EUROPESE
COMMISSIE

Brussel, 10.1.2017
COM(2017) 10 final

2017/0003 (COD)

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

met betrekking tot de eerbiediging van het privéleven en de bescherming van persoonsgegevens in elektronische communicatie, en tot intrekking van Richtlijn 2002/58/EG (richtlijn betreffende privacy en elektronische communicatie)

(Voor de EER relevante tekst)

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

TOELICHTING

1. ACHTERGROND VAN HET VOORSTEL

1.1. Motivering en doel van het voorstel

De strategie voor de digitale eengemaakte markt[1] heeft als doelstelling het vertrouwen in en de veiligheid van digitale diensten te verhogen. De hervorming van het kader voor gegevensbescherming, en met name de goedkeuring van Verordening (EU) 2016/679, de algemene verordening gegevensbescherming[2], was een belangrijke stap in die richting. In de strategie voor de digitale eengemaakte markt werd ook de herziening van Richtlijn 2002/58/EG[3] (hierna "**e-privacyrichtlijn**")aangekondigd om een hoog niveau van bescherming van de persoonlijke levenssfeer voor gebruikers van elektronische-communicatiediensten en een gelijk speelveld voor alle marktdeelnemers te garanderen. Dit voorstel strekt tot herziening van de e-privacyrichtlijn, en voorziet daarbij in de doelstellingen van de strategie voor de digitale eengemaakte markt alsook in de samenhang met de algemene verordening gegevensbescherming.

De e-privacyrichtlijn garandeert de bescherming van de fundamentele rechten en vrijheden, met name het recht op eerbiediging van het privéleven, de vertrouwelijkheid van de communicatie en de bescherming van persoonsgegevens in de sector elektronische communicatie. Ook wordt het vrije verkeer van elektronische-communicatiegegevens, -uitrusting en -diensten in de Unie gegarandeerd. Zij implementeert in het afgeleide recht van de Unie het fundamentele recht op eerbiediging van het privéleven met betrekking tot communicatie, zoals verankerd in artikel 7 van het Handvest van de grondrechten van de Europese Unie (hierna "**Handvest**").

In overeenstemming met de vereisten inzake "betere regelgeving" heeft de Commissie een ex-postprogramma voor gezonde en resultaatgerichte regelgeving (hierna "**REFIT-evaluatie**") van de e-privacyrichtlijn verricht. Uit de evaluatie blijkt dat de doelstellingen en beginselen van het huidige kader gezond blijven. Sinds de laatste herziening van de e-privacyrichtlijn in 2009 hebben zich op de markt echter belangrijke technologische en economische ontwikkelingen voorgedaan. Consumenten en bedrijven worden steeds meer afhankelijk van nieuwe internetdiensten waardoor persoonlijke communicatie zoals Voice over IP, instantmessaging en webmaildiensten in de plaats komen van traditionele communicatiediensten. Deze over-the-topcommunicatiediensten (hierna "**OTT's**") vallen over het algemeen niet onder het bestaande regelgevingskader voor elektronische communicatie, waaronder de e-privacyrichtlijn, van de Unie. Bijgevolg heeft de richtlijn geen gelijke tred gehouden met de technologische ontwikkelingen, hetgeen geleid heeft tot een leemte in de bescherming van communicatie via nieuwe diensten.

---

1 Mededeling van de Commissie aan het Europees Parlement, de Raad, het Economisch en Sociaal Comité en het Comité van de Regio's, Strategie voor een digitale eengemaakte markt voor Europa, COM(2015) 192 final.

2 Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1).

3 Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (PB L 201 van 31.7.2002, blz. 37).

1.2. Samenhang met bestaande bepalingen op het beleidsterrein

Dit voorstel is een *lex specialis* bij de algemene verordening gegevensbescherming en zal voorzien in de nadere omschrijving en de aanvulling daarvan voor elektronische-communicatiegegevens die als persoonsgegevens worden aangemerkt. Alle onderwerpen in verband met de verwerking van persoonsgegevens die niet uitdrukkelijk door het voorstel worden behandeld, vallen onder de algemene verordening. De afstemming op die verordening heeft ertoe geleid dat een aantal bepalingen ingetrokken worden, zoals de beveiligingsverplichtingen van artikel 4 van de e-privacyrichtlijn.

1.3. Samenhang met andere beleidsterreinen van de Unie

De e-privacy-richtlijn maakt deel uit van het regelgevingskader voor elektronische communicatie. In 2016 heeft de Commissie, bij de herziening van dit kader, een voorstel voor een richtlijn tot vaststelling van het Europees wetboek voor elektronische communicatie[4] (hierna "**Europees wetboek**") aangenomen. Hoewel dit voorstel geen deel uitmaakt van het Europees wetboek; is het deels gebaseerd op de daarin omschreven definities, waaronder die van "elektronische-communicatiedienst". Zoals in het Europees wetboek, worden in dit voorstel ook de aanbieders van OTT-diensten tot het toepassingsgebied gerekend, hetgeen de marktrealiteit weerspiegelt. Daarnaast vormt het Europees wetboek voor elektronische communicatie een aanvulling op dit voorstel door de veiligheid van elektronische-communicatiediensten te waarborgen.

De richtlijn radioapparatuur (Richtlijn 2014/53/EU)[5] waarborgt een eengemaakte markt voor radioapparatuur. Zij schrijft met name voor dat radioapparatuur, voor in de handel te worden gebracht, beveiligingen moet bevatten om de bescherming van de persoonsgegevens en de privacy van de gebruiker te waarborgen. Krachtens deze richtlijn alsmede krachtens Verordening (EU) nr. 1025/2012 betreffende Europese normalisatie[6] is de Commissie gemachtigd om maatregelen te nemen. Dit voorstel heeft geen gevolgen voor de richtlijn radioapparatuur.

Het voorstel bevat geen specifieke bepalingen op het gebied van gegevensbewaring. De inhoud van artikel 15 van de e-privacyrichtlijn blijft behouden en wordt in overeenstemming gebracht met de specifieke bewoordingen van artikel 23 van de algemene verordening gegevensbescherming, op basis waarvan de lidstaten gemachtigd worden de reikwijdte te beperken van de rechten en plichten waarin bepaalde artikelen van de e-privacyrichtlijn voorzien. Het staat de lidstaten derhalve vrij een nationaal kader voor gegevensbewaring te behouden of te creëren dat onder meer voorziet in doelgerichte bewaringsmaatregelen, voor zover dit kader strookt met het recht van de Unie rekening houdend met de jurisprudentie van

---

4 Voorstel van de Commissie voor een richtlijn van het Europees Parlement en de Raad tot vaststelling van het Europees wetboek voor elektronische communicatie (herschikking) (COM/2016/0590 final – 2016/0288 (COD)).

5 Richtlijn 2014/53/EU van het Europees Parlement en de Raad van 16 april 2014 betreffende de harmonisatie van de wetgevingen van de lidstaten inzake het op de markt aanbieden van radioapparatuur en tot intrekking van Richtlijn 1999/5/EG (PB L 153 van 22.5.2014, blz. 62).

6 Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad van 25 oktober 2012 betreffende Europese normalisatie, tot wijziging van de Richtlijnen 89/686/EEG en 93/15/EEG van de Raad alsmede de Richtlijnen 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG en 2009/105/EG van het Europees Parlement en de Raad en tot intrekking van Beschikking 87/95/EEG van de Raad en Besluit nr. 1673/2006/EG van het Europees Parlement en de Raad (PB L 316 van 14.11.2012, blz. 12).

het Hof van Justitie over de uitlegging van de e-privacyrichtlijn en het EU-Handvest van de grondrechten[7].

Tot slot is het voorstel niet van toepassing op activiteiten van instellingen, organen en instanties van de Unie. De beginselen en de desbetreffende verplichtingen met betrekking tot het recht op eerbiediging van het privéleven en communicatie met betrekking tot de verwerking van elektronische-communicatiegegevens zijn echter opgenomen in het voorstel voor een verordening tot intrekking van Verordening (EG) nr. 45/2001[8].

2. RECHTSGRONDSLAG, SUBSIDIARITEIT EN EVENREDIGHEID

2.1. Rechtsgrondslag

Artikel 16 en artikel 114 van het Verdrag betreffende de werking van de Europese Unie (VWEU) vormen de rechtsgrondslag van het voorstel.

Artikel 16 VWEU voorziet in een specifieke rechtsgrondslag voor de vaststelling van voorschriften betreffende de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens door de instellingen van de Unie, door de lidstaten bij de uitoefening van activiteiten die binnen het toepassingsgebied van het recht van de Unie vallen, alsmede voorschriften betreffende het vrij verkeer van die gegevens. Aangezien elektronische communicatie waarbij een natuurlijke persoon betrokken is, normaal gezien als persoonsgegevens wordt aangemerkt, moet de bescherming van natuurlijke personen ten aanzien van de privacy van de communicatie en de verwerking van deze gegevens, op artikel 16 worden gebaseerd.

Daarnaast beoogt het voorstel de bescherming van communicatie en daarmee verband houdende rechtmatige belangen van rechtspersonen. De inhoud en de reikwijdte van de rechten krachtens artikel 7 van het Handvest zijn in overeenstemming met artikel 52, lid 3, van het Handvest, dezelfde als die welke in artikel 8, lid 1, van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (**EVRM**) zijn neergelegd. Wat de reikwijdte van artikel 7 van het Handvest betreft, bevestigen de rechtspraak van het Hof van Justitie[9]en van het Europees Hof voor de rechten van de mens[10] dat beroepsactiviteiten van rechtspersonen niet mogen worden uitgesloten van de bescherming van het recht dat door artikel 7 van het Handvest en artikel 8 van het EVRM wordt gegarandeerd.

Aangezien het initiatief een tweeledig doel heeft en het onderdeel bescherming van communicatie van rechtspersonen en het doel om de interne markt voor elektronische communicatie te voltooien en de werking daarvan te garanderen, wat dit betreft niet als louter bijkomstig kan worden beschouwd, moet het initiatief ook op artikel 114 van het VWEU zijn gebaseerd.

---

7 Zie gevoegde zaken C-293/12 en C-594/12, Digital Rights Ireland and Seitlinger en andere, ECLI:EU:C:2014:238; gevoegde zaken C-203/15 en C-698/15, Tele2 Sverige AB en Secretary of State for the Home Department, ECLI:EU:C:2016:970.

8 Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens (PB L 8 van 12.1.2001, blz. 1-22).

9 Zie arrest Varec SA, C-450/06, ECLI:EU:C:2008:91, punt 48.

10 Zie met name EHRM, Niemietz/Duitsland, arrest van 16 december 1992, serie A nr. 251-B, § 29; Société Colas Est e.a./Frankrijk, nr. 37971/97, § 41; EHRM 2002-III; arrest Peck/Verenigd Koninkrijk, nr. 44647/98, § 57, EHRM 2003-I; alsmede Vinci Construction en GTM Génie Civil et Services/Frankrijk, nrs. 63629/10 en 60567/10, § 63, 2 april 2015.

2.2. Subsidiariteit

Eerbiediging van communicatie is een grondrecht dat in het Handvest is erkend. Uit de inhoud van elektronische communicatie kan zeer gevoelige informatie aan het licht komen over de eindgebruikers die bij de communicatie betrokken zijn. Op dezelfde manier kunnen metagegevens op basis van elektronische communicatie ook zeer gevoelige en persoonlijke informatie weergeven, zoals uitdrukkelijk is erkend door het Hof van Justitie[11]. De meeste lidstaten erkennen eveneens de noodzaak om communicatie te beschermen als een afzonderlijk grondwettelijk recht. Hoewel het voor de lidstaten mogelijk is een beleid te voeren om te waarborgen dat dit recht niet wordt geschonden, zal dit zonder regels van de Unie niet op eenvormige wijze worden bereikt en zou dit leiden tot belemmeringen voor het grensoverschrijdende verkeer van persoonsgegevens en niet-persoonsgebonden gegevens met betrekking tot het gebruik van elektronische-communicatiediensten. Uiteindelijk is het noodzakelijk met het oog op de samenhang met de algemene verordening gegevensbescherming de e-privacyrichtlijn te herzien en de twee instrumenten onderling in overeenstemming te brengen.

Door de technologische ontwikkelingen en de ambities van de strategie voor de digitale eengemaakte markt is nog duidelijker geworden dat actie op het niveau van de Unie noodzakelijk is. Het welslagen van deze Europese strategie hangt af van hoe doeltreffend de EU optreedt om de nationale compartimentering en belemmeringen af te breken en de voordelen en besparingen van een Europese digitale interne markt aan te grijpen. Bovendien reikt de omvang van het probleem, aangezien het internet en de digitale technologieën geen grenzen kennen, verder dan het grondgebied van een enkele lidstaat. De problemen die zich tegenwoordig voordoen, kunnen niet door de lidstaten worden verholpen. Om de digitale eengemaakte markt naar behoren te laten werken, moet een gelijk speelveld worden gecreëerd voor marktdeelnemers die substitueerbare diensten aanbieden, en moeten eindgebruikers op het niveau van de Unie een gelijke bescherming genieten.

2.3. Evenredigheid

Om te zorgen voor een doeltreffende wettelijke bescherming van de eerbiediging van het privéleven en de communicatie, moet het toepassingsgebied worden uitgebreid zodat ook OTT-aanbieders daarbinnen vallen. Hoewel verschillende populaire OTT-aanbieders reeds voldoen, of gedeeltelijk voldoen, aan het beginsel van vertrouwelijkheid van communicatie, kan de bescherming van de grondrechten niet worden overgelaten aan zelfregulering door het bedrijfsleven. Ook het belang van doeltreffende bescherming van de privacy van eindapparatuur neemt toe nu deze in het privé- en beroepsleven onmisbaar is geworden voor de opslag van gevoelige gegevens. De tenuitvoerlegging van de e-privacyrichtlijn is niet doeltreffend gebleken om eindgebruikers weerbaarder te maken. Om dat doel te bereiken is het dan ook noodzakelijk het beginsel toe te passen door de toestemming te centraliseren in software en gebruikers aan te spreken met informatie over de privacyinstellingen. Wat de handhaving van deze verordening betreft, wordt vertrouwd op de toezichthoudende autoriteiten en het coherentiemechanisme van de algemene verordening gegevensbescherming. Voorts biedt het voorstel de lidstaten de mogelijkheid om afwijkende nationale maatregelen te nemen voor specifieke legitieme doeleinden. Het gaat dus niet verder dan wat nodig is om de doelstellingen te verwezenlijken en is in overeenstemming met het evenredigheidsbeginsel zoals neergelegd in artikel 5 van het Verdrag betreffende de Europese Unie. De verplichtingen die aan de betrokken diensten worden opgelegd, worden zo beperkt mogelijk gehouden zonder dat afbreuk wordt gedaan aan de betrokken grondrechten.

[11] Zie voetnoot 7.

2.4. Keuze van het instrument

De Commissie dient een voorstel voor een verordening in om samenhang met de algemene verordening gegevensbescherming en rechtszekerheid voor gebruikers en ondernemingen te garanderen, doordat uiteenlopende interpretaties in de lidstaten wordt voorkomen. Een verordening kan zorgen voor een gelijk niveau van bescherming voor gebruikers in de hele Unie en lagere nalevingskosten voor ondernemingen die grensoverschrijdend werken.

3. RESULTATEN VAN EX-POSTEVALUATIES, RAADPLEGINGEN VAN BELANGHEBBENDEN EN EFFECTBEOORDELINGEN

3.1. Ex-postevaluatie van bestaande wetgeving en controle van de resultaatgerichtheid ervan

In de REFIT-evaluatie is onderzocht hoe efficiënt de e-privacyrichtlijn heeft bijgedragen tot de passende bescherming van de eerbiediging van de persoonlijke levenssfeer en de vertrouwelijkheid van communicatie in de EU. Ook werd onderzocht of er overlappingen in voorkwamen.

Uit de REFIT-evaluatie is gebleken dat de genoemde doelstellingen van de richtlijn **relevant** blijven. Terwijl de algemene verordening gegevensbescherming de bescherming van persoonsgegevens garandeert, waarborgt de e-privacyrichtlijn het vertrouwelijke karakter van het communicatieverkeer, waaronder eventueel ook niet-persoonsgebonden gegevens en gegevens in verband met een rechtspersoon. Daarom moet een afzonderlijk instrument zorgen voor een doeltreffende bescherming van artikel 7 van het Handvest. Andere bepalingen, zoals de regels voor het verzenden van ongewenste commerciële communicatie, zijn ook nog steeds relevant gebleken.

Wat **effectiviteit en efficiëntie** betreft, is de REFIT-evaluatie tot de bevinding gekomen dat de richtlijn niet volledig heeft voldaan aan haar doelstellingen. De onduidelijke formulering van sommige bepalingen en de dubbelzinnigheid in juridische begrippen stonden harmonisering in de weg, hetgeen problemen voor grensoverschrijdende werking van ondernemingen meebracht. Uit de evaluatie is voorts gebleken dat een aantal bepalingen hebben gezorgd voor een onnodige last voor bedrijven en consumenten. De toestemmingsregel ter bescherming van de vertrouwelijkheid van eindapparatuur heeft bijvoorbeeld niet voldaan aan zijn doelstellingen aangezien eindgebruikers te maken krijgen met verzoeken om permanente cookies te aanvaarden zonder dat zij de betekenis ervan begrijpen, en in sommige gevallen zelfs zonder hun toestemming aan cookies blootgesteld zijn. De toestemmingsregel is overbeschermend aangezien hij ook betrekking heeft op praktijken die de privacy niet aantasten, en biedt te weinig bescherming aangezien hij niet duidelijk betrekking heeft op bepaalde volgtechnieken (bv. vingerafdruklezing) die mogelijk geen toegang of opslag in het toestel inhouden. Ten slotte kan de tenuitvoerlegging ervan duur zijn voor bedrijven.

De conclusie van de evaluatie luidde dat de e-privacyregels **op Europees niveau** nog steeds **toegevoegde waarde** bieden voor de verwezenlijking van de doelstelling, namelijk in het licht van de toenemend grensoverschrijdende markt voor elektronische communicatie de privacy in de onlinewereld verzekeren. Verder werd aangetoond dat de regels **samenhangen** met andere relevante EU-wetgeving, ofschoon er enkele overlappingen zijn geconstateerd ten opzichte van de nieuwe algemene verordening gegevensbescherming (zie in punt 1.2).

3.2. Raadplegingen van belanghebbenden

De Commissie organiseerde een openbare raadpleging tussen 12 april tot en met 5 juli 2016 en ontving 421 reacties[12]. De belangrijkste bevindingen zijn[13]:

– **Behoefte aan speciale voorschriften voor de elektronische-communicatiesector inzake het vertrouwelijke karakter van elektronische communicatie:** 83,4 % van de ondervraagde burgers, consumenten en organisaties uit het maatschappelijk middenveld en 88,9 % van overheidsinstanties zijn het hiermee eens, maar 63,4 % van de respondenten uit het bedrijfsleven niet.

– **Uitbreiding van het toepassingsgebied tot nieuwe communicatiediensten (OTT's):** 76 % van de burgers en organisaties uit het maatschappelijk middenveld en 93,1 % van overheidsinstanties zijn het daarmee eens, terwijl slechts 36,2 % van de respondenten uit het bedrijfsleven gewonnen zijn voor die uitbreiding.

– **Wijziging van de vrijstellingen voor verlening van toestemming voor de verwerking van verkeers- en locatiegegevens:** 49,1 % van de burgers, consumenten en organisaties uit het maatschappelijk middenveld en 36 % van de overheidsinstanties zien liever geen uitbreiding van deze vrijstellingen, terwijl 36 % van de bedrijven daar voorstander van zijn; twee derde van de bedrijven pleiten voor de gewone intrekking van de bepalingen.

– **Steun voor voorgestelde oplossingen in verband met de toestemming voor cookies:** 81,2 % van de burgers en 63 % van de overheidsinstanties steunen het opleggen van verplichtingen aan fabrikanten van eindapparatuur om producten op de markt te brengen met geactiveerde standaardinstellingen voor privacy, terwijl 58,3 % van het bedrijfsleven voorstander is van de optie zelf-/coregulering.

Voorts heeft de Europese Commissie in april 2016 twee workshops georganiseerd, één die openstond voor alle belanghebbenden en één die openstond voor bevoegde nationale autoriteiten. Hierop werden de belangrijkste vragen van de openbare raadplegingen behandeld. De standpunten die tijdens de workshops naar voren kwamen, weerspiegelden het resultaat van de openbare raadpleging.

Om meningen van de burgers in te winnen, werd in de hele Unie een Eurobarometer-enquête over e-privacy[14] gehouden. De belangrijkste bevindingen zijn[15]:

– 78 % vindt het zeer belangrijk dat persoonlijke informatie op hun computer, smartphone of tablet alleen kan worden opgevraagd met hun toestemming.

– 72 % vindt dat het zeer belangrijk dat de geheimhouding van hun e-mails en online instant messaging gewaarborgd is.

– 89 % is het eens met de voorgestelde optie dat de standaardinstellingen van hun browser het uitwisselen van informatie moet tegengaan.

3.3. Bijeenbrengen en benutten van deskundigheid

De Commissie heeft gebruikgemaakt van het volgende externe deskundigenadvies:

---

12 162 bijdragen van burgers, 33 van het maatschappelijk middenveld en consumentenorganisaties; 186 van het bedrijfsleven en 40 van overheden, waaronder de bevoegde autoriteiten voor handhaving van de e-privacyrichtlijn.

13 Het volledige verslag is beschikbaar op: https://ec.europa.eu/digital-single-market/news-redirect/37204.

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

15 Het volledige verslag is beschikbaar op: https://ec.europa.eu/digital-single-market/news-redirect/37205.

– gerichte raadplegingen van deskundigengroepen van de EU: advies van de groep gegevensbescherming artikel 29; advies van de Europese Toezichthouder voor gegevensbescherming; advies van het REFIT-platform; standpunt van BEREC; standpunten van ENISA en standpunten van de leden van het samenwerkingsnetwerk voor de handhaving van de wetgeving op het gebied van consumentenbescherming.

– Externe deskundigheid, met name de volgende twee studies:

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

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

3.4. Effectbeoordeling

Er werd voor dit voorstel een effectbeoordeling verricht, die op 28 september 2016 werd door de Raad voor regelgevingstoetsing positief beoordeeld[16]. Om gevolg te geven aan de aanbevelingen van de Raad is in de effectbeoordeling betere toelichting gegeven over de reikwijdte van het initiatief, de samenhang met andere rechtsinstrumenten (algemene verordening gegevensbescherming, Europees wetboek voor elektronische communicatie, richtlijn radioapparatuur) en de noodzaak van een afzonderlijk instrument. Het basisscenario is nader uitgewerkt en verduidelijkt. De analyse van de effecten is versterkt en de beoordeling bevat een evenwichtiger, duidelijker en krachtiger beschrijving van de verwachte kosten en baten.

De volgende beleidsopties zijn getoetst aan de criteria effectiviteit, efficiëntie en coherentie:

– **Optie 1:** Niet-wetgevende maatregelen ("soft law");

– **Optie 2:** Beperkte versterking van privacy/vertrouwelijkheid en vereenvoudiging;

– **Optie 3:** Matige versterking van privacy/vertrouwelijkheid en vereenvoudiging;

– **Optie 4:** Ingrijpende versterking van privacy/vertrouwelijkheid en vereenvoudiging;

– **Optie 5:** Intrekking van de e-privacyrichtlijn.

Optie 3 is in de meeste opzichten aangewezen als de **voorkeursoptie** om de doelstellingen te bereiken, rekening houdend met de efficiëntie en de samenhang. De voornaamste voordelen zijn:

– betere bescherming van de vertrouwelijkheid van elektronische communicatie door uitbreiding van het toepassingsgebied van het rechtsinstrument om nieuwe functioneel gelijkwaardige elektronische-communicatiediensten daarin op te nemen. Daarnaast versterkt de verordening de controle van de eindgebruiker door te verduidelijken dat de toestemming kan worden verleend via passende technische instellingen.

– betere bescherming tegen ongewenste communicatie, met de invoering van de verplichting tot het verstrekken van de identificatie van de oproepende lijn of van een verplicht kengetal voor marketinggesprekken en ruimere mogelijkheden om oproepen van ongewenste nummers te blokkeren.

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

– Vereenvoudiging en verduidelijking van het regelgevingsklimaat door de vrije speelruimte voor lidstaten te beperken, intrekking van achterhaalde bepalingen en verruiming van de uitzonderingen op de toestemmingsregels.

De economische effecten van optie 3 zullen naar verwachting in het algemeen evenredig zijn met de doelstellingen van het voorstel. Er ontstaan ondernemingskansen in verband met de verwerking van communicatiegegevens voor traditionele elektronische-communicatiediensten, terwijl aanbieders van OTT-diensten aan dezelfde regels worden onderworpen. Dit brengt in bepaalde mate extra nalevingskosten mee voor deze marktdeelnemers. Deze wijziging is echter niet van wezenlijke invloed op de OTT's die reeds werkzaam zijn op basis van toestemming. Tot slot zou het effect van de optie niet merkbaar zijn in de lidstaten die deze regels reeds tot OTT's hebben uitgebreid.

Door de toestemming te centraliseren in software zoals internetbrowsers, gebruikers zelf ertoe aan te zetten hun privacyinstellingen te kiezen en de uitzonderingen op de toestemmingsregel voor cookies te verruimen, zou een aanzienlijk deel van de ondernemingen komaf kunnen maken met cookiebanners en -berichten, waardoor de mogelijkheid ontstaat voor aanzienlijke kostenbesparingen en vereenvoudiging. Voor online werkende adverteerders kan het echter moeilijker worden toestemming te verkrijgen als een aanzienlijk deel van de gebruikers kiezen voor de instelling "cookies van derden afwijzen". Tegelijkertijd verliezen website-exploitanten door het centraliseren van de toestemming niet de mogelijkheid om toestemming te verkrijgen door middel van individuele verzoeken aan eindgebruikers en zo hun huidige bedrijfsmodel te behouden. Extra kosten zouden opduiken voor sommige aanbieders van browsers of soortgelijke software omdat zij privacyvriendelijke instellingen moeten garanderen.

In de externe studie zijn drie verschillende uitvoeringsscenario's voor optie 3 aangewezen, naargelang van de entiteit die het dialoogvenster instelt tussen de gebruiker welke zijn keuze heeft voor de instellingen "cookies van derden afwijzen" of "volg-mij-niet", en de bezochte websites vastgesteld, met het verzoek aan de internetgebruiker om zijn/haar keuze te heroverwegen. Met deze technische taak kunnen de volgende entiteiten worden belast: 1) software zoals internetbrowsers; 2) de tracker van derden; 3) de afzonderlijke websites (d.w.z. de dienst van de informatiemaatschappij die door de gebruiker is aangevraagd). Ten opzichte van het basisscenario zou optie 3 leiden tot algemene besparingen in de nalevingskosten met 70 % (948,8 miljoen EUR) in het eerste scenario van het voorstel (browser). In andere scenario's zouden de kostenbesparingen lager zijn. Aangezien de totale besparingen grotendeels voortkomen uiteen zeer sterke daling van het aantal betrokken bedrijven, zou het afzonderlijke bedrag van nalevingskosten dat één bedrijf naar verwachting moet dragen, gemiddeld hoger liggen dan vandaag.

3.5. Gezonde regelgeving en vereenvoudiging

De voorgestelde beleidsmaatregelen in het kader van de voorkeursoptie beantwoorden aan de doelstelling van vereenvoudiging en vermindering van de administratieve lasten, in overeenstemming met de resultaten van de Refit-evaluatie en het advies van het Refit-platform[17].

Het Refit-platform heeft drie reeksen aanbevelingen tot de Commissie gericht:

– de bescherming van het privéleven van burgers moet worden versterkt door de e-privacyrichtlijn af te stemmen op de algemene verordening gegevensbescherming;

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

– de bescherming van burgers tegen ongevraagde marketing moet doeltreffender worden door uitzonderingen toe te voegen aan de "toestemmingsregel" voor cookies;

– de Commissie pakt nationale toepassingsproblemen aan en bevordert de uitwisseling van beste praktijken tussen de lidstaten.

Het voorstel omvat met name:

– gebruik van technologieneutrale definities om nieuwe diensten en technologieën te kunnen bestrijken, zodat de verordening voorbereid is op de toekomst;

– intrekking van de beveiligingsregels om dubbele regelgeving te vermijden;

– verduidelijking van de werkingssfeer om het risico van verschillen in tenuitvoerlegging door de lidstaten weg te nemen/ te beperken (punt 3 van het advies);

– verduidelijking en vereenvoudiging van de toestemmingsregel voor gebruik van cookies en andere identificatie-elementen, zoals uiteengezet in de punten 3.1 en 3.4 (punt 2 van het advies);

– afstemming van de toezichthoudende autoriteiten op de autoriteiten die bevoegd zijn voor de handhaving van de algemene verordening gegevensbescherming en gebruik van het coherentiemechanisme van die verordening.

3.6. Gevolgen voor de grondrechten

Het voorstel beoogt de bescherming van de persoonlijke levenssfeer en de persoonsgegevens die in verband met elektronische communicatie worden verwerkt meer effectief te maken en op een hoger niveau te brengen, in overeenstemming met de artikelen 7 en 8 van het Handvest, en meer rechtszekerheid te garanderen. Het voorstel vormt een aanvulling op en een nadere uitwerking van de algemene verordening gegevensbescherming. Doeltreffende bescherming van de vertrouwelijkheid van communicatie is van essentieel belang voor de uitoefening van de vrijheid van meningsuiting en van informatie, en van andere verwante rechten, zoals het recht op bescherming van persoonsgegevens, de vrijheid van gedachte, geweten en godsdienst.

4. GEVOLGEN VOOR DE BEGROTING

Het voorstel heeft geen gevolgen voor de begroting van de Unie.

5. OVERIGE ELEMENTEN

5.1. Uitvoeringsplanning en regelingen betreffende controle, evaluatie en rapportage

De Commissie zal toezicht houden op de toepassing van deze verordening en brengt om de drie jaar verslag over haar evaluatie uit bij het Europees Parlement, de Raad en het Europees Economisch en Sociaal Comité. Deze verslagen zijn openbaar en geven nadere toelichting over de daadwerkelijke toepassing en handhaving van deze verordening.

5.2. Toelichting bij de specifieke bepalingen van het voorstel

Hoofdstuk I bevat de algemene bepalingen: het onderwerp (artikel 1), het toepassingsgebied (artikelen 2 en 3) en de definities, met inbegrip van verwijzingen naar de desbetreffende definities uit andere EU-instrumenten, zoals de algemene verordening gegevensbescherming.

Hoofdstuk II bevat de belangrijkste bepalingen om de vertrouwelijkheid van de elektronische communicatie te waarborgen (artikel 5) en omschrijft de beperkte toegestane doeleinden en

voorwaarden voor de verwerking van dergelijke gegevens (artikelen 6 en 7). Voorst wordt de bescherming van eindapparatuur behandeld (i) door de integriteit van de erin opgeslagen informatie te waarborgen en (ii) door bescherming van informatie afkomstig van eindapparatuur, aangezien deze de identificatie van de eindgebruiker mogelijk kan maken (artikel 8). Ten slotte bevat artikel 9 nadere gegevens over de toestemming van de eindgebruikers, een centrale rechtsgrondslag van deze verordening, met een uitdrukkelijke verwijzing naar de definitie en de voorwaarden als bepaald in de algemene verordening gegevensbescherming, terwijl artikel 10 voorziet in de verplichting voor aanbieders van software voor elektronische communicatie om eindgebruikers te helpen bij het maken van effectieve keuzes over privacyinstellingen. Artikel 11 beschrijft volgens welke doeleinden en onder welke voorwaarden de lidstaten de bovenstaande voorschriften kunnen beperken.

Hoofdstuk III heeft betrekking op de rechten van eindgebruikers om ter bescherming van hun privacy de verzending en de ontvangst van elektronische communicatie te controleren: (i) het recht van eindgebruikers om met het oog op de anonimiteit de weergave van de identificatie van de oproepende lijn te verhinderen (artikel 12), met bepaalde beperkingen (artikel 13); en (ii) de verplichting voor aanbieders van algemeen beschikbare nummergebaseerde persoonlijke communicatiediensten om te voorzien in de mogelijkheid tot beperking van de ontvangst van ongewenste oproepen (artikel 14). Dit hoofdstuk regelt ook onder welke voorwaarden eindgebruikers kunnen worden opgenomen in algemeen beschikbare repertoria (artikel 15) en ongevraagde communicatie voor doeleinden van direct marketing kan plaatsvinden (artikel 17). Het handelt ook over veiligheidsrisico's en voorziet in een verplichting voor aanbieders van elektronische-communicatiediensten om de eindgebruikers te waarschuwen in geval van een bijzonder risico dat gevaar kan opleveren voor de veiligheid van netwerken en diensten. De beveiligingsverplichtingen in de algemene verordening gegevensbescherming en het Europees wetboek voor elektronische communicatie zullen gelden voor de aanbieders van elektronische-communicatiediensten.

Hoofdstuk IV regelt het toezicht op en de handhaving van deze verordening en belast de toezichthoudende autoriteiten voor de algemene verordening gegevensbescherming hiermee, gelet op de sterke synergieën tussen vraagstukken met betrekking tot de algemene gegevensbescherming en de vertrouwelijkheid van communicatie (artikel 18). De bevoegdheden van het Europees Comité voor gegevensbescherming worden uitgebreid (artikel 19) en het mechanisme voor samenwerking en coherentie van de algemene verordening gegevensbescherming zal van toepassing zijn in het geval van grensoverschrijdende aangelegenheden met betrekking tot deze verordening (artikel 20).

Hoofdstuk V beschrijft de verschillende rechtsmiddelen waarover de eindgebruikers kunnen beschikken (artikelen 21 en 22) en de mogelijke sancties (artikel 24), waaronder de algemene voorwaarden voor het opleggen van administratieve geldboetes (artikel 23).

Hoofdstuk VI heeft betrekking op de vaststelling van gedelegeerde en uitvoeringshandelingen overeenkomstig de artikelen 290 en 291 van het Verdrag.

Tot slot bevat hoofdstuk VII de slotbepalingen van deze verordening: de intrekking van de e-privacyrichtlijn, het toezicht en de evaluatie, de inwerkingtreding en de toepassing. Wat de evaluatie betreft, zal de Commissie met name onderzoeken of een afzonderlijke rechtshandeling nodig blijft in het licht van juridische, technische of economische ontwikkelingen en rekening houdend met de eerste evaluatie van Verordening (EU) 2016/679, die uiterlijk op 25 mei 2020 zal plaatsvinden.

2017/0003 (COD)

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

met betrekking tot de eerbiediging van het privéleven en de bescherming van persoonsgegevens in elektronische communicatie, en tot intrekking van Richtlijn 2002/58/EG (richtlijn betreffende privacy en elektronische communicatie)

(Voor de EER relevante tekst)

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name de artikelen 16 en 114,

Gezien het voorstel van de Europese Commissie,

Na toezending van het ontwerp van wetgevingshandeling aan de nationale parlementen,

Gezien het advies van het Europees Economisch en Sociaal Comité[1],

Gezien het advies van het Comité van de Regio's[2],

Gezien het advies van de Europese toezichthouder voor gegevensbescherming[3],

Handelend volgens de gewone wetgevingsprocedure,

Overwegende hetgeen volgt:

(1) Artikel 7 van het Handvest van de grondrechten van de Europese Unie ("Handvest") beschermt het grondrecht van eenieder op eerbiediging van zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn communicatie. Eerbiediging van de privacy van de communicatie is een essentieel onderdeel van dit recht. De vertrouwelijkheid van de elektronische communicatie zorgt ervoor dat de informatie die tussen partijen wordt uitgewisseld en de externe aspecten van die communicatie, waaronder het tijdstip waarop de informatie is verzonden, van waar, naar wie, niet aan anderen wordt meegedeeld dan aan de partijen die bij de communicatie betrokken zijn. Het beginsel van vertrouwelijkheid moet van toepassing zijn op huidige en toekomstige communicatiemiddelen, met inbegrip van gesprekken, internettoegang, applicaties voor instant messaging, e-mailverkeer, internettelefoon en persoonlijke berichten die via de sociale media worden verzonden.

(2) De inhoud van elektronische communicatie kan zeer gevoelige informatie weergeven over de natuurlijke personen die bij de communicatie betrokken zijn, gaande van persoonlijke ervaringen en emoties tot medische gegevens, seksuele voorkeur en politieke standpunten, die, wanneer zij openbaar worden gemaakt, zouden kunnen leiden tot persoonlijke en maatschappelijke schade, economische verliezen of

[1] PB C, blz. .
[2] PB C, blz. .
[3] PB C, blz. .

complicaties. Op dezelfde manier kunnen metagegevens met betrekking tot elektronische communicatie ook zeer gevoelige en persoonlijke informatie weergeven. Deze metagegevens omvatten de opgeroepen nummers, de bezochte websites, de geografische locatie, het tijdstip, de datum en de duur wanneer een persoon een oproep doet, enz., op basis waarvan precieze conclusies kunnen worden getrokken over het privéleven van de personen die bij de elektronische communicatie betrokken zijn, zoals hun sociale relaties, hun dagelijkse gewoonten en activiteiten, hun interesses, smaken, enz.

(3) Elektronische-communicatiegegevens kunnen ook informatie betreffende rechtspersonen weergeven, zoals bedrijfsgeheimen of andere gevoelige gegevens met een economische waarde. Derhalve moeten de bepalingen van deze verordening gelden voor zowel natuurlijke personen als rechtspersonen. Voorts moet deze verordening ervoor zorgen dat de bepalingen van Verordening (EU) 2016/679 van het Europees Parlement en de Raad[4] eveneens toegepast worden op eindgebruikers die rechtspersonen zijn. Hieronder valt de definitie van toestemming krachtens Verordening (EU) 2016/679. Wanneer naar de goedkeuring van eindgebruikers, waaronder rechtspersonen, wordt verwezen, moet deze definitie worden toegepast. Voorts moeten rechtspersonen ten aanzien van de toezichthoudende autoriteiten dezelfde rechten hebben als eindgebruikers die natuurlijke personen zijn: de toezichthoudende autoriteiten uit hoofde van deze verordening moeten verder ook worden belast met het toezicht op de toepassing van deze verordening ten aanzien van rechtspersonen.

(4) Op grond van artikel 8, lid 1, van het Handvest en artikel 16, lid 1, van het Verdrag betreffende de werking van de Europese Unie heeft eenieder recht op bescherming van de hem betreffende persoonsgegevens. Bij Verordening (EU) 2016/679 worden regels vastgesteld betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van persoonsgegevens. Elektronische-communicatiegegevens kunnen persoonsgegevens omvatten zoals gedefinieerd in Verordening (EU) 2016/679.

(5) De bepalingen van deze verordening vormen een specificatie van en een aanvulling op de algemene regels inzake bescherming van persoonsgegevens neergelegd in Verordening (EU) 2016/679 wat betreft de elektronische-communicatiegegevens die als persoonsgegevens worden aangemerkt. Deze verordening leidt dus niet tot een lager niveau van bescherming van natuurlijke personen in de zin van Verordening (EU) 2016/679. Verwerking van elektronische-communicatiegegevens door aanbieders van elektronische-communicatiediensten moet alleen worden toegestaan in overeenstemming met deze verordening.

(6) Hoewel de beginselen en de belangrijkste bepalingen van Richtlijn 2002/58/EG van het Europees Parlement en de Raad[5] in het algemeen geldig blijven, heeft deze richtlijn geen gelijke tred gehouden met de ontwikkeling van de technologie en de

---

4 Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1).

5 Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (Richtlijn betreffende privacy en elektronische communicatie) (PB L 201 van 31.7.2002, blz. 37).

markt, hetgeen resulteert in inconsistenties of gebreken in de doeltreffende bescherming van de privacy en de vertrouwelijkheid met betrekking tot elektronische communicatie. Tot deze ontwikkelingen behoort de komst op de markt van elektronische-communicatiediensten die uit het standpunt van de consument verwisselbaar zijn met traditionele diensten maar niet hoeven te voldoen aan dezelfde reeks regels. Een andere ontwikkeling heeft betrekking op nieuwe technieken voor het volgen van het onlinegedrag van eindgebruikers, die niet onder Richtlijn 2002/58/EG vallen. Richtlijn 2002/58/EEG moet derhalve worden ingetrokken en vervangen door deze verordening.

(7) De lidstaten moeten, binnen de grenzen van deze verordening, nationale bepalingen kunnen handhaven of invoeren om met het oog op een effectieve uitvoering en interpretatie van de regels van deze verordening de toepassing ervan nader te specificeren en te verduidelijken. Daarom moet in de beoordelingsmarge die de lidstaten op dit gebied hebben, gezorgd worden voor een evenwicht tussen de bescherming van de persoonlijke levenssfeer en persoonsgegevens en het vrije verkeer van elektronische-communicatiegegevens.

(8) Deze verordening moet van toepassing zijn op aanbieders van elektronische-communicatiediensten, aanbieders van algemeen beschikbare telefoongidsen en aanbieders van software voor elektronische communicatie, waaronder het opvragen en weergeven van informatie op het internet. Deze verordening moet eveneens van toepassing zijn op natuurlijke en rechtspersonen die gebruik maken van elektronische-communicatiediensten om commerciële boodschappen van direct marketing te verzenden of om informatie te verzamelen die verbonden is aan of opgeslagen is in eindapparatuur van eindgebruikers.

(9) Deze verordening moet van toepassing te zijn op elektronische-communicatiegegevens die verwerkt zijn in verband met het aanbieden en het gebruiken van elektronische-communicatiediensten in de Unie, ongeacht of de verwerking in de Unie plaatsvindt. Om te vermijden dat eindgebruikers in de Unie verstoken blijven van doeltreffende bescherming, dient deze verordening verder ook van toepassing te zijn op elektronische-communicatiegegevens die zijn verwerkt in verband met het aanbieden van elektronische-communicatiediensten van buiten de Unie aan eindgebruikers in de Unie.

(10) Radioapparatuur en bijbehorende software die in de Unie op de markt wordt gebracht, moet voldoen aan Richtlijn 2014/53/EU van het Europees Parlement en de Raad[6]. Deze verordening mag geen afbreuk doen aan de toepasselijkheid van de voorschriften van Richtlijn 2014/53/EU of aan de bevoegdheid van de Commissie om overeenkomstig Richtlijn 2014/53/EU gedelegeerde handelingen vast te stellen waarbij voorgeschreven wordt dat bepaalde categorieën of klassen radioapparatuur voorzieningen moeten bevatten om de bescherming van persoonsgegevens en de persoonlijke levenssfeer van eindgebruikers te garanderen.

(11) De diensten die voor communicatiedoeleinden worden gebruikt en de technische middelen die daarbij worden aangewend, hebben een sterke ontwikkeling doorgemaakt. Eindgebruikers maken in de plaats van traditionele spraaktelefonie, tekstboodschappen (SMS) en elektronische post (e-mail) steeds vaker gebruik van

[6] Richtlijn 2014/53/EU van het Europees Parlement en de Raad van 16 april 2014 betreffende de harmonisatie van de wetgevingen van de lidstaten inzake het op de markt aanbieden van radioapparatuur en tot intrekking van Richtlijn 1999/5/EG (PB L 153 van 22.5.2014, blz. 62).

functioneel gelijkwaardige onlinediensten zoals Voice over IP, berichtendiensten en webmail. Met het oog op een effectieve en gelijke bescherming van eindgebruikers bij het gebruik van functioneel gelijkwaardige diensten wordt in deze verordening de definitie van elektronische-communicatiediensten gebruikt die in de [richtlijn van het Europees Parlement en de Raad tot vaststelling van het Europees wetboek voor elektronische communicatie[7]] is voorgesteld. Deze definitie omvat niet alleen diensten voor toegang tot internet en diensten die geheel of gedeeltelijk bestaan in het overbrengen van signalen, maar ook persoonlijke communicatiediensten, die al dan niet gebruik maken van nummers, zoals bijvoorbeeld Voice over IP, berichtendiensten en webmail. De bescherming van de vertrouwelijkheid van de communicatie is van cruciaal belang, ook met betrekking tot persoonlijke communicatiediensten die ondergeschikt zijn ten opzichte van een andere dienst; daarom moeten dergelijke diensten die ook een communicatiefunctie dienen, onder deze verordening vallen.

(12) Aangesloten apparaten en machines gaan steeds meer met elkaar communiceren via elektronische-communicatienetwerken ("internet van dingen"). De transmissie van communicatie tussen machines ("machine-to-machine") houdt in dat signalen via een netwerk worden overgedragen, en vormt dus meestal een elektronische-communicatiedienst. Met het oog op een volledige bescherming van het recht op privacy en vertrouwelijkheid van communicatie alsook om een betrouwbaar en veilig internet van dingen te bevorderen in het kader van de digitale interne markt, moet worden verduidelijkt dat deze verordening van toepassing dient te zijn op de doorgifte van communicatie tussen machines. Derhalve moet het beginsel van vertrouwelijkheid zoals vastgelegd in deze verordening ook van toepassing zijn op de doorgifte van communicatie tussen machines. Er moet ook voor specifieke voorzieningen worden gezorgd in het kader van sectorale wetgeving, zoals Richtlijn 2014/53/EU.

(13) De ontwikkeling van snelle en efficiënte draadloze technologieën heeft ertoe bijgedragen dat internettoegang via draadloze netwerken in toenemende mate voor iedereen toegankelijk wordt gesteld in openbare en semi-openbare ruimten zoals „hotspots", die zich op verschillende plaatsen in de stad, supermarkten, winkelcentra en ziekenhuizen bevinden. Voor zover deze communicatienetwerken worden verleend aan een onbepaalde groep van eindgebruikers, moet het vertrouwelijke karakter van de communicatie via dergelijke netwerken worden beschermd. Het feit dat draadloze elektronische-communicatiediensten ondergeschikt kunnen zijn aan andere diensten, mag niet ten koste gaan van de bescherming van de vertrouwelijkheid van communicatiegegevens en de toepassing van deze verordening. Daarom moet deze verordening van toepassing zijn op elektronische-communicatiegegevens die gebruikmaken van elektronische-communicatiediensten en openbare communicatienetwerken. Deze verordening mag daarentegen niet van toepassing zijn op gesloten groepen eindgebruikers zoals bedrijfsnetwerken, waarvan de toegang beperkt is tot leden van de onderneming.

(14) Elektronische-communicatiegegevens moeten voldoende ruim en op technologisch neutrale wijze worden gedefinieerd zodat de definitie slaat op alle informatie die betrekking heeft op de doorgegeven of uitgewisselde inhoud (inhoud van elektronische communicatie), alsook op de informatie over eindgebruikers van elektronische-communicatiediensten die verwerkt wordt met het oog op de transmissie, de distributie

[7] Voorstel van de Commissie voor een richtlijn van het Europees Parlement en de Raad tot vaststelling van het Europees wetboek voor elektronische communicatie (herschikking) (COM/2016/0590 final — 2016/0288 (COD)).

of de uitwisseling van elektronische-communicatie-inhoud, waaronder gegevens om de bron en de bestemming, te traceren en te omschrijven de geografische lokalisatie en de datum, het tijdstip, de duur en het soort communicatie. Ongeacht of deze signalen en de bijbehorende gegevens door middel van kabels, radiogolven, optische of elektromagnetische middelen waaronder satellietnetwerken, kabelnetwerken, (circuit- en pakketgeschakelde, met inbegrip van internet) vaste en mobiele terrestrische netwerken of elektriciteitskabelsystemen worden overgebracht, de gegevens met betrekking tot deze signalen moeten worden beschouwd als elektronische-communicatiemetagegevens en moeten derhalve onderworpen zijn aan de bepalingen van deze verordening. Tot de elektronische-communicatiemetagegevens kan ook de informatie worden gerekend die deel uitmaakt van de inschrijving op de dienst, wanneer deze informatie verwerkt wordt met het oog op de transmissie, de distributie of de uitwisseling van elektronische-communicatie-inhoud.

(15) Elektronische-communicatiegegevens moeten als vertrouwelijk moeten worden behandeld. Dit betekent dat elke interferentie in de transmissie van elektronische-communicatiegegevens, hetzij rechtstreeks door menselijk ingrijpen, hetzij via de tussenkomst van geautomatiseerde verwerking door machines, zonder de toestemming van alle communicerende partijen, moet worden verboden. Het verbod op interceptie van communicatiegegevens moet gelden tijdens de overdracht ervan, met andere woorden totdat de inhoud van de elektronische communicatie door de beoogde geadresseerde is ontvangen. Het onderscheppen van elektronische communicatie kan zich bijvoorbeeld voordoen wanneer iemand anders dan de communicerende partijen naar oproepen luistert, de inhoud van elektronische communicatie of de bijbehorende metagegevens leest, scant of opslaat voor andere doeleinden dan de uitwisseling van communicatie. Interceptie vindt ook plaats wanneer derden toezicht houden op de bezochte websites, het tijdstip van de bezoeken, de interactie met anderen, enzovoort, zonder toestemming van de betrokken eindgebruiker. Naarmate de technologie zich verder ontwikkelt, zijn ook de technische mogelijkheden voor interceptie toegenomen. Deze middelen kunnen variëren van de installatie van apparatuur waarmee gegevens van eindapparatuur worden verzameld gegevens over welbepaalde terreinen, zoals de zogenoemde "IMSI-catchers" (international mobile subscriber identity), tot programma’s en technieken die bijvoorbeeld ongemerkt surfgewoonten volgen om eindgebruikersprofielen te creëren. Andere voorbeelden van interceptie zijn het opvangen van payloadgegevens of gegevens over inhoud uit niet-versleutelde draadloze netwerken en routers, met inbegrip van surfgewoonten, zonder toestemming van de eindgebruiker.

(16) Het verbod op de opslag van communicatie is niet bedoeld om de automatische, tussentijdse en tijdelijke opslag van deze informatie te verbieden voor zover deze plaatsvindt met als uitsluitend doel de transmissie in het elektronische-communicatienetwerk tot stand te brengen. Evenmin mag een verbod worden ingesteld op verwerking van elektronische-communicatiegegevens om de veiligheid en de continuïteit van de elektronische-communicatiediensten te garanderen, waaronder de controle van veiligheidsbedreigingen zoals de aanwezigheid van malware of de verwerking van metagegevens om de vereiste kwaliteit van de dienstverlening, zoals latency, jitter, enz. te waarborgen.

(17) Verwerking van elektronische-communicatiegegevens kan nuttig zijn voor ondernemingen, consumenten en de samenleving in haar geheel. Ten opzichte van Richtlijn 2002/58/EG verruimt deze verordening de mogelijkheden voor aanbieders van elektronische-communicatiediensten om metagegevens van elektronische

communicatie te verwerken op basis van de toestemming van eindgebruikers. Eindgebruikers hechten echter veel belang aan de vertrouwelijkheid van hun communicatie, waaronder hun onlineactiviteiten, en willen controle uitoefenen over het gebruik van elektronische-communicatiegegevens voor andere doeleinden dan de overdracht van de communicatie. Daarom moeten aanbieders van elektronische-communicatiediensten op basis van deze verordening ertoe verplicht worden van de eindgebruikers toestemming te verkrijgen voor de verwerking van elektronische-communicatiemetagegevens, waaronder gegevens betreffende de locatie van de apparatuur die gegenereerd worden om de toegang tot en de verbinding met de dienst te verlenen en te onderhouden. Locatiegegevens die in een andere context dan bij het aanbieden van elektronische communicatiediensten worden gegenereerd, hoeven niet te worden beschouwd als metagegevens. Als voorbeeld van commercieel gebruik van elektronische-communicatiemetagegevens door aanbieders van elektronische-communicatiediensten kan het verstrekken van "heatmaps" worden aangehaald, een grafische voorstelling van gegevens met kleuren om de aanwezigheid van individuele personen aan te geven. Om verkeersbewegingen in bepaalde richtingen gedurende een bepaalde periode weer te geven, is een identificatiecode nodig om de posities van individuele personen op bepaalde tijdstippen met elkaar te verbinden. Deze identificatiecode zou ontbreken indien anonieme gegevens dienden te worden gebruikt en dan kon een dergelijke beweging niet worden weergegeven. Een dergelijk gebruik van elektronische-communicatiemetagegevens kan bijvoorbeeld nuttig zijn voor autoriteiten en exploitanten van openbaar vervoer om te bepalen waar zij nieuwe infrastructuur moeten ontwikkelen, op basis van het gebruik van en de druk op de bestaande structuur. Wanneer een bepaald soort verwerking van metagegevens van elektronische communicatie, in het bijzonder wanneer nieuwe technologieën worden gebruikt en rekening houdend met de aard, het bereik, de context en de doelen van de verwerking, een groot risico kan opleveren voor de rechten en vrijheden van natuurlijke personen, moet overeenkomstig de artikelen 35 en 36 van Verordening (EU) 2016/679 vóór de verwerking van de gegevens een effectbeoordeling inzake gegevensbescherming worden verricht en moet naargelang van het geval de toezichthoudende autoriteit worden geraadpleegd.

(18) De eindgebruikers kunnen hun toestemming voor de verwerking van hun metagegevens verlenen om specifieke diensten te ontvangen zoals diensten van bescherming tegen frauduleuze activiteiten (door analyse van gebruiksgegevens, locatie en klantenrekening in real time). In de digitale economie worden diensten vaak geleverd voor een andere tegenprestatie dan geld, bijvoorbeeld door eindgebruikers bloot te stellen aan reclame. Voor de toepassing van deze verordening moet de goedkeuring van een eindgebruiker, ongeacht of het om een natuurlijke dan wel een rechtspersoon gaat, dezelfde betekenis krijgen en aan dezelfde voorwaarden worden onderworpen als de toestemming van de betrokkene overeenkomstig Verordening (EU) 2016/679. Een basistoegang tot breedbandinternet en spraakcommunicatiediensten moeten worden beschouwd als essentiële diensten waarmee particulieren kunnen communiceren en deelnemen aan de voordelen van de digitale economie. De toestemming voor de verwerking van gegevens van internet- of spraakcommunicatiegebruik is niet geldig indien de betrokkene geen echte vrije keuze heeft of niet in staat is zijn toestemming te weigeren of in te trekken zonder nadelige gevolgen.

(19) De inhoud van elektronische communicatie behoort tot het wezen van het grondrecht op eerbiediging van het privéleven en het familie- en gezinsleven, de woning en de communicatie zoals beschermd door artikel 7 van het Handvest. Elke interferentie in

de inhoud van elektronische communicatie mag alleen worden toegestaan onder zeer duidelijk omschreven voorwaarden, voor specifieke doeleinden en moet worden onderworpen aan passende waarborgen tegen misbruik. Deze verordening voorziet in de mogelijkheid voor aanbieders van elektronische-communicatiediensten om elektronische-communicatiegegevens in doorvoer te verwerken, op voorwaarde dat alle betrokken eindgebruikers hun toestemming met kennis van zaken hebben gegeven. Zo kunnen aanbieders diensten leveren die het scannen van e-mails impliceren om een aantal vooraf bepaalde materialen te verwijderen. Gezien de gevoeligheid van de inhoud van communicatie stelt deze verordening een vermoeden in dat de verwerking van dergelijke inhoudgegevens zal resulteren in hoge risico's voor de rechten en vrijheden van natuurlijke personen. Bij de verwerking van dit soort gegevens moet de aanbieder van de elektronische-communicatiediensten altijd de toezichthoudende autoriteit raadplegen voordat de verwerking plaatsvindt. Deze raadpleging dient te verlopen in overeenstemming met artikel 36, leden 2 en 3, van Verordening (EU) 2016/679. Het vermoeden geldt niet wanneer de verwerking van inhoudgegevens plaatsvindt om op verzoek van de eindgebruiker een dienst te verstrekken, wanneer de eindgebruiker heeft ingestemd met deze verwerking en deze wordt verricht voor de doeleinden en de duur die strikt noodzakelijk en evenredig zijn voor deze dienst. Nadat inhoud van elektronische communicatie door de eindgebruiker is verzonden en door de beoogde eindgebruiker of eindgebruikers is ontvangen, kan deze worden geregistreerd en opgeslagen door de eindgebruiker(s) of een derde die door hem belast is met de registratie en de opslag van deze gegevens. Elke verwerking van persoonsgegevens dient in overeenstemming te zijn met Verordening (EU) 2016/679.

(20) Eindapparatuur van gebruikers van elektronische-communicatienetwerken en informatie met betrekking tot het gebruik van dergelijke eindapparatuur, ongeacht of deze met name in dergelijke apparatuur wordt opgeslagen of daardoor wordt uitgezonden, wordt opgevraagd of verwerkt om een verbinding met andere apparaten of netwerkuitrusting mogelijk te maken, behoren tot de persoonlijke levenssfeer van de eindgebruikers die krachtens het Handvest van de grondrechten van de Europese Unie en het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden moet worden beschermd. Aangezien in dergelijke apparatuur gegevens zitten of verwerkt worden die nadere informatie kunnen vrijgeven over iemands persoonlijke, politieke of maatschappelijke ingesteldheid, waaronder de inhoud van de communicatie, foto’s, de locatie van de personen door gebruik van de GPS-functie van het apparaat, contactlijsten en andere informatie die reeds in het apparaat is opgeslagen, moet de informatie met betrekking tot deze apparaten een sterkere privacybescherming krijgen. Voorts kunnen zogenoemde spyware, webbugs, verborgen identificatoren, tracking cookies en andere soortgelijke ongewenste volgsystemen de eindapparatuur van de eindgebruiker zonder zijn medeweten binnendringen om toegang te zoeken tot informatie, verborgen informatie op te slaan of de activiteiten te volgen. Informatie met betrekking tot de uitrusting van eindgebruiker kan ook op afstand worden verzameld met het oog op identificatie en traceeractiviteit, met gebruik van technieken zoals de zogenoemde "device fingerprinting", vaak zonder medeweten van de eindgebruiker, hetgeen kan leiden tot ernstig inbreuken op de persoonlijke levenssfeer van deze eindgebruikers. Technieken om ongemerkt handelingen van eindgebruikers te controleren, bijvoorbeeld door hun onlineactiviteiten op het internet of de locatie van hun eindapparatuur te volgen of de werking van de eindapparatuur van eindgebruikers te verstoren, vormen een ernstige bedreiging voor de privacy van de eindgebruikers. Daarom mag een dergelijke

interferentie met de eindapparatuur van de eindgebruiker alleen worden toegestaan met de toestemming van de eindgebruiker en voor specifieke en transparante toepassingen.

(21) Uitzonderingen op het verplicht verkrijgen van toestemming om gebruik te maken van de verwerkings- en opslagcapaciteit van eindapparatuur of om toegang te krijgen tot informatie die in eindapparatuur is opgeslagen, moeten beperkt blijven tot situaties waarin er geen of slechts in zeer beperkte mate sprake is van inmenging in de persoonlijke levenssfeer. Zo hoeft geen toestemming te worden gevraagd om technische opslag of toegang mogelijk te maken wanneer dit strikt noodzakelijk en evenredig is voor het rechtmatige doel het gebruik mogelijk te maken van een specifieke dienst die een eindgebruiker uitdrukkelijk heeft aangevraagd. Het kan gaan om de opslag van cookies voor de duur van één bezoeksessie op een website waarop de gegevens van de eindgebruiker worden bijgehouden tijdens het invullen van een onlineformulier dat uit verschillende pagina's bestaat. Cookies kunnen ook een legitiem en nuttig hulpmiddel zijn om bijvoorbeeld het bezoekersverkeer op een website te meten. In het geval van aanbieders van diensten van de informatiemaatschappij die de configuratie controleren om de dienst in overeenstemming met de instellingen van de eindgebruiker te verlenen, en bij het louter registreren van het feit dat het apparaat van de eindgebruiker niet in staat is de door de eindgebruiker opgevraagde inhoud te ontvangen, is er geen sprake van toegang tot het apparaat of gebruik van de verwerkingscapaciteit van het apparaat.

(22) De aangewende methoden om informatie te verstrekken en om de toestemming van de eindgebruiker te verkrijgen moeten zo gebruiksvriendelijk mogelijk zijn. Gezien het alomtegenwoordige gebruik van tracking cookies en andere volgtechnieken worden eindgebruikers steeds vaker verzocht om toestemming voor de opslag van dergelijke tracking cookies in hun eindapparatuur. Het gevolg is dat eindgebruikers worden overstelpt met verzoeken om toestemming. Het gebruik van technische middelen om toestemming te verlenen, bijvoorbeeld door middel van transparante en gebruiksvriendelijke instellingen, kan dit probleem verhelpen. Daarom moet deze verordening voorzien in de mogelijkheid om de toestemming uit te drukken door gebruik van passende instellingen van de browser of een andere applicatie. De keuzes die eindgebruikers maken bij het invoeren van de algemene privacyinstellingen van een browser of een andere applicatie, moeten bindend zijn en moeten kunnen worden afgedwongen ten aanzien van derden. Een webbrowser is een soort softwareapplicatie die het opvragen en het weergeven van informatie op het internet mogelijk maakt. Andere soorten applicaties, zoals applicaties om gesprekken te verrichten of boodschappen te verzenden of voor verkeersnavigatie, bieden ook dezelfde capaciteiten. Webbrowsers vervullen in vele gevallen een bemiddelende functie tussen de eindgebruiker en de website. Uit dit oogpunt bekleden zij een bevoorrechte positie en spelen zij om een actieve rol om de eindgebruiker te helpen greep te krijgen op de stroom van informatie van en naar de eindapparatuur. Meer in het bijzonder kunnen webbrowsers worden gebruikt als poortwachters en dus als hulpmiddel voor eindgebruikers om toegang tot informatie uit hun eindapparatuur (bijvoorbeeld computer, tablet of smartphone) of opslag van dergelijke informatie te voorkomen.

(23) De beginselen van gegevensbescherming door ontwerp en door standaardinstellingen werden vastgelegd in artikel 25 van Verordening (EU) 2016/679. Momenteel is de standaardinstelling voor cookies in de meest voorkomende browsers het "aanvaarden van alle cookies". Daarom moeten aanbieders van software voor het opvragen en het weergeven van informatie op het internet ertoe verplicht worden de software zo te

configureren dat de optie wordt geboden om derden te verhinderen informatie in de eindapparatuur op te slaan; dit wordt vaak aangeboden als "cookies van derden verwerpen". Aan eindgebruikers moet een reeks privacyopties worden geboden, variërend van hogere (bijvoorbeeld "nooit cookies accepteren") tot lagere privacy (bijvoorbeeld "altijd cookies accepteren") met een tussenniveau (bijvoorbeeld "cookies van derden verwerpen" of "alleen first party cookies accepteren"). Deze privacyinstellingen moeten op een duidelijk zichtbare en begrijpelijke wijze worden gepresenteerd.

(24) Om de toestemming van eindgebruikers zoals gedefinieerd in Verordening (EU) 2016/679 te kunnen verkrijgen, bijvoorbeeld voor de opslag van tracking cookies van derden, moeten webbrowsers onder meer een ondubbelzinnige actieve handeling van de eindgebruiker van eindapparatuur eisen waaruit blijkt dat hij of zij vrijelijk, specifiek met kennis van zaken en ondubbelzinnig instemt met de opslag van en de toegang tot dergelijke cookies in en vanuit de eindapparatuur. Dergelijke handeling kan worden beschouwd als actief, bijvoorbeeld indien de eindgebruikers actief "cookies van derden aanvaarden" moeten selecteren om hun toestemming te bevestigen en indien hun de nodige informatie wordt verstrekt om de keuze te maken. Daarom moeten aanbieders van software die internettoegang mogelijk maakt, ertoe verplicht worden eindgebruikers op het moment van de installatie te informeren over de mogelijkheid om tussen de verschillende opties de privacyinstellingen te kiezen en hen vragen om een keuze. De verstrekte informatie mag eindgebruikers er niet van weerhouden de hogere privacyinstellingen te selecteren en moet relevante informatie bieden over de risico's die verbonden zijn aan de optie om opslag van cookies van derden in de computer toe te staan, onder meer met betrekking tot het verzamelen van langetermijngegevens uit de individuele browsergeschiedenis van een persoon en het gebruik van die gegevens om gerichte advertenties te sturen. Webbrowsers worden ertoe aangezet de eindgebruikers gemakkelijke middelen te verschaffen om de privacyinstellingen op elk moment tijdens het gebruik te wijzigen, en om de gebruiker uitzonderingen te laten maken of een witte lijst te laten aanleggen voor bepaalde websites of te laten verduidelijken voor welke websites cookies (van derden) nooit dan wel altijd zijn toegestaan.

(25) Voor de toegang tot elektronische-communicatienetwerken moet regelmatig een aantal gegevenspakketjes worden uitgezonden om een verbinding met het netwerk of met andere apparaten op het netwerk op te sporen of in stand te houden. Verder moet aan apparaten een uniek adres worden toegewezen om identificeerbaar te zijn om op dat netwerk. Ook voor draadloze- en mobieletelefoonnormen moeten actieve signalen worden uitgezonden met unieke identificatoren zoals een MAC-adres, de IMEI (International Mobile Equipment Identity station), de IMSI, enzovoort. Een enkel draadloos basisstation (d.w.z. een zender en ontvanger), zoals een draadloos toegangspunt, heeft een bepaald bereik waarbinnen deze informatie kan worden opgevangen. Er zijn dienstverrichters op de markt gekomen met een aanbod van volgdiensten op basis van het scannen van aan de uitrusting verbonden informatie, die diverse functies kunnen verrichten, onder meer het tellen van personen, de verstrekking van gegevens over het aantal personen in de wachtrij, de controle van het aantal mensen in een specifiek gebied, enz. Deze informatie kan worden gebruikt voor meer agressieve doeleinden, zoals het verzenden van commerciële boodschappen aan eindgebruikers, bijvoorbeeld bij het binnengaan van een winkel, met gepersonaliseerde aanbiedingen. Hoewel sommige van deze functies geen hoge risico's voor de persoonlijke levenssfeer inhouden, wordt bij andere functies bijvoorbeeld gebruik gemaakt van het traceren van personen in de tijd, onder meer voor herhaalde bezoeken

aan specifieke plaatsen. Aanbieders die zich op dergelijke praktijken toeleggen, moeten aan de rand van het dekkingsgebied duidelijk zichtbare berichten aanbrengen waarmee eindgebruikers voordat zij het afgebakende gebied betreden, worden geïnformeerd over de operationele werking van de technologie binnen een bepaalde perimeter, het doel van de volgtechniek, de persoon die daarvoor verantwoordelijkheid draagt en het bestaan van elke maatregel die de eindgebruiker van de eindapparatuur kan nemen om het verzamelen van gegevens te beperken of te beëindigen. Er moet aanvullende informatie worden verstrekt wanneer er persoonsgegevens overeenkomstig artikel 13 van Verordening (EU) nr. 2016/679 worden verzameld.

(26) Wanneer de verwerking van elektronische-communicatiegegevens door aanbieders van elektronische-communicatiediensten binnen het toepassingsgebied van de verordening valt, dient te worden voorzien in de mogelijkheid voor de Unie of de lidstaten om onder specifieke voorwaarden bepaalde rechten en verplichtingen bij wet te beperken indien een dergelijke beperking een noodzakelijke en evenredige maatregel in een democratische samenleving vormt ter bescherming van specifieke openbare belangen, waaronder de nationale veiligheid, de landsverdediging, de openbare veiligheid, het voorkomen, opsporen, onderzoeken of vervolgen van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van bedreigingen voor de openbare veiligheid en andere belangrijke doelstellingen van algemeen belang van de Unie of van een lidstaat, met name een belangrijk economisch of financieel belang van de Unie of een lidstaat, of een taak op het gebied van controle, inspectie of regelgeving die verbonden is aan de uitoefening van het openbaar gezag voor deze belangen. Deze verordening mag derhalve geen afbreuk doen aan het vermogen van de lidstaten om wettelijk toegestane interceptie van elektronische communicatie te verrichten of andere maatregelen te nemen, indien die noodzakelijk en evenredig is ter bescherming van de bovengenoemde openbare belangen, in overeenstemming met het Handvest van de grondrechten van de Europese Unie en het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, zoals uitgelegd door het Hof van Justitie en het Europees Hof voor de rechten van de mens. Aanbieders van elektronische-communicatiediensten moeten zorgen voor passende procedures om legitieme verzoeken van bevoegde autoriteiten te vergemakkelijken, indien nodig ook rekening houdend met de rol van de overeenkomstig artikel 3, lid 3, aangewezen vertegenwoordiger.

(27) Wat de identificatie van de oproepende lijn betreft, moet bescherming worden geboden voor het recht van de oproeper om de weergave van de identificatie van het oproepende nummer te blokkeren en het recht van de opgeroepene om niet geïdentificeerde oproepen te weigeren. Bepaalde eindgebruikers, zoals hulplijnen en soortgelijke instanties, hebben er belang bij de anonimiteit van de oproepers te waarborgen. Wat de identificatie van het opgeroepen nummer betreft, moet het recht en het rechtmatige belang van de opgeroepene worden beschermd om de weergave van de identificatie van het nummer waarmee de oproeper in werkelijkheid verbonden is, te blokkeren.

(28) Het is gerechtvaardigd om in specifieke gevallen de uitschakeling van de identificatie van het oproepende nummer op te heffen. De rechten van eindgebruikers op bescherming van hun privéleven moeten worden beperkt wat betreft de identificatie van het oproepende nummer, wanneer dit noodzakelijk is om hinderlijke oproepen te traceren, en wat betreft de identificatie van het oproepende nummer en de

locatiegegevens, wanneer dit noodzakelijk is om nooddiensten zoals eCall in staat te stellen hun taken zo effectief mogelijk uit te voeren.

(29) Er bestaat technologie waarmee aanbieders van elektronische-communicatiediensten de ontvangst van ongewenste oproepen van eindgebruikers op verschillende manieren kunnen beperken, onder meer door stille oproepen en andere frauduleuze en hinderlijke oproepen te blokkeren. Aanbieders van algemeen beschikbare nummergebaseerde persoonlijke communicatiediensten dienen deze technologie in te voeren en eindgebruikers kosteloos te beschermen tegen hinderlijke oproepen. Aanbieders moeten ervoor zorgen dat de eindgebruikers op de hoogte zijn van het bestaan van dergelijke functies, bijvoorbeeld door dit gegeven op hun website bekend te maken.

(30) Algemeen beschikbare telefoongidsen van eindgebruikers van elektronische-communicatiediensten zijn ruim verspreid. Een algemeen beschikbare telefoongids is een gids of dienst die informatie over eindgebruikers bevat zoals telefoonnummers (inclusief mobiele telefoonnummers), e-mailadressen, contactgegevens, en voorziet ook in inlichtingendiensten. Het recht op eerbiediging van het privéleven en op bescherming van de persoonsgegevens van natuurlijke personen vereist dat eindgebruikers die natuurlijke personen zijn, om toestemming worden verzocht voordat hun persoonlijke gegevens in een repertorium worden opgenomen. De rechtmatige belangen van rechtspersonen vereisen dat eindgebruikers die juridische entiteiten zijn, het recht hebben om bezwaar te maken tegen opname van de hen betreffende gegevens in een repertorium.

(31) Indien eindgebruikers die natuurlijke personen zijn, hun toestemming geven voor de opname van hun gegevens in dergelijke telefoongidsen, moeten zij door middel van hun toestemming kunnen bepalen welke categorieën persoonsgegevens in het repertorium worden opgenomen (bijvoorbeeld naam, e-mailadres, woonadres, gebruikersnaam, telefoonnummer). Daarnaast moeten eindgebruikers door aanbieders van algemeen beschikbare telefoongidsen worden geïnformeerd over de doeleinden van de gids en de zoekfuncties die deze biedt, voordat zij in de lijst worden opgenomen. Eindgebruikers moeten door middel van hun toestemming kunnen bepalen welke categorieën persoonsgegevens en contactgegevens kunnen worden opgevraagd. De categorieën persoonsgegevens die in het repertorium zijn opgenomen, en de categorieën persoonsgegevens op basis waarvan contactgegevens van eindgebruikers kunnen worden opgevraagd, hoeven niet noodzakelijk dezelfde te zijn.

(32) In deze verordening heeft direct marketing betrekking op elke vorm van reclame waarbij een natuurlijke of rechtspersoon directmarketingberichten rechtstreeks toezendt aan een of meer geïdentificeerde of identificeerbare eindgebruikers die gebruik maken van elektronische-communicatiediensten. Naast het aanbieden van producten en diensten voor commerciële doeleinden moet dit ook betrekking hebben op berichten die politieke partijen via elektronische-communicatiediensten aan natuurlijke personen zenden om hun partij te promoten. Hetzelfde moet gelden voor berichten van andere organisaties zonder winstoogmerk om de doelstellingen van de organisatie te ondersteunen.

(33) Er moeten garanties komen om eindgebruikers te beschermen tegen ongewenste communicatie voor directmarketingdoeleinden, die een inbreuk vormt op het privéleven van eindgebruikers. De mate waarin inbreuk de privacy wordt gepleegd en overlast wordt veroorzaakt, wordt vrij gelijk geacht onafhankelijk van het brede scala van technologieën en kanalen die voor deze elektronische communicatie worden

gebruikt, of het nu gaat om automatische oproep- en communicatiesystemen dan wel om applicaties voor instant messaging, e-mail, SMS, MMS, bluetooth, enz. Met het oog op een doeltreffende bescherming van particulieren tegen inbreuken op hun persoonlijke levenssfeer en van de rechtmatige belangen van rechtspersonen, Het is het derhalve gerechtvaardigd voor te schrijven dat de toestemming van de eindgebruiker moet worden verkregen voordat commerciële elektronische communicatie voor doeleinden van direct marketing aan eindgebruikers kan worden toegezonden. Omwille van de rechtszekerheid en om ervoor te zorgen dat de regelgeving ter bescherming tegen ongewenste elektronische communicatie ook in de toekomst haar nut kan blijven bewijzen, moet één enkel pakket regels worden vastgesteld dat niet verschilt naargelang van de toegepaste technologie om deze ongewenste communicatie over te brengen, en moet tegelijkertijd een gelijkwaardig niveau van bescherming voor alle burgers in de hele Unie worden gewaarborgd. Het is echter redelijk het gebruik van e-mailcontactgegevens binnen de context van een bestaande klantrelatie toe te staan voor het aanbieden van soortgelijke producten of diensten. Deze mogelijkheid mag alleen maar openstaan voor dezelfde onderneming die de elektronische contactgegevens heeft verkregen overeenkomstig Verordening (EU) 2016/679.

(34) Wanneer een eindgebruiker zijn toestemming heeft gegeven om ongevraagde communicatie voor directmarketingdoeleinden te ontvangen, moet hij nog steeds de mogelijkheid hebben om zijn toestemming te allen tijde op eenvoudige wijze in te trekken. Met het oog op een doeltreffende handhaving van de Unievoorschriften inzake ongewenste direct marketing is een verbod noodzakelijk op het afschermen van de identiteit en het gebruiken van valse identiteiten, valse terugzendadressen of nummers bij verzending van ongevraagde commerciële communicatie van direct marketing. Ongevraagde commerciële communicatie moet derhalve duidelijk als zodanig herkenbaar zijn en moet melding maken van de identiteit van de rechtspersoon of de natuurlijke persoon die de mededeling verricht of namens wie het bericht wordt verzonden. Aan de ontvanger van het bericht moet de nodige informatie worden verstrekt om zijn hun recht van bezwaar tegen verdere ontvangst van schriftelijke en/of mondelinge reclameboodschappen uit te oefenen.

(35) Om de gemakkelijke intrekking van de toestemming mogelijk te maken, moeten natuurlijke of rechtspersonen die direct marketing per e-mail verrichten, een link of een geldig e-mailadres vermelden dat gemakkelijk door de eindgebruiker kan worden gebruikt om zijn toestemming in te trekken. Natuurlijke of rechtspersonen die zich toeleggen op direct marketing verrichten via spraakoproepen en oproepen door automatische oproep- en communicatiesystemen, moeten de identiteit bekendmaken van de lijn waarop de onderneming kan worden opgeroepen, of een specifieke code vermelden ter identificatie van het feit dat het om een marketingoproep gaat.

(36) Telefoongesprekken van direct marketing die geen gebruik maken van automatische oproep- en communicatiesystemen, zijn duurder voor de verzender en brengen geen financiële kosten mee voor de eindgebruiker. De lidstaten moeten daarom de mogelijkheid hebben nationale systemen in te stellen of te handhaven waarbij dergelijke oproepen alleen zijn toegestaan in het geval van eindgebruikers die geen bezwaar hebben gemaakt.

(37) Dienstverleners die elektronische-communicatiediensten aanbieden, moeten eindgebruikers in kennis stellen van maatregelen die zij kunnen nemen om de veiligheid van hun communicatie te beschermen, bijvoorbeeld door gebruik te maken van specifieke soorten software of encryptietechnologieën. Het voorschrift dat

eindgebruikers in kennis moeten worden gesteld van bijzondere veiligheidsrisico's, ontheft de dienstenaanbieder niet van de verplichting om op eigen kosten onmiddellijk passende maatregelen te nemen om nieuwe onvoorziene veiligheidsrisico's te vermijden en het gebruikelijke beveiligingsniveau van de dienst te herstellen. Het verstrekken van informatie over veiligheidsrisico's aan de abonnee dient kosteloos te geschieden. De beveiliging wordt beoordeeld in het licht van artikel 32 van Verordening (EU) 2016/679.

(38) Om volledige samenhang met Verordening (EU) 2016/679 te garanderen, moet de handhaving van de bepalingen van deze verordening worden toevertrouwd aan dezelfde autoriteiten die belast zijn met de handhaving van de bepalingen van Verordening (EU) 2016/679 en berust de onderhavige verordening op het coherentiemechanisme van Verordening (EU) 2016/679. De lidstaten moeten de mogelijkheid hebben om in overeenstemming met hun constitutionele, organisatorische en bestuurlijke structuur meer dan één toezichthoudende autoriteit in te stellen. De toezichthoudende autoriteiten moeten ook belast worden met het toezicht op de toepassing van deze verordening ten aanzien van elektronische-communicatiegegevens van juridische entiteiten. Dergelijke bijkomende taken mogen niet ten koste gaan van de capaciteit van de toezichthoudende autoriteit om haar taken met betrekking tot de bescherming van persoonsgegevens in het kader van Verordening (EU) nr. 2016/679 en deze verordening uit te oefenen. Elke toezichthoudende autoriteit dient te beschikken over de bijkomende financiële en personele middelen, dienstruimten en infrastructuur die nodig zijn om haar taken uit hoofde van deze verordening doeltreffend uit te voeren.

(39) Elke toezichthoudende autoriteit moet bevoegd zijn om op het grondgebied van haar lidstaat de bevoegdheden uit te oefenen en de taken uit te voeren die zijn vastgesteld in deze verordening. Met het oog op een consequente monitoring en handhaving van deze verordening in de hele Unie dienen de toezichthoudende autoriteiten in elke lidstaat dezelfde taken en effectieve bevoegdheden te hebben, onverminderd de bevoegdheden van de met vervolging belaste autoriteiten in het kader van de nationale wetgeving om inbreuken op deze verordening ter kennis te brengen van de gerechtelijke autoriteiten en in rechte op te treden. De lidstaten en hun toezichthoudende autoriteiten worden ertoe aangezet rekening te houden met de specifieke behoeften van micro-, kleine en middelgrote ondernemingen bij de toepassing van deze verordening.

(40) Om de handhaving van de regels van deze verordening te verbeteren dient elke toezichthoudende autoriteit bevoegd te zijn om sancties op te leggen, met inbegrip van administratieve boetes voor inbreuken op deze verordening, in aanvulling op of in plaats van andere passende maatregelen overeenkomstig deze verordening. In deze verordening dienen de inbreuken te worden benoemd, evenals de maxima en de criteria voor de vaststelling van de daaraan verbonden administratieve geldboetes, die per afzonderlijk geval door de bevoegde toezichthoudende autoriteit dienen te worden bepaald rekening houdend met alle relevante omstandigheden van de specifieke situatie en met inachtneming van met name de aard, de ernst en de duur van de inbreuk en van de gevolgen ervan en de maatregelen die zijn genomen om naleving van de verplichtingen uit hoofde van deze verordening te waarborgen en de gevolgen van de inbreuk te voorkomen of te beperken. Met het oog op de vaststelling van een geldboete uit hoofde van deze verordening moet een onderneming worden begrepen als een onderneming in overeenstemming met de artikelen 101 en 102 van het Verdrag.

(41) Met het oog op de verwezenlijking van de doelstellingen van deze verordening, namelijk de bescherming van de grondrechten en de fundamentele vrijheden van natuurlijke personen, in het bijzonder hun recht op bescherming van persoonsgegevens, en het waarborgen van het vrije verkeer van persoonsgegevens in de Unie, dient aan de Commissie de bevoegdheid te worden verleend om handelingen overeenkomstig artikel 290 VWEU vast te stellen. Met name dienen gedelegeerde handelingen te worden vastgesteld met betrekking tot de te verschaffen informatie, inclusief door middel van gestandaardiseerde iconen, om de betrokkene een goed zichtbaar en begrijpelijk overzicht te bieden van het verzamelen van gegevens uit eindapparatuur, de doelstelling daarvan, de persoon die daarvoor verantwoordelijk is en alle maatregelen die de eindgebruiker van de eindapparatuur kan nemen om het verzamelen van gegevens zoveel mogelijk te beperken. Ook moeten gedelegeerde handelingen worden vastgesteld om een code te bepalen voor identificatie van oproepen van direct marketing die onder meer via automatische oproep- en communicatiesystemen worden verricht. Het is van bijzonder belang dat de Commissie tot passende raadpleging overgaat overeenkomstig de beginselen die zijn neergelegd in het interinstitutioneel akkoord over beter wetgeven van 13 april 2016[8]. Met name om te zorgen voor gelijke deelname aan de voorbereiding van gedelegeerde handelingen ontvangen het Europees Parlement en de Raad alle documenten op hetzelfde tijdstip als de deskundigen van de lidstaten, en hebben hun deskundigen systematisch toegang tot de vergaderingen van de deskundigengroepen van de Commissie die de gedelegeerde handelingen voorbereiden. Om te zorgen voor uniforme voorwaarden voor de tenuitvoerlegging van deze verordening dienen aan de Commissie uitvoeringsbevoegdheden te worden verleend waar dit in deze verordening is bepaald. Die bevoegdheden moeten worden uitgeoefend overeenkomstig Verordening (EU) nr. 182/2011.

(42) Daar de doelstelling van deze verordening, namelijk het waarborgen van een gelijkwaardig niveau van bescherming voor natuurlijke personen en rechtspersonen en van het vrije verkeer van persoonsgegevens in de hele Unie, niet voldoende door de lidstaten alleen kan worden verwezenlijkt en derhalve, gezien de omvang en de gevolgen van de maatregelen, beter door de Unie kan worden verwezenlijkt, kan de Unie, overeenkomstig het in artikel 5 van het Verdrag betreffende de Europese Unie neergelegde subsidiariteitsbeginsel, maatregelen nemen. In overeenstemming met het evenredigheidsbeginsel van dat artikel gaat deze verordening niet verder dan hetgeen noodzakelijk is voor het bereiken van deze doelstelling,

(43) Richtlijn 2002/58/EG dient te worden ingetrokken,

HEBBEN DE VOLGENDE VERORDENING VASTGESTELD:

[8] Interinstitutioneel akkoord tussen het Europees Parlement, de Raad van de Europese Unie en de Europese Commissie van 13 april 2016 over beter wetgeven (PB L 123 van 12.5.2016, blz. 1).

HOOFDSTUK I
ALGEMENE BEPALINGEN

Artikel 1
Onderwerp

1. Deze verordening voorziet in regels betreffende de bescherming van de grondrechten en fundamentele vrijheden van natuurlijke en rechtspersonen in de levering en het gebruik van elektronische-communicatiediensten, en in het bijzonder het recht op eerbiediging van het privéleven en de communicatie en de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens.

2. Deze verordening waarborgt het vrije verkeer van elektronische-communicatiegegevens en elektronische-communicatiediensten in de Unie, dat niet mag worden beperkt of verboden om redenen die verband houden met de eerbiediging van het privéleven en de communicatie van natuurlijke en rechtspersonen en de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens.

3. De bepalingen van deze verordening vormen een specificatie van en een aanvulling op Verordening (EU) 2016/679 door bijzondere voorschriften vast te stellen voor de toepassing van de leden 1 en 2.

Artikel 2
Materieel toepassingsgebied

1. Deze verordening is van toepassing op de verwerking van elektronische-communicatiegegevens in verband met het aanbieden en het gebruiken van elektronische-communicatiediensten en op informatie met betrekking tot de eindapparatuur van eindgebruikers.

2. Deze verordening is niet van toepassing op:

(a) activiteiten die buiten het toepassingsgebied van het Unierecht vallen;

(b) activiteiten van de lidstaten die binnen de werkingssfeer van hoofdstuk 2 van titel V van het Verdrag betreffende de Europese Unie vallen;

(c) elektronische-communicatiediensten die niet algemeen beschikbaar zijn;

(d) activiteiten van bevoegde autoriteiten met het oog op de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.

3. De verwerking van elektronische-communicatiegegevens door de instellingen, organen, bureaus en agentschappen van de Unie wordt geregeld bij Verordening (EU) 00/0000 [nieuwe verordening ter vervanging van Verordening nr. 45/2001].

4. Deze verordening doet niet af aan de toepassing van Richtlijn 2000/31/EG[9], met name de bepalingen inzake de aansprakelijkheid van als tussenpersoon optredende dienstverleners in de artikelen 12 tot en met 15 van die richtlijn.

5. Deze verordening laat de toepassing van Richtlijn 2014/53/EG onverlet.

Artikel 3
Territoriaal toepassingsgebied en vertegenwoordiger

1. Deze verordening is van toepassing op:

(a) het aanbieden van elektronische-communicatiediensten aan eindgebruikers in de Unie, ongeacht of een betaling door de eindgebruiker is vereist;

(b) het gebruik van deze diensten;

(c) de bescherming van informatie met betrekking tot de eindapparatuur van eindgebruikers die zich in de Unie bevinden.

2. Indien de aanbieder van een elektronische-communicatiedienst niet in de Unie is gevestigd, wijst hij schriftelijk een vertegenwoordiger in de Unie aan.

3. De vertegenwoordiger is gevestigd in een van de lidstaten waar de eindgebruikers van deze elektronische-communicatiediensten zijn gevestigd.

4. De vertegenwoordiger heeft de bevoegdheid om in aanvulling op of in de plaats van de dienstverrichter die hij vertegenwoordigt, met name ten aanzien van toezichthoudende autoriteiten en eindgebruikers, met het oog op de naleving van deze verordening vragen te beantwoorden en informatie te verstrekken over alle aangelegenheden in verband met de verwerking van elektronische-communicatiegegevens.

5. De aanwijzing van een vertegenwoordiger in de zin van lid 2 doet niet af aan de mogelijkheid om rechtsvorderingen in te stellen tegen een natuurlijke of rechtspersoon die elektronische-communicatiegegevens verwerkt in verband met het aanbieden van elektronische-communicatiediensten van buiten de Unie aan eindgebruikers in de Unie.

Artikel 4
Definities

1. Voor de toepassing van deze verordening zijn de volgende definities van toepassing:

(a) de definities in Verordening (EU) 2016/679;

(b) de definities van „elektronische-communicatienetwerk”, „elektronische-communicatiedienst”, „persoonlijke communicatiedienst”, „nummergebaseerde persoonlijke communicatiedienst”, "nummeronafhankelijke persoonlijke communicatiedienst", "eindgebruiker" en "oproep" in de punten (1), (4), (5), (6), (7), (14) en (21) van artikel 2 van de [richtlijn tot vaststelling van het Europees wetboek voor elektronische communicatie];

[9] Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt ("richtlijn inzake elektronische handel") (PB L 178 van 17.7.2000, blz. 1-16).

(c) de definitie van „eindapparatuur” in punt (1) van artikel 1 van Richtlijn 2008/63/EG van de Commissie[10].

2. Voor de toepassing van punt b) van lid 1 omvat de definitie van „persoonlijke communicatiedienst” diensten die persoonlijke en interactieve communicatie mogelijk maken als een louter bijkomstig kenmerk dat onlosmakelijk verbonden is met een andere dienst.

3. Voorts gelden voor de toepassing van deze verordening de volgende definities:

(a) "elektronische-communicatiegegevens": inhoud en metagegevens van elektronische communicatie;

(b) "elektronische-communicatie-inhoud": de uitgewisselde inhoud door middel van elektronische-communicatiediensten, zoals tekst, spraak, video, beelden en geluid;

(c) "elektronische-communicatiemetagegevens: gegevens die worden verwerkt in een elektronische-communicatienetwerk met het oog op de transmissie, de distributie of de uitwisseling van elektronische-communicatie-inhoud; met inbegrip van gegevens die worden gebruikt voor de opsporing en identificatie van de bron en de bestemming van de communicatie, gegevens betreffende de locatie van de apparatuur die bij het aanbieden van elektronische-communicatiediensten worden gegenereerd, en de datum, het tijdstip, de duur en de aard van de communicatie;

(d) „algemeen beschikbare telefoongids”: een repertorium van eindgebruikers van elektronische-communicatiediensten, in gedrukte of elektronische vorm, dat wordt gepubliceerd of aan het publiek of een deel van het publiek beschikbaar wordt gesteld, inclusief door middel van een informatiedienst;

(e) „e-mail”: een elektronisch bericht met informatie, zoals tekst, spraak, video, geluid of beeld, verzonden via een elektronische-communicatienetwerk, dat in het netwerk of daarmee verbonden computerfaciliteiten of in de eindapparatuur van de ontvanger kan worden opgeslagen;

(f) „directmarketingberichten”: elke vorm van reclame, zowel geschreven als mondeling, gericht aan één of meer geïdentificeerde of identificeerbare eindgebruikers van elektronische-communicatiediensten, inclusief het gebruik van automatische oproep- en communicatiesystemen met of zonder menselijke interactie, e-mail, SMS, enz.;

(g) „spraakoproepen voor direct marketing”: directe spraakoproepen die geen gebruik van automatische oproep- en communicatiesystemen inhouden;

(h) „automatische oproep- en communicatiesystemen”: systemen die in staat zijn in overeenstemming met instructies die voor dat systeem zijn ingesteld, oproepen naar één of meer ontvangers automatisch in te leiden en niet-directe spraakelementen door te sturen, met inbegrip van oproepen waarbij gebruik wordt gemaakt van automatische oproep- en communicatiesystemen die de opgeroepen persoon in verbinding stellen met een persoon.

HOOFDSTUK II
BESCHERMING VAN ELECTRONISCHE COMMUNICATIE

[10] Richtlijn 2008/63/EG van de Commissie van 20 juni 2008 betreffende de mededinging op de markten van telecommunicatie-eindapparatuur (PB L 162 van 21.6.2008, blz. 20).

VAN NATUURLIJKE EN RECHTSPERSONEN EN VAN IN HUN EINDAPPARATUUR OPGESLAGEN INFORMATIE

Artikel 5
Vertrouwelijkheid van elektronische-communicatiegegevens

Elektronische-communicatiegegevens zijn vertrouwelijk. Elke interferentie met elektronische-communicatiegegevens, zoals door het afluisteren, aftappen, opslaan, controleren, scannen of anderszins onderscheppen, controleren of verwerken van elektronische-communicatiegegevens door andere personen dan de eindgebruikers, is verboden, tenzij toegestaan door deze verordening.

Artikel 6
Toegestane verwerking van elektronische-communicatiegegevens

1. Aanbieders van elektronische-communicatienetwerken en -diensten kunnen elektronische-communicatiegegevens verwerken indien:

(a) dit noodzakelijk is om de transmissie van de communicatie tot stand te brengen, voor de duur die nodig is voor dat doel; of

(b) dit noodzakelijk is om de veiligheid van elektronische-communicatienetwerken en -diensten in stand te houden of te herstellen, of technische storingen en/of fouten in de transmissie van elektronische communicatie op te sporen, voor de duur die nodig is voor dat doel.

2. Aanbieders van elektronische-communicatienetwerken en -diensten kunnen elektronische-communicatiemetagegevens verwerken indien:

(a) dit noodzakelijk is om te voldoen aan dwingende eisen inzake kwaliteit van de dienstverlening overeenkomstig de [richtlijn tot vaststelling van het Europees wetboek voor elektronische communicatie] of Verordening (EU) 2015/2120[11] voor de duur die nodig is voor dat doel; of

(b) dit noodzakelijk is ten behoeve van de facturering, de berekening van interconnectiebetalingen, de opsporing of de beëindiging van frauduleus of onrechtmatig gebruik van of inschrijving op elektronische-communicatiediensten; of

(c) de betrokken eindgebruiker zijn toestemming heeft gegeven voor de verwerking van de metagegevens van zijn communicatie betreffende een of meer specifieke doeleinden, inclusief voor het verstrekken van bepaalde diensten aan deze eindgebruikers, op voorwaarde dat de betrokken doeleinden niet kunnen worden bereikt door verwerking van anoniem gemaakte gegevens.

3. Aanbieders van elektronische-communicatiediensten kunnen elektronische-communicatie-inhoud alleen verwerken:

[11] Verordening (EU) 2015/2120 van het Europees Parlement en de Raad van 25 november 2015 tot vaststelling van maatregelen betreffende het open internet en tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronische-communicatienetwerken en -diensten en Verordening (EU) nr. 531/2012 betreffende roaming op openbare mobielecommunicatienetwerken binnen de Unie (PB L 310 van 26.11.2015, blz. 1).

(a) uitsluitend met het oog op het aanbieden van een bepaalde dienst aan een eindgebruiker wanneer de betrokken eindgebruiker zijn toestemming heeft gegeven voor de verwerking van zijn elektronische-communicatie-inhoud en de aangeboden dienst niet kan worden verricht zonder de verwerking van deze inhoud; of

(b) indien alle betrokken eindgebruikers hun toestemming hebben gegeven voor de verwerking van hun elektronische-communicatie-inhoud voor een of meer specifieke doeleinden die niet kunnen worden verwezenlijkt door de verwerking van anoniem gemaakte gegevens. en de aanbieder de toezichthoudende autoriteit heeft geraadpleegd. De punten (2) en (3) van artikel 36 van Verordening (EU) 2016/679 zijn van toepassing op de raadpleging van de toezichthoudende autoriteit.

Artikel 7

Opslag en wissing van elektronische-communicatiegegevens

1. Onverminderd punt b) van artikel 6, lid 1, en de punten a) en b) van artikel 6, lid 3, wist de aanbieder van de elektronische-communicatiedienst de elektronische-communicatie-inhoud of maakt hij deze gegevens anoniem nadat de beoogde ontvanger de inhoud van de elektronische communicatie heeft ontvangen. Deze gegevens kunnen overeenkomstig Verordening (EU) 2016/679 worden geregistreerd of opgeslagen door de eindgebruikers of door een derde die door hen is belast met het registreren, opslaan of anderszins verwerken van deze gegevens.

2. Onverminderd punt b) van artikel 6, lid 1, en de punten a) en c) van artikel 6, lid 2, wist de aanbieder van de elektronische-communicatiedienst de elektronische-communicatiemetagegevens of maakt hij deze gegevens anoniem wanneer deze niet langer noodzakelijk zijn voor het doel van de overdracht van communicatie.

3. Wanneer de verwerking van elektronische-communicatiemetagegevens plaatsvindt met het oog op facturering overeenkomstig punt (b) van artikel 6, lid 2, kunnen de desbetreffende metagegevens worden bewaard tot het einde van de termijn waarbinnen de rekening in rechte kan worden bestreden of de betaling overeenkomstig de nationale wetgeving kan worden gevorderd.

Artikel 8

Bescherming van gegevens die opgeslagen zijn en verband houden met eindapparatuur van eindgebruikers

1. Het gebruik van verwerkings- en opslagcapaciteit van eindapparatuur en het verzamelen van gegevens uit eindapparatuur van eindgebruikers, onder meer over de software en de hardware, anders dan door de betrokken eindgebruiker, is verboden uitgezonderd om de volgende redenen:

(a) het is noodzakelijk met als uitsluitend doel de overdracht van elektronische communicatie over een elektronisch-communicatienetwerk te verrichten; of

(b) de eindgebruiker heeft zijn toestemming gegeven; of

(c) het is noodzakelijk voor het aanbieden van een door de eindgebruiker aangevraagde dienst van de informatiemaatschappij; of

(d) het is noodzakelijk om de omvang van het publiek van een website te meten, mits deze meting door de aanbieder van de door de eindgebruiker aangevraagde dienst van de informatiemaatschappij wordt verricht.

2. Het verzamelen van gegevens uit eindapparatuur om een aansluiting op andere apparatuur en/of netwerkuitrusting mogelijk te maken, is verboden tenzij:

(a) het uitsluitend plaatsvindt met het doel en gedurende de tijd die nodig is om een aansluiting tot stand te brengen; of

(b) een duidelijk en zichtbaar bericht is aangebracht met ten minste vermelding van de wijze waarop de gegevensverzameling plaatsvindt, de doeleinden, de persoon die ervoor verantwoordelijk is en de andere informatie die vereist is krachtens artikel 13 van Verordening (EU) 2016/679 wanneer persoonsgegevens worden verzameld, alsmede de maatregelen die de eindgebruiker van de eindapparatuur kan nemen om het verzamelen van gegevens te beperken of te beëindigen.

Het verzamelen van deze gegevens vereist de toepassing van geschikte technische en organisatorische maatregelen om een op de risico's afgestemd beveiligingsniveau te waarborgen, zoals bedoeld in artikel 32 van Verordening (EU) nr. 2016/679.

3. De overeenkomstig punt b) van lid 2 te leveren informatie kan in combinatie met gestandaardiseerde iconen worden verstrekt om een nuttig overzicht van de gegevensverzameling te geven op een gemakkelijk zichtbare, begrijpelijke en duidelijk leesbare wijze.

4. De Commissie is bevoegd overeenkomstig artikel 27 gedelegeerde handelingen vast te stellen om te bepalen welke informatie de gestandaardiseerde iconen dienen weer te geven en op welke wijze de gestandaardiseerde iconen dienen te worden aangebracht.

Artikel 9
Toestemming

1. De definitie van en de voorwaarden voor toestemming als bedoeld in artikel 4, punt 11, en artikel 7 van Verordening (EU) 2016/679 zijn van toepassing.

2. Onverminderd lid 1 kan de toestemming, indien technisch mogelijk en haalbaar, voor de toepassing van punt b) van artikel 8, lid 1, worden uitgedrukt door gebruik te maken van de passende technische instellingen van een softwaretoepassing die toegang tot het internet mogelijk maakt.

3. Eindgebruikers die toestemming hebben gegeven voor de verwerking van elektronische-communicatiegegevens als bedoeld in punt c) van artikel 6, lid 2, en de punten a) en b) van artikel 6, lid 3, worden in de gelegenheid gesteld om hun toestemming te allen tijde in te trekken, zoals bepaald in artikel 7, lid 3, van Verordening (EU) 2016/679, en worden periodiek om de zes maanden aan deze mogelijkheid herinnerd zolang de verwerking voortduurt.

Artikel 10
Te verstrekken informatie en opties voor privacyinstellingen

1. Software die in de handel wordt gebracht om elektronische communicatie waaronder het opvragen en weergeven van informatie op het internet mogelijk te maken, biedt de optie om derden te verhinderen informatie in de eindapparatuur van de eindgebruiker op te slaan of reeds op die eindapparatuur opgeslagen informatie te verwerken.

2. Bij de installatie van de software wordt de eindgebruiker geïnformeerd over de opties in de privacyinstellingen en wordt hij ertoe verplicht voor de voortzetting van de installatie een instelling te aanvaarden.

3. In geval van software die op 25 mei 2018 reeds is geïnstalleerd, wordt aan de vereisten van de leden 1 en 2 voldaan bij de eerste update van de software, maar niet later dan op 25 augustus 2018.

Artikel 11
Beperkingen

1. In de wetgeving van de Unie of van de lidstaat kan het toepassingsgebied van de rechten en verplichtingen waarin de artikelen 5 tot en met 8 voorzien, bij wettelijke maatregel worden beperkt wanneer deze beperking in overeenstemming is met de wezenlijke inhoud van de grondrechten en fundamentele vrijheden en een noodzakelijke, passende en evenredige maatregel in een democratische samenleving is ter vrijwaring van een of meerdere algemene openbare belangen als bedoeld in artikel 23, lid 1, onder a) tot en met e), van Verordening (EU) 2016/679 of een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt met de uitoefening van het openbaar gezag voor deze belangen.

2. Aanbieders van elektronische-communicatiediensten voeren interne procedures in voor de afhandeling van verzoeken om toegang tot elektronische-communicatiegegevens van eindgebruikers op basis van een krachtens lid 1 vastgestelde wetgevende handeling. Zij verstrekken de bevoegde toezichthoudende instantie op verzoek informatie over deze procedures, het aantal ontvangen verzoeken, de aangevoerde wettelijke motivering en het antwoord daarop.

HOOFDSTUK III
RECHTEN VAN NATUURLIJKE EN RECHTSPERSONEN OM ELEKTRONISCHE COMMUNICATIE TE CONTROLEREN

Artikel 12
Weergave en beperking van de identificatie van het oproepende en het opgeroepen nummer

1. Wanneer de weergave van de identificatie van het oproepende en het opgeroepen nummer overeenkomstig artikel [107] van de [richtlijn tot vaststelling van het Europees wetboek voor elektronische communicatie] wordt aangeboden, verstrekken de aanbieders van algemeen beschikbare nummergebaseerde persoonlijke communicatiediensten:

(a) de oproepende eindgebruiker met de mogelijkheid om de weergave van de identificatie van het oproepende nummer per oproep, per aansluiting of permanent te verhinderen;

(b) de opgeroepen eindgebruiker met de mogelijkheid om de weergave van de identificatie van het oproepende nummer te verhinderen;

(c) de opgeroepen eindgebruiker met de mogelijkheid om binnenkomende oproepen te weigeren wanneer de oproepende eindgebruiker de weergave van de identificatie van het oproepende nummer heeft verhinderd;

(d) de opgeroepen eindgebruiker met de mogelijkheid om de weergave van de identificatie van het doorverbonden nummer voor de oproepende eindgebruiker te verhinderen.

2. De mogelijkheden als bedoeld in de punten (a), (b), (c) en (d) van lid 1 worden aan eindgebruikers op eenvoudige wijze en kosteloos aangeboden.

3. Punt (a) van lid 1 geldt eveneens voor oproepen vanuit de Unie naar derde landen. De punten (b), (c) en (d) van lid 1 gelden eveneens voor inkomende oproepen vanuit derde landen.

4. Wanneer de weergave van de identificatie van het oproepende of doorverbonden nummer wordt aangeboden, verstrekken aanbieders van algemeen beschikbare nummergebaseerde persoonlijke communicatiediensten het publiek informatie over de mogelijkheden bedoeld in de punten (a), (b), (c) en (d) van lid 1.

Artikel 13
Uitzonderingen op de weergave en beperking van de identificatie van het oproepende en het doorverbonden nummer

1. Ongeacht of de oproepende eindgebruiker de weergave van de identificatie van het oproepende nummer heeft verhinderd, schakelen aanbieders van algemeen beschikbare nummergebaseerde persoonlijke communicatiediensten in geval van een oproep naar de nooddiensten de verhindering van weergave van de identificatie van het oproepende nummer en de weigering of het ontbreken van toestemming van een eindgebruiker voor de verwerking van metagegevens per afzonderlijke lijn uit voor de organisaties die noodoproepen behandelen, waaronder alarmcentrales, om respons te kunnen geven aan deze oproepen.

2. De lidstaten stellen nadere bepalingen vast met betrekking tot de vaststelling van de procedures en de omstandigheden waarin aanbieders van algemeen beschikbare persoonlijke communicatiediensten de verhindering van de weergave van de identificatie van het oproepende nummer tijdelijk uitschakelen, wanneer eindgebruikers verzoeken om de opsporing van kwaadwillige of hinderlijke oproepen.

Artikel 14
Blokkering van inkomende oproepen

Aanbieders van algemeen beschikbare persoonlijke communicatiediensten ontwikkelen geavanceerde maatregelen om de ontvangst van ongewenste oproepen door eindgebruikers te beperken en verstrekken de opgeroepen eindgebruiker eveneens kosteloos de volgende mogelijkheden om:

(a) binnenkomende oproepen van specifieke nummers of uit anonieme bronnen te blokkeren;

(b) de automatische doorschakeling van oproepen door een derde naar de eindapparatuur van de eindgebruiker te beëindigen.

Artikel 15
Algemeen beschikbare telefoongidsen

1. Aanbieders van algemeen beschikbare telefoongidsen verkrijgen de toestemming van eindgebruikers die natuurlijke personen zijn, om hun persoonsgegevens in het repertorium op te nemen, en verkrijgen van deze eindgebruikers bijgevolg toestemming voor de opname van gegevens per categorie persoonsgegevens, voor zover deze relevant zijn voor de doeleinden van het repertorium zoals bepaald door de aanbieder van de telefoongids. De aanbieders verstrekken eindgebruikers die natuurlijke personen zijn, de middelen om deze gegevens te verifiëren, te corrigeren en te wissen.

2. Aanbieders van algemeen beschikbare telefoongidsen informeren eindgebruikers die natuurlijke personen zijn, van wie persoonsgegevens beschikbaar zijn in het repertorium, over de beschikbare zoekfuncties van het repertorium en verkrijgen toestemming van de eindgebruiker voordat zij deze zoekfuncties in verband met hun eigen gegevens mogelijk maken.

3. Aanbieders van algemeen beschikbare telefoongidsen verstrekken eindgebruikers die rechtspersonen zijn, de mogelijkheid om bezwaar te maken tegen opname van hen betreffende gegevens in het repertorium. De aanbieders verstrekken eindgebruikers die rechtspersonen zijn, de middelen om deze gegevens te verifiëren, te corrigeren en te wissen.

4. De mogelijkheid voor eindgebruikers om niet te worden opgenomen in een algemeen beschikbare telefoongids, of om hen betreffende gegevens te verifiëren, te corrigeren of te wissen, wordt kosteloos verstrekt.

Artikel 16
Ongewenste communicatie

1. Natuurlijke of rechtspersonen kunnen gebruik maken van elektronische-communicatiediensten voor de verzending van directmarketingberichten aan eindgebruikers die natuurlijke personen zijn, die hun toestemming hebben gegeven.

2. Wanneer een natuurlijke of rechtspersoon in het kader van de verkoop van een product of een dienst van zijn klanten elektronische contactgegevens voor elektronische post heeft verkregen overeenkomstig Verordening (EU) 2016/679, kan hij deze elektronische contactgegevens voor direct marketing van soortgelijke eigen producten of diensten gebruiken mits de klanten duidelijk en expliciet in de gelegenheid zijn gesteld om kosteloos en op gemakkelijke wijze bezwaar te maken tegen dit gebruik. Het recht om bezwaar te maken wordt verleend op het tijdstip van de gegevensverzameling en telkens wanneer een bericht wordt verzonden.

3. Onverminderd de leden 1 en 2 verstrekken natuurlijke of rechtspersonen die gebruikmaken van elektronische-communicatiediensten voor de doeleinden van direct marketing:

(a) de identiteit van een lijn waarop contact met hen kan worden opgenomen; of

(b) een specifieke code of kengetal waaruit blijkt dat de oproep een marketingoproep is.

4. Onverminderd lid 1 kunnen de lidstaten bij wet bepalen dat het verzenden van spraakoproepen voor direct marketing aan eindgebruikers die natuurlijke personen zijn, alleen wordt toegestaan voor eindgebruikers die natuurlijke personen zijn, die geen bezwaar tegen ontvangst van deze oproepen kenbaar hebben gemaakt.

5. De lidstaten zorgen er in het kader van het Unierecht en het toepasselijke nationale recht voor dat de rechtmatige belangen van eindgebruikers die rechtspersonen zijn, met betrekking tot ongewenste communicatie via middelen als bedoeld in lid 1 voldoende worden beschermd.

6. Elke natuurlijke of rechtspersoon die gebruik maakt van elektronische-communicatiediensten voor de verzending van directmarketingberichten, informeert de eindgebruikers over de commerciële aard van de communicatie en de identiteit van de natuurlijke of rechtspersoon namens wie de communicatie wordt verzonden, en verstrekt de ontvangers de nodige informatie om het recht tot intrekking van hun toestemming voor verdere ontvangst van marketingberichten op eenvoudige wijze uit te oefenen.

7. De Commissie is bevoegd uitvoeringsmaatregelen in overeenstemming met artikel 26, lid 2, vast te stellen tot nadere specificatie van de code of kengetal voor het identificeren van marketingberichten overeenkomstig punt b) van lid 3.

Artikel 17
Informatie over geconstateerde veiligheidsrisico's

In geval van een bijzonder risico dat de veiligheid van elektronische-communicatienetwerken en -diensten kan aantasten, informeert de aanbieder van een elektronische-communicatiedienst de eindgebruikers over dat risico en, indien het risico buiten het toepassingsgebied van de door de aanbieder te nemen maatregelen valt, over mogelijke hulpmiddelen, waaronder een indicatie van de verwachte kosten.

HOOFDSTUK IV
ONAFHANKELIJKE TOEZICHTHOUDENDE AUTORITEITEN EN HANDHAVING

Artikel 18
Onafhankelijke toezichthoudende autoriteiten

1. De onafhankelijke toezichthoudende autoriteit of autoriteiten die verantwoordelijk zijn voor het toezicht op de toepassing van Verordening (EU) 2016/679, zijn eveneens verantwoordelijk voor het toezicht op de toepassing van deze verordening. De hoofdstukken VI en VII van Verordening (EG) 2016/679 zijn *mutatis mutandis* van toepassing. De taken en bevoegdheden van de toezichthoudende autoriteiten worden uitgeoefend met betrekking tot eindgebruikers.

2. De toezichthoudende autoriteit of autoriteiten als bedoeld in lid 1 werken indien passend samen met de nationale regelgevende autoriteiten die die zijn ingesteld krachtens de [richtlijn tot vaststelling van het Europees wetboek voor elektronische communicatie].

Artikel 19
Europees Comité voor gegevensbescherming

Het Europees Comité voor gegevensbescherming, dat is ingesteld krachtens artikel 68 van Verordening (EU) 2016/679, is bevoegd om te zorgen voor de consistente toepassing van hoofdstuk II van deze verordening. Daartoe oefent het Europees Comité voor

gegevensbescherming de taken uit die zijn vastgesteld in artikel 70 van Verordening (EU) 2016/679. Het Comité heeft eveneens de volgende taken:

(a) de Commissie adviseren over voorstellen tot wijziging van deze verordening;

(b) op eigen initiatief of op verzoek van een van zijn leden dan wel op verzoek van de Commissie kwesties onderzoeken die betrekking hebben op de toepassing van deze verordening, en richtsnoeren, aanbevelingen en beste praktijken uitvaardigen om de consistente toepassing van deze verordening te bevorderen.

Artikel 20
Procedures voor samenwerking en consistentie

Elke toezichthoudende autoriteit draagt bij tot de consistente toepassing van deze verordening in de hele Unie. Daartoe werken de toezichthoudende autoriteiten in overeenstemming met hoofdstuk VII van Verordening (EU) 2016/679 onderling en met de Commissie samen met betrekking tot de aangelegenheden die onder hoofdstuk II van deze verordening vallen.

HOOFDSTUK V
RECHTSMIDDELEN, AANSPRAKELIJKHEID EN STRAFFEN

Artikel 21
Rechtsmiddelen

1. Onverminderd andere mogelijkheden van administratief beroep of voorziening in rechte heeft elke eindgebruiker van elektronische-communicatiediensten dezelfde rechtsmiddelen als bedoeld in de artikelen 77, 78 en 79 van Verordening (EU) 2016/679.

2. Elke andere natuurlijke of rechtspersoon dan de eindgebruiker die benadeeld is door inbreuken op deze verordening en een rechtmatig belang heeft bij het staken of het verbieden van beweerde schendingen, met inbegrip van aanbieders van elektronische-communicatiediensten die hun rechtmatige commerciële belangen beschermen, kan beroep in rechte instellen tegen deze inbreuken.

Artikel 22
Recht op schadevergoeding en aansprakelijkheid

Elke eindgebruiker van elektronische-communicatiediensten die materiële of immateriële schade heeft geleden ten gevolge van een inbreuk op deze verordening, heeft het recht om van de persoon die de inbreuk heeft gepleegd, vergoeding voor de geleden schade te ontvangen, tenzij deze persoon bewijst dat hij op geen enkele wijze verantwoordelijk is voor het schadeveroorzakende feit overeenkomstig artikel 82 van Verordening (EU) 2016/679.

Artikel 23
Algemene voorwaarden voor het opleggen van administratieve geldboetes

1. Voor de toepassing van dit artikel is hoofdstuk VII van Verordening (EU) 2016/679 van toepassing op inbreuken op deze verordening.

2. Inbreuken op onderstaande bepalingen van deze verordening zijn overeenkomstig lid 1 onderworpen aan administratieve geldboetes tot 10 000 000 EUR of, in het

geval van een onderneming, tot 2 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is:

(a) de verplichtingen van een natuurlijke of rechtspersoon die elektronische-communicatiegegevens verwerkt, overeenkomstig artikel 8;

(b) de verplichtingen van aanbieders van software om elektronische communicatie mogelijk te maken, overeenkomstig artikel 10;

(c) de verplichtingen van aanbieders van algemeen beschikbare telefoongidsen, overeenkomstig artikel 15;

(d) de verplichtingen van elke natuurlijke of rechtspersoon die gebruik maakt van elektronische-communicatiediensten, overeenkomstig artikel 16.

3. Inbreuken op het beginsel van vertrouwelijkheid van communicatie, toegestane verwerking van elektronische-communicatiegegevens en termijnen voor wissing overeenkomstig de artikelen 5, 6 en 7 zijn overeenkomstig lid 1 van dit artikel onderworpen aan administratieve geldboetes tot 20 000 000 EUR of, in het geval van een onderneming, tot 4 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is.

4. De lidstaten stellen de regels inzake de sancties voor inbreuken op de artikelen 12, 13, 14 en 17 vast.

5. Niet-naleving van een bevel van een toezichthoudende autoriteit als bedoeld in artikel 18 wordt onderworpen aan administratieve geldboetes tot 20 000 000 EUR of, in het geval van een onderneming, tot 4 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is.

6. Onverminderd de bevoegdheden van de toezichthoudende autoriteiten om corrigerende maatregelen te nemen overeenkomstig artikel 18 kan elke lidstaat regels vaststellen om te bepalen of en in hoeverre administratieve geldboetes kunnen worden opgelegd aan overheidsinstanties en overheidsorganen die in deze lidstaat zijn gevestigd.

7. De uitoefening door de toezichthoudende autoriteit van haar bevoegdheden krachtens dit artikel is onderworpen aan passende procedurele waarborgen overeenkomstig het recht van de Unie en de lidstaten, waaronder een doeltreffende voorziening in rechte en eerlijke rechtsbedeling.

8. Wanneer het rechtsstelsel van de lidstaat niet in administratieve geldboetes voorziet, kan dit artikel aldus worden toegepast dat de geldboete door de bevoegde toezichthoudende autoriteit wordt geïnitieerd en door bevoegde nationale rechtscolleges worden opgelegd, waarbij wordt gewaarborgd dat deze rechtsmiddelen doeltreffend zijn en een gelijkwaardig effect hebben als de door toezichthoudende autoriteiten opgelegde administratieve geldboetes. De boetes zijn in elk geval doeltreffend, evenredig en afschrikkend. Deze lidstaten delen de Commissie uiterlijk op [xxx] de wetgevingsbepalingen mee die zij op grond van dit lid vaststellen, en melden onverwijld alle latere wijzigingen of wijzigingen die daarop van invloed zijn.

Artikel 24
Sancties

1. De lidstaten stellen de regels vast inzake andere sancties die van toepassing zijn op inbreuken op deze verordening, in het bijzonder voor inbreuken die niet aan administratieve geldboetes overeenkomstig artikel 23 zijn onderworpen, en treffen alle nodige maatregelen om ervoor te zorgen dat deze worden toegepast. Deze sancties moeten doeltreffend, evenredig en afschrikkend zijn.

2. Elke lidstaat deelt de Commissie uiterlijk 18 maanden na de in artikel 29, lid 2, bepaalde datum de wetgevingsbepalingen mee die hij overeenkomstig lid 1 heeft vastgesteld, en meldt onverwijld alle latere wijzigingen of wijzigingen die daarop van invloed zijn.

HOOFDSTUK VI
GEDELEGEERDE HANDELINGEN EN UITVOERINGSHANDELINGEN

Artikel 25
Uitoefening van de bevoegdheidsdelegatie

1. De bevoegdheid om gedelegeerde handelingen vast te stellen, wordt aan de Commissie toegekend onder de in dit artikel neergelegde voorwaarden.

2. De bevoegdheid om de in artikel 8, lid 4, bedoelde gedelegeerde handelingen vast te stellen, wordt de Commissie met ingang van [de datum van inwerkingtreding van deze verordening] voor onbepaalde tijd verleend.

3. Het Europees Parlement of de Raad kan de in de artikel 8, lid 4, bedoelde bevoegdheidsdelegatie te allen tijde intrekken. Het besluit tot intrekking beëindigt de delegatie van de in dat besluit genoemde bevoegdheid. Het wordt van kracht op de dag na die van de bekendmaking ervan in het Publicatieblad van de Europese Unie of op een daarin genoemde latere datum. Het laat de geldigheid van de reeds van kracht zijnde gedelegeerde handelingen onverlet.

4. Vóór de vaststelling van een gedelegeerde handeling raadpleegt de Commissie de door elke lidstaat aangewezen deskundigen overeenkomstig de beginselen die zijn vastgesteld in het interinstitutioneel akkoord van 13 april 2016 over beter wetgeven.

5. Zodra de Commissie een gedelegeerde handeling heeft vastgesteld, doet zij daarvan gelijktijdig kennisgeving aan het Europees Parlement en de Raad.

6. Een overeenkomstig artikel 8, lid 4, vastgestelde gedelegeerde handeling treedt alleen in werking indien het Europees Parlement noch de Raad daartegen binnen een termijn van twee maanden na de kennisgeving van de handeling aan het Europees Parlement en de Raad bezwaar heeft gemaakt, of indien zowel het Europees Parlement als de Raad voor het verstrijken van die termijn de Commissie hebben medegedeeld dat zij daartegen geen bezwaar zullen maken. Die termijn wordt op initiatief van het Europees Parlement of de Raad met twee maanden verlengd.

Artikel 26
Comitéprocedure

1. De Commissie wordt bijgestaan door het Comité voor communicatie dat is ingesteld bij artikel 110 van de [richtlijn tot vaststelling van het Europees wetboek voor

elektronische communicatie]. Dit comité is een comité in de zin van Verordening (EU) nr. 182/2011[12].

2. Wanneer naar dit lid wordt verwezen, is artikel 5 van Verordening (EU) nr. 182/2011 van toepassing.

HOOFDSTUK VII
SLOTBEPALINGEN

Artikel 27
Intrekking

1. Richtlijn 2002/58/EG wordt met ingang van 25 mei 2018 ingetrokken.

2. Verwijzingen naar de ingetrokken richtlijn gelden als verwijzingen naar deze verordening.

Artikel 28
Bepaling inzake monitoring en evaluatie

Uiterlijk 1 januari 2018 stelt de Commissie een gedetailleerd programma op voor de monitoring van de doeltreffendheid van deze verordening.

Uiterlijk drie jaar na de datum van toepassing van deze verordening en nadien om de drie jaar verricht de Commissie een evaluatie van de verordening en brengt zij aan het Europees Parlement, de Raad en het Europees Economisch en Sociaal Comité verslag uit over de belangrijkste bevindingen. Bij de evaluatie wordt, in voorkomend geval, een voorstel gevoegd voor wijziging of intrekking van deze verordening in het licht van juridische, technische of economische ontwikkelingen.

Artikel 29
Inwerkingtreding en toepassing

1. Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie.*

2. Zij is van toepassing met ingang van 25 mei 2018.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel,

Voor het Europees Parlement	*Voor de Raad*
De voorzitter	*De voorzitter*

[12] Verordening (EU) nr. 182/2011 van het Europees Parlement en de Raad van 16 februari 2011 tot vaststelling van de algemene voorschriften en beginselen die van toepassing zijn op de wijze waarop de lidstaten de uitoefening van de uitvoeringsbevoegdheden door de Commissie controleren (PB L 55 van 28.2.2011, blz. 13).