*Mr. M.A.M. Verveld-Suijkerbuijk**

Het Europese voorstel voor een e-Privacy-verordening

58

Trefwoorden:
vertrouwelijkheid van communicatie, cookies, direct marketing, e-privacy

Het voorstel voor een verordening op het gebied van privacy en elektronische communicatie bevat nieuwe regels op het gebied van e-privacy. In het voorstel worden persoonlijke communicatiediensten gebonden aan de regels die tot op heden alleen golden voor traditionele elektronische-communicatiediensten. Verder bevat het voorstel aangepaste regels op het gebied van cookies, vertrouwelijkheid van communicatie en direct marketing. Het doel van de Europese Commissie is om de verordening per 25 mei 2018 (tegelijk met de Algemene verordening gegevensbescherming) van toepassing te laten zijn.

1 Inleiding

Op 10 januari 2017 publiceerde de Europese Commissie een voorstel voor een verordening op het gebied van privacy en elektronische communicatie (hierna: Verordening).[1] De Verordening heeft als voornaamste doel de privacy bij elektronische communicatie beter te beschermen. De Verordening vervangt de e-Privacyrichtlijn en krijgt rechtstreekse werking in de Europese lidstaten.[2] Dit artikel vormt een verkenning van de Verordening. In dit artikel komen, na een korte introductie over de Verordening, de volgende hoofdzaken uit de Verordening aan bod: de bescherming van elektronische communicatie (paragraaf 3), de cookiebepaling (paragaaf 4), direct marketing (paragraaf 5), het toezicht op de Verordening en de mogelijke sancties bij niet-naleving (paragraaf 6).

2 De Verordening

2.1 *Verhouding tot Algemene verordening gegevensbescherming*

Met de Verordening moet een volwaardig en compleet wettelijk kader voor gegevensbescherming in Europa ontstaan, in samenhang met een nieuw voorstel voor een verordening met betrekking tot de gegevensbescherming bij EU-instellingen en EU-organen, een beschrijving van de strategie voor de internationale uitwisseling van persoonsgegevens, en de Algemene verordening gegevensbescherming (AVG).[3] Net als de AVG, is de Verordening, als het aan de Europese Commissie ligt, per 25 mei 2018 van toepassing. De AVG bevat algemene regels op het gebied van bescherming van persoonsgegevens. De bescherming die volgt uit de AVG geldt alleen voor natuurlijke personen. De Verordening zorgt ervoor dat ook gegevens die geen persoonsgegevens zijn en gegevens van rechtspersonen, waar nodig, worden beschermd. De AVG en de Verordening vullen elkaar dus aan. De Europese Commissie heeft beoogd de Verordening consistent te laten zijn met de AVG.[4] Een mooi voorbeeld hiervan is dat het toestemmingsbegrip uit de Verordening is gekoppeld aan het toestemmingsbegrip uit de AVG.

2.2 *Verordening en geen richtlijn*

De nieuwe regels op het gebied van e-privacy worden neergelegd in een verordening en niet in een richtlijn. Volgens de Europese Commissie is behoefte aan een verordening. Een verordening dient de rechtszekerheid van gebruikers en ondernemingen, zorgt voor een gelijk niveau van bescherming voor gebruikers binnen de ge-

---

* **Marrit Verveld-Suijkerbuijk is advocaat (www.marritverveld.com).**

1 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 [*sic*] betreffende privacy en elektronische communicatie), COM(2017)10 def.

2 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) (*PbEG* 2002, L 201/37).

3 Europese Commissie, *Commissievoorstel: strengere privacyregels voor onlinecommunicatie en betere databeschermingsregels voor EU-instellingen*, Brussel, 10 januari 2017, europa.eu/rapid/press-release_IP-17-16_nl.htm; Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, COM(2017)8 final; Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World, COM(2017)7 final. Verordening (EU) 679/2016 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) (*PbEU* 2016, L 119/1).

4 Paragraaf 2.4 COM(2017)10 def.

hele Unie en leidt tot lagere nalevingskosten voor ondernemingen die grensoverschrijdend werken.[5]

2.3 *Van toepassing per 25 mei 2018*

De Europese Commissie heeft de ambitie de Verordening van toepassing te laten zijn vanaf 25 mei 2018, het moment dat ook de AVG in werking treedt.[6] De Verordening moet nog worden goedgekeurd door het Europees Parlement en de Raad van Ministers. Het streven is dat dat uiterlijk gebeurt in de zomer van 2017. Het is de vraag of dit lukt; er is kritiek op de inhoud en, vanuit diverse lidstaten, ook kritiek op de keuze van een verordening in plaats van een richtlijn. Als de Verordening in de zomer van 2017 wordt goedgekeurd betekent dit dat lidstaten dan (minder dan) een jaar hebben om de bestaande wetgeving aan te passen.[7] Ondernemingen hebben een jaar (of minder wat betreft de nationale invulling van de regelgeving) om te zorgen dat de nieuwe regelgeving wordt nageleefd. Dat is kort.

2.4 *Consequenties voor Nederlandse wetgeving*

In Nederland zijn de regels met betrekking tot elektronische communicatie en privacy (e-privacy) hoofdzakelijk neergelegd in hoofdstuk 11 van de Telecommunicatiewet. Dit hoofdstuk is gebaseerd op de Europese e-Privacyrichtlijn.[8] Diverse bepalingen uit hoofdstuk 11 van de Telecommunicatiewet moeten, als de Verordening wordt aangenomen, worden ingetrokken. Vanwege de rechtstreekse werking wordt de Verordening niet omgezet in Nederlandse wetgeving. Er is niet aan te ontkomen dat in Nederland uitvoeringswetgeving moet worden ontworpen om gebruik te maken van de ruimte die de Verordening biedt om in nationale regelgeving op onderdelen beperkingen te stellen.[9] Ook kunnen in uitvoeringswetgeving regels worden opgenomen over onderwerpen als sancties en toezicht.[10]

3 Bescherming van elektronische communicatie

Bij de bepalingen over de bescherming van elektronische communicatie staan de begrippen 'elektronische-communicatienetwerken', 'elektronische-communicatiediensten' en 'elektronische-communicatiegegevens' centraal. Om die reden wordt hier eerst de reikwijdte van deze begrippen besproken, daarna zal aandacht worden besteed aan de inhoud van de beschermingsbepalingen.

3.1 *Reikwijdte: elektronische-communicatienetwerken en -diensten*

Onder de definitie van elektronische-communicatienetwerken en -diensten vallen diensten voor toegang tot het internet, diensten die geheel of gedeeltelijk bestaan uit het overbrengen van signalen en persoonlijke communicatiediensten die gebruikmaken van internet.[11] Deze laatste categorie viel niet onder het bereik van de e-Privacyrichtlijn en de Telecommunicatiewet, de eerste twee al wel. Door deze diensten wel onder het bereik te scharen, vult de Verordening een leemte in de bescherming van communicatie via deze diensten.[12] Voorbeelden van diensten in deze categorie zijn zogenaamde *over-the-top*-diensten zoals WhatsApp, Skype en Twitter.

Op het gebied van de bescherming van persoonsgegevens geldt voor deze partijen in Nederland uiteraard de Wet bescherming persoonsgegevens (Wbp). Ondanks het ontbreken van regelgeving op het gebied van e-privacy beschermen verschillende dienstverleners in deze categorie de vertrouwelijkheid van informatie in de praktijk al in toenemende mate. Met de Verordening gaat deze vrijblijvendheid verloren, voor deze aanbieders gelden dezelfde regels als voor de traditionele communicatiediensten en ontstaat een *level playing field*.[13]

Ook de communicatie tussen apparaten (*machine-to-machine*), waarbij signalen via een netwerk worden overgebracht, wordt beschouwd als een elektronische-communicatiedienst.[14] Hierbij kan worden gedacht aan de slimme energiemeter die bijvoorbeeld (via communicatie met andere apparaten) weet wanneer men thuis is en de temperatuur binnenshuis daarop automatisch bijstelt.

3.2 *Reikwijdte: elektronische-communicatiegegevens*

Elektronische-communicatiegegevens zijn zowel inhoudelijke gegevens van elektronische communicatie als metagegevens. Van inhoudelijke gegevens wordt gesproken als het gaat over de, via elektronische-communicatiediensten uitgewisselde, inhoud zoals tekst, spraak, video, beelden en geluid.[15] Metagegevens zijn gegevens die worden verwerkt met het oog op de transmissie, de distributie of de uitwisseling van de inhoud. Bij metagegevens kan worden gedacht aan informatie over bezochte websites, de locatie van de gebruiker, datum, tijd, duur en aard van de communicatie.[16] Ook deze gegevens

5 Paragraaf 2.4 COM(2017)10 def.
6 Artikel 29 lid 2 COM(2017)10 def.
7 *Kamerstukken II* 2016/17, 22112, 2306, p. 11.
8 Richtlijn 2002/58/EG (*PbEG* 2002, L 201/37).
9 Bijvoorbeeld artikel 11 lid 1 en artikel 16 lid 4 COM(2017)10 def.
10 Artikel 18 en 24 COM(2017)10 def.
11 Overweging 11 en 12 COM(2017)10 def., artikel 4 lid 1 sub b COM(2017)10 def. juncto 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 def.).
12 Paragraaf 1.1 COM(2017)10 def.
13 *Kamerstukken II* 2016/17, 22112, 2306, p. 6.
14 Overweging 12 COM(2017)10 def.
15 Artikel 4 lid 3 sub b COM(2017)10 def.
16 Overweging 14 en artikel 4 lid 3 sub a COM(2017)10 def.

kunnen zeer gevoelige en persoonlijke informatie weergeven.[17]

Elektronische-communicatiegegevens kunnen betrekking hebben op natuurlijke personen en rechtspersonen. Daarmee kunnen deze gegevens persoonsgegevens bevatten, maar ook kunnen daar andersoortige gegevens onder vallen. Ook die andersoortige gegevens genieten dus bescherming onder de Verordening. Op de elektronische-communicatiegegevens die te kwalificeren zijn als persoonsgegeven, is de Wbp en vanaf 25 mei 2018 de AVG van toepassing.

3.3 *Uitgangspunt: vertrouwelijkheid van elektronische-communicatiegegevens*

Het uitgangspunt van de Verordening is dat elektronische-communicatiegegevens vertrouwelijk zijn. De Verordening bevat een algeheel verbod om die gegevens te onderscheppen, af te luisteren, af te tappen, op te slaan, te controleren enzovoort, voor zover dat niet is toegestaan door de Verordening.[18]

3.4 *Situaties waarin elektronische-communicatiegegevens mogen worden verwerkt*

De Verordening kent verschillende verwerkingsgronden op basis waarvan verwerking van elektronische-communicatiegegevens is toegestaan door aanbieders van elektronische-communicatienetwerken en/of -diensten. Zo mogen elektronische-communicatiegegevens (inhoudelijke en metagegevens) worden verwerkt door elektronische-communicatienetwerken en -diensten als dit noodzakelijk is voor het overbrengen van de communicatie of noodzakelijk voor de veiligheid van het netwerk of de dienst of om technische storingen op te sporen.[19]

Metagegevens mogen alleen door elektronische-communicatienetwerken en -diensten worden verwerkt als dit noodzakelijk is om te voldoen aan dwingende kwaliteitseisen of noodzakelijk voor de facturering of de opsporing of de beëindiging van frauduleus of onrechtmatig gebruik van elektronische-communicatiediensten. Ook mogen metagegevens worden verwerkt als de betreffende eindgebruiker (een gebruiker: natuurlijke persoon of rechtspersoon die geen openbaar communicatienetwerk of openbare elektronische-communicatiediensten aanbiedt) zijn toestemming heeft gegeven voor de verwerking met het oog op een of meer specifieke doeleinden, mits de doeleinden niet kunnen worden bereikt met anonieme gegevens.[20]

Inhoudelijke gegevens mogen worden verwerkt door elektronische-communicatiediensten, met het oog op het uitsluitend aanbieden van een bepaalde dienst aan een eindgebruiker, voor zover de eindgebruiker toestemming heeft gegeven en de dienst niet kan worden verricht zonder de verwerking van de inhoud.[21] Als sprake is van meer dan één eindgebruiker, mogen inhoudelijke gegevens worden verwerkt als alle eindgebruikers toestemming hebben gegeven voor het gebruik vanwege een of meer specifieke doeleinden en die doeleinden niet kunnen worden bereikt met geanonimiseerde gegevens.[22] De laatste grond kan bijvoorbeeld worden gebruikt voor diensten zoals het scannen van e-mails om vooraf gedefinieerde materialen te verwijderen. Gezien de gevoeligheid van dit soort verwerkingen, bestaat er bij toepassing van deze laatstgenoemde verwerkingsgrond een vermoeden van een hoog risico voor de privacy en moet de aanbieder van de dienst de toezichthoudende autoriteit voorafgaand raadplegen.[23]

Voor de traditionele communicatiediensten heeft het hier beschreven regime beperkt impact; het regime leidt tot een beperkte verruiming van de verwerkingsgronden. Nieuw is bijvoorbeeld de verwerkingsgrond om gegevens te verwerken om te voldoen aan dwingende kwaliteitseisen. Voor de aanbieders die nog niet onder het bereik van de e-privacyregelgeving vielen is daarentegen de impact groot; de hier besproken regels gelden op basis van de huidige regelgeving niet voor deze partijen. Deze partijen zijn in Nederland op dit moment, wat betreft de verwerking van elektronische-communicatiegegevens, alleen gebonden aan de Wbp.

3.5 *Toestemming*

Waar volgens de Verordening gewerkt mag worden met toestemming, moet de toestemming voldoen aan de vereisten die daaraan in de AVG worden gesteld. Dit betekent onder meer dat de toestemming vrij, specifiek, geïnformeerd en ondubbelzinnig moet zijn en dat de toestemming aantoonbaar moet zijn. Als de eindgebruiker toestemming geeft in het kader van een schriftelijke verklaring die ook op andere aangelegenheden betrekking heeft, moet het verzoek om toestemming in een begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal worden gepresenteerd zodat een duidelijk onderscheid kan worden gemaakt met de andere aangelegenheden.[24]

Gebruikers die toestemming hebben gegeven voor de verwerking van elektronische-communicatiegegevens moeten in de gelegenheid worden gesteld om hun toestemming te allen tijde in te trekken. Zij moeten daar

17 Overweging 2 COM(2017)10 def.
18 Artikel 5 COM(2017)10 def.
19 Artikel 6 lid 1 sub a COM(2017)10 def. en artikel 6 lid 1 sub b COM(2017)10 def.
20 COM(2016)0590 def. en Verordening (EU) 2120/2015 (*PbEU* 2015, L 310/1) en artikel 6 lid 1 sub c Verordening.
21 Artikel 6 lid 3 sub a COM(2017)10 def.
22 Artikel 6 lid 3 sub b COM(2017)10 def.
23 Overweging 19 COM(2017)10 def. en artikel 36 lid 2 en 3 Verordening (EU) 679/2016 (*PbEU* 2016, L 119/1).
24 Artikel 7 Verordening (EU) 679/2016 (*PbEU* 2016, L 119/1).

periodiek om de zes maanden aan worden herinnerd zolang de verwerking voortduurt.[25]

3.6 *Verwijderen of anonimiseren van elektronische-communicatiegegevens*

De Verordening verplicht de aanbieder van de elektronische-communicatiedienst om de inhoudelijke communicatiegegevens te wissen of anoniem te maken nadat de beoogde ontvanger deze gegevens heeft ontvangen.[26] Naar het idee van de Nederlandse regering laat de Verordening geen ruimte om inhoudelijke gegevens op te slaan nadat de ontvanger de gegevens heeft ontvangen, ook niet als de ontvanger daar toestemming voor heeft gegeven.[27] Uit de relevante bepalingen van de Verordening blijkt echter dat de verplichting tot verwijdering geldt 'onverminderd' de mogelijkheid inhoudelijke gegevens te verwerken als dit voor de veiligheid van de dienst noodzakelijk is of als hiervoor specifieke toestemming is gegeven door de eindgebruiker(s).[28] Het lijkt er dus op dat verwijdering ook na ontvangst van de gegevens niet nodig is in deze situaties. De tekst of considerans van de Verordening kan op dit onderdeel wel wat verduidelijking gebruiken.

Metagegevens moeten worden verwijderd of geanonimiseerd wanneer deze gegevens niet langer noodzakelijk zijn voor het doel van de overdracht van communicatie.[29] Wanneer de metagegevens worden verwerkt met het oog op de facturering mogen deze gegevens worden bewaard tot het verstrijken van de termijn waarbinnen de rekening in rechte kan worden bestreden of de betaling kan worden gevorderd.[30] Ook met betrekking tot deze gegevens zou meer expliciet kunnen worden gemaakt hoe deze verplichting zich verhoudt tot het gebruik van toestemming als verwerkingsgrond.

4 Opslaan en verzamelen van gegevens uit het eindapparaat (cookiebepaling)

4.1 *Situaties waarin gegevens mogen worden opgeslagen of verzameld*

Een ander belangrijk onderdeel van de Verordening vormen de wijzigingen met betrekking tot het opslaan of verzamelen van gegevens uit of op het eindapparaat van een eindgebruiker. Het eindapparaat is het apparaat dat is aangesloten op een netwerk, zoals een computer of smartphone.[31] In de praktijk is sprake van het opslaan of verzamelen van gegevens uit of op het eindapparaat bij bijvoorbeeld het gebruik van *cookies*.

Op basis van de Verordening is het opslaan van gegevens op het apparaat of verzamelen van gegevens uit het apparaat toegestaan met toestemming van de eindgebruiker. Deze toestemming moet voldoen aan de vereisten uit de AVG en dus voldoende specifiek zijn. Toestemming moet, waar technisch mogelijk en haalbaar, volgens de Verordening kunnen worden gegeven via software-instellingen.[32] Dit is gebruiksvriendelijk, maar het is de vraag of toestemming die via software wordt gegeven voldoende specifiek kan zijn en voldoet aan het toestemmingsvereiste uit de AVG; een browser die bij de installatie om toestemming vraagt voor het plaatsen en lezen van cookies in het algemeen lijkt op het eerste gezicht niet heel specifiek. De Nederlandse regering heeft laten weten zich in te willen zetten om hier meer duidelijkheid over te krijgen.[33]

Zonder toestemming mag informatie worden opgeslagen of verzameld in situaties die minder belastend voor de privacy worden beschouwd. Dit zijn de situaties waarin dit technisch noodzakelijk is voor de communicatie, noodzakelijk is voor het leveren van de door de gebruiker gevraagde dienst (bijvoorbeeld om de inhoud van een winkelwagentje te bewaren of om gelijke informatie op online-formulieren van meerdere pagina's in te vullen) of om informatie te verkrijgen over de kwaliteit of effectiviteit van de dienst (bijvoorbeeld om het aantal bezoekers op een website te tellen, zogenaamde analytische cookies).[34] Deze situaties sluiten aan bij het op dit moment in Nederland geldende regime. Een verschil met het huidige Nederlandse regime is dat de analytische cookies in Nederland ook geplaatst mogen worden door derde partijen. De Verordening biedt daar op dit moment geen ruimte voor. Dit sluit niet aan bij de huidige praktijk waarin partijen regelmatig gebruikmaken van derden om een website te monitoren.[35]

Aan het bestaande regime worden met de Verordening verder enkele bijzondere regels toegevoegd.

4.2 *Opt-out voor gegevens die uit apparatuur worden verzameld voor aansluiting*

Allereerst wordt een zogenaamd *opt-out*-regime geïntroduceerd voor een bijzondere categorie gegevens: gegevens die uit apparatuur worden verzameld 'om een aanslui-

25 Artikel 9 lid 3 COM(2017)10 def.
26 Artikel 7 lid 1 COM(2017)10 def.
27 *Kamerstukken II* 2016/17, 22112, 2306, p. 7.
28 Artikel 7 lid 1 juncto artikel 6 lid 1 sub b en artikel 6 lid 3 sub a en b COM(2017)10 def. Zie ook Europese Commissie, *Digital Single Market – Stronger privacy rules for electronic communication*, 10 januari 2017, europa.eu/rapid/press-release_MEMO-17-17_en.htm.
29 Artikel 7 lid 2 COM(2017)10 def.
30 Artikel 7 lid 3 COM(2017)10 def.
31 Richtlijn 2008/63/EG van de Europese Commissie van 20 juni 2008 betreffende de mededinging op de markten van telecommunicatie-eindapparatuur (*PbEU* 2008, L 162/20).
32 Artikel 9 lid 2 COM(2017)10 def.
33 *Kamerstukken II* 2016/17, 22112, 2306, p. 7.
34 Artikel 8 lid 1 COM(2017)10 def.
35 *Kamerstukken II* 2016/17, 22112, 2306, p. 8.

ting op andere apparatuur of op een netwerkuitrusting mogelijk te maken'. Deze gegevens mogen worden verzameld zo lang de eindgebruiker is geïnformeerd in lijn met de Verordening en daartegen geen bezwaar heeft gemaakt.[36] Ook mogen deze gegevens worden verzameld voor het doel en gedurende de tijd die nodig is om een aansluiting tot stand te brengen.[37]

Het gaat hier om gegevens als een IP-adres of MAC-adres, die relevant zijn om een aansluiting mogelijk te maken, maar dus ook kunnen worden gebruikt voor andere diensten, zoals bijvoorbeeld *wifitracking*.[38] Bij wifitracking worden signalen die een apparaat uitzendt om contact te maken of te zoeken met een wifinetwerk, gebruikt om een persoon te lokaliseren en vervolgens te benaderen met bijvoorbeeld gepersonaliseerde aanbiedingen. Volgens de Verordening mag dit dus, mits de eindgebruiker is geïnformeerd en geen bezwaar heeft. De informatieverplichting is vergaand en houdt in dat een duidelijk en zichtbaar bericht is aangebracht met ten minste de vermelding van de wijze waarop de gegevensverzameling plaatsvindt, de doeleinden, de persoon die ervoor verantwoordelijk is en de maatregelen die de eindgebruiker kan nemen om het gebruik te beperken of te beëindigen. Ook moet worden voldaan aan de informatieverplichtingen uit de AVG.[39] Voor partijen die gebruikmaken van wifitracking zal het in de praktijk een uitdaging zijn ervoor te zorgen dat hun *targets* op het juiste moment en op de juiste wijze worden geïnformeerd. De bescherming van het privéleven van de *targets* bij het gebruik van een ingrijpende toepassing als wifitracking gaat daarmee hand in hand.[40]

4.3 *Software*

Een tweede belangrijke wijziging op dit gebied is dat software voor elektronische communicatie de optie moet bieden om te voorkomen dat derden informatie opslaan op een apparaat of gegevens verzamelen van een apparaat.[41] De gebruiker moet bij de installatie van dergelijke software worden geïnformeerd over de opties in de privacy-instellingen en wordt verplicht voor de voortzetting van de installatie een instelling te aanvaarden.[42] Bestaande software moet die keuze bij de eerste update aan de gebruiker voorleggen.[43] Met deze wijzigingen wordt tegemoetgekomen aan de ergernissen bij gebruikers ten aanzien van cookie-pop-ups en wordt de gebruiksvriendelijkheid bevorderd.[44]

Een eerdere versie van de Verordening bevatte een verdergaande verplichting; hardware- en softwareleveranciers werden daarin verplicht hun producten standaard te voorzien van privacyvriendelijke instellingen. Dit voorstel werd door 89% van de geconsulteerde burgers in de EU ondersteund, maar heeft het uiteindelijk niet gered tot de Verordening.[45] De Verordening sluit hiermee niet aan bij de AVG, waarin *privacy by default* verplicht is gesteld.[46]

5 Direct marketing

De Verordening staat, net als de Telecommunicatiewet en de e-Privacyrichtlijn, direct marketing via elektronische-communicatiediensten toe voor gebruikers die toestemming hebben gegeven. Hieronder vallen ook directmarketingberichten van politieke partijen of organisaties zonder winstoogmerk.[47] Dit laatste is een wijziging ten opzichte van de e-Privacyrichtlijn, maar was in de Nederlandse wet al een uitgangspunt.[48] Nieuw ten opzichte van het in Nederland geldende kader is dat ook direct marketing via de telefoon in de Verordening onder het toestemmingsvereiste valt. Lidstaten mogen dit systeem in nationale regelgeving echter wijzigen naar een opt-out-systeem, zoals we in Nederland met het bel-me-nietregister kennen.[49]

6 Toezicht en sancties

In Nederland zijn op dit moment verschillende toezichthouders betrokken bij het toezicht op de naleving van e-privacyregelgeving. Dit zijn de Autoriteit Consument en Markt, het Agentschap Telecom en, voor zover algemene regels op het gebied van bescherming van persoonsgegevens in het geding zijn, de Autoriteit Persoonsgegevens. Volgens de Verordening moet het toezicht op de naleving van de Verordening worden ondergebracht bij de nationale privacytoezichthouder, zodat een volledige samenhang met de AVG wordt gegarandeerd.[50] De Nederlandse regering oordeelt negatief over dit voorstel en

36 Artikel 8 lid 2 sub b COM(2017)10 def.
37 Artikel 8 lid 2 sub a COM(2017)10 def.
38 Overweging 25 COM(2017)10 def.
39 Artikel 13 Verordening (EU) 679/2016 (*PbEU* 2016, L 119/1).
40 H. Uršič, '"The bad" and "the good" of the ePrivacy regulation proposal', 19 januari 2017, leidenlawblog.nl/articles/the-bad-and-the-good-of-the-eprivacy-regulation-proposal.
41 Artikel 10 lid 1 COM(2017)10 def.
42 Artikel 10 lid 2 COM(2017)10 def.
43 Artikel 10 lid 3 COM(2017)10 def.
44 *Kamerstukken II* 2016/17, 22112, 2306, p. 4.
45 Bits of freedom, 'Europees voorstel over ePrivacy aangekondigd. Een eerste indruk', 10 januari 2017, www.bof.nl/2017/01/10/europees-voorstel-over-eprivacy-aangekondigd-een-eerste-indruk/.
46 Artikel 25 lid 1 Verordening (EU) 679/2016 (*PbEU* 2016, L 119/1).
47 Overweging 32 COM(2017)10 def.
48 Artikel 11.7 lid 2 Telecommunicatiewet.
49 Artikel 16 lid 4 COM(2017)10 def.
50 Artikel 18 lid 1 en overweging 38 COM(2017)10 def.

meent dat iedere lidstaat de keuze moet hebben te bepalen waar het toezicht het meest adequaat is belegd.[51]

De boetebedragen in de Verordening variëren afhankelijk van de inbreuk. Zo kunnen overtredingen op het gebied van de cookiebepaling, software en direct marketing worden bestraft met een geldboete tot € 10 000 000 of bij ondernemingen tot 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar als dat bedrag hoger is.[52] Overtredingen met betrekking tot de vertrouwelijkheid van communicatie kunnen zelfs worden bestraft met een geldboete tot € 20 000 000 of bij ondernemingen tot 4% van de totale wereldwijde jaaromzet in het voorgaande boekjaar als dat bedrag hoger is.[53]

7 Afsluiting

Er moet nog hard worden gewerkt om de Verordening deze zomer aan te nemen en vanaf 25 mei 2018 van toepassing te kunnen laten zijn. Verschillende regels behoeven verduidelijking. De tijd die in Brussel wordt genomen om tot een compromis te komen, gaat ten koste van de tijd die nationale overheden en ondernemingen hebben om met de nieuwe regels te gaan werken. Zeker voor partijen die tot nu toe niet onder het bereik van de e-privacyregelgeving vielen zal het niet in alle gevallen eenvoudig zijn op tijd *compliant* te zijn, terwijl het juist voor het creëren van het level playing field en het vertrouwen van de burger in de bescherming van zijn privéleven bij elektronische communicatie, van groot belang is dat ook zij de (nieuwe) regels naleven.

Schematisch overzicht van wijzigingen op hoofdlijnen (zie artikel voor details)

	Telecommunicatiewet (implementatie van e-Privacyrichtlijn)	**Verordening**
Europees instrument	Richtlijn	Verordening (rechtstreekse werking)
Toepassingsbereik (m.b.t. verwerking elektronische-communicatiegegevens)	Elektronische-communicatienetwerken en elektronische-communicatiediensten (zonder persoonlijke communicatiediensten)	Elektronische-communicatienetwerken, elektronische-communicatiediensten (waaronder persoonlijke communicatiediensten)
Gronden voor verwerking van elektronische-communicatiegegevens	Toestemming, noodzakelijk voor integriteit en veiligheid van de netwerken en diensten, noodzakelijk voor het overbrengen van informatie via de netwerken en diensten of noodzakelijk ter uitvoering van een wettelijk voorschrift of rechterlijk bevel	Beperkte uitbreiding van onder Telecommunicatiewet en e-Privacyrichtlijn bestaande gronden, zoals bijvoorbeeld het verwerken vanwege dwingende kwaliteitseisen
Cookies	Mogen worden gebruikt als gebruiker is geïnformeerd en toestemming heeft gegeven	Mogen worden gebruikt als gebruiker geïnformeerde, specifieke toestemming heeft gegeven (AVG criteria); toestemming mag worden gegeven via technische instellingen van een softwaretoepassing, indien technisch mogelijk en haalbaar
Analytische cookies	Mogen worden gebruikt door de aanbieder van de dienst en door derden in opdracht van de aanbieder van de dienst	Mogen worden gebruikt door de aanbieder van de dienst en volgens de letterlijke tekst van de Verordening niet door derden in opdracht van de aanbieder van de dienst
Software	–	Software die in de handel wordt gebracht om elektronische communicatie mogelijk te maken biedt opties voor privacy-instellingen
Direct marketing	Toestemming nodig bij direct marketing via automatische oproep- en communicatiesystemen zonder menselijke tussenkomst, faxen en elektronische berichten	Toestemming nodig bij direct marketing via elektronische communicatie, waaronder spraakoproepen met menselijke tussenkomst (telefoon); mogelijkheid in nationale wetge-

51 *Kamerstukken II* 2016/17, 22112, 2306, p. 10.
52 Artikel 23 lid 2 COM(2017)10 def.
53 Artikel 23 lid 3 COM(2017)10 def.

		ving opt-out-regime zoals bel-me-niet-register te introduceren.
Toezicht	Belegd bij Autoriteit Consument en Markt, Agentschap Telecom en AP	Moet worden belegd bij nationale privacytoezichthouder
Boetes	Niet Europeesrechtelijk geregeld; nationale bepalingen opgenomen in Hoofdstuk 15 Telecommunicatiewet; maximumboete € 900 000 of tot 1% van omzet; boete te verdubbelen in geval van recidive	Maximumboete € 10 000 000 of tot 2% van de omzet of maximumboete € 20 000 000 of tot 4% van de omzet, afhankelijk van inbreuk