EUROPEISKA
KOMMISSIONEN

Bryssel den 10.1.2017
COM(2017) 10 final

2017/0003 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om respekt för privatlivet och skydd av personuppgifter i samband med elektronisk kommunikation och om upphävande av direktiv 2002/58/EG (förordning om integritet och elektronisk kommunikation)

(Text av betydelse för EES)

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

MOTIVERING

1. BAKGRUND TILL FÖRSLAGET

1.1. Motiv och syfte med förslaget

Strategin för den digitala inre marknaden (***strategin***)[1] syftar till att öka förtroendet och säkerheten när det gäller digitala tjänster. Reformen av ramen för dataskydd, och i synnerhet antagandet av förordning (EU) 2016/679, (**den allmänna dataskyddsförordningen**)[2] var central i detta hänseende. I strategin aviserades också en översyn av direktiv 2002/58/EG (**direktivet om integritet och elektronisk kommunikation**)[3] för att säkra en hög nivå av integritetsskydd för användare av elektroniska kommunikationstjänster och lika konkurrensvillkor för alla marknadsaktörer. Detta förslag innehåller den översyn av direktivet om integritet och elektronisk kommunikation som planerades i strategin och säkerställer konsekvens med den allmänna dataskyddsförordningen.

Direktivet om integritet och elektronisk kommunikation säkerställer ett skydd av grundläggande rättigheter och friheter, i synnerhet rätten till respekt för privatliv, konfidentialitet vid kommunikation och skydd av personuppgifter inom sektorn för elektronisk kommunikation. Direktivet garanterar också den fria rörligheten inom unionen för data, utrustning och tjänster när det gäller elektronisk kommunikation. Direktivet innebär att den grundläggande rätten till respekt för privatliv, när det gäller kommunikation, genomförs i unionens sekundärlagstiftning, i enlighet med artikel 7 i Europeiska unionens stadga om de grundläggande rättigheterna (***stadgan***).

I enlighet med kraven på bättre lagstiftning har kommissionen gjort en efterhandsutvärdering av lagstiftningens ändamålsenlighet och resultat (***Refit-utvärdering***) när det gäller direktivet om integritet och elektronisk kommunikation. Utvärderingen visar att den nuvarande ramens syften och principen är fortsatt relevanta. Viktig teknisk och ekonomisk utveckling har dock ägt rum på marknaden sedan den senaste ändringen av direktivet 2009. Konsumenter och företag förlitar sig allt oftare på nya internetbaserade tjänster för interpersonell kommunikation, t.ex. VoIP, meddelandetjänster och webbaserade e-posttjänster, i stället för traditionella kommunikationstjänster. Dessa s.k. OTT-tjänster (***over-the-top-tjänster***) omfattas i allmänhet inte av unionens nuvarande ram för elektronisk kommunikation, såsom direktivet om integritet och elektronisk kommunikation. Därför har direktivet inte hållit jämna steg med den tekniska utvecklingen, vilket har rätt till ett bristfälligt skydd av kommunikation som förmedlas genom nya tjänster.

1.2. Förenlighet med befintliga bestämmelser inom området

Detta förslag är *lex specialis* till den allmänna dataskyddsförordningen och kompletterar den när det gäller sådana data från elektronisk kommunikation som klassificeras som personuppgifter. Alla frågor som rör behandling av som inte specifikt tas upp i det här förslaget omfattas av den allmänna dataskyddsförordningen. Anpassningen till den allmänna

---

1 Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén, En strategi för en inre digital marknad COM(2015) 192 final.

2 Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), (EUT L 119, 4.5.2016, s. 1).

3 Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 31.7.2002, s. 37).

dataskyddsförordningen medförde att några bestämmelser upphävdes, t.ex. artikel 4 i direktivet om integritet och elektronisk kommunikation.

1.3. Förenlighet med unionens politik inom andra områden

Direktivet om integritet och elektronisk kommunikation ingår i den rättsliga ramen för elektronisk kommunikation. År 2016 antog kommissionen förslaget till direktiv om inrättande av en europeisk kodex för elektronisk kommunikation(***kodexen***)[4], som innebar en ändring av ramen. Det föreliggande förslaget ingår inte i kodexen, men det förlitar sig delvis på definitionerna i den, t.ex. definitionen av ”elektroniska kommunikationstjänster”. Precis som kodexen innebär förslaget in OTT-leverantörer tas med i tillämpningsområdet för att återspegla verkligheten på marknaden. Kodexen kompletterar också detta förslag genom att garantera säkerheten för elektroniska kommunikationstjänster.

Direktiv 2014/53/EU (***direktivet om radioutrustning***)[5] säkerställer en inre marknad för radioutrustning. Enligt direktivet måste radioutrustning innan den släpps ut på marknaden innehålla skyddsmekanismer för att säkerställa att användarens personuppgifter och personliga integritet skyddas Enligt direktivet och den europeiska standardiseringsförordningen (EU) 1025/2012[6] har kommissionen befogenhet att anta åtgärder. Detta förslag påverkar inte direktivet om radioutrustning.

Detta förslag innehåller inte några särskilda bestämmelser på området datalagring. Det behåller sakinnehållet i artikel 14 i direktivet om integritet och elektronisk kommunikation och anpassar det till de specifika formuleringarna i artikel 23 i den allmänna dataskyddsförordningen, som innehåller grunderna för när medlemsstaterna får begränsa rättigheter och skyldigheter i särskilda artiklar i direktivet om integritet och elektronisk kommunikation. Därmed är medlemsstaterna fria att behålla eller skapa nationella datalagringsramar som bl.a. omfattar riktade lagringsåtgärder, i den mån som dessa ramar är förenliga med unionsrätten, med beaktande av domstolens rättspraxis i fråga om tolkning av direktivet om integritet och elektronisk kommunikation och stadgan om de grundläggande rättigheterna[7].

Slutligen ska förslaget inte tillämpas på verksamheten i unionens institutioner, organ och byråer. Dess principer och relevanta skyldigheter när det gäller rätten till respekt för privatlivet och kommunikation i samband med behandling av data från elektronisk kommunikation har dock tagits med i förslaget till en förordning om upphävande av förordning (EG) nr 45/2001[8].

---

4 Kommissionens förslag till Europaparlamentets och rådets direktiv om inrättande av en europeisk kodex för elektronisk kommunikation (omarbetning) (COM/2016/0590 final - 2016/0288 (COD)).

5 Europaparlamentets och rådets direktiv 2014/53/EU av den 16 april 2014 om harmonisering av medlemsstaternas lagstiftning om tillhandahållande på marknaden av radioutrustning och om upphävande av direktiv 1999/5/EG (EUT L 153, 22.5.2014, s. 62).

6 Europaparlamentets och rådets förordning (EU) nr 1025/2012 av den 25 oktober 2012 om europeisk standardisering och om ändring av rådets direktiv 89/686/EEG och 93/15/EEG samt av Europaparlamentets och rådets direktiv 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG och 2009/105/EG samt om upphävande av rådets beslut 87/95/EEG och Europaparlamentets och rådets beslut 1673/2006/EG (EUT L 316, 14.11.2012, s. 12).

7 Se förenade målen C-293/12 och C-594/12, Digital Rights Ireland och Seitlinger m.fl., ECLI:EU:C:2014:238. Förenade målen C-203/15 och C-698/15 Tele2 Sverige AB och Secretary of State for the Home Department, ECLI:EU:C:2016:970.

8 Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter (EGT L 8, 12.1.2001, s. 1).

2. RÄTTSLIG GRUND, SUBSIDIARITETSPRINCIPEN OCH PROPORTIONALITETSPRINCIPEN

2.1. Rättslig grund

Artiklarna 16 och 114 i fördraget om Europeiska unionens funktionssätt(**EUF-fördraget**) är de relevanta rättsliga grunderna för förslaget.

Genom artikel 16 i EUF-fördaget införs en särskild rättslig grund för antagandet av bestämmelser för att skydda enskilda personer avseende på behandling av personuppgifter hos unionens institutioner och i medlemsstaterna, när dessa utövar verksamhet som omfattas av unionsrättens tillämpningsområde, samt bestämmelser om den fria rörligheten för sådana uppgifter. Eftersom elektronisk kommunikation där en fysisk person deltar normalt anses som personuppgifter bör skyddet av fysiska personer när det gäller kommunikationens konfidentialitet och behandlingen av sådana personuppgifter baseras på artikel 16.

Förslaget syftar dessutom till att skydda juridiska personers kommunikation och därmed sammanhängande legitima intressen. Innebörden och räckvidden för de rättigheter som anges i artikel 7 i stadgan ska, i enlighet med artikel 52.3 i stadgan, vara desamma som de som fastställs i artikel 8.1 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (***Europakonventionen***). När det gäller räckvidden för artikel 7 i stadgan bekräftar rättspraxis från Europeiska unionens domstol (***domstolen***)[9] och Europeiska domstolen för de mänskliga rättigheterna[10] att juridiska personers yrkesmässiga verksamhet inte får uteslutas från skydd av den rätt som garanteras enligt artikel 7 i stadgan och artikel 8 i Europakonventionen.

Initiativet har två syften, och den del som rör skydd av juridiska personers kommunikation och målet att skapa en inre marknad för denna elektroniska kommunikation och säkerställa dess funktioner i detta hänseende kan inte anses som endast av underordnad betydelse. Därför bör initiativet baseras på artikel 114 i EUF-fördraget.

2.2. Subsidiaritetsprincipen

Respekten för kommunikation är en grundläggande rätt som erkänns i stadgan. Innehållet i elektronisk kommunikation kan avslöja ytterst känslig information omslutanvändare som deltar i kommunikationen. Metadata från elektronisk kommunikation kan också röja väldigt känslig och personlig information, vilket uttryckligen erkänts av domstolen[11]. De flesta medlemsstater erkänner också behovet av att skydda kommunikation som en distinkt konstitutionell rättighet. Det är möjligt för medlemsstater att genomföra politiska åtgärder som säkerställer att denna rättighet inte överträds, men detta skulle inte kunna uppnås på ett enhetligt sätt utan unionsbestämmelser, och det skulle innebära begränsningar för de gränsöverskridande flödena av personuppgifter och andra data kopplade till användningen av elektroniska kommunikationstjänster. För att säkra fortsatt enhetlighet med den allmänna dataskyddsförordningen är det slutligen nödvändigt att se över direktivet om integritet och elektronisk kommunikation och anta åtgärder för att se till att de två instrumenten är i linje med varandra.

---

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

10 Se bl.a. Europadomstolens dom av den 16 december 1992 i målet Niemietz mot Tyskland, serie A nr 251-B, § 29, Société Colas Est m.fl. mot Frankrike, nr 37971/97, § 41, ECHR 2002-III, Peck mot Förenade kungariket, nr 44647/98, § 57, ECHR 2003-I, samt även Vinci Construction och GTM Génie Civil et Services mot Frankrike, nr 63629/10 och 60567/10, § 63, 2 april 2015.

11 Se fotnot 7.

Den tekniska utvecklingen och ambitionerna i strategin för en digital inre marknad har stärkt argumenten för åtgärder på EU-nivå. Framgången för EU-strategin beror på hur effektivt EU kan få bort nationella barriärer och gripa fördelarna och vinsterna av en europeisk digital inre marknad. Eftersom internet och digital teknik inte känner av några gränser har problemet en omfattning som omfattar mer än en enskild medlemsstats territorium. Medlemsstaterna kan inte på egen hand få bukt med dessa brister på ett effektivt sätt. Lika konkurrensvillkor för ekonomiska aktörer som tillhandahåller utbytbara tjänster och likvärdigt skydd för slutanvändare på unionsnivå är en förutsättning för att strategin för en digital inre marknad ska kunna fungera.

2.3. Proportionalitetsprincipen

För att säkerställa ett effektivt rättsligt skydd av respekt för privatliv och kommunikation måste tillämpningsområdet utvidgas till att omfatta OTT-leverantörer. Flera populära OTT-leverantörer följer redan helt eller delvis principen om konfidentialitet vid kommunikation, men skyddet av grundläggande rättigheter kan inte överlåtas till självreglering inom branschen. Det har också blivit viktigare med ett effektivt skydd av terminalutrustningens integritet, eftersom denna har blivit oumbärlig i privatlivet och yrkeslivet för lagring av känslig information. Genomförandet av direktivet om integritet och elektronisk kommunikation inte medfört effektiv egenmakt för slutanvändarna. För att uppnå syftet är det därför nödvändigt att genomföra principen genom att centralisera samtycket i programvara och mana på användarna genom information om sekretessinställningarna. Kontrollen av att denna förordning efterlevs ska säkerställas genom tillsynsmyndigheterna och mekanismen för enhetlighet enligt den allmänna dataskyddsförordningen. Förslaget tillåter att medlemsstaterna vidtar nationella undantagsåtgärder för särskilda berättigade syften. Förslaget går därför inte utöver vad som är nödvändigt för att uppnå målen utan uppfyller proportionalitetsprincipen enligt artikel 5 i fördraget om Europeiska unionen. Skyldigheterna för berörda avdelningar hålls på lägsta möjliga nivå, utan att det inkräktar på de berörda grundläggande rättigheterna.

2.4. Val av instrument

Kommissionen lägger fram ett förslag till förordning för att säkra enhetlighet med den allmänna dataskyddsförordningen och rättssäkerhet för både användare och företag genom att motverka olika tolkningar i olika medlemsstater. En förordning kan säkerställa samma skyddsnivå i hela unionen för användarna och lägre kostnader för att följa bestämmelserna för företag som bedriver verksamhet över gränserna.

3. RESULTAT AV EFTERHANDSUTVÄRDERINGAR, SAMRÅD MED BERÖRDA PARTER OCH KONSEKVENSBEDÖMNINGAR

3.1. Efterhandsutvärderingar/kontroller av ändamålsenligheten med befintlig lagstiftning

I Refit-utvärderingen granskades hur effektivt direktivet om integritet och elektronisk kommunikation bidragit till ett tillfredsställande skydd av respekten för privatliv och konfidentialitet vid kommunikation i EU. Man strävad också efter att identifiera eventuella redundanser.

Slutsatsen var att direktivets ovannämnda mål fortfarande är **relevanta**. Den allmänna dataskyddsförordningen säkerställer skyddet av personuppgifter medan direktivet om integritet och elektronisk kommunikation säkerställer konfidentialiteten vid kommunikation, som även kan innefatta andra data än personuppgifter och data som rör en juridisk person. Därför bör ett separat instrument säkerställa ett effektivt skydd för artikel 7 i stadgan. Andra

bestämmelser, som bestämmelserna om sändande av icke begärd marknadsföringskommunikation har också visat sig vara fortsatt relevanta.

När det gäller **effektivitet och ändamålsenlighet** fann man att direktivet inte helt uppnått sina mål. Den oklara formuleringen av vissa bestämmelser och tvetydiga juridiska begrepp har äventyrat harmoniseringen och därigenom skapat utmaningar för företag som vill bedriva verksamhet över gränserna. Utvärderingen visade vidare att vissa bestämmelser har varit onödigt betungande för företag och konsumenter. Exempelvis har bestämmelsen om samtycke, som ska skydda konfidentialiteten för terminalutrustning, inte lyckats uppnå sina mål, och slutanvändarna får uppmaningar om att godkänna kartläggningskakor utan att förstå innebörden och utsätts i vissa fall till och med för kakor som sänds utan deras samtycke. Bestämmelsen om samtycke är överinkluderande, eftersom den även omfattar metoder som inte inkräktar på den personlig integriteten, och underinkluderar den, eftersom den inte tydligt täcker viss kartläggningsteknik (t.ex. *device fingerprinting*) som inte medför åtkomst till/lagring i enheten. Slutligen kan genomförandet vara dyrt för företagen.

Utvärderingen kom fram till att bestämmelserna om integritet och elektronisk kommunikation fortfarande har ett **EU-mervärde** när det gäller att bättre uppnå målet att säkerställa onlineintegritet i ljuset av en alltmer internationell marknad för elektronisk kommunikation. Den visade också att bestämmelserna i stort är **förenliga** med annan lagstiftning på området, men några redundanser har identifierats i förhållande till den nya allmänna dataskyddsförordningen(se avsnitt 1.2).

3.2. Samråd med berörda parter

Kommissionen anordnade ett offentligt samråd under perioden 12 april–5 juli 2016 och fick in´ 421 svar[12]. De viktigaste resultaten var följande[13]:

– **Behovet av särskilda bestämmelser för sektorn för elektronisk kommunikation är det gäller konfidentialitet vid elektronisk kommunikation**: Stöds av 83,4 % av medborgarna, konsumentorganisationerna och civilsamhällets organisationer samt 88,9 % av de offentliga organen, medan 63,4 % av branschdeltagarna motsätter sig.

– **Utvidgning av tillämpningsområdet till att omfatta nya kommunikationstjänster (OTT-tjänster)**: Stöds av 76 % av medborgarna och det civila samhället och av 93,1 % av de offentliga organen, medan endast 36,2 % av branschdeltagarna förespråkar en sådan utvidgning.

– **Ändring av undantagen från samtycke för behandling av trafikdata och lokaliseringsdata**: 49,1 % av medborgarna, konsumentorganisationerna och civilsamhällesorganisationerna föredrar att inte bredda undantagen, medan 36 % av de offentliga organen helst inte vill bredda undantagen och 2/3 av branschen vill att bestämmelserna upphävs.

– **Stöd åt de föreslagna lösningarna på frågan om samtycke till kakor**: 81,2 % av medborgarna och 63 % av de offentliga organen stödjer införandet av en skyldighet för tillverkare av terminalutrustning att saluföra produkter där en sekretessinställning

[12] 162 bidrag från medborgare, 33 från det civila samhället och konsumentorganisationer, 186 från branschen och 40 från offentliga organ, inklusive de behöriga myndigheter som kontrollerar att direktivet om integritet och elektronisk kommunikation efterlevs.

[13] Den fullständiga rapporten finns på internet: https://ec.europa.eu/digital-single-market/news-redirect/37204.

som innebär integritetsskydd som standard är aktiverad, medan 58,3 % av branschen förespråkar alternativet att stödja självreglering eller samreglering.

Europeiska kommissionen anordnade också två seminarier i april 2016, en som var öppen för alla intressenter och en som var öppen för de nationella behöriga myndigheterna. Där behandlades de viktigaste frågorna från det offentliga samrådet. De synpunkter som framkom under seminarierna återspeglade resultatet av det offentliga samrådet.

För att få in synpunkter från medborgarna genomfördes en Eurobarometerundersökning om integritet och elektronisk kommunikation[14] i hela EU. De viktigaste resultaten var följande[15]:

– 78 % säger att det är väldigt viktigt att personlig information på deras dator, smarttelefon eller datorplatta endast kan nås med deras tillåtelse.

– 72 % säger att det är väldigt viktigt att konfidentialiteten för deras e-postmeddelanden och snabbmeddelanden garanteras.

– 89 % stödjer det föreslagna alternativet att standardinställningen i deras webbläsare skulle stoppa delning av deras information.

3.3. Insamling och användning av sakkunnigutlåtanden

Kommissionen förlitade sig på följande externa sakkunskap:

– Riktade samråd med EU:s expertgrupper: Yttrande från artikel 29-gruppen, yttrande från Europeiska datatillsynsmannen, yttrande från Refit-plattformen, synpunkter från Berec, samt synpunkter från Enisa och medlemmar i nätverket av offentliga tillsynsmyndigheter för att skydda konsumenterna.

– Extern sakkunskap, i synnerhet följande två studier:

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

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

3.4. Konsekvensbedömning

En konsekvensbedömning har gjorts av detta förslag, och den 28 september 2016 avgav nämnden för lagstiftningskontroll ett positivt yttrande[16]. För att avspegla nämndens rekommendationer förtydligar konsekvensbedömningen initiativets tillämpningsområde, dess förenlighet med andra rättsliga instrument (den allmänna dataskyddsförordningen, kodexen, direktivet om radioutrustning). Utgångsscenariot utvecklas ytterligare och förtydligas. Analysen av konsekvenserna har stärkts och gjorts mer balanserad och förtydligar och stärker beskrivningen av förväntade kostnader och vinster.

Följande alternativ granskades utifrån kriterierna ändamålsenlighet, effektivitet och samstämmighet.

– **Alternativ 1:** Andra åtgärder än lagstiftning (icke-bindande instrument).

---

14 *2016 Eurobarometer survey (EB) 443 on e-Privacy* (SMART 2016/079).

15 Den fullständiga rapporten finns på internet: https://ec.europa.eu/digital-single-market/news-redirect/37205.

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

– **Alternativ 2:** Begränsad förstärkning av personlig integritet/konfidentialitet samt förenkling.

– **Alternativ 3:** Måttlig förstärkning av personlig integritet/konfidentialitet samt förenkling.

– **Alternativ 4:** Långtående förstärkning av personlig integritet/konfidentialitet samt förenkling.

– **Alternativ 5:** Upphävande av direktivet om integritet och elektronisk kommunikation.

Alternativ 3 var det alternativ som i de flesta avseenden **föredrogs** för att uppnå målen, med beaktande av effektiviteten och samstämmigheten. De viktigaste fördelarna är följande:

– Förbättrat skydd av konfidentialiteten vid elektronisk kommunikation genom att det rättsliga instrumentets tillämpningsområde utvidgas till att omfatta nya funktionsmässigt likvärdiga elektroniska kommunikationstjänster. Förordningen ökar också slutanvändarnas kontroll genom att klargöra att samtycke kan uttryckas med hjälp av lämpliga tekniska inställningar.

– Förbättrat skydd mot icke begärd kommunikation, i och med införandet av en skyldighet att tillhandahålla identifikation av det uppringande numret eller ett obligatoriskt prefix för markandsföringssamtal samt ökade möjligheter att blockera samtal från oönskade nummer.

– Förenklade och förtydligade regleringsvillkor i och med att man minskar det manöverutrymme som lämnats åt medlemsstaterna, upphäver föråldrade bestämmelser och breddar undantagen från samtyckesbestämmelserna.

De ekonomiska konsekvenserna av alternativ 3 väntas i stort stå i proportion till förslagets syften. Affärsmöjligheter kopplade till behandlingen av kommunikationsdata öppnas för traditionella elektroniska kommunikationstjänster, samtidigt som OTT-leverantörer blir föremål för samma bestämmelser. Detta medför vissa ytterligare kostnader för att uppfylla kraven för dessa operatörer. Förändringen kommer inte i någon väsentlig grad att påverka de OTT-leverantörer som redan baserar sin verksamhet på samtycke. Slutligen skulle alternativet inte få några konsekvenser i medlemsstater som redan har utvidgat dessa bestämmelser till att omfatta OTT-leverantörer.

Genom att centralisera samtycket i mjukvara – som t.ex. webbläsare – och uppmana användare att välja sina sekretessinställningar och utvidga undantaget från samtyckesbestämmelsen skulle en betydande andel av företagen kunna sluta med webbannonser och meddelanden, vilket kan ge betydande kostnadsbesparingar och förenklingar. Det kan dock bli svårare för riktade onlineannonsörer att erhålla samtycke om en stor andel av användarna använder inställningen ”avvisa tredjepartskakor”. Samtidigt innebär inte en centralisering av samtycket att webbplatsoperatörer berövas möjligheten att erhålla samtycke genom individuella förfrågningar till slutanvändare och därigenom bibehålla sin nuvarande affärsmodell. Ytterligare kostnader skulle tillkomma för en del leverantörer av webbläsare och liknande programvara, eftersom de skulle behöva säkerställa integritetsvänliga inställningar.

I den externa studien identifierades tre olika genomförandescenarion för alternativ 3, beroende på vilken enhet som etablerar dialogrutan mellan användare som har valt inställningar som ”avvisa tredjepartskakor” eller ”kartlägg inte” och besökta webbplatser som vill att användaren ska ompröva sitt val. De enheter som skulle kunna ansvara för denna tekniska uppgift är följande: 1) Programvara såsom webbläsare. 2) Kartläggande tredjepart. 3)

Den enskilda webbplatsen (dvs. den informationssamhällestjänst som användaren begärt). Enligt det första scenariot skulle alternativ 3 ge totala besparingar i fråga om efterlevnadskostnader på 70 % (948,8 miljoner euro i besparingar) jämfört med utgångsscenariot. Kostnadsbesparingarna skulle vara lägre i de andra scenariona. De totala besparingarna beror i huvudsak på en stor minskning av antalet företag som påverkas, men efterlevnadskostnaderna för enskilda företag förväntas i genomsnitt bli högre än i dag.

3.5. Lagstiftningens ändamålsenlighet och förenkling

De åtgärder som föreslås enligt det förespråkade alternativet är inriktade på förenkling och minskade administrativa bördor, i enlighet med resultaten från Refit-utvärderingen och yttrandet från Refit-plattformen[17].

Refit-plattformen utfärdade tre rekommendationer till kommissionen:

– Skyddet av medborgarnas privatliv borde stärkas genom att direktivet om integritet och elektronisk kommunikation anpassas till den allmänna dataskyddsförordningen.

– Medborgarnas skydd mot icke begärd marknadsföring bör effektiviseras genom att man lägger till undantag från bestämmelsen om samtycke till kakor.

– Kommissionen hanterar nationella genomförandeproblem och främjar utbyte av bästa praxis mellan medlemsstaterna.

Förslaget omfattar mer specifikt följande:

– Användning av teknikneutrala definitioner för att innefatta nya tjänster och tekniktyper så att förordningen blir framtidssäkrad.

– Upphävande av säkerhetsbestämmelserna för att undvika dubbelreglering.

– Förtydligande av tillämpningsområdet för att undanröja/minska risken för olika genomförande i olika medlemsstater.

– Förtydligande och förenkling av bestämmelsen om samtycke till användning av kakor och andra identifikatorer, såsom förklaras i 3.1 och 3.4 (punkt 2 i yttrandet).

– Anpassning av tillsynsmyndigheten till de myndigheter som har behörighet att kontrollera efterlevnaden av den allmänna dataskyddsförordningen och mekanismen för enhetlighet enligt den förordningen.

3.6. Konsekvenser för de grundläggande rättigheterna

Förslaget syftar till att effektivisering och till att öka skyddsnivån för personlig integritet och personuppgifter som behandlas i samband med elektronisk kommunikation i enlighet med artiklarna 7 och 8 i stadgan och garantera ökad rättssäkerhet. Förslaget kompletterar och preciserar den allmänna dataskyddsförordningen. Ett effektivt skydd av konfidentialiteten vid kommunikation är avgörande för att yttrandefriheten, informationsfriheten och andra näraliggande rättigheter ska kunna utövas, t.ex. rätten till skydd av personuppgifter eller tankefrihet, samvetsfrihet och religionsfrihet.

4. BUDGETKONSEKVENSER

Förslaget påverkar inte unionens budget.

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

5. ÖVRIGA INSLAG

5.1. Genomförandeplaner samt åtgärder för övervakning, utvärdering och rapportering

Kommissionen kommer att övervaka tillämpningen av denna förordning och lämna en rapport om sin utvärdering till Europaparlamentet och rådet och Europeiska ekonomiska sociala kommittén vart tredje år. Dessa rapporter kommer att vara offentliga och redogöra för den praktiska tillämpningen och kontrollen av efterlevnaden när det gäller denna förordning.

5.2. Ingående redogörelse för de specifika bestämmelserna i förslaget

Kapitel I innehåller allmänna bestämmelser: Syftet (artikel 1), tillämpningsområdet (artiklarna 2 och 3) och definitionerna, inklusive hänvisningar till tillämpliga definitioner i andra EU-instrument, som den allmänna dataskyddsförordningen.

Kapitel II innehåller de viktigaste bestämmelserna som säkerställer konfidentialiteten vid elektronisk kommunikation (artikel 5) och de begränsade tillåtna syften och de villkor som gäller för behandling av sådana kommunikationsdata (artiklarna 6 och 7). Kapitlet behandlar också skydd för terminalutrustning genom att i) garantera integriteten för den information som lagras i utrustningen, och ii) skydda information som utsänds från terminalutrustningen, eftersom den kan möjliggöra identifikation av slutanvändaren (artikel 8). Slutligen beskriver artikel 9 slutanvändarnas samtycke, en central laglig grund för denna förordning, som uttryckligen hänvisar till den definition och de villkor som föreskrivs i den allmänna dataskyddsförordningen, medan artikel 10 föreskriver att leverantörer av programvara som används för elektronisk kommunikation ska vara skyldiga att hjälpa slutanvändare att göra ändamålsenliga val av sekretessinställningar. Artikel 11 beskriver syftena och villkoren för medlemsstaternas begränsningar av ovannämnda bestämmelser.

Kapitel III rör slutanvändarnas rättighet att kontrollera sändande och mottagande av elektronisk kommunikation för att skydda sin personliga integritet: i) slutanvändarnas rätt att förhindra presentation av det uppringande numret för att garantera anonymitet (artikel 12) och begränsningarna av denna rätt (artikel 13), och ii) skyldigheten för leverantörer av allmänt tillgänglig nummerbaserad kommunikation att tillhandahålla en möjlighet att begränsa mottagandet av oönskade samtal (artikel 14). Detta kapitel reglerar också villkoren för när slutanvändarna får inkluderas i allmänt tillgängliga förteckningar (artikel 15) och villkoren för när icke begärd kommunikation får sändas i direktmarknadsföringssyfte (artikel 17). Kapitlet behandlar också säkerhetsrisker och föreskriver en skyldighet för leverantörer av elektroniska kommunikationstjänster att varna slutanvändarna vid särskilda risker som kan äventyra säkerheten för nät och tjänster. De säkerhetsrelaterade skyldigheterna i den allmänna dataskyddsförordningen och kodexen kommer att gälla för leverantörer av elektroniska kommunikationstjänster.

Kapitel IV omfattar övervakningen och kontrollen av efterlevnaden av denna förordning, som anförtros åt de tillsynsmyndigheter som ansvarar för den allmänna dataskyddsförordningen, med tanke på de stora synergieffekter som finns mellan allmänna dataskyddsfrågor och konfidentialitet vid kommunikation (artikel 18). Europeiska dataskyddsstyrelsens befogenheter utvidgas (artikel 19) och mekanismen för samarbete och enhetlighet enligt den allmänna dataskyddsförordningen kommer att gälla i samband med gränsöverskridande ärenden som rör denna förordning (artikel 20).

I kapitel anges de olika rättsmedel som slutanvändarna har tillgång till (artiklarna 21 och 22) och de sanktioner som kan åläggas (artikel 24), inklusive de allmänna villkoren för administrativa sanktionsavgifter.

Kapitel VI handlar om antagandet av delegerade akter och genomförandeakter i enlighet med artiklarna 290 och 291 i fördraget.

Kapitel VII innehåller också förordningens slutbestämmelser: Upphävande av direktivet om integritet och elektronisk kommunikation, övervakning och översyn, ikraftträdande och tillämpning. När det gäller översynen avser kommissionen att bl.a. utvärdera om det fortfarande är nödvändigt med en separat rättsakt mot bakgrund av den rättsliga, tekniska eller ekonomiska utvecklingen och med beaktande av den första utvärderingen av förordning (EU) nr 2016/679 som ska läggas fram den 25 maj 2020

2017/0003 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om respekt för privatlivet och skydd av personuppgifter i samband med elektronisk kommunikation och om upphävande av direktiv 2002/58/EG (förordning om integritet och elektronisk kommunikation)

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artiklarna 16 och 114,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande[1],

med beaktande av Regionkommitténs yttrande[2],

med beaktande av Europeiska datatillsynsmannens yttrande[3],

i enlighet med det ordinarie lagstiftningsförfarandet, och

av följande skäl:

(1) Artikel 7 i Europeiska unionens stadga om de grundläggande rättigheterna (*stadgan*) skyddar allas grundläggande rätt till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer. Respekten för kommunikationernas integritet är en viktig dimension av denna rätt. Konfidentialitet vid elektronisk kommunikation säkerställer att den information som utbyts mellan parter och de externa elementen av sådan kommunikation – inbegripet tidpunkten för överföringen, varifrån och till vem – inte röjs för någon annan än de parter som deltar i kommunikationen. Konfidentialitetsprincipen bör tillämpas på existerande och framtida kommunikationsmedel, inklusive röstsamtal, internettillgång, tillämpningar för snabbmeddelanden, e-post, internettelefoni och personliga meddelanden via sociala medier.

(2) Innehållet i elektronisk kommunikation kan avslöja ytterst känslig information om de fysiska personer som deltar i kommunikationen, alltifrån personliga erfarenheter och känslor till sjukdomstillstånd, sexuella preferenser och politiska åsikter, som om de röjs skulle kunna medföra personliga och sociala konsekvenser, ekonomiska förluster eller obehag. Metadata från elektronisk kommunikation kan också röja väldigt känslig

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

och personlig information. Några exempel på sådana metadata är uppringda nummer, besökta webbplatser och geografisk lokalisering samt tidpunkt, datum och varaktighet för ett samtal som ringts av en enskild person. Utifrån detta kan exakta slutsatser dras om privatlivet för de personer som deltar i den elektroniska kommunikationen, t.ex. deras sociala relationer, vanor och aktiviteter i vardagslivet, intressen samt tycke och smak.

(3) Data från elektronisk kommunikation kan också röja information om juridiska personer, t.ex. affärshemligheter eller annan känslig information av ekonomiskt värde. Därför bör bestämmelserna i denna förordning tillämpas på både fysiska och juridiska personer. Förordningen bör också säkerställa att bestämmelserna i Europaparlamentets och rådets förordning (EU) 2016/679[4] även tillämpas på slutanvändare som är juridiska personer. Detta inbegriper definitionen av samtycke enligt förordning (EU) 2016/679. När det hänvisas till en slutanvändares samtycke, inklusive juridiska personers, bör denna definition gälla. Juridiska personer bör ha samma rättigheter som slutanvändare som är fysiska personer när det gäller tillsynsmyndigheterna. Tillsynsmyndigheterna enligt denna förordning bör också ha ansvaret för att övervaka förordningens tillämpning på juridiska personer.

(4) I enlighet med artikel 8.1 i stadgan och artikel 16.1 i fördraget om Europeiska unionens funktionssätt har var och en rätt till skydd av de personuppgifter som rör honom eller henne. I förordning (EU) 2016/679 fastställs bestämmelser om skydd för fysiska personer med avseende på behandlingen av personuppgifter och bestämmelser om fri rörlighet för personuppgifter. Data från elektronisk kommunikation kan innefatta personuppgifter enligt definitionen i förordning (EU) 2016/679.

(5) Bestämmelserna i denna förordning preciserar och kompletterar de allmänna bestämmelserna om skydd av personuppgifter enligt förordning (EU) 2016/679 när det gäller sådana data från elektronisk kommunikation som kan kategoriseras som personuppgifter. Förordningen innebär därmed inte någon sänkning av den skyddsnivå som fysiska personer har enligt (EU) 2016/679. Behandling av data från elektronisk kommunikation som utförs av leverantörer av elektroniska kommunikationstjänster bör endast tillåtas i enlighet med denna förordning.

(6) Principerna och de viktigaste bestämmelserna i Europaparlamentets och rådets direktiv 2002/58/EG[5] är i princip fortfarande giltiga, men direktivet har inte helt hållit takten med teknikens och marknadsvillkorens utveckling, vilket i praktiken medfört ett inkonsekvent eller otillräckligt skydd av integritet och konfidentialitet i samband med elektronisk kommunikation. Ett exempel på denna utveckling är inträdet på marknaden av elektroniska kommunikationstjänster som ur ett konsumentperspektiv är utbytbara med traditionella tjänster, men som inte behöver följa samma bestämmelser. Ett annat exempel är ny teknik som gör det möjligt att kartlägga slutanvändares onlinebeteende och som inte omfattas av direktiv 2002/58/EG. Direktiv 2002/58/EG bör därför upphävas och ersättas med denna förordning.

---

4 Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), (EUT L 119, 4.5.2016, s. 1).

5 Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 31.7.2002, s. 37).

(7) Medlemsstaterna bör inom denna förordnings gränser ha rätt att behålla eller införa nationella bestämmelser som ytterligare specificerar och förtydligar tillämpningen av förordningens bestämmelser, för att säkerställa en effektiv tillämpning och tolkning av dessa. Därför bör det utrymme för egna bedömningar som medlemsstaterna har i detta hänseende präglas av en jämvikt mellan skyddet av privatliv och personuppgifter och den fria rörligheten för data från elektronisk kommunikation.

(8) Denna förordning bör tillämpas på leverantörer av elektroniska kommunikationstjänster, leverantörer av allmänt tillgängliga förteckningar och på leverantörer av programvara som möjliggör elektronisk kommunikation, inklusive åtkomst till och presentation av information på internet. Förordningen bör också tillämpas på fysiska och juridiska personer som använder elektroniska kommunikationstjänster för att sända kommersiell direktmarknadsföring eller samla in information som rör slutanvändarnas terminalutrustning eller lagras i denna.

(9) Förordningen bör tillämpas på data från elektronisk kommunikation som behandlas i samband med tillhandahållandet och användningen av elektroniska kommunikationstjänster i unionen, oavsett om behandlingen sker inom unionen eller inte. För att inte beröva slutanvändarna i unionen ett effektivt skydd bör förordningen också tillämpas på data från elektronisk kommunikation som behandlas i samband med elektroniska kommunikationstjänster som tillhandahålls från platser utanför unionen till slutanvändare i unionen.

(10) Radioutrustning och programvara för radioutrustning som släpps ut på unionens inre marknad måste uppfylla kraven i Europaparlamentets och rådets direktiv 2014/53/EU[6]. Denna förordning bör inte påverka tillämpligheten för något krav i direktiv 2014/53/EU eller kommissionens befogenhet att anta delegerade akter i enlighet med direktiv 2014/53/EU som föreskriver att vissa kategorier eller klasser av radioutrustningen ska innehålla skyddsmekanismer för att säkerställa att slutanvändares personuppgifter och personliga integritet skyddas.

(11) De tjänster som används i kommunikationssyfte, och de tekniska metoderna för att leverera sådana, har utvecklats avsevärt. I stället för traditionella röstsamtal, textmeddelanden (sms) och tjänster för överföring av e-postmeddelanden väljer slutanvändarna allt oftare likvärdiga onlinetjänster som IP-telefoni, meddelandetjänster och webbaserade e-posttjänster. För att säkerställa ett effektivt och likvärdigt skydd för slutanvändare som använder funktionsmässigt likvärdiga tjänster använder denna förordning den definition av elektroniska kommunikationstjänster som fastställs i [Europaparlamentets och rådets direktiv om inrättande av en europeisk kodex för elektronisk kommunikation[7]]. Definitionen omfattar inte bara internetanslutningstjänster och tjänster som helt eller delvis utgörs av överföring av signaler utan även interpersonella kommunikationstjänster, nummerbaserade eller inte, som t.ex. VoIP, meddelandetjänster och webbaserade e-posttjänster. Skyddet av kommunikationens konfidentialitet är avgörande även när det gäller interpersonella kommunikationstjänster som är sidotjänster till en annan tjänst. Därför bör sådana typer av tjänster som också har kommunikationsfunktioner omfattas av denna förordning.

---

6 Europaparlamentets och rådets direktiv 2014/53/EU av den 16 april 2014 om harmonisering av medlemsstaternas lagstiftning om tillhandahållande på marknaden av radioutrustning och om upphävande av direktiv 1999/5/EG (EUT L 153, 22.5.2014, s. 62).

7 Kommissionens förslag till Europaparlamentets och rådets direktiv om inrättande av en europeisk kodex för elektronisk kommunikation (omarbetning) (COM/2016/0590 final - 2016/0288 (COD)).

(12) Det har blivit allt vanligare med uppkopplade enheter och maskiner som kommunicerar med varandra via elektroniska kommunikationsnät (*sakernas internet*). Kommunikation från maskin till maskin sker genom överföring av signaler via ett nät och utgör därmed vanligtvis en elektronisk kommunikationstjänst. För att säkerställa ett fullständigt skydd av rätten till personlig integritet och kommunikationens konfidentialitet, och för att främja ett säkert sakernas internet som inger förtroende på den digitala inre marknaden, bör det klargöras att denna förordning bör tillämpas på överföring av kommunikation från maskin till maskin. Därför bör principen om konfidentialitet enligt denna förordning även tillämpas på överföringen av kommunikation från maskin till maskin. Särskilda skyddsåtgärder skulle också kunna antas enligt sektorslagstiftning, som direktiv 2014/53/EU.

(13) Utvecklingen av snabb och effektiv trådlös teknik har bidragit till att ge allmänheten en ökad internettillgång via trådlösa nät som är tillgängliga för alla i offentliga och halvoffentliga utrymmen, såsom surfzoner på olika platser i städer, varuhus, köpcentrum och sjukhus. I den mån som dessa kommunikationsnät tillhandahålls åt en odefinierad grupp slutanvändare bör konfidentialiteten skyddas för de meddelanden som överförs via sådana nät. Det faktum att trådlösa elektroniska kommunikationstjänster kan vara sidotjänster till andra tjänster bör inte hindra att konfidentialiteten säkerställs för kommunikationsdata eller att denna förordning tillämpas. Därför bör denna förordning tillämpas på data från elektronisk kommunikation som använder elektroniska kommunikationstjänster och offentliga kommunikationsnät. Däremot bör denna förordning inte tillämpas på slutna grupper av slutanvändare, som företagsnät, där åtkomsten begränsas till företagsmedlemmar.

(14) Data från elektronisk kommunikation bör definieras på ett tillräckligt brett och teknikneutralt sätt, så att begreppet omfattar all information om det innehåll som överförs eller utbyts (elektroniskt kommunikationsinnehåll) och information om slutanvändare av elektroniska kommunikationstjänster som behandlas i syfte att överföra, distribuera eller möjliggöra utbyte av elektroniskt kommunikationsinnehåll. Detta innefattar data för att spåra och identifiera meddelandets källa och adressat samt geografisk lokalisering, datum, varaktighet och typ av kommunikation. Oavsett om sådana signaler och tillhörande data överförs via tråd, radio, optiska eller andra elektromagnetiska system, inklusive satellitnät, kabelnät, fasta (kretskopplade och paketväxlade, inklusive internet) och mobila markbundna nät eller elkabelsystem, bör data förbundna med sådana signaler anses som metadata från elektronisk kommunikation och därför omfattas av bestämmelserna i denna förordning. Metadata från elektronisk kommunikation kan innefatta sådan information som ingår i abonnemanget på tjänsten när denna information behandlas i syfte att överföra, distribuera eller utbyta innehåll från elektronisk kommunikation.

(15) Data från elektronisk kommunikation bör behandlas som konfidentiella. Det betyder att varje ingrepp avseende överföring av data från elektronisk kommunikation, oavsett om det sker direkt genom mänsklig inblandning eller via automatiserad maskinell behandling, utan samtycke från samtliga kommunicerande parter bör vara förbjuden. Förbudet mot uppfångande av kommunikationsdata bör tillämpas under överföringen av data, dvs. fram till den avsedda adressatens mottagande av innehållet i den elektroniska kommunikationen. Uppfångande av data från elektronisk kommunikation kan t.ex. ske när någon annan än de kommunicerande parterna lyssnar på samtal eller läser, skannar eller lagrar innehållet i elektronisk kommunikation eller tillhörande metadata för andra syften än utbyte av kommunikation. Uppfångande kan även ske när tredje part övervakar besökta webbplatser och tidpunkterna för besök och interaktion

med andra etc. utan den berörda slutanvändarens samtycke. I takt med att tekniken utvecklats har antalet tekniska metoder för uppfångande också ökat. Det kan handla om allt ifrån installation av utrustning som samlar in data från terminalutrustning i utvalda områden, som utrustning för Imsi-spårning (*International Mobile Subscriber Identity*), till program och tekniker för t.ex. upprepad övervakning av surfvanor för att skapa slutanvändarprofiler. Andra exempel på uppfångande är när man fångar upp nyttolastdata eller innehållsdata från okrypterade trådlösa nät och routrar, inklusive surfvanor, utan slutanvändarens samtycke.

(16) Förbudet mot lagring av kommunikation är inte avsett att hindra någon automatisk, mellanliggande och tillfällig lagring av denna information i den mån som lagringen endast sker i syftet att utföra överföringen i det elektroniska kommunikationsnätet. Det bör inte heller hindra behandling av data från elektronisk kommunikation för att säkerställa de elektroniska kommunikationstjänsternas säkerhet och kontinuitet, inklusive kontroll av säkerhetshot, såsom förekomst av sabotageprogram, eller behandling av metadata för att uppfylla de nödvändiga tjänstekvalitetskraven, som t.ex. latens och variation i fördröjningen.

(17) Behandling av data från elektronisk kommunikation kan vara till nytta för företag, konsumenter och samhället som helhet. Jämfört med direktiv 2002/58/EG breddar denna förordning möjligheterna för leverantörer av elektroniska kommunikationstjänster att behandla metadata från elektronisk kommunikation baserat på slutanvändarnas samtycke. Slutanvändarna lägger dock stor vikt på konfidentialiteten för sin kommunikation, vilket även inkluderar deras onlineaktiviteter, och på att de vill ha kontroll över hur deras data från elektronisk kommunikation används för andra syften än överföring av kommunikationen. Därför bör denna förordning ålägga leverantörer av elektroniska kommunikationstjänster att erhålla användarnas samtycke till behandling av metadata från elektronisk kommunikation, vilket bör innefatta data om enhetens lokalisering som genereras för beviljande och bibehållande av åtkomst och uppkoppling till tjänsten. Lokaliseringsdata som genereras i andra sammanhang än tillhandahållande av elektroniska kommunikationstjänster bör inte anses som metadata. Några exempel på kommersiell användning av metadata från elektronisk kommunikation hos leverantörer av elektroniska kommunikationstjänster är tillhandahållande av värmekartor, en grafisk återgivning av data med hjälp av färger för att visa var det finns människor. För att visa trafikrörelser i vissa riktningar under en viss tidsperiod behövs en identifikator för att länka individers positioner i vissa tidsintervall. Denna identifikator skulle saknas om anonyma data användes och sådana rörelser skulle inte kunna visas. Sådan användning av metadata från elektronisk kommunikation skulle t.ex. kunna hjälpa offentliga organ och kollektivtrafikoperatörer att fastställa var ny infrastruktur ska utvecklas, baserat på den befintliga strukturens användning och belastning. Om en typ av behandling av metadata från elektronisk kommunikation, i synnerhet när ny teknik används och med beaktande av behandlingens art, omfattning, sammanhang och syfte, sannolikt kan medföra en hög risk för fysiska personers rättigheter och friheter bör man före behandlingen genomföra en konsekvensanalys avseende dataskydd och, allt efter omständigheterna, ett samråd med tillsynsmyndigheten, i enlighet med artiklarna 35 och 36 i förordning (EU) 2016/679.

(18) Slutanvändare kan ge sitt samtycke till att deras metadata behandlas, för att få tillgång till särskilda tjänster såsom skyddstjänster mot bedrägerier (genom analys av användningsdata, lokalisering och kundkonto i realtid). I den digitala ekonomin tillhandahålls ofta tjänster i utbyte mot annat än pengar, som t.ex. genom att

slutanvändarna exponeras för reklam. För denna förordnings syften bör en slutanvändares samtycke, oavsett om det rör sig om en fysisk person eller en juridisk person, ha samma betydelse och omfattas av samma villkor som samtycke av den registrerade enligt förordning (EU) 2016/679. Grundläggande bredbandstillgång och röstkommunikationstjänster ska anses som grundläggande tjänster för att individer ska kunna kommunicera och delta till gagn för den digitala ekonomin. Ett samtycke till behandling av data från användning av internet eller röstkommunikation kommer inte att vara giltigt om den registrerade inte har något verkligt eller fritt val, eller inte kan vägra eller dra tillbaka sitt samtycke utan negativa konsekvenser.

(19) Innehållet i elektronisk kommunikation berör den grundläggande rätten till respekt för privatliv och familjeliv, bostad och kommunikationer som skyddas enligt artikel 7 i stadgan. Ingrepp som avser innehållet i elektronisk kommunikation bör endast tillåtas under mycket tydligt definierade villkor och för särskilda syften, och bör omfattas av lämpliga skyddsmekanismer mot missbruk. Denna förordning ger leverantörer av elektroniska kommunikationstjänster möjlighet att behandla data från elektronisk kommunikation, med informerat samtycke från alla berörda slutanvändare. Leverantörer kan t.ex. erbjuda tjänster som innebär att man skannar e-postmeddelanden för att avlägsna visst på förhand definierat material. Med tanke på hur känsligt innehållet i kommunikation är omfattar denna förordning en presumtion att behandlingen av sådana innehållsdata kommer att medföra höga risker för fysiska personers rättigheter och friheter. Vid behandlingen av sådana typer av data bör leverantören av den elektroniska kommunikationstjänsten alltid samråda med tillsynsmyndigheten före behandlingen. Sådana samråd bör ske i enlighet med artikel 36.2 och 36.3 i förordning (EU) 2016/679. Presumtionen omfattar inte behandling av innehållsdata för tillhandahållandet av en tjänst som begärs av en slutanvändare om slutanvändaren har samtyckt till sådan behandling och behandlingen utförs för de syften och med den varaktighet som är strikt nödvändiga och proportionella för sådana tjänster. Efter att innehållet i elektronisk kommunikation sänts av slutanvändaren och mottagits av den avsedda slutanvändaren (en eller flera) får den registreras eller lagras av slutanvändaren, slutanvändarna eller en tredje part som de anförtrott uppgiften att registrera eller lagra sådana data. Varje behandling av sådana data bör vara förenlig med förordning (EU) 2016/679.

(20) Terminalutrustning för slutanvändare av elektroniska kommunikationsnät och all information om användningen av sådan terminalutrustning, oavsett om informationen lagras eller utsänds av sådan utrustning, begärs från den eller behandlas så att utrustningen kan uppkopplas till en annan enhet eller nätutrustning, tillhör slutanvändarnas privata sfär som kräver skydd enligt Europeiska unionens stadga om de grundläggande rättigheterna och den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna. I och med att sådan utrustning innehåller eller behandlar information som kan röja uppgifter om en persons känslomässiga, politiska och sociala komplexitet, inklusive innehållet i meddelanden, bilder, lokaliseringsuppgifter för personer genom åtkomst till anordningens GPS-funktioner, kontaktlistor och annan information som redan finns lagrad i enheten, bör informationen i sådana enheter omfattas av ett utökat integritetsskydd. S.k. spionprogram, pixeltaggar, gömda identifikatorer, kartläggningskakor och andra liknande oönskade kartläggningsverktyg kan gå in i slutanvändarens terminalutrustning utan dennes vetskap för att få tillgång till information, lagra gömd information eller kartlägga aktiviteter. Information om slutanvändarens enhet kan också samlas in på distans för identifiering och kartläggning, med användning av sådan teknik som s.k. *device fingerprinting*

(signaturinsamling), ofta utan att slutanvändaren vet om det, vilket kan inkräkta allvarligt på slutanvändarnas personliga integritet. Teknik för upprepad övervakning av slutanvändarnas handlingar, t.ex. genom kartläggning av deras onlineaktivitet eller lokaliseringen för deras terminalutrustning, eller teknik som underminerar driften av slutanvändarnas terminalutrustning, utgör ett allvarligt hot mot slutanvändarnas personliga integritet. Därför bör sådana ingrepp som avser slutanvändarens terminalutrustning endast tillåtas med slutanvändarens samtycke och för specifika och öppet redovisade syften.

(21) Undantagen från skyldigheten att erhålla samtycke till att använda behandlings- och lagringskapacitet hos terminalutrustning eller till att få tillgång till information som lagras i terminalutrustningen bör begränsas till situationer som medför inget eller endast minimalt intrång i den personliga integriteten. Samtycke bör t.ex. inte krävas för att tillåta sådan teknisk lagring eller åtkomst som är strikt nödvändig och proportionell för det legitima syftet att möjliggöra användningen av en viss tjänst som uttryckligen begärs av slutanvändaren. Detta kan innefatta lagring av kakor för tidsrymden av en enda upprättad session på en webbplats för att hålla reda på slutanvändarens inmatade uppgifter vid ifyllandet av onlineformulär med flera sidor. Kakor kan också vara ett legitimt och användbart verktyg för att t.ex. mäta webbtrafik till en webbplats. Informationssamhällesleverantörer som gör konfigurationskontroller för att tillhandahålla en tjänst i enlighet med slutanvändarens inställningar och enbart loggning av det faktum att slutanvändarens enhet inte lyckas ta emot innehåll som begärs av slutanvändaren bör inte utgöra åtkomst till en sådan enhet eller användning av enhetens behandlingskapacitet.

(22) De metoder som används för att tillhandahålla information och erhålla slutanvändarens samtycke bör vara så användarvänliga som möjligt. Den allmänna användningen av kartläggningskakor och annan kartläggningsteknik innebär att slutanvändarna allt oftare uppmanas att ge sitt samtycke till att sådana kartläggningskakor lagras i deras terminalutrustning. Därmed översvämmas slutanvändarna av uppmaningar att lämna samtycke. Användning av tekniska metoder för att lämna samtycke, t.ex. genom öppet redovisade och användarvänliga inställningar, skulle kunna lösa detta problem. Därför bör denna förordning omfatta en möjlighet att uttrycka samtycke genom användning av lämpliga inställningar i en webbläsare eller annan tillämpning. De val som slutanvändarna gör då de lägger in sekretessinställningarna för en webbläsare eller andra tillämpningar bör vara bindande för, och verkställningsbara gentemot, alla tredje parter. Webbläsare är en typ av programvara som gör det möjligt att hämta och lägga ut information på internet. Andra typer av tillämpningar, t.ex. sådana som tillåter uppringning och meddelandetjänster eller som tillhandahåller färdanvisningar, har också samma funktioner. Webbläsare fungerar som förbindelselänkar för det som sker mellan slutanvändaren och webbplatsen. Ur detta perspektiv har webbläsarna en privilegierad position när det gäller möjligheten att inta en aktiv roll för att hjälpa slutanvändaren att kontrollera flödet av information till och från terminalutrustningen. Webbläsare kan användas som grindvakter och därigenom hjälpa slutanvändarna att hindra åtkomst till eller lagring av information från deras terminalutrustning (t.ex. smarttelefon, datorplatta eller dator).

(23) Principerna för inbyggt dataskydd och dataskydd som standard kodifierades genom artikel 25 i förordning (EU) 2016/679. I dag är de förvalda inställningarna i de flesta moderna webbläsare att ”godta alla kakor” Därför bör leverantörer av mjukvara som gör det möjligt att hämta och lägga ut information på internet vara skyldiga att konfigurera programvaran så att den omfattar alternativet att hindra tredje parter från

att lagra information i terminalutrustningen. Detta uttrycks ofta som ”avvisa tredjepartskakor”. Slutanvändarna bör erbjudas ett antal sekretessinställningsalternativ, från högre (t.ex. ”godta aldrig kakor”) till lägre nivå (t.ex. ”godta alltid kakor”) och mellannivå (t.ex. ”avvisa tredjepartskakor” eller ”godta endast förstapartskakor”). Sådana sekretessinställningar bör presenteras på ett väl synligt och begripligt sätt.

(24) För att webbläsare ska kunna erhålla slutanvändarnas samtycke enligt förordning (EU) 2016/679 till t.ex. lagring av tredjeparts kartläggningskakor bör de bl.a. kräva en entydig bekräftande handling från slutanvändaren av terminalutrustningen som utrycker att denna ger ett frivilligt, specifikt, informerat och otvetydigt medgivande till lagring av och åtkomst till sådana kakor i och från terminalutrustningen. Sådana handlingar kan anses vara jakande t.ex. om slutanvändaren aktivt måste välja ”godta tredjepartskakor” för att bekräfta sitt samtycke och ges den information som behövs för att kunna göra valet. Därför är det nödvändigt att föreskriva att leverantörer av programvara som ger tillgång till internet i samband med installationen ska informera slutanvändarna om möjligheten att välja mellan de alternativa sekretessinställningarna och be dem att göra ett val. Den information som lämnas bör inte avskräcka slutanvändare från att välja högre sekretessinställningar och den bör innehålla relevant information om riskerna med att tillåta att tredjepartskakor lagras i datorn, inklusive sammanställningen av arkiverade uppgifter om personers webbläsarhistorik under längre tid och användningen av sådana uppgifter för individanpassad reklam. Webbläsare uppmuntras att tillhandahålla enkla sätt för slutanvändare att när som helst ändra sekretessinställningarna och att låta användaren göra undantag för eller ”vitlista” vissa webbplatser eller ange för vilka webbplatser som (tredje)partskakor alltid eller aldrig tillåts.

(25) För åtkomst till elektroniska kommunikationsnät krävs det regelbunden sändning av vissa datapaket för att hitta eller upprätthålla en anslutning till nätet eller till andra enheter på nätet. Enheterna måste också ha tilldelats en unik adress för att kunna identifieras i det aktuella nätet. Standarderna för trådlös och mobil telefoni omfattar också sändning av aktiva signaler som innehåller identifikatorer som t.ex. en MAC-adress, IMEI (*International Mobile Station Equipment Identity*) och IMSI. En enda trådlös basstation (dvs. en sändare och mottagare), såsom en trådlös accesspunkt, har en specifik räckvidd inom vilken sådan information kan fångas upp. Det har kommit nya tjänsteleverantörer som erbjuder kartläggningstjänster baserade på skanning av utrustningsrelaterad information med många olika funktioner, inklusive personräkning, där man tillhandahåller data om antalet personer som står i kö, fastställer antalet personer i ett visst område etc. Denna information får användas för mer inkräktande syften, som att sända kommersiella meddelanden med individanpassade erbjudanden till slutanvändare, t.ex. när de går in i affärer. Vissa av dessa funktioner medför inte några höga risker för den personliga integriteten, men andra gör det, t.ex. sådana som kartlägger individer över tid, inklusive upprepade besök på specificerade platser. Leverantörer som använder sådana metoder bör visa tydliga meddelanden på kanten av täckningsområdet som innan slutanvändarna går in på det definierade området informerar dem om att tekniken används inom ett visst område, om syftet med kartläggningen, om den person som är ansvarig för det och om förekomsten av eventuella åtgärder som terminalutrustningens slutanvändare kan vidta för att minimera eller stoppa insamlingen. Ytterligare information bör tillhandahållas när personuppgifter samlas in i enlighet med artikel 13 i förordning (EU) 2016/679.

(26) När behandling av data från elektronisk kommunikation, som utförs av leverantörer av elektroniska kommunikationstjänster, omfattas av denna förordning, bör förordningen

omfatta en möjlighet för unionen eller medlemsstaterna att, under särskilda villkor, i lag begränsa vissa skyldigheter och rättigheter, om en sådan begränsning utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle för att skydda särskilda allmänna intressen, inklusive nationell säkerhet, försvar och allmän säkerhet samt för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, vilket innefattar skydd mot och förebyggande av hot mot allmän säkerhet och andra viktiga mål i unionens eller en medlemsstats allmänintresse, i synnerhet när det gäller ett viktigt ekonomiskt eller finansiellt intresse för unionen eller en medlemsstat, eller en övervakning, inspektion eller regleringsfunktion som är knuten till myndighetsutövning avseende sådana intressen. Därför bör denna förordning inte påverka medlemsstaternas möjlighet att på lagligt sätt uppfånga elektronisk kommunikation eller att vidta andra åtgärder, om det är nödvändigt och proportionellt för något av dessa ändamål och sker i enlighet med Europeiska unionens stadga om de grundläggande rättigheterna och den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, i den tolkning dessa fått i rättspraxis från Europeiska domstolen för de mänskliga rättigheterna. Leverantörer av elektroniska kommunikationstjänster bör ha lämpliga förfaranden som främjar legitima krav från behöriga myndigheter, vilka även beaktar den utsedda företrädarens roll enligt artikel 3.3 när så är relevant.

(27) När det gäller nummerpresentation är det nödvändigt att skydda den uppringande partens rätt att förhindra identifiering av det nummer från vilket samtalet görs och den uppringda partens rätt att avvisa samtal från oidentifierade nummer. Det ligger i vissa slutanvändares intresse, i synnerhet hjälplinjer och liknande organisationer, att garantera de uppringandes anonymitet. När det gäller nummerpresentation är det nödvändigt att skydda den uppringande partens rätt och berättigade intresse av att förhindra identifiering av det nummer från vilket samtalet faktiskt görs.

(28) Det är i särskilda fall berättigat att förhindra att skydd mot nummerpresentation används. Slutanvändarnas rätt till integritet avseende nummerpresentation bör begränsas till när det är nödvändigt för att spåra okynnessamtal och i fråga om nummerpresentation och lokaliseringsuppgifter när det är nödvändigt för att larmtjänster, som eCall, ska kunna utföra sina uppgifter så effektivt som möjligt.

(29) Det finns teknik som gör det möjligt för leverantörer av elektroniska kommunikationstjänster att begränsa slutanvändarnas mottagande av oönskade samtal på olika sätt, inklusive blockering av tysta samtal och andra bedrägliga samtal och okynnessamtal. Leverantörer av allmänt tillgängliga nummerbaserade interpersonella kommunikationstjänster bör använda denna teknik och avgiftsfritt skydda slutanvändarna mot okynnessamtal. Leverantörerna bör se till att slutanvändarna är medvetna om förekomsten av sådana funktioner, t.ex. genom att publicera detta faktum på sin webbplats.

(30) Allmänt tillgängliga förteckningar över slutanvändare av elektroniska kommunikationstjänster har bred spridning. Allmänt tillgängliga förteckningar avser varje förteckning eller tjänst som innehåller slutanvändarnas uppgifter, som telefonnummer (inklusive mobilnummer) och e-postadress och som även omfattar upplysningstjänster. För en fysisk persons rätt till personlig integritet och skydd av personuppgifter krävs att slutanvändare som är fysiska personer ombeds lämna samtycke innan deras personuppgifter förs in i en förteckning. Juridiska personers legitima intressen kräver att slutanvändare som är juridiska personer har rätt att invända mot att data som rör dem förs in i en förteckning.

(31) Om slutanvändare som är fysiska personer lämnar sitt samtycke till att deras uppgifter förs in i sådana förteckningar bör de på basis av samtycke kunna bestämma vilka kategorier av personuppgifter som ska finnas med i förteckningen (t.ex. namn, e-postadress, hemadress, användarnamn, telefonnummer). Leverantörer av allmänt tillgängliga förteckningar bör också informera slutanvändarna om förteckningens syften och sökfunktioner innan de tar med dem i förteckningen. Slutanvändarna bör genom samtycke kunna bestämma vilka kategorier av personuppgifter som ska kunna användas för sökningar avseende deras kontaktuppgifter. De kategorier av personuppgifter som tas med i förteckningen och de kategorier av personuppgifter som kan användas för sökningar avseende slutanvändarens kontaktuppgifter är inte nödvändigtvis identiska.

(32) I denna förordning avses med direktmarknadsföring varje form av reklam där en fysisk eller juridisk person sänder direktmarknadsföringsmeddelanden direkt till en eller flera identifierade eller identifierbara slutanvändare via elektroniska kommunikationstjänster. Utöver erbjudanden om produkter och tjänster för kommersiella syften bör detta också inkludera meddelanden som sänds av politiska partier som kontaktar fysiska personer via elektroniska kommunikationstjänster för att främja sina partier. Samma sak bör gälla för meddelanden som sänds av andra ideella organisationer för att stödja organisationens syften.

(33) Det bör också finnas mekanismer som skyddar slutanvändarna mot oönskad kommunikation i direktmarknadsföringssyften, som inkräktar på slutanvändarnas privatliv. Graden av olägenhet och intrång i den enskildes personliga integritet anses vara relativt lika oavsett vilken av de många olika typer av tekniker och kanaler som används för denna elektroniska kommunikation och oavsett om det är genom automatiska uppringnings- och kommunikationssystem, tillämpningar för snabbmeddelanden, e-post, sms, mms och Bluetooth etc. Därför är det motivera att kräva att slutanvändarens samtycke erhålls innan kommersiell elektronisk kommunikation i direktmarknadsföringssyfte sänds till slutanvändare, för att effektivt skydda enskilda mot intrång i deras personliga integritet och skydda juridiska personers legitima intressen. Med tanke på den rättsliga förutsebarheten och behovet av att säkerställa att bestämmelserna som skyddar mot icke begärd elektronisk kommunikation förblir framtidssäkrade är det motiverat att fastställa en enda uppsättning bestämmelser som inte varierar beroende på vilken teknik som används för att förmedla dessa icke begärda meddelanden och samtidigt garantera en likvärdig skyddsnivå för alla medborgare i unionen. Det är dock rimligt att tillåta användning av e-postkontaktuppgifter inom ramen för ett befintligt kundförhållande för att erbjuda liknande produkter och tjänster. Sådana möjligheter bör endast gälla för samma företag som har erhållit de elektroniska kontaktuppgifterna i enlighet med förordning (EU) 2016/679.

(34) När slutanvändare har lämnat sitt samtycke till att ta emot icke begärda meddelanden i direktmarknadsföringssyfte bör de ändå kunna dra tillbaka sitt samtycke när som helst och på ett enkelt sätt. För att göra det enklare att kontrollera efterlevnaden av unionsbestämmelserna om icke begärda direktmarknadsföringsmeddelanden är det nödvändigt att förbjuda att man döljer identiteten eller använder falska identiteter eller falska returadresser eller nummer när icke begärda kommersiella meddelanden sänds i direktmarknadsföringssyfte. Icke begärd marknadsföringskommunikation bör därför vara tydligt igenkännbar som sådan och bör visa identiteten på den juridiska eller fysiska person som sänder meddelandet och tillhandahålla den information som

mottagarna behöver för att utöva sin rätt att tacka nej till att få ytterligare skriftliga och/eller muntliga marknadsföringsmeddelanden.

(35) För att göra det enkelt att dra tillbaka sitt samtycke bör juridiska eller fysiska personer som sänder direktmarknadsföringskommunikation per e-post bifoga en länk eller en giltig e-postadress, som slutanvändarna enkelt kan använda för att dra tillbaka sitt samtycke. När fysiska eller juridiska personer utför direktmarknadsföringskommunikation genom personsamtal och samtal via automatiska uppringnings- och kommunikationssystem bör identiteten för den anropande linje som kan användas för att ringa upp företaget visas eller en särskild kod som identifierar samtalet som ett marknadsföringssamtal anges.

(36) Personsamtal för direktmarknadsföring som inte inbegriper användning av automatiska uppringnings- och kommunikationssystem är dyrare för avsändaren och medför inte några finansiella kostnader för slutanvändarna. Medlemsstaterna bör därför kunna införa och/eller behålla nationella system som endast tillåter sådana samtal till slutanvändare som inte har motsatt sig det.

(37) Tjänsteleverantörer som erbjuder elektroniska kommunikationstjänster bör informera slutanvändarna om åtgärder som de kan vidta för att skydda säkerheten för sin kommunikation, t.ex. genom att använda specifika typer av programvara eller krypteringsteknik. Kravet på att informera slutanvändarna om särskilda säkerhetsrisker befriar inte en tjänsteleverantör från skyldigheten att på egen bekostnad vidta lämpliga och omedelbara åtgärder för att avhjälpa nya oförutsedda säkerhetsrisker och återställa tjänstens normala säkerhetsnivå. Information om säkerhetsrisker bör lämnas till abonnenten utan avgift. Säkerheten bedöms mot bakgrund av artikel 32 i förordning (EU) 2016/679.

(38) För att säkra full överensstämmelse med förordning (EU) nr 2016/679 bör kontrollen av efterlevnaden av bestämmelserna i denna förordning anförtros åt samma myndigheter som ansvarar för att kontrollera efterlevnaden av bestämmelserna i förordning (EU) nr 2016/679, och denna förordning förlitar sig på mekanismen för enhetlighet enligt förordning (EU) nr 2016/679. Medlemsstaterna bör kunna ha fler än en tillsynsmyndighet om det behövs för att ta hänsyn till den egna konstitutionella, organisatoriska och administrativa strukturen. Tillsynsmyndigheterna bör också ha ansvaret för att övervaka denna förordnings tillämpning när det gäller data från elektronisk kommunikation för juridiska personer. Sådana tilläggsuppgifter bör inte äventyra tillsynsmyndighetens förmåga att utföra sina uppgifter vad gäller skydd av personuppgifter enligt förordning (EU) 2016/679 och denna förordning. Varje tillsynsmyndighet bör tilldelas de ytterligare ekonomiska resurser och personalresurser, lokaler och infrastrukturer som krävs för att den effektivt ska kunna utföra sina uppgifter enligt denna förordning.

(39) Varje tillsynsmyndighet bör ha behörighet att inom sin egen medlemsstats territorium utöva de befogenheter och utföra de uppgifter som anges i denna förordning. För att säkerställa en konsekvent övervakning och kontroll av efterlevnaden av denna förordning i hela unionen bör tillsynsmyndigheterna ha samma uppgifter och effektiva befogenheter i varje medlemsstat, utan att det påverkar åklagarmyndigheternas befogenheter enligt medlemsstaternas nationella rätt, att upplysa de rättsliga myndigheterna om överträdelser av denna förordning och delta i rättsliga förfaranden. Medlemsstaterna och deras tillsynsmyndigheter uppmuntras att vid tillämpningen av denna förordning ta hänsyn till mikroföretagens samt de små och medelstora företagens särskilda behov.

(40) För att stärka kontrollen av att bestämmelserna i denna förordning efterlevs bör varje tillsynsmyndighet ha befogenhet att besluta om sanktioner, inbegripet administrativa sanktionsavgifter, för överträdelser av denna förordning, utöver eller i stället för andra lämpliga åtgärder enligt förordningen. Det bör i denna förordning anges vilka överträdelserna är, den övre gränsen för och kriterierna för fastställande av de administrativa sanktionsavgifterna, som i varje enskilt fall bör bestämmas av den behöriga tillsynsmyndigheten med beaktande av alla relevanta omständigheter i det särskilda fallet, med vederbörlig hänsyn bl.a. till överträdelsens karaktär, svårighetsgrad och varaktighet samt till dess följder och till de åtgärder som vidtas för att sörja för fullgörandet av skyldigheterna enligt denna förordning och för att förebygga eller lindra konsekvenserna av överträdelsen. När det gäller fastställandet av en sanktionsavgift enligt denna förordning bör ett företag förstås som ett företag i enlighet med artiklarna 101 och 102 i fördraget.

(41) I syfte att uppnå målen för denna förordning, nämligen att skydda fysiska personers grundläggande rättigheter och friheter och i synnerhet deras rätt till skydd av personuppgifter och för att säkra det fria flödet av personuppgifter inom unionen, bör befogenheten att anta akter i enlighet med artikel 290 i fördraget delegeras till kommissionen för att komplettera denna förordning. Delegerade akter bör framför allt antas när det gäller den information som ska visas, även med hjälp av standardiserade ikoner, för att ge en väl synlig och begriplig översikt över insamlingen av information som utsänds från terminalutrustningen, insamlingens syfte, den person som är ansvarig för insamlingen samt vilka åtgärder som terminalutrustningens slutanvändare kan använda för att minimera insamlingen. Delegerade akter krävs också för att specificera en kod för att identifiera direktmarknadsföringssamtal, inklusive sådana som görs genom automatiska uppringnings- och kommunikationssystem. Det är särskilt viktigt att kommissionen genomför lämpliga samråd och att dessa samråd genomförs i enlighet med principerna i det interinstitutionella avtalet om bättre lagstiftning av den 13 april 2016[8]. För att säkerställa lika stor delaktighet i förberedelsen av delegerade akter erhåller Europaparlamentet och rådet alla handlingar samtidigt som medlemsstaternas experter, och deras experter ges systematiskt tillträde till möten i kommissionens expertgrupper som arbetar med förberedelse av delegerade akter. För att säkerställa enhetliga villkor för tillämpningen av denna förordning bör kommissionen också ges genomförandebefogenheter i enlighet med denna förordning. Dessa befogenheter bör utövas i enlighet med förordning (EU) nr 182/2011.

(42) Eftersom målet för denna förordning, nämligen att säkerställa en likvärdig nivå för skyddet av fysiska och juridiska personer och det fria flödet av data från elektronisk kommunikation inom hela unionen, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av åtgärdens omfattning eller verkningar, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen (EU-fördraget). I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå detta mål.

(43) Direktiv 2002/58/EG bör upphävas.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

[8] Interinstitutionellt avtal av den 13 april 2016 mellan Europaparlamentet, Europeiska unionens råd och Europeiska kommissionen om bättre lagstiftning (EUT L 123, 12.5.2016, s. 1).

KAPITEL I
ALLMÄNNA BESTÄMMELSER

Artikel 1
Syfte

1. I denna förordning fastställs bestämmelser om skydd av de grundläggande rättigheterna och friheterna för fysiska och juridiska personer vid tillhandahållandet och användningen av elektroniska kommunikationstjänster, i synnerhet rätten till respekt för privatliv och kommunikation samt skyddet av fysiska personer med avseende på behandling av personuppgifter.

2. Denna förordning säkerställer fri rörlighet för data från elektronisk kommunikation och elektroniska kommunikationstjänster inom unionen, som varken ska begränsas eller förbjudas av skäl som rör respekt för privatlivet och kommunikation för fysiska och juridiska personer samt skydd för fysiska personer med avseende på behandling av personuppgifter.

3. Bestämmelserna i denna förordning preciserar och kompletterar förordning (EU) nr 2016/679 genom att fastställa särskilda bestämmelser för de syften som anges i punkterna 1 och 2.

Artikel 2
Materiellt tillämpningsområde

1. Denna förordning ska tillämpas på sådan behandling av data från elektronisk kommunikation som utförs i samband med tillhandahållandet och användningen av elektroniska kommunikationstjänster samt på information som rör slutanvändares terminalutrustning.

2. Denna förordning ska inte tillämpas på följande:

(a) Verksamhet som faller utanför unionslagstiftningens tillämpningsområde.

(b) Medlemsstaternas verksamhet som omfattas av avdelning V kapitel 2 i fördraget om Europeiska unionen.

(c) Elektroniska kommunikationstjänster som inte är allmänt tillgängliga.

(d) Verksamhet som behöriga myndigheter utför i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, i vilket även ingår att skydda mot samt förebygga hot mot den allmänna säkerheten.

3. Behandling av data från elektronisk kommunikation som utförs av unionens institutioner, organ och byråer regleras i förordning (EU) 00/0000 [ny förordning som ersätter förordning 45/2001].

4. Denna förordning ska inte påverka tillämpningen av direktiv 2000/31/EG[9], i synnerhet inte bestämmelserna om tjänstelevererande mellanhänders ansvar enligt artiklarna 12 och 15 i det direktivet.

[9] Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden (”Direktiv om elektronisk handel”) (EGT L 178, 17.7.2000, s. 1).

5. Denna förordning ska inte påverka tillämpningen av bestämmelserna i direktiv 2014/53/EG.

Artikel 3
Territoriellt tillämpningsområde och företrädare

1. Denna förordning ska tillämpas på följande:

(a) Tillhandahållande av elektroniska kommunikationstjänster till slutanvändare i unionen, oavsett om någon betalning krävs av slutanvändaren eller inte.

(b) Användning av sådana tjänster.

(c) Skydd av information som rör terminalutrustningen för slutanvändare i unionen.

2. När leverantören av en elektronisk kommunikationstjänst inte är etablerad i unionen ska den skriftligen utse en företrädare i unionen.

3. Företrädaren ska vara etablerad i en av de medlemsstater där slutanvändarna av sådana elektroniska kommunikationstjänster befinner sig.

4. Företrädaren ska ha befogenhet att besvara frågor och tillhandahålla information som ett komplement till eller i stället för den leverantör som företrädaren representerar, i synnerhet till tillsynsmyndigheter och slutanvändare, om alla frågor som rör behandling av data från elektronisk kommunikation i syfte att säkerställa överensstämmelse med denna förordning.

5. Utseendet av en företrädare enligt punkt 2 ska inte påverka rättsliga åtgärder som kan inledas mot en fysisk eller juridisk person som behandlar data från elektronisk kommunikation i samband med tillhandahållandet av elektroniska kommunikationstjänster från länder utanför unionen till slutanvändare inom unionen.

Artikel 4
Definitioner

1. I denna förordning gäller följande definitioner:

(a) Definitionerna i förordning (EU) nr 2016/679.

(b) Definitionerna av ”elektroniskt kommunikationsnät”, "elektronisk kommunikationstjänst”, ”interpersonell kommunikationstjänst”, ”nummerbaserad interpersonell kommunikationstjänst”, ”slutanvändare” och ”samtal” i punkterna 1, 4, 5, 6, 7, 14 respektive 21 i artikel 2 i [rådets direktiv om inrättande av en europeisk kodex för elektronisk kommunikation].

(c) Definitionen av ”terminalutrustning” i artikel 1.1 i kommissionens direktiv 2008/63/EG[10].

2. Vid tillämpning av punkt 1 b ska definitionen av ”interpersonell kommunikationstjänst” innefatta tjänster som möjliggör interpersonell och interaktiv kommunikation enbart som en extrafunktion av mindre betydelse som är direkt kopplad till en annan tjänst.

3. I denna förordning gäller dessutom följande definitioner:

[10] Kommissionens direktiv 2008/63/EG av den 20 juni 2008 om konkurrens på marknaderna för teleterminalutrustning (EUT L 162, 21.6.2008, s. 20).

(a) *data från elektronisk kommunikation*: innehåll och metadata från elektronisk kommunikation.

(b) *innehåll från elektronisk kommunikation*: innehåll som utbyts genom elektroniska kommunikationstjänster, såsom text, tal, videoklipp, bilder och ljud.

(c) *metadata från elektronisk kommunikation*: data som behandlas i ett elektroniskt kommunikationsnät i syfte att sända, förmedla eller utbyta innehåll från elektronisk kommunikation; detta innefattar data för att spåra och identifiera källan och adressaten för ett meddelande, data om enhetens lokalisering som genereras i samband med tillhandahållandet av elektroniska kommunikationstjänster, samt datum, tidpunkt, varaktighet och typ av kommunikation.

(d) *allmänt tillgänglig förteckning:* en förteckning över slutanvändare av elektroniska kommunikationstjänster, oavsett om den är i tryckt eller elektronisk form, som offentliggörs eller görs tillgänglig för allmänheten eller en del av allmänheten, även genom en upplysningstjänst.

(e) *e-post*: varje elektroniskt meddelande som innehåller information som t.ex. text, tal, video, ljud eller bild som sänds via ett elektroniskt kommunikationsnät och som kan lagras i nätet eller i tillhörande databehandlingsanläggningar, eller i mottagarens terminalutrustning.

(f) *direktmarknadsföringskommunikation*: varje form av annonsering, skriftlig eller muntlig, som sänds till en eller flera identifierade eller identifierbara slutanvändare av elektroniska kommunikationstjänster, inklusive användning av automatiska uppringnings- och kommunikationssystem med eller utan mänsklig medverkan, e-post, sms osv.

(g) *personsamtal för direktmarknadsföring*: direktsamtal som inte medför någon användning av automatiska uppringnings- och kommunikationssystem.

(h) *automatiska uppringnings- och kommunikationssystem:* system som automatiskt kan inleda samtal till en eller flera mottagare i enlighet med instruktioner som fastställts för systemet och överföra ljud som inte är direktsamtal, inklusive samtal som görs med hjälp av automatiska uppringnings- och kommunikationssystem som kopplar den uppringande personen till en individ.

KAPITEL I
SKYDD AV FYSISKA OCH JURIDISKA PERSONERS ELEKTRONISKA KOMMUNIKATION OCH AV INFORMATION SOM LAGRAS I DERAS TERMINALUTRUSTNING

Artikel 5
Konfidentialitet för data från elektronisk kommunikation

Data från elektronisk kommunikation ska vara konfidentiella. Varje ingrepp avseende data från elektronisk kommunikation, som t.ex. genom lyssnande, avlyssning, lagring, övervakning, skanning eller andra typer av uppfångande, bevakning eller behandling av data från elektronisk kommunikation, av andra personer än slutanvändarna, ska vara förbjuden utom när den är tillåten enligt denna förordning.

Artikel 6
Tillåten behandling av data från elektronisk kommunikation

1. Leverantörer av elektroniska kommunikationstjänster och kommunikationsnät får behandla data från elektronisk kommunikation om

(a) det är nödvändigt för överföringen av meddelandet under den tidsperiod som är nödvändig för detta syfte, eller

(b) det är nödvändigt för att bevara eller återupprätta säkerheten för elektroniska kommunikationsnät och elektroniska kommunikationstjänster, eller för att upptäcka tekniska fel och/eller brister i överföringen av elektronisk kommunikation, under den tidsperiod som är nödvändig för detta syfte.

2. Leverantörer av elektroniska kommunikationstjänster får behandla metadata från elektronisk kommunikation om

(a) det är nödvändigt för att uppfylla obligatoriska skyldigheter avseende tjänstekvalitet enligt [direktivet om inrättande av en europeisk kodex för elektronisk kommunikation] eller förordning (EU) 2015/2120[11] under den tidsperiod som är nödvändig för detta syfte, eller

(b) det är nödvändigt för fakturering eller beräkning av samtrafikavgifter, eller för att upptäcka eller stoppa bedrägeri eller missbruk i samband med användning av, eller abonnemang på, elektroniska kommunikationstjänster, eller

(c) den berörda slutanvändaren har lämnat sitt samtycke till att hans eller hennes kommunikationsmetadata behandlas för ett eller flera specificerade syften, inbegripet för tillhandahållandet av specifika tjänster till sådana slutanvändare, förutsatt att de berörda syftena inte kan uppfyllas genom behandling av anonymiserad information.

3. Leverantörer av elektroniska kommunikationstjänster får behandla innehåll från elektronisk kommunikation enbart

(a) i det enda syftet att tillhandahålla en specifik tjänst till en slutanvändare, om berörd slutanvändare (en eller flera) har lämnat sitt samtycke till behandlingen av hans eller hennes innehåll från elektronisk kommunikation och tillhandahållandet av denna tjänst inte kan genomföras utan behandlingen av sådant innehåll, eller

b) om samtliga berörda slutanvändare har lämnat sitt samtycke till behandling av deras innehåll från elektronisk kommunikation för ett eller flera specificerade syften som inte kan uppfyllas genom behandling av information som anonymiserats, och leverantören har samrått med tillsynsmyndigheten. Artikel 36.2 och 36.3 i förordning (EU) 2016/679 ska tillämpas på samrådet med tillsynsmyndigheten.

[11] Europaparlamentets och rådets förordning (EU) 2015/2120 av den 25 november 2015 om åtgärder rörande en öppen internetanslutning och om ändring av direktiv 2002/22/EG om samhällsomfattande tjänster och användares rättigheter avseende elektroniska kommunikationsnät och kommunikationstjänster och förordning (EU) nr 531/2012 om roaming i allmänna mobilnät i unionen (EUT L 310, 26.11.2015, s. 1).

Artikel 7

Lagring och radering av data från elektronisk kommunikation

1. Utan att det påverkar tillämpningen av artikel 6.1 b och artikel 6.3 a och b ska leverantören av den elektroniska kommunikationstjänsten radera innehåll från elektronisk kommunikation eller anonymisera dessa data efter att innehållet mottagits av den avsedda mottagaren eller de avsedda mottagarna. Sådana data får registreras eller lagras av slutanvändarna eller av tredje part som av dem anförtrotts uppgiften att registrera, lagra eller på annat sätt behandla sådana data, i enlighet med förordning (EU) 2016/679.

2. Utan att det påverkar tillämpningen av artikel 6.1 b och artikel 6.2 a och c ska leverantören av den elektroniska kommunikationstjänsten radera metadata från elektronisk kommunikation eller anonymisera dessa data när de inte längre behövs för syftet att överföra kommunikationen.

3. Om behandling av metadata från elektronisk kommunikation sker i faktureringssyfte i enlighet med artikel 6.2 b får berörda metadata behållas fram till utgången av den period under vilken det lagligen går att göra invändningar mot fakturan eller kräva betalning enligt nationell lagstiftning.

Artikel 8

Skydd av information som lagras i eller avser slutanvändarnas terminalutrustning

1. Användning av behandlings- och lagringskapacitet i terminalutrustning och insamling av information från slutanvändarnas terminalutrustning, inklusive om programvara och hårdvara, som görs av någon annan än den berörda slutanvändaren ska vara förbjuden, utom om

(a) den är nödvändig för det enda syftet att utföra överföringen av elektronisk kommunikation via ett elektroniskt kommunikationsnät, eller

(b) slutanvändaren har lämnat sitt samtycke, eller

(c) den är nödvändig för tillhandahållandet av en informationssamhällestjänst som begärs av slutanvändaren, eller

(d) den är nödvändig för mätning av webbpublik, förutsatt att dessa mätningar utförs av leverantören av den informationssamhällestjänst som begärs av slutanvändaren.

2. Insamling av sådan information som terminalutrustningen utsänder för att kunna kopplas upp till en annan enhet eller till nätutrustning ska vara förbjuden, utom om

(a) den görs enbart för att upprätta en anslutning och under den tidsperiod som krävs för detta, eller

(b) ett entydigt och framträdande meddelande visas som informerar om åtminstone insamlingsmetoderna, insamlingens syfte, ansvarig person och övrig information som krävs enligt artikel 13 i förordning (EU) nr 2016/679, när personuppgifter samlas in, samt om åtgärder som terminalutrustningens slutanvändare kan vidta för att stoppa eller minimera insamlingen.

Villkoret för insamlingen av sådan information ska vara att lämpliga tekniska och organisatoriska åtgärder vidtas för att säkerställa en säkerhetsnivå som är anpassad till riskerna, enligt artikel 32 i förordning (EU) 2016/679.

3. Den information som ska tillhandahållas enligt punkt 2 b får tillhandahållas i kombination med standardiserade ikoner för att ge en meningsfull översikt över insamlingen på ett väl synligt, begripligt och tydligt läsbart sätt.

4. Kommissionen ska ges befogenhet att anta delegerade akter i enlighet med artikel 27 för att fastställa vilken information som ska visas med hjälp av den standardiserade ikonen samt förfarandena för tillhandahållande av standardiserade ikoner.

Artikel 9
Samtycke

1. Definitionen av och villkoren för samtycke enligt artiklarna 4.11 och 7 i förordning (EU) 2016/679 ska tillämpas.

2. Utan att det påverkar tillämpningen av punkt 1 får samtycke, när det är tekniskt möjligt och genomförbart, för syftena i artikel 8.1 b, uttryckas genom användning av lämpliga tekniska inställningar i en programvara som möjliggör internettillgång.

3. Slutanvändare som har samtyckt till behandling av data från elektronisk kommunikation enligt artikel 6.2 c och artikel 6.3 a och b ska ges möjlighet att när som helst dra tillbaka sitt samtycke i enlighet med artikel 7.3 i förordning (EU) 2016/679 och ska påminnas om denna möjlighet vid periodiska sexmånadersintervall, så länge som behandlingen fortsätter.

Artikel 10
Information och alternativ som ska tillhandahållas avseende sekretessinställningar

1. Programvara som släpps ut på marknaden vilken tillåter elektronisk kommunikation, inklusive att hämta och lägga ut information på internet, ska erbjuda möjligheten att hindra tredje part från att lagra information på en slutanvändares terminalutrustning eller behandla information som redan lagras på den utrustningen.

2. Vid installationen ska programvaran informera slutanvändaren om de alternativa sekretessinställningarna, och slutanvändarens samtycke till en inställning ska krävas för att installationen ska kunna fortsätta.

3. När det gäller programvara som redan är installerad den 25 maj 2018 ska kraven enligt punkterna 1 och 2 uppfyllas vid tidpunkten för den första uppdateringen av programvaran, men senast den 25 augusti 2018.

Artikel 11
Begränsningar

1. Unionsrätten eller medlemsstaters lagstiftning kan genom en lagstiftningsåtgärd begränsa tillämpningsområdet för de skyldigheter och rättigheter som föreskrivs i artiklarna 5–8 om begränsningen iakttar det väsentliga i de grundläggande rättigheterna och friheterna och utgör en nödvändig ändamålsenlig och proportionell åtgärd i ett demokratiskt samhälle för att skydda ett eller flera av de allmänna intressen som avses i artikel 23.1 a–e i förordning (EU) 2016/679 eller utgör en tillsyns-, inspektions- eller regleringsfunktion som är förbunden med myndighetsutövning avseende sådana allmänna intressen.

2. Leverantörer av elektroniska kommunikationstjänster ska införa interna förfaranden för att besvara ansökningar om tillgång till data från slutanvändarnas elektroniska kommunikation baserat på en lagstiftningsåtgärd i enlighet med punkt 1. De ska på

begäran förse den behöriga tillsynsmyndigheten med information om dessa förfaranden, antalet förfrågningar som mottagits, vilken juridisk motivering som framförts och vilket svar leverantören lämnat.

KAPITEL III
FYSISKA OCH JURIDISKA PERSONERS RÄTT ATT KONTROLLERA ELEKTRONISK KOMMUNIKATION

Artikel 12

Presentation och skydd när det gäller identifiering av det anropande och uppkopplade numret

1. När presentation erbjuds för identifiering av det anropande och uppkopplade numret i enlighet med artikel [107] i [direktivet om inrättande av en europeisk kodex för elektronisk kommunikation] ska leverantörer av allmänt tillgängliga nummerbaserade interpersonella kommunikationstjänster tillhandahålla följande:

(a) Den uppringande slutanvändaren ska ha möjlighet att förhindra presentation för identifiering av det uppringande numret per samtal, per linje eller permanent.

(b) Den uppringda slutanvändaren ska ha möjlighet att förhindra presentation för identifiering av det uppringande numret för inkommande samtal.

(c) Den uppringda slutanvändaren ska ha möjlighet att avvisa inkommande samtal när presentation för identifiering av det uppringande numret har förhindrats av den uppringande slutanvändaren.

(d) Den uppringda slutanvändaren ska ha möjlighet att förhindra presentation för identifiering av det uppkopplade numret för den uppringande slutanvändaren.

2. Slutanvändarna ska enkelt och avgiftsfritt ges tillgång till möjligheterna enligt punkt 1 a, b, c och d.

3. Punkt 1 a ska också tillämpas på samtal från unionen till tredjeländer. Punkt 1 b, c och d ska också tillämpas på inkommande samtal från tredjeländer.

4. När presentation för identifiering av uppringande eller uppringt nummer erbjuds ska leverantörer av allmänt tillgängliga nummerbaserade interpersonella kommunikationstjänster informera allmänheten om möjligheterna enligt punkt 1 a, b, c och d.

Artikel 13

Undantag från presentation och skydd när det gäller identifiering av det anropande och uppkopplade numret

1. Oavsett om den uppringande slutanvändaren har förhindrat presentation för identifiering av uppringande nummer eller inte ska leverantörer av allmänt tillgängliga nummerbaserade interpersonella kommunikationstjänster, när ett samtal rings till larmtjänster, åsidosätta skyddet mot nummerpresentation, och slutanvändarens vägran eller bristande samtycke till behandling av metadata, per linje för organisationer som sysslar med larmkommunikation, inklusive larmcentraler, i syfte att reagera på sådan kommunikation.

2. Medlemsstaterna ska fastställa mer detaljerade bestämmelser för att fastställa förfarandena och villkoren för när leverantörer av allmänt tillgängliga nummerbaserade interpersonella kommunikationstjänster ska åsidosätta skyddet mot

presentation av det uppringande numret på tillfällig basis när slutanvändare begär att hotfulla samtal eller okynnessamtal ska spåras.

Artikel 14
Blockering av inkommande samtal

Leverantörer av allmänt tillgängliga nummerbaserade interpersonella kommunikationstjänster ska utnyttja de bästa tillgängliga metoderna för att begränsa slutanvändarnas mottagande av oönskade samtal och de ska också tillhandahålla följande möjligheter för den uppringda slutanvändaren, avgiftsfritt:

(a) Att blockera inkommande samtal från specifika nummer eller från anonyma källor.

(b) Att stoppa automatisk omstyrning av samtal som görs av tredje part till slutanvändarens terminalutrustning.

Artikel 15
Allmänt tillgängliga förteckningar

1. Leverantörer av allmänt tillgängliga förteckningar ska erhålla samtycke från slutanvändare som är fysiska personer för att ta med deras personuppgifter i förteckningen, och ska följaktligen erhålla samtycke från dessa slutanvändare för inkluderandet av data per kategori personuppgifter, i den mån som sådana data är relevanta för förteckningens syfte enligt vad som fastställts av leverantören av förteckningen. Leverantörerna ska tillhandahålla ett sätt för slutanvändare som är fysiska personer att kontrollera, korrigera och stryka sådana data.

2. Leverantörer av allmänt tillgängliga förteckningar ska informera slutanvändare som är fysiska personer och vars personuppgifter finns i förteckningen om förteckningens tillgängliga sökfunktioner och erhålla slutanvändarnas samtycke innan de möjliggör sådana sökfunktioner för deras data.

3. Leverantörer av allmänt tillgängliga förteckningar ska ge slutanvändare som är juridiska personer möjlighet att invända mot att data som rör dem tas med i förteckningen. Leverantörerna ska ge sådana slutanvändare som är juridiska personer ett sätt att kontrollera, korrigera och radera sådana data.

4. Möjligheten för slutanvändare att inte finnas med i en allmänt tillgänglig förteckning eller att kontrollera, korrigera och stryka data som rör dem ska tillhandahållas kostnadsfritt.

Artikel 16
Icke begärda meddelanden

1. Fysiska eller juridiska personer får använda elektroniska kommunikationstjänster i syfte att sända direktmarknadsföringskommunikation till slutanvändare som är fysiska personer och som har lämnat sitt samtycke.

2. Om en fysisk eller juridisk person erhåller elektroniska kontaktuppgifter för e-post från sin kund, i samband med försäljningen av en produkt eller en tjänst, i enlighet med förordning (EU) nr 2016/679, får den fysiska eller juridiska personen använda dessa elektroniska kontaktuppgifter för direktmarknadsföring avseende egna liknande produkter och tjänster endast om kunden klart och tydligt ges möjlighet att invända mot sådan användning, avgiftsfritt och på ett enkelt sätt. Rätten att göra

invändningar ska ges vid tidpunkten för insamlingen och varje gång ett meddelande sänds.

3. Utan att det påverkar punkterna 1 och 2 ska fysiska eller juridiska personer som använder elektroniska kommunikationstjänster för direktmarknadsföringssamtal

(a) visa identiteten för en förbindelse där de kan kontaktas, eller

(b) visa en särskild kod eller ett särskilt prefix som visar att samtalet är ett marknadsföringssamtal.

4. Trots punkt 1 får medlemsstaterna genom lagstiftning föreskriva att personsamtal för direktmarknadsföring som rings till slutanvändare som är fysiska personer endast ska tillåtas när det gäller slutanvändare som är fysiska personer och som inte har uttryckt någon invändning mot att ta emot sådan kommunikation.

5. Medlemsstaterna ska, inom ramen för unionslagstiftning och tillämplig nationell lagstiftning, säkerställa att de legitima intressena för slutanvändare som är juridiska personer med avseende på icke begärda meddelanden som sänds med sådana metoder som avses i punkt 1 har ett tillräckligt skydd.

6. Fysiska eller juridiska personer som använder elektroniska kommunikationstjänster för att överföra direktmarknadsföringskommunikation ska informera slutanvändarna om att kommunikationen är av marknadsföringsart och om identiteten på den juridiska eller fysiska person på vars vägnar som meddelandet sänds samt tillhandahålla den information som mottagarna behöver för att på ett enkelt sätt utöva sin rätt att dra tillbaka sitt samtycke till att få ytterligare marknadsföringsmeddelanden.

7. Kommissionen ska ges befogenhet att anta delegerade akter i enlighet med artikel 26.2 för att specificera koden eller prefixet för att identifiera marknadsföringssamtal, i enlighet med punkt 3 b.

Artikel 17
Information om säkerhetsrisker som upptäcks

När det finns en särskild risk som kan äventyra säkerheten för nät och elektroniska kommunikationstjänster ska leverantören av en elektronisk kommunikationstjänst informera slutanvändarna om risken och, om risken ligger utanför räckvidden för de åtgärder som ska vidtas av tjänsteleverantören, informera slutanvändarna om möjliga avhjälpande åtgärder, inklusive en angivelse av de troliga kostnaderna för detta.

KAPITEL IV
OBEROENDE TILLSYNSMYNDIGHETER OCH KONTROLL AV EFTERLEVNADEN

Artikel 18
Oberoende tillsynsmyndigheter

1. De oberoende tillsynsmyndigheter (en eller flera) som ansvarar för att övervaka tillämpningen av förordning (EU) nr 2016/679 ska också ansvara för att övervaka tillämpningen av denna förordning. Kapitlen VI och VII i förordning (EG) nr 2016/679 ska gälla i tillämpliga delar. Tillsynsmyndigheternas uppgifter och befogenheter ska utövas när det gäller slutanvändarna.

2. Den eller de tillsynsmyndigheter som avses i punkt 1 ska så fort det är lämpligt samarbeta med de nationella tillsynsmyndigheter som inrättats i enlighet med [direktivet om inrättande av en europeisk kodex för elektronisk kommunikation].

Artikel 19
Europeiska dataskyddsstyrelsen

Europeiska dataskyddsstyrelsen, som inrättats genom artikel 68 i förordning (EU) 2016/679, ska ha behörighet att säkerställa en enhetlig tillämpning av denna förordning. Därför ska Europeiska dataskyddsstyrelsen utöva de uppgifter som anges i artikel 70 i förordning (EU) 2016/679. Europeiska dataskyddsstyrelsen ska också ha följande uppgifter:

(a) Ge kommissionen råd om eventuella föreslagna ändringar av denna förordning.

(b) På eget initiativ eller på begäran av en av sina ledamöter eller av kommissionen behandla frågor om tillämpningen av denna förordning och utfärda riktlinjer, rekommendationer och bästa praxis i syfte att främja en enhetlig tillämpning av denna förordning,

Artikel 20
Förfaranden för samarbete och enhetlighet

Varje tillsynsmyndighet ska bidra till en enhetlig tillämpning av denna förordning i hela unionen. I detta syfte ska tillsynsmyndigheterna samarbeta med varandra och med kommissionen i enlighet med kapitel VII i förordning (EU) 2016/679 när det gäller frågor som omfattas av denna förordning.

KAPITEL V
RÄTTSMEDEL, ANSVAR SAMT SANKTIONER

Artikel 21
Rättsmedel

1. Utan att det påverkar något annat administrativt prövningsförfarande eller rättsmedel, ska varje slutanvändare av elektroniska kommunikationstjänster ha samma rättsmedel som föreskrivs i artiklarna 77, 78 och 79 i förordning (EU) 2016/679.

2. Varje annan fysisk eller juridisk person än slutanvändarna som påverkas negativt av överträdelser av denna förordning, och som har ett legitimt intresse av att påstådda överträdelser upphör eller förbjuds, inklusive leverantörer av elektroniska kommunikationstjänster som skyddar sina legitima affärsintressen, ska ha rätt att vidta rättsliga åtgärder med avseende på sådana överträdelser.

Artikel 22
Ansvar och rätt till ersättning

Varje slutanvändare av elektroniska kommunikationstjänster som har lidit materiell eller immateriell skada till följd av en överträdelse av denna förordning ska ha rätt att få ersättning från den felande parten för den skada som åsamkats, om inte den felande parten kan bevisa att den inte på något sätt är ansvarig för den händelse som gett upphov till skadan i enlighet med artikel 82 i förordning (EU) 2016/679.

Artikel 23

Allmänna villkor för påförande av administrativa sanktionsavgifter

1. Vid tillämpningen av denna artikel ska kapitel VII i förordning (EU) 2016/679 tillämpas på överträdelser av denna förordning.

2. Vid överträdelser av följande bestämmelser ska det i enlighet med punkt 1 påföras administrativa sanktionsavgifter på upp till 10 000 000 EUR eller, om det gäller ett företag, på upp till 2 % av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst:

(a) Skyldigheter för juridiska eller fysiska personer som behandlar data från elektronisk kommunikation i enlighet med artikel 8.

(b) Skyldigheter för leverantörer av programvara som möjliggör elektronisk kommunikation, i enlighet med artikel 10.

(c) Skyldigheter för leverantörer av allmänt tillgängliga förteckningar i enlighet med artikel 15.

(d) Skyldigheter för juridiska eller fysiska personer som använder elektroniska kommunikationstjänster i enlighet med artikel 16.

3. Överträdelser av principen om konfidentialitet vid kommunikation, tillåten behandling av data från elektronisk kommunikation och tidsfrister för radering enligt artiklarna 5, 6 och 7 ska, i enlighet med punkt 1 i denna artikel, medföra administrativa sanktionsavgifter på upp till 20 000 000 EUR eller, om det gäller ett företag, på upp till 4 % av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst.

4. Medlemsstaterna ska fastställa bestämmelser om sanktioner för överträdelser av artiklarna 12, 13, 14 och 17.

5. Vid underlåtenhet att rätta sig efter ett föreläggande från tillsynsmyndigheten enligt artikel 18 ska det påföras administrativa sanktionsavgifter på upp till 20 000 000 EUR eller, om det gäller ett företag, på upp till 4 % av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst:

6. Utan att det påverkar tillsynsmyndigheternas korrigerande befogenheter enligt artikel 18 får varje medlemsstat fastställa regler för huruvida och i vilken utsträckning administrativa sanktionsavgifter kan påföras offentliga myndigheter och organ som är inrättade i medlemsstaten.

7. Tillsynsmyndighetens utövande av sina befogenheter enligt denna artikel ska omfattas av lämpliga rättssäkerhetsgarantier i enlighet med unionsrätten och medlemsstaternas nationella rätt, inbegripet effektiva rättsmedel och rättssäkerhet.

8. Om det i medlemsstatens rättssystem inte finns några föreskrifter om administrativa sanktionsavgifter får den här artikeln tillämpas så att förfarandet inleds av den behöriga tillsynsmyndigheten och sanktionsavgifterna sedan utdöms av behörig nationell domstol, varvid det säkerställs att rättsmedlen är effektiva och har motsvarande verkan som de administrativa sanktionsavgifter som påförs av tillsynsmyndigheter. De sanktionsavgifter som påförs ska i alla händelser vara effektiva, proportionella och avskräckande. Dessa medlemsstater ska till kommissionen anmäla de bestämmelser i deras lagstiftning som de antar i enlighet med denna punkt senast den [xxx], samt utan dröjsmål anmäla eventuell senare ändringslagstiftning eller ändringar som berör dem.

Artikel 24
Sanktioner

1. Medlemsstaterna ska fastställa regler om andra sanktioner för överträdelser av denna förordning, särskilt för överträdelser som inte är föremål för administrativa sanktionsavgifter enligt artikel 23, och vidta alla nödvändiga åtgärder för att säkerställa att de genomförs. Dessa sanktioner ska vara effektiva, proportionella och avskräckande.

2. Varje medlemsstat ska senast 18 månader efter den dag som anges i artikel 29.1 anmäla till kommissionen vilka nationella bestämmelser den antar som en följd av bestämmelserna i punkt 1, och alla framtida ändringar som rör dessa bestämmelser ska anmälas utan dröjsmål.

KAPITEL VI
DELEGERADE AKTER OCH GENOMFÖRANDEAKTER

Artikel 25
Utövande av delegering

1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.

2. Den befogenhet att anta delegerade akter som avses i artikel 8.4 ska ges till kommissionen tills vidare från och med [dagen för denna förordnings ikraftträdande].

3. Den delegering av befogenhet som avses i artikel 8.4 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i Europeiska unionens officiella tidning, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.

4. Innan kommissionen antar en delegerad akt ska den samråda med experter som utsetts av varje medlemsstat i enlighet med principerna i det interinstitutionella avtalet om bättre lagstiftning av den 13 april 2016.

5. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.

6. En delegerad akt som antas enligt artikel 8.4 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period av två månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med två månader på Europaparlamentets eller rådets initiativ.

Artikel 26
Kommitté

1. Kommissionen ska biträdas av kommunikationskommittén som inrättats enligt artikel 110 i [direktivet om inrättande av en europeisk kodex för elektronisk

kommunikation]. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011[12].

2. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.

KAPITEL VII
SLUTBESTÄMMELSER

Artikel 27
Upphävande

1. Direktiv 2002/58/EG ska upphöra att gälla med verkan från och med den 25 maj 2018.

2. Hänvisningar till det upphävda direktivet ska anses som hänvisningar till denna förordning.

Artikel 28
Övervakning och utvärdering

Senast den 1 januari 2018 ska kommissionen fastställa ett detaljerat program för övervakning av denna förordnings effektivitet.

Senast tre år efter den dag då denna förordning börjar tillämpas, och därefter vart tredje år, ska kommissionen göra en utvärdering av denna förordning och lägga fram de huvudsakliga resultaten för Europaparlamentet, rådet och Europeiska ekonomiska och sociala kommittén. Utvärderingen ska, när så är lämpligt, ligga till grund för ett förslag till ändring eller upphävande av denna förordning mot bakgrund av den rättsliga, tekniska eller ekonomiska utvecklingen.

Artikel 29
Ikraftträdande och tillämpning

1. Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

2. Den ska tillämpas från och med den 25 maj 2018.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den

På Europaparlamentets vägnar	*På rådets vägnar*
Ordförande	*Ordförande*

[12] Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter (EUT L 55, 28.2.2011, s. 13).