -numre, når der sendes uanmodede kommercielle direkte markedføringsmeddelelser. Uanmodede markedsføringsmeddelelser bør derfor være lette at genkende som sådanne, og de bør angive identiteten af den juridiske eller fysiske person, der afsender meddelelsen, eller på vegne af hvem den sendes, og de bør endvidere give modtagerne de nødvendige oplysninger til at gøre brug af deres ret til at modsætte sig modtagelsen af flere skriftlige eller mundtlige markedsføringsmeddelelser.

(35) For at gøre det let at trække sit samtykke tilbage bør juridiske og fysiske personer, der sender direkte markedsføringsmeddelelser via e-mail, inkludere et link eller en e-mailadresse, hvor slutbrugerne let kan trække deres samtykke tilbage. Når juridiske og fysiske personer foretager direkte markedsføringsmeddelelser via telefonopkald og via automatiserede opkalds- og kommunikationssystemer, bør der vises et nummer, hvorpå den opkaldende virksomhed kan ringes op, eller en kode, der afspejler det forhold, at der er tale om et markedsføringsopkald.

(36) Direkte markedsføringsopkald, der ikke omfatter brugen af automatiserede opkalds- og kommunikationssystemer, er dyrere for den opkaldende part og pålægger ikke slutbrugeren nogen finansielle omkostninger. Medlemsstaterne bør derfor kunne indføre og/eller bevare nationale systemer, der kun tillader sådanne opkald til slutbrugere, der ikke har frabedt sig dem.

(37) Tjenesteudbydere, som leverer elektroniske kommunikationstjenester, bør informere slutbrugerne om, hvordan de kan sikre deres kommunikation, f.eks. ved at anvende bestemte typer software eller krypteringsteknologi. Kravet om at underrette slutbrugerne om særlige sikkerhedsrisici fritager ikke tjenesteudbyderen for forpligtelsen til for egen regning omgående at træffe passende foranstaltninger til at forebygge nye uforudsete sikkerhedsrisici og genoprette det normale sikkerhedsniveau for tjenesten. Underretning af abonnenten om sikkerhedsrisici bør være gebyrfri. Sikkerheden evalueres på baggrund af artikel 32 i forordning (EU) 2016/679.

(38) For at sikre fuld overensstemmelse med forordning (EU) 2016/679 bør håndhævelsen af bestemmelserne i denne forordning overlades til de myndigheder, der også er ansvarlige for håndhævelsen af bestemmelserne i forordning (EU) 2016/679, og sammenhængsmekanismen i forordning (EU) 2016/679 bør også finde anvendelse i forbindelse med nærværende forordning. Medlemsstaterne bør kunne have mere end én tilsynsmyndighed for at afspejle deres forfatningsmæssige, organisatoriske og administrative struktur. Tilsynsmyndighederne bør også være ansvarlige for overvågningen af forordningens anvendelse på elektroniske kommunikationsdata vedrørende juridiske personer. Sådanne supplerende opgaver bør ikke bringe tilsynsmyndighedens evne til at udføre sine opgaver inden for beskyttelse af personoplysninger i henhold til forordning (EU) 2016/679 og nærværende forordning i fare. Hver tilsynsmyndighed bør tildeles de nødvendige supplerende finansielle og menneskelige ressourcer samt lokaler og infrastruktur til effektivt at kunne udføre sine opgaver i henhold til denne forordning.

(39) Hver tilsynsmyndighed bør på sin egen medlemsstats område have kompetence til at udøve sine beføjelser og varetage de opgaver, der er angivet i denne forordning. For at sikre ensartet tilsyn med og håndhævelse af denne forordning i hele Unionen bør tilsynsmyndighederne have samme opgaver og effektive beføjelser i hver medlemsstat til at indbringe overtrædelser af denne forordning for de retslige myndigheder og deltage i retssager, uden at dette dog indskrænker de retsforfølgende myndigheders beføjelser i henhold til medlemsstaternes nationale ret. Medlemsstaterne og deres

tilsynsmyndigheder opfordres til at tage hensyn til mikrovirksomheders og små og mellemstore virksomheders særlige behov i forbindelse med anvendelsen af denne forordning.

(40) For at styrke håndhævelsen af reglerne i denne forordning bør hver tilsynsmyndighed have beføjelser til at pålægge sanktioner, herunder administrative bøder, for overtrædelser af forordningen i tillæg til eller i stedet for eventuelle andre hensigtsmæssige foranstaltninger i henhold til denne forordning. Denne forordning bør indeholde bestemmelser om overtrædelser og maksimumsbeløb og kriterier for fastsættelse af de tilknyttede administrative bøder, der bør bestemmes af den kompetente tilsynsmyndighed i hvert enkelt tilfælde under hensyntagen til alle relevante omstændigheder i den specifikke situation og med behørig hensyntagen til karakteren, alvoren og varigheden af overtrædelsen og dens konsekvenser og de foranstaltninger, der er truffet for at sikre overholdelse af forpligtelserne i henhold til denne forordning og for at forebygge eller begrænse følgerne af overtrædelsen. Med henblik på at fastsætte bøder i henhold til denne forordning forstås en virksomhed i denne forbindelse som en virksomhed som omhandlet i artikel 101 og 102 i traktaten.

(41) For at opfylde denne forordnings målsætninger, dvs. at beskytte fysiske personers grundlæggende rettigheder og frihedsrettigheder, navnlig deres ret til beskyttelse af personoplysninger, og for at sikre fri udveksling af personoplysninger i Unionen bør beføjelsen til at vedtage retsakter i henhold til artikel 290 i traktaten delegeres til Kommissionen med henblik på at supplere denne forordning. Navnlig bør der vedtages delegerede retsakter vedrørende de oplysninger, der skal fremlægges, herunder standardiserede ikoner, som skal give et let synligt og forståeligt overblik over indsamlingen af oplysninger, som terminaludstyret udsender, oplysningernes formål, den ansvarlige for oplysningerne og eventuelle foranstaltninger, som terminaludstyrets slutbruger kan træffe for at minimere indsamlingen. Delegerede retsakter er også nødvendige for at fastsætte en kode, der kan identificere direkte markedsføringsopkald, herunder opkald foretaget via automatiserede opkalds- og kommunikationssystemer. Det er navnlig vigtigt, at Kommissionen gennemfører relevante høringer, og at disse høringer gennemføres i overensstemmelse med principperne i den interinstitutionelle aftale om bedre lovgivning af 13. april 2016[8]. For at sikre lige deltagelse i forberedelsen af delegerede retsakter modtager Europa-Parlamentet og Rådet alle dokumenter på samme tid som medlemsstaternes eksperter, og deres eksperter har systematisk adgang til møder i Kommissionens ekspertgrupper, der beskæftiger sig med forberedelse af delegerede retsakter. For at sikre ensartede betingelser for gennemførelsen af denne forordning bør Kommissionen endvidere tillægges gennemførelsesbeføjelser, når dette er fastsat i denne forordning. Disse beføjelser bør udøves i overensstemmelse med forordning (EU) nr. 182/2011.

(42) Målet for denne forordning, nemlig at sikre et ensartet niveau for beskyttelse af fysiske og juridiske personer og fri udveksling af elektronisk kommunikation i Unionen, kan ikke i tilstrækkelig grad opfyldes af medlemsstaterne, men kan på grund af handlingens omfang og virkninger bedre nås på EU-plan; Unionen kan derfor vedtage foranstaltninger i overensstemmelse med nærhedsprincippet, jf. artikel 5 i traktaten om Den Europæiske Union. I overensstemmelse med proportionalitetsprincippet, jf. nævnte artikel, går denne forordning ikke ud over, hvad der er nødvendigt for at nå dette mål.

---

[8] Interinstitutionel aftale mellem Europa-Parlamentet, Rådet for Den Europæiske Union og Europa-Kommissionen om bedre lovgivning af 13. april 2016 (EUT L 123 af 12.5.2016, s. 1-14).

(43) Direktiv 2002/58/EF bør ophæves —

VEDTAGET DENNE FORORDNING:

KAPITEL I
GENERELLE BESTEMMELSER

Artikel 1
Genstand

1. I denne forordning fastsættes regler for beskyttelse af fysiske og juridiske personers grundlæggende rettigheder og frihedsrettigheder i forbindelse med levering og anvendelse af elektroniske kommunikationstjenester og navnlig for retten til respekt for privatlivet og kommunikation, samt at der sørges for beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger.

2. Denne forordning sikrer fri bevægelighed for elektroniske kommunikationsdata og elektroniske kommunikationstjenester i Unionen, som hverken begrænses eller forbydes af hensyn til respekten for juridiske og fysiske personers privatliv og kommunikation og beskyttelsen af fysiske personer i forbindelse med behandlingen af personoplysninger.

3. Bestemmelserne i denne forordning præciserer og supplerer forordning (EU) 2016/679 ved at fastsætte specifikke regler for de i stk. 1 og 2 nævnte formål.

Artikel 2
Materielt anvendelsesområde

1. Denne forordning finder anvendelse på behandling af elektroniske kommunikationsdata, der gennemføres i forbindelse med levering og anvendelse af elektroniske kommunikationstjenester og med oplysninger hidrørende fra slutbrugeres terminaludstyr.

2. Forordningen finder ikke anvendelse på:

(a) aktiviteter, som falder uden for EU-rettens anvendelsesområde

(b) medlemsstaternes aktiviteter, der falder inden for anvendelsesområdet for afsnit V, kapitel 2, i traktaten om Den Europæiske Union

(c) elektroniske kommunikationstjenester, som ikke er offentligt tilgængelige

(d) aktiviteter, som foretages af kompetente myndigheder med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod og forebygge trusler mod den offentlige sikkerhed.

3. Behandling af elektroniske kommunikationsdata foretaget af Unionens institutioner, organer, kontorer og agenturer er reguleret i forordning (EU) 00/0000 [ny forordning, som erstatter forordning 45/2001].

4. Denne forordning berører ikke anvendelsen af direktiv 2000/31/EF[9], navnlig reglerne om formidleransvar for tjenesteydere, der er fastsat i artikel 12-15 i nævnte direktiv.

5. Denne forordning berører ikke bestemmelserne i direktiv 2014/53/EU.

[9] Europa-Parlamentets og Rådets direktiv 2000/31/EF af 8. juni 2000 om visse retlige aspekter af informationssamfundstjenester, navnlig elektronisk handel, i det indre marked ("Direktivet om elektronisk handel") (EFT L 178 af 17.7.2000, s. 1-16).

Artikel 3
Territorielt anvendelsesområde og repræsentation

1. Denne forordning finder anvendelse på:

(a) levering af elektroniske kommunikationstjenester til slutbrugere i Unionen, uanset om der kræves betaling af slutbrugeren eller ej

(b) anvendelsen af disse tjenester

(c) beskyttelse af oplysninger vedrørende terminaludstyr tilhørende slutbrugere, der befinder sig i Unionen.

2. Hvis leverandøren af en elektronisk kommunikationstjeneste ikke er etableret i Unionen, udpeger denne skriftligt en repræsentant i Unionen.

3. Repræsentanten skal befinde sig i en af de medlemsstater, hvor slutbrugerne af nævnte elektroniske kommunikationstjenester befinder sig.

4. Repræsentanten skal have beføjelser til at besvare spørgsmål og udlevere oplysninger tillige med eller i stedet for den leverandør, der repræsenteres, til tilsynsmyndigheder og slutbrugere i forbindelse med alle spørgsmål vedrørende behandlingen af elektroniske kommunikationsdata med henblik på at sikre overholdelse af denne forordning.

5. Udpegningen af en repræsentant i henhold til stk. 2 berører ikke eventuelle retlige skridt mod en fysisk eller juridisk person, som behandler elektroniske kommunikationsdata i forbindelse med levering af elektroniske kommunikationstjenester uden for Unionen til slutbrugere i Unionen.

Artikel 4
Definitioner

1. I denne forordning gælder følgende definitioner:

(a) definitionerne i forordning (EU) 2016/679

(b) definitionerne af "elektronisk kommunikationsnet", "elektronisk kommunikationstjeneste", "nummerbaseret interpersonel kommunikationstjeneste", "nummeruafhængig interpersonel kommunikationstjeneste", "slutbruger" og "opkald" i henholdsvis artikel 2, stk. 1, 4, 5, 6, 7, 14 og 21, i [direktiv om en europæisk kodeks for elektronisk kommunikation]

(c) definitionen af "terminaludstyr" i artikel 1, stk. 1, i Kommissionens direktiv 2008/63/EF[10].

2. I forbindelse med stk. 1, litra b), omfatter definitionen af "interpersonelle kommunikationstjenester" tjenester, der muliggør interpersonel og interaktiv kommunikation som en mindre ledsagende funktion, der er uløseligt forbundet med en anden tjeneste.

3. I denne forordning forstås desuden ved:

(a) "elektroniske kommunikationsdata": elektronisk kommunikationsindhold og elektroniske kommunikationsmetadata

[10] Kommissionens direktiv 2008/63/EF af 20. juni 2008 om konkurrence på markederne for teleterminaludstyr (EUT L 162 af 21.6.2008, s. 20-26).

(b) "elektronisk kommunikationsindhold": indhold, der udveksles ved hjælp af elektroniske kommunikationstjenester, som f.eks. nedskrevne eller talte beskeder, videoer, billeder og lyd

(c) "elektroniske kommunikationsmetadata": data behandlet i et elektronisk kommunikationsnet med henblik på at videresende, distribuere eller udveksle elektronisk kommunikationsindhold, herunder data, som anvendes til at spore og identificere kilden til og modtageren af en kommunikation, data vedrørende apparatets placering genereret i forbindelse med levering af elektroniske kommunikationstjenester, dato, tidspunkt, varighed for kommunikationen samt kommunikationstypen

(d) "offentligt tilgængelig fortegnelse": en fortegnelse over slutbrugere af elektroniske kommunikationstjenester, uanset om denne er trykt eller i elektronisk form, som udgives eller gøres tilgængelig for offentligheden eller en del heraf, eventuelt via en nummeroplysningstjeneste

(e) "e-mail": elektronisk meddelelse, der indeholder oplysninger som f.eks. nedskrevne eller talte beskeder, videoer, lyd eller billeder, som er sendt via et elektronisk kommunikationsnet, og som kan lagres i nettet eller på tilhørende computeranlæg eller modtagerens terminaludstyr

(f) "direkte markedsføringsmeddelelse": enhver form for reklame, uanset om den er skreven eller talt, som er sendt til en eller flere identificerede eller identificerbare slutbrugere af elektroniske kommunikationstjenester, herunder brugen af automatiserede opkalds- og kommunikationssystemer med eller uden menneskelig interaktion, e-mail, sms osv.

(g) "direkte markedsføringsopkald": telefonopkald, der ikke omfatter brugen af automatiserede opkalds- og kommunikationssystemer

(h) "automatiserede opkalds- og kommunikationssystemer": systemer, der er i stand til automatisk at foretage et opkald til en eller flere modtagere i henhold til de instruktioner, der er fastsat for systemet, og at udsende lyde, som ikke er live tale, herunder opkald foretaget ved hjælp af automatiserede opkalds- og kommunikationssystemer, som sætter den opkaldte person i forbindelse med et menneske.

KAPITEL II
BESKYTTELSE AF FYSISKE OG JURIDISKE PERSONERS ELEKTRONISKE KOMMUNIKATION OG OPLYSNINGER LAGRET PÅ DERES TERMINALUDSTYR

Artikel 5
Fortroligheden af elektroniske kommunikationsdata

Elektroniske kommunikationsdata skal behandles fortroligt. Påvirkning af elektroniske kommunikationsdata som f.eks. aflytning, registrering, lagring, overvågning, skanning og andre former for opfangning, overvågning eller behandling af elektroniske kommunikationsdata foretaget af andre end slutbrugerne er forbudt, dog med forbehold af undtagelserne i denne forordning.

Artikel 6
Tilladt behandling af elektroniske kommunikationsdata

1. Leverandører af elektroniske kommunikationsnet og -tjenester må behandle elektroniske kommunikationsdata, hvis:

(a) det er nødvendigt for at gennemføre videresendelsen af meddelelsen i den periode, der er nødvendig, for at dette kan ske, eller

(b) det er nødvendigt for at bevare eller genoprette sikkerheden i de elektroniske kommunikationsnet og -tjenester, eller for at afsløre tekniske svigt og/eller fejl i videresendelsen af den elektroniske kommunikation i den perioder, der er nødvendig, for at dette kan ske.

2. Leverandører af elektroniske kommunikationstjenester må behandle elektroniske kommunikationsmetadata, hvis:

(a) det er nødvendigt for at leve op til de obligatoriske krav til tjenestekvalitet, som fremgår af [direktiv om en europæisk kodeks for elektronisk kommunikation] eller af forordning (EU) 2015/2120[11] i den periode, der er nødvendig, for at dette kan ske, eller

(b) det er nødvendigt for at fakturere, beregne afregning for samtrafik, opdage og stoppe bedrageri med, misbrug af eller abonnement på elektroniske kommunikationstjenester, eller

(c) den pågældende slutbruger har givet samtykke til behandlingen af sine kommunikationsmetadata til et eller flere specifikke formål, herunder levering af specifikke tjenester til nævnte slutbrugere, forudsat at det eller disse formål ikke kunne opnås ved at behandle anonymiserede oplysninger.

3. Leverandører af elektroniske kommunikationstjenester må kun behandle elektronisk kommunikationsindhold i følgende situationer:

(a) med henblik på at levere specifikke tjenester til en slutbruger, hvis den eller de pågældende slutbruger eller slutbrugere har givet samtykke til behandling af vedkommendes elektroniske kommunikationsindhold, og tjenesten ikke kan leveres uden behandling af dette indhold, eller

b) hvis alle slutbrugere har givet samtykke til behandling af deres elektroniske kommunikationsindhold til et eller flere specifikke formål, som ikke kan opnås ved behandling af anonymiserede oplysninger, og leverandøren har hørt tilsynsmyndigheden. Stk. 2 og 3 i artikel 36 i forordning (EU) 2016/649 finder anvendelse på høringen af tilsynsmyndigheden.

[11] Europa-Parlamentets og Rådets forordning (EU) 2015/2120 af 25. november 2015 om foranstaltninger vedrørende adgang til det åbne internet og om ændring af direktiv 2002/22/EF om forsyningspligt og brugerrettigheder i forbindelse med elektroniske kommunikationsnet og -tjenester og forordning (EU) nr. 531/2012 om roaming på offentlige mobilkommunikationsnet i Unionen (EUT L 310 af 26.11.2015, s. 1-18).

Artikel 7

Opbevaring og sletning af elektroniske kommunikationsdata

1. Med forbehold af artikel 6, stk. 1, litra b), og artikel 6, stk. 3, litra a) og b), skal leverandører af elektroniske kommunikationstjenester slette det elektroniske kommunikationsindhold eller anonymisere de pågældende data, når den eller de tilsigtede modtager eller modtagere har modtaget det elektroniske kommunikationsindhold. Disse data må lagres og opbevares af slutbrugerne eller af en tredjepart, som er blevet betroet at lagre, opbevare eller på andre måder behandle dataene i henhold til forordning (EU) 2016/679.

2. Med forbehold af artikel 6, stk. 1, litra b), og artikel 6, stk. 2, litra a) og b), skal leverandører af elektroniske kommunikationstjenester slette elektroniske kommunikationsmetadata eller anonymisere dem, når de ikke længere er nødvendige for videresendelsen af en kommunikation.

3. Når behandling af elektroniske kommunikationsmetadata finder sted med henblik på fakturering, jf. artikel 6, stk. 2, litra b), må de relevante metadata opbevares indtil udløbet af den periode, hvori der retligt kan klages over regningen eller betaling kan opkræves, jf. national lovgivning.

Artikel 8

Beskyttelse af oplysninger, der opbevares på eller vedrører slutbrugerens terminaludstyr

1. Anvendelse af terminaludstyrets databehandlings- og opbevaringsfunktioner og indsamling af oplysninger fra slutbrugeres terminaludstyr, herunder om software og hardware, er forbudt for andre end de pågældende slutbrugere, medmindre:

(a) det er nødvendigt med det formål at videresende en elektronisk kommunikation via et elektronisk kommunikationsnet, eller

(b) slutbrugeren har givet sit samtykke, eller

(c) det er nødvendigt for at levere en informationssamfundstjeneste, som slutbrugeren har bestilt, eller

(d) det er nødvendigt til måling af internetbesøgende, forudsat at en sådan måling gennemføres af leverandøren af en informationssamfundstjeneste, som slutbrugeren har bestilt.

2. Indsamling af oplysninger, der udsendes af terminaludstyr og gør det i stand til at opnå forbindelse til andre apparater og/eller netudstyr, er forbudt, medmindre:

(a) det udelukkende gøres i den strengt nødvendige periode for at etablere en forbindelse, eller

(b) der vises en klar og fremtrædende meddelelse, der som minimum oplyser om de forskellige typer indsamling, deres formål, den ansvarlige for indsamlingen samt andre oplysninger, som er påkrævet i henhold til artikel 13 i forordning (EU) 2016/679, når der indsamles personoplysninger, samt eventuelle foranstaltninger slutbrugeren af terminaludstyret kan træffe med henblik på at stoppe eller minimere indsamlingen.

Indsamlingen af disse oplysninger er betinget af, at der er anvendt hensigtsmæssige tekniske og organisatoriske foranstaltninger til at opretholde et sikkerhedsniveau, som er passende i forhold til risiciene, jf. artikel 32 i forordning (EU) 2016/679.

3. De oplysninger, der skal gives i henhold til stk. 2, litra b), kan gives sammen med standardiserede ikoner for at give et meningsfuldt overblik over indsamlingen af oplysninger på en klart synlig, letforståelig og letlæselig måde.

4. Kommissionen tillægges beføjelse til at vedtage delegerede retsakter i overensstemmelse med artikel 27 med henblik på at fastlægge de oplysninger, der skal fremgå af standardiserede ikoner, og procedurerne for tilvejebringelse af standardiserede ikoner.

Artikel 9
Samtykke

1. Definitionen af og betingelserne for samtykke, som fremgår af artikel 4, stk. 11, og artikel 7, i forordning (EU) 2016/679/EU, finder anvendelse.

2. Med forbehold af stk. 1, kan samtykke, hvor det er teknisk muligt, jf. artikel 8, stk. 1, litra b), afgives ved hjælp af passende tekniske indstillinger i en softwareapplikation, der muliggør adgang til internettet.

3. Slutbrugere, der har givet samtykke til behandling af elektroniske kommunikationsdata, som angivet i artikel 6, stk. 2, litra c), og artikel 6, stk. 3, litra a) og b), skal have mulighed for til enhver tid at trække deres samtykke tilbage, jf. artikel 7, stk. 3, i forordning (EU) 2016/679, og de skal mindes om muligheden hver sjette måned, så længe databehandlingen finder sted.

Artikel 10
Information om og muligheder for privatlivsindstillinger

1. Software på markedet, som muliggør elektronisk kommunikation, herunder søgning og fremvisning af oplysninger på internettet, giver mulighed for at forhindre tredjeparter i at lagre oplysninger på en slutbrugers terminaludstyr eller i at behandle oplysninger, der er lagret på terminaludstyret.

2. Softwaren oplyser i forbindelse med installationen slutbrugeren om mulighederne i privatlivsindstillingerne og kræver, inden installationen kan fortsætte, at slutbrugeren vælger en indstilling.

3. Hvis softwaren allerede var installeret den 25. maj 2018, opfyldes kravene i stk. 1 og 2 ved den første opdatering af softwaren, dog senest den 25. august 2018.

Artikel 11
Begrænsninger

1. EU-retten eller medlemsstaternes nationale ret kan gennem lovgivningsmæssige foranstaltninger begrænse anvendelsesområdet for de rettigheder og forpligtelser, der fremgår af artikel 5-8, hvis en sådan begrænsning respekterer kernen i de grundlæggende rettigheder og frihedsrettigheder og er en nødvendig, hensigtsmæssig og forholdsmæssig foranstaltning i et demokratisk samfund for at sikre en eller flere af de samfundsinteresser, der er fastsat i artikel 23, stk. 1, litra a) - e), i forordning (EU) 2016/679, eller kontrol-, tilsyns- eller reguleringsfunktioner, der er forbundet med offentlig myndighedsudøvelse for sådanne interesser.

2. Leverandører af elektroniske kommunikationstjenester fastlægger interne procedurer til at besvare anmodninger om adgang til slutbrugeres elektroniske kommunikationsdata på grundlag af lovgivningsmæssige foranstaltninger vedtaget i

henhold til stk. 1. De skal efter anmodning forelægge den kompetente tilsynsmyndighed oplysninger om disse procedurer, antallet af modtagne anmodninger, den anvendte retlige begrundelse og deres reaktion.

KAPITEL III
FYSISKE OG JURIDISKE PERSONERS RET TIL KONTROL MED ELEKTRONISK KOMMUNIKATION

Artikel 12

Visning af opkaldende nummer og opkaldt nummer samt begrænsning heraf

1. Hvis der er mulighed for at få vist opkaldende nummer og opkaldt nummer, jf. artikel [107] i [direktiv om en europæisk kodeks for elektronisk kommunikation], stiller leverandører af offentligt tilgængelige nummerbaserede interpersonelle kommunikationstjenester følgende muligheder til rådighed:

(a) den opkaldende slutbruger kan forhindre visning af det opkaldende nummer pr. opkald, pr. forbindelse eller permanent

(b) den opkaldte slutbruger kan forhindre visning af det opkaldende nummer ved indgående opkald

(c) den opkaldte slutbruger kan afvise indgående opkald, hvis nummervisning er blevet forhindret af den opkaldende slutbruger

(d) den opkaldte slutbruger kan forhindre visning af det opkaldte nummer til den opkaldende slutbruger.

2. De muligheder, der er henvist til i stk. 1, litra a), b), c) og d), stilles gebyrfrit til slutbrugernes rådighed via simple midler.

3. Stk. 1, litra a), finder endvidere anvendelse på opkald til tredjelande fra Unionen. Stk. 1, litra b), c) og d), finder endvidere anvendelse på indgående opkald fra tredjelande.

4. Når der er adgang til visning af opkaldende nummer eller opkaldt nummer, oplyser leverandører af offentligt tilgængelige nummerbaserede interpersonelle kommunikationstjenester offentligheden om mulighederne i stk. 1, litra a), b), c) og d).

Artikel 13

Undtagelser fra visning af opkaldende nummer og opkaldt nummer samt begrænsning heraf

1. Uanset om den opkaldende slutbruger har forhindret visning af det opkaldende nummer, skal leverandører af offentligt tilgængelige nummerbaserede interpersonelle kommunikationstjenester i tilfælde af opkald til en nødtjeneste tilsidesætte den manglende nummervisning og det manglende samtykke fra slutbrugeren til behandling af metadata på linjebasis for organisationer, der tager sig af nødkommunikation, herunder offentlige alarmcentraler, med henblik på at besvare denne type kommunikation.

2. Medlemsstaterne indfører mere specifikke bestemmelser vedrørende indførelsen af procedurer og vilkår for, hvornår leverandører af offentligt tilgængelige nummerbaserede interpersonelle kommunikationstjenester midlertidigt skal

tilsidesætte nummervisning af det opkaldende nummer, hvis slutbrugere anmoder om at få sporet chikaneopkald eller generende opkald.

Artikel 14
Blokering af indgående opkald

Leverandører af offentligt tilgængelige nummerbaserede interpersonelle kommunikationstjenester gør brug af de nyeste foranstaltninger til at begrænse uønskede opkald til slutbrugerne og stiller endvidere følgende muligheder gebyrfrit til rådighed for den opkaldte slutbruger:

(a) blokering af indgående opkald fra specifikke numre eller fra anonyme kilder

(b) annullering af automatisk viderestilling fra en tredjepart til slutbrugerens terminaludstyr.

Artikel 15
Offentligt tilgængelige fortegnelser

1. Leverandører af offentligt tilgængelige fortegnelser indhenter samtykke fra de slutbrugere, som er fysiske personer, inden deres personoplysninger opføres i fortegnelsen, og de indhenter følgelig samtykke fra slutbrugerne til opføring af data pr. kategori af personoplysninger, i det omfang sådanne oplysninger er relevante for fortegnelsen, hvilket afgøres af leverandøren af fortegnelsen. Leverandører giver slutbrugere, som er fysiske personer, mulighed for at kontrollere, rette og slette disse oplysninger.

2. Leverandører af offentligt tilgængelige fortegnelser informerer de slutbrugere, som er fysiske personer, hvis personoplysninger er opført i fortegnelsen, om fortegnelsens tilgængelige søgefunktioner og indhenter slutbrugernes samtykke, inden de muliggør søgefunktioner vedrørende disse personoplysninger.

3. Leverandører af offentligt tilgængelige fortegnelser giver slutbrugere, som er juridiske personer, mulighed for at gøre indsigelse mod, at deres oplysninger bliver opført i en fortegnelse. Leverandører giver slutbrugere, som er juridiske personer, mulighed for at kontrollere, rette og slette disse oplysninger.

4. Slutbrugeres mulighed for at blive udeladt af en offentligt tilgængelig fortegnelse eller for at kontrollere, rette eller slette eventuelle oplysninger, der vedrører dem, stilles gebyrfrit til rådighed.

Artikel 16
Uanmodet kommunikation

1. Fysiske og juridiske personer kan gøre brug af elektroniske kommunikationstjenester til at sende direkte markedsføringsmeddelelser til slutbrugere, som er fysiske personer og har givet samtykke hertil.

2. Hvis en fysisk eller juridisk person indhenter elektroniske kontaktoplysninger til e-mail fra sine kunder i forbindelse med salget af et produkt eller en tjeneste, jf. forordning (EU) 2016/679, må den pågældende fysiske eller juridiske person kun anvende de elektroniske kontaktoplysninger til direkte markedsføring af sine egne lignende produkter eller tjenester, hvis kunderne klart og utvetydigt har fået mulighed for let og gebyrfrit at afvise en sådan anvendelse. Retten til at afvise denne

anvendelse gives ved indsamling af oplysningerne, og hver gang der sendes en meddelelse.

3. Med forbehold af stk. 1 og 2 skal fysiske og juridiske personer, som gør brug af elektroniske kommunikationstjenester til at foretage direkte markedsføringsopkald, gøre følgende:

(a) vise et nummer, hvorpå de kan kontaktes, eller

(b) vise en specifik kode/eller et præfiks, der afspejler det forhold, at der er tale om et markedsføringsopkald.

4. Uanset bestemmelserne i stk. 1 kan medlemsstaterne fastsætte ved lov, at direkte markedsføringsopkald til slutbrugere, som er fysiske personer, kun er tilladt til de slutbrugere, som er fysiske personer, der ikke har frabedt sig at modtage denne type henvendelser.

5. Medlemsstaterne sikrer endvidere inden for rammerne af gældende EU-ret og national ret, at de legitime interesser for slutbrugere, som er juridiske personer, for så vidt angår uanmodet kommunikation, der gennemføres i henhold til stk. 1, nyder tilstrækkelig beskyttelse.

6. Fysiske eller juridiske personer, der anvender elektroniske kommunikationstjenester til at afsende direkte markedsføringsmeddelelser, informerer slutbrugerne om, at der er tale om direkte markedsføring, samt om identiteten af den fysiske eller juridiske person på hvis vegne meddelelsen fremsendes, og de giver endvidere modtagerne de nødvendige oplysninger til at gøre brug af deres ret til på en nem måde at trække deres samtykke til at modtage flere markedsføringsmeddelelser tilbage.

7. Kommissionen tillægges beføjelse til at vedtage gennemførelsesforanstaltninger i henhold til artikel 26, stk. 2, der fastsætter den kode/eller det præfiks, der kendetegner markedsføringsopkald, jf. stk. 3, litra b).

Artikel 17
Oplysning om konstaterede sikkerhedstrusler

Hvor der er særlig risiko for, at netsikkerheden og sikkerheden for elektroniske kommunikationstjenester kompromitteres, oplyser leverandøren af den elektroniske kommunikationstjeneste slutbrugerne herom samt, hvis risikoen ligger uden for de foranstaltninger, der skal træffes af leverandøren, om, hvorledes sådanne risici i givet fald kan forebygges og angiver hvilke omkostninger, der sandsynligvis vil være forbundet hermed.

KAPITEL IV
UAFHÆNGIGE TILSYNSMYNDIGHEDER OG HÅNDHÆVELSE

Artikel 18
Uafhængige tilsynsmyndigheder

1. Den eller de uafhængige tilsynsmyndighed eller -myndigheder, som er ansvarlige for at føre tilsyn med anvendelsen af forordning (EU) 2016/679, er også ansvarlig for tilsynet med anvendelsen af denne forordning. Kapitel VI og VII i forordning (EU) 2016/679 finder tilsvarende anvendelse. Tilsynsmyndighedernes opgaver og beføjelser udføres under hensyntagen til slutbrugerne.

2. Tilsynsmyndigheden eller tilsynsmyndighederne i stk. 1 samarbejder, når det er nødvendigt, med de nationale tilsynsmyndigheder, der er udpeget i henhold til [direktiv om en europæisk kodeks for elektronisk kommunikation].

Artikel 19
Det Europæiske Databeskyttelsesråd

Det Europæiske Databeskyttelsesråd, som blev oprettet i henhold til artikel 68 i forordning (EU) 2016/679, har kompetence til at sikre ensartet anvendelse af denne forordning. Med henblik herpå udfører Det Europæiske Databeskyttelsesråd de opgaver, der er fastsat i artikel 70 i forordning (EU) 2016/679. Rådet har derudover følgende opgaver:

(a) rådgive Kommissionen om eventuelle foreslåede ændringer af denne forordning

(b) på eget initiativ, efter anmodning fra et af sine medlemmer eller efter anmodning fra Kommissionen undersøge ethvert spørgsmål vedrørende anvendelsen af denne forordning og udstede retningslinjer, henstillinger og bedste praksis for at fremme ensartet anvendelse af denne forordning.

Artikel 20
Procedurer for samarbejde og ensartet anvendelse

Hver enkelt tilsynsmyndighed bidrager til ensartet anvendelse af denne forordning i hele Unionen. Med henblik herpå samarbejder tilsynsmyndighederne med hverandre og Kommissionen i henhold til kapitel VII i forordning (EU) 2016/679 om anliggender omfattet af denne forordning.

KAPITEL V
RETSMIDLER, ANSVAR OG SANKTIONER

Artikel 21
Retsmidler

1. Uden at det berører en eventuel administrativ klageadgang eller adgang til retsmidler, har enhver slutbruger af elektroniske kommunikationstjenester ret til at gøre brug af de retsmidler, der fremgår af artikel 77, 78 og 79 i forordning (EU) 2016/679.

2. Enhver fysisk eller juridisk person andre end slutbrugere, der påvirkes negativt af overtrædelser af denne forordning, og som har en legitim interesse i ophør af eller forbud mod de påståede overtrædelser, herunder en leverandør af elektroniske kommunikationstjenester der beskytter sin legitime forretningsinteresse, har ret til at få sådanne overtrædelser indbragt for en domsstol.

Artikel 22
Ret til erstatning og erstatningsansvar

Enhver slutbruger af elektroniske kommunikationstjenester, som har lidt materiel eller immateriel skade som følge af en overtrædelse af denne forordning, har ret til erstatning fra skadevolder for den lidte skade, medmindre skadevolderen kan bevise, at denne ikke på nogen måde er ansvarlig for den begivenhed, der gav anledning til skaden, jf. artikel 82 i forordning (EU) 2016/679.

Artikel 23

Generelle betingelser for pålæggelse af administrative bøder

1. Kapitel VII i forordning (EU) 2016/679 finder anvendelse med henblik på overtrædelser af denne forordning.

2. Overtrædelse af følgende bestemmelser i denne forordning straffes i overensstemmelse med stk. 1 med administrative bøder på op til 10 000 000 EUR, eller hvis det drejer sig om en virksomhed, med op til 2 % af dens samlede globale årlige omsætning i det foregående regnskabsår, såfremt dette beløb er højere:

(a) forpligtelserne for enhver juridisk eller fysisk person, der behandler elektroniske kommunikationsdata, jf. artikel 8

(b) forpligtelserne for enhver leverandør af software, der muliggør elektronisk kommunikation, jf. artikel 10

(c) forpligtelserne for enhver leverandør af offentligt tilgængelige fortegnelser, jf. artikel 15

(d) forpligtelserne for enhver juridisk eller fysisk person, der anvender elektroniske kommunikationstjenester, jf. artikel 16.

3. Overtrædelse af princippet om kommunikationshemmelighed, tilladt behandling af elektroniske kommunikationsdata og fristerne for sletning som omhandlet i artikel 5, 6 og 7, straffes i overensstemmelse med nærværende artikels stk. 1 med administrative bøder på op til 20 000 000 EUR, eller hvis det drejer sig om en virksomhed, med op til 4 % af dens samlede globale årlige omsætning i det foregående regnskabsår, såfremt dette beløb er højere.

4. Medlemsstaterne fastsætter reglerne for, hvilke sanktioner der er for overtrædelse af artikel 12, 13, 14 og 17.

5. Manglende overholdelse af et påbud fra tilsynsmyndigheden som omhandlet i artikel 18 straffes med administrative bøder på op til 20 000 000 EUR, eller hvis det drejer sig om en virksomhed, med op til 4 % af dens samlede globale årlige omsætning i det foregående regnskabsår, såfremt dette beløb er højere.

6. Uden at det berører tilsynsmyndighedernes korrigerende beføjelser i henhold til artikel 18, kan hver medlemsstat fastsætte regler om, hvorvidt og i hvilket omfang administrative bøder må pålægges offentlige myndigheder og organer, der er etableret i den pågældende medlemsstat.

7. Tilsynsmyndighedens udøvelse af beføjelser i henhold til denne artikel er underlagt fornødne proceduremæssige garantier i overensstemmelse med EU-retten og medlemsstaternes nationale ret, bl.a. effektive retsmidler og retfærdig procedure.

8. Hvis en medlemsstats retssystem ikke giver mulighed for at pålægge administrative bøder, kan denne artikel anvendes på en sådan måde, at den kompetente tilsynsmyndighed tager skridt til bøder, og de kompetente nationale domstole pålægger dem, idet det sikres, at disse retsmidler er effektive, og at deres virkning svarer til virkningen af administrative bøder, som pålægges af tilsynsmyndighederne. Bøder skal under alle omstændigheder være effektive, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning. De pågældende medlemsstater giver Kommissionen meddelelse om bestemmelserne i de love, som de vedtager i henhold til dette stykke, senest den [xxx] og underretter den straks om alle senere ændringslove eller ændringer, der berører dem.

Artikel 24
Sanktioner

1. Medlemsstaterne fastsætter regler om andre sanktioner, der skal anvendes i tilfælde af overtrædelser af denne forordning, navnlig overtrædelser, som ikke er underlagt administrative bøder i henhold til artikel 23, og træffer alle nødvendige foranstaltninger for at sikre, at de anvendes. Sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning.

2. Hver medlemsstat giver senest 18 måneder efter den dato, der fremgår af artikel 29, stk. 2, Kommissionen meddelelse om de bestemmelser, som den vedtager i henhold til stk. 1, og underretter den straks om alle senere ændringer, der berører dem.

KAPITEL VI
DELEGEREDE RETSAKTER OG GENNEMFØRELSESFORANSTALTNINGER

Artikel 25
Udøvelse af de delegerede beføjelser

1. Beføjelsen til at vedtage delegerede retsakter tillægges Kommissionen på de i denne artikel fastlagte betingelser.

2. De beføjelser til at vedtage delegerede retsakter, der er omhandlet i artikel 8, stk. 4, tillægges Kommissionen for en ubestemt periode fra [datoen for denne forordnings ikrafttræden].

3. Delegationen af beføjelser efter artikel 8, stk. 4, kan til enhver tid tilbagekaldes af Europa-Parlamentet eller af Rådet. En afgørelse om tilbagekaldelse bringer delegationen af de beføjelser, der er angivet i den pågældende afgørelse, til ophør. Afgørelsen får virkning dagen efter offentliggørelsen i Den Europæiske Unions Tidende eller på et senere tidspunkt, der angives i afgørelsen. Den berører ikke gyldigheden af delegerede retsakter, der allerede er i kraft.

4. Inden vedtagelsen af en delegeret retsakt hører Kommissionen eksperter, som er udpeget af hver enkelt medlemsstat, i overensstemmelse med principperne i den interinstitutionelle aftale om bedre lovgivning af 13. april 2016.

5. Så snart Kommissionen vedtager en delegeret retsakt, giver den samtidigt Europa-Parlamentet og Rådet meddelelse herom.

6. En delegeret retsakt vedtaget i henhold til artikel 8, stk. 4, træder kun i kraft, hvis hverken Europa-Parlamentet eller Rådet har gjort indsigelse inden for en frist på to måneder fra meddelelsen af den pågældende retsakt til Europa-Parlamentet og Rådet, eller hvis Europa-Parlamentet og Rådet inden udløbet af denne frist begge har informeret Kommissionen om, at de ikke agter at gøre indsigelse. Fristen forlænges med to måneder på Europa-Parlamentets eller Rådets initiativ.

Artikel 26
Udvalg

1. Kommissionen bistås af Kommunikationsudvalget, som er nedsat i henhold til artikel 110 i [direktiv om en europæisk kodeks for elektronisk kommunikation]. Dette udvalg er et udvalg som omhandlet i forordning (EU) nr. 182/2011[12].

2. Når der henvises til dette stykke, finder artikel 5 i forordning (EU) nr. 182/2011 anvendelse.

KAPITEL VII
AFSLUTTENDE BESTEMMELSER

Artikel 27
Ophævelse

1. Direktiv 2002/58/EF ophæves med virkning fra den 25. maj 2018.

2. Henvisninger til det ophævede direktiv gælder som henvisninger til denne forordning.

Artikel 28
Tilsyn og evaluering

Kommissionen fastlægger senest den 1. januar 2018 et detaljeret program for tilsyn med effektiviteten af denne forordning.

Kommissionen gennemfører senest tre år efter datoen for denne forordnings anvendelse og hvert tredje år herefter en evaluering af forordningen og fremlægger de vigtigste resultater for Europa-Parlamentet, Rådet og Det Økonomiske og Sociale Udvalg. Evalueringen skal, hvor det er relevant, danne grundlag for forslag til ændring eller ophævelse af denne forordning i lyset af den retlige, tekniske og økonomiske udvikling.

Artikel 29
Ikrafttræden og anvendelse

1. Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

2. Den anvendes fra den 25. maj 2018.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

[12] Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011 af 16. februar 2011 om de generelle regler og principper for, hvordan medlemsstaterne skal kontrollere Kommissionens udøvelse af gennemførelsesbeføjelser (EUT L 55 af 28.2.2011, s. 13-18).

Udfærdiget i Bruxelles, den .

På Europa-Parlamentets vegne
Formanden

På Rådets vegne
Formanden