Factsheet
De e-Privacy Verordening

De e-Privacy Verordening

De ePV; wanneer gebeurt er eindelijk iets mee?

Een onderwerp dat inmiddels al lange tijd ter discussie staat: de nieuwe e-Privacy Verordening (ePV).[i] In deze factsheet zullen we je meenemen in de totstandkoming en de huidige stand van zaken van deze te verwachten Verordening. Vervolgens zullen we een overzicht geven waarin je in één oogopslag kunt zien wat deze ePV nou waarschijnlijk écht gaat veranderen en wat dit voor organisaties zal gaan betekenen in de praktijk.

Herkomst en doel ePV

Op dit moment vormen de Algemene verordening gegevensbescherming (AVG) en de e-Privacyrichtlijn (ePR)[ii] uit 2002 samen het juridisch kader dat de digitale privacy van natuurlijke personen regelt. In Nederland is de ePR geïmplementeerd in de Telecommunicatiewet (Tw). In 2017 kwam de Europese Commissie met het initiatief om de ePV op te stellen die de huidige ePR (en dus deels de Tw) moet vervangen en de AVG zal gaan aanvullen. Vervanging van de ePR is nodig om de Europese wetgeving beter aan te laten sluiten bij alle technologische en digitale ontwikkelingen van de afgelopen jaren.[iii]

De ePR en daarmee de Tw zijn namelijk niet meer in overeenstemming met de huidige technologische en digitale ontwikkelingen. Consumenten worden steeds afhankelijker van nieuwe internetdiensten die in de plaats komen van traditionele communicatiediensten. Deze nieuwe internetdiensten (onder de ePV aangegeven als: "over-the-top communicatiediensten") vallen nu over het algemeen niet onder de huidige regelgeving voor elektronische communicatie.[iv] Onder de Tw wordt onder een 'elektronische communicatiedienst' verstaan: "*gewoonlijk tegen vergoeding aangeboden dienst die geheel of hoofdzakelijk bestaat in het overbrengen van signalen via elektronische communicatienetwerken, waaronder telecommunicatiediensten en transmissiediensten op netwerken die voor omroep worden gebruikt, doch niet de dienst waarbij met behulp van elektronische communicatienetwerken en -diensten overgebrachte inhoud wordt geleverd of redactioneel wordt gecontroleerd*.[v]

De ePV streeft ernaar om de regels voor traditionele telecombedrijven te moderniseren en zal het toepassingsbereik dan ook uitbreiden naar nieuwe elektrische communicatiediensten.[vi] De ePV heeft een grotere reikwijdt, en zal dus van toepassing zijn op een grotere groep aanbieders van communicatiediensten, dan de momenteel geldende ePR en Tw. De ePV zal ook gaan gelden voor nieuwe aanbieders die online communicatiediensten aanbieden, zoals Facebook, Twitter, Whatsapp, Skype, Snapchat, IMessage en Gmail.[vi]

Het verschil tussen de ePR en de ePV is dat de ePV een Europese Verordening is welke directe werking heeft in de EU, in tegenstelling tot een richtlijn die eerst in nationale wetgeving moet worden omgezet. Met de komst van de ePV zullen dezelfde regels met betrekking tot e-privacy gaan gelden en ontstaan er gelijke spelregels in alle landen van de EU. De ePV en de AVG zijn beiden Europese Verordeningen die betrekking hebben op privacy, maar ze hebben wel een ander toepassingsgebied. Waar de AVG ziet op iedere vorm van verwerking van persoonsgegevens,[vii] richt de ePV zich uitsluitend op de verwerking van persoonsgegevens voor elektronische communicatiediensten. De ePV heeft dus een specifieker toepassingsgebied dan de AVG en is daarmee een bijzondere wet. Bijzondere wetten gaan voor op algemene wetten. De Tw en de ePV zijn beiden bijzondere wetten die voorrang hebben op de AVG als algemene wet. Indien een onderwerp niet is geregeld in de Tw of de ePV dan geldt 'gewoon' de AVG.[viii]

De ePV zal zorgen voor gelijke spelregels voor online communicatie . Hierbij zal niet alleen de inhoud van de online communicatie beschermd worden, maar ook de metadata ervan, waaronder tijdstip en plaats van verzenden.[ix] De ePV gaat naast het beschermen van online communicatie, ook in op andere regels voor online diensten waaronder cookies, spam, direct marketing, en het gebruik van Social Media om consumenten gerichter te benaderen.[x] De ePV heeft verschillende doelstellingen, waaronder:

- Regels die gelden voor de traditionele telecombedrijven uitbreiden naar 'over-the-top communicatiediensten', zoals Facebook, WhatsApp en Skype;
- Het toezicht op de naleving van e-privacy sterker en effectiever maken;
- De regels rondom 'spam' aanscherpen;

- De regels omtrent ‘cookies’ aanpassen en aanscherpen;
- Meer mogelijkheden tot controle bij burgers leggen met betrekking tot het gebruik van data uit hun digitale communicatie, vooral door burgers hiervoor toestemming te vragen;
- De inhoud en metadata van elektronische communicatie beschermen.[xi]

De stand van zaken en tijdlijn

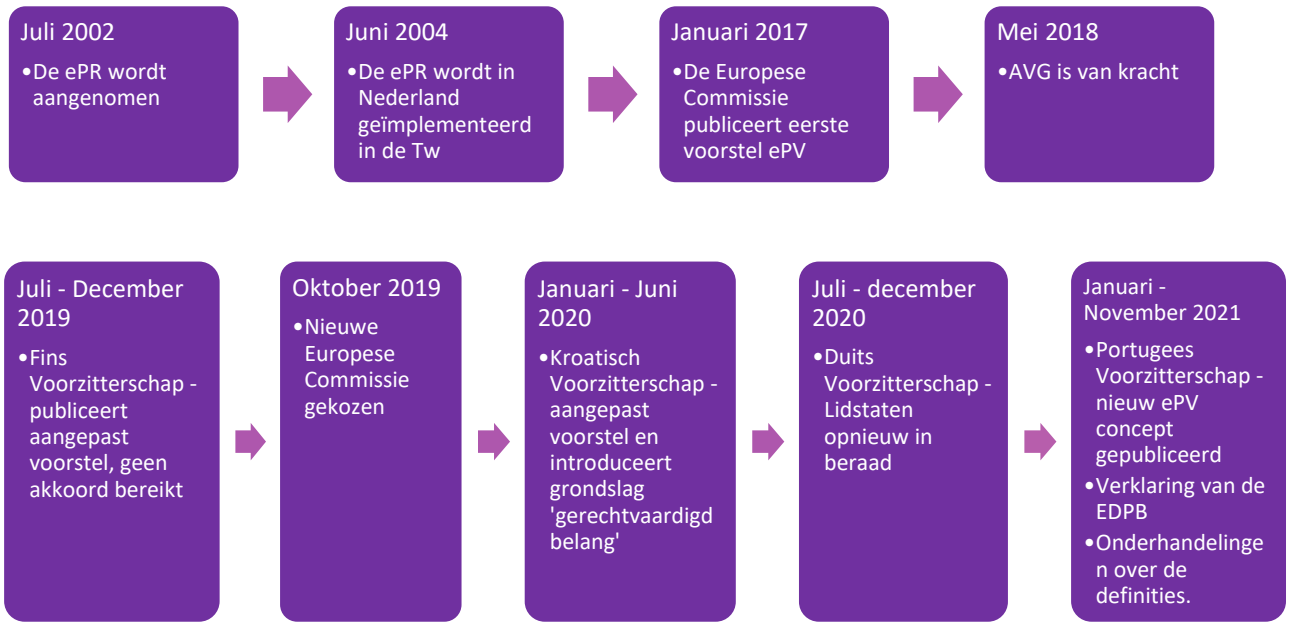
Een eerste voorstel voor de ePV werd al gedaan in januari 2017 door de Europese Commissie.[xii] Hierna volgde moeizame onderhandelingen tussen de Europese Raad en het Europees Parlement.[xiii] Oorspronkelijk was het de bedoeling om de ePV op 25 mei 2018 samen met de AVG van toepassing te laten gelden. Dit is helaas niet gelukt en de ePV laat inmiddels al een hele tijd op zich wachten. Dit komt onder andere doordat er al jaren grote meningsverschillen zijn tussen de verschillende Europese Lidstaten, die zijn vertegenwoordigd in de Europese Raad van Ministers.[xiv] Vervolgens waren er in 2019 Europese verkiezingen en in 2020 was er hinder als gevolg van de Covid-19 pandemie waardoor verdere vertraging is opgelopen.[xv]

Uit het conceptvoorstel van de ePV daterend van 6 maart 2020 blijkt dat de verschillende Europese organen, zoals het Parlement en de Raad, in onderhandeling zijn over de materiële reikwijdte van de ePV.[xvi] Alle Lidstaten krijgen momenteel nog steeds de gelegenheid om te reageren op de voorgestelde wijzigingen die verderop in deze factsheet worden besproken. Het kan dan ook zijn dat de wijzigingen die wij verder zullen bespreken door de nieuwe onderhandelingsresultaten weer zullen veranderen.

Op 9 maart 2021 heeft de European Data Protection Board (EDPB) een verklaring over de ePV gepubliceerd.[xvii] Hierin merkt de EDPB op dat de nieuwe wet het niveau van bescherming van persoonsgegevens van Europeanen niet mag verlagen. De ePV moet de AVG aanvullen, niet wijzigen. Om dat te kunnen waarborgen, heeft de EDPB een aantal wijzigingen vastgesteld.

De belangrijkste wijzigingen:
- De ePV zou het toestemmingsvereiste voor cookies moeten handhaven. Onder de ePV zouden bijv. cookiewalls verboden moeten worden.
- Gegevens uit vertrouwelijke communicatie, zoals WhatsApp-berichten, mogen niet verder worden verwerkt, tenzij een beperkte uitzondering geldt, namelijk toestemming.
- Het toezicht op gebruik van persoonsgegevens onder de ePV, zou bij dezelfde toezichthouders moeten liggen als het toezicht op de AVG. En niet gefragmentariseerd, zoals in het huidige voorstel is opgenomen.

Tijdlijn


Juli 2002
•De ePR wordt aangenomen
Juni 2004
•De ePR wordt in Nederland geïmplementeerd in de Tw
Januari 2017
•De Europese Commissie publiceert eerste voorstel ePV
Mei 2018
•AVG is van kracht
Juli - December 2019
•Fins Voorzitterschap - publiceert aangepast voorstel, geen akkoord bereikt
Oktober 2019
•Nieuwe Europese Commissie gekozen
Januari - Juni 2020
•Kroatisch Voorzitterschap - aangepast voorstel en introduceert grondslag 'gerechtvaardigd belang'
Juli - december 2020
•Duits Voorzitterschap - Lidstaten opnieuw in beraad
Januari - November 2021
•Portugees Voorzitterschap - nieuw ePV concept gepubliceerd
•Verklaring van de EDPB
•Onderhandelingen over de definities.

Belangrijkste wijzigingen ePV versus AVG/ePR/Tw

De ePV bevat verschillende rechten en verplichtingen die zullen gaan afwijken van de bestaande wetgeving. Belangrijke elementen uit het voorstel van de ePV zijn:

- De ePV heeft, anders dan de ePR, rechtstreekse werking in de gehele EU;
- De voorgestelde regels gelden niet enkel en alleen voor de traditionele telecombedrijven, maar ook voor nieuwe onlinediensten, zoals WhatsApp, Skype en Facebook;
- Uitgangspunt van de ePV is dat alle elektronische communicatie geheim moet zijn. Niet alleen de inhoud van elektronische communicatie, maar ook de metadata valt onder de ePV (zoals tijdstip en plaats). Indien betrokkenen toestemming geven, krijgen organisaties pas meer mogelijkheden om aanvullende diensten aan te bieden;
- De regels omtrent cookies worden aangepast en gebruiksvriendelijker gemaakt. Een website hoeft, op basis
  van de voorgestelde regels, geen toestemming meer te vragen voor cookies die nodig zijn om een website of applicatie goed te laten werken of
  voor cookies waarmee een website het aantal bezoekers telt. Voor andere cookies dan de hierboven genoemde gelden wél aanvullende maatregelen.[xvii]

De belangrijkste onderwerpen die de ePV gaat regelen voor de verwerking van persoonsgegevens voor elektronische communicatiediensten hebben wij hieronder overzichtelijk in een tabel opgenomen, zodat in een oogopslag duidelijk wordt wat er nou precies gaat veranderen ten opzichte van de huidige regelgeving.[xviii] Let wel, deze wijzigingen zijn gebaseerd op de meest recente conceptversie van de ePV, welke nog verandert kan worden.

Geldend recht ePR/Tw	Voorgesteld ePV
"Deze richtlijn heeft een algemeen toepassingsbereik. De richtlijn is daarom mede van toepassing op het gebruik van openbare telecommunicatienetwerken en -diensten en de verwerking van persoonsgegevens die bij dat gebruik beschikbaar komen. De richtlijn geeft echter aan dat op bijzondere terreinen aanvullende richtlijnen kunnen worden vastgesteld."[xix]	<u>Art. 2 – Materieel toepassingsgebied.</u> De verordening heeft betrekking op: • Elektronische-communicatiegegevens en daaraan verwante metadata; • Eindsystemen van de eindgebruiker; • Het aanbieden van een publiek toegankelijk ***directory*** van eindgebruikers van elektronische-communicatieservices; • Het versturen van direct marketing naar eindgebruikers.
Concluderend: ***De ePV specificeert het materiële toepassingsgebied waar de Tw dit niet deed. Zo zien we nu dat de verordening specifiek betrekking heeft op een aantal punten die voorheen onder "het gebruik van openbare telecommunicatienetwerken en -diensten en de verwerking van persoonsgegevens die bij dat gebruik beschikbaar komen" vielen.***	
De Tw is een nationale implementatie van de ePR waardoor je ten opzichte van andere Lidstaten implementatieverschillen hebt.	<u>Art. 3 – Territoriaal toepassingsgebied en vertegenwoordiger.</u> De verordening is van toepassing op: • Het aanbieden van elektronische-communicatiediensten aan eindgebruikers; • Het verwerken van elektronische-communicatie inhoud en metadata van eindgebruikers; • De bescherming van informatie met betrekking tot de eindapparatuur van eindgebruikers; • Het aanbieden van publiek toegankelijke ***directories*** van eindgebruikers van elektronische-communicatieservices; • Het sturen van direct marketing naar eindgebruikers. Al het bovenstaande heeft betrekking op eindgebruikers binnen de Europese Unie. Op het moment dat de aanbieder van bovengenoemde niet in de Unie gevestigd is dient deze, binnen een maand vanaf het begin van de activiteiten, een vertegenwoordiger aan te wijzen in de Unie. Deze verplichting geldt niet als de activiteiten sporadisch plaatsvinden of waarschijnlijk niet zullen

Geldend recht ePR/Tw	Voorgesteld ePV
	resulteren in een risico voor de rechten van de eindgebruikers. De ePV is ook van toepassing op de verwerking van persoonsgegevens door een verwerkingsverantwoordelijke welke niet gevestigd is in de Europese Unie, maar op een plaats waar lidstatelijk recht van toepassing is op grond van publiekelijk internationaal recht.
Concluderend: ***Er is een duidelijk verschil tussen de ePV en de Tw. Waar de Tw slechts een Nederlandse wet is (al dan niet geïmplementeerd vanuit de ePR) geldt de ePV als Verordening van alle Lidstaten van de Europese Unie. In die zin is de ePV te vergelijken met de AVG.***	
Art. 11 Tw Art. 11.1 sub g Tw Toestemming van een gebruiker of abonnee: toestemming van een betrokkene als bedoeld in art. 4 lid 1 onderdeel 11 van de AVG, met dien verstande dat de toestemming mede betrekking kan hebben op gegevens van abonnees die geen natuurlijke personen zijn. Art. 11.2 t/m 11.7 Tw De hoofdregel uit de Tw is dat digitale direct marketing alleen gestuurd mag worden indien hiervoor toestemming van de ontvanger is verkregen. **E-mailmarketing** • Voor het verzenden van commerciële e-mails is toestemming nodig; • Voor het verzenden van e-mails richting klanten of relaties gelden andere voorwaarden; • Iedere geadresseerde mag zich verzetten tegen verder gebruik van zijn e-mailadres **Telemarketing** • Voor het **telefonisch** benaderen van betrokkenen met een commercieel,	Art. 4a (oud 9) – Toestemming. De voorwaarde voor toestemming uit Verordening 2016/679/EU geldt voor natuurlijke- en rechtspersonen.[1] Toestemming mag worden uitgedrukt door gebruik te maken van passende technische instellingen van software ***placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet.*** Op het moment dat het datasubject niet geïdentificeerd kan worden is het voldoende als aangetoond kan worden dat toestemming is verleend door de eindapparatuur van de eindgebruiker. Eindgebruikers moeten periodiek herinnerd worden aan de mogelijkheid om de verleende toestemming in te trekken.

Geldend recht ePR/Tw	Voorgesteld ePV
charitatief of ideëel doel hoeft geen toestemming gevraagd te worden • Voorafgaand moeten belbestanden worden bekijken uit het "Bel-Me-Niet Register" en de "Recht van verzet-lijst". Deze mensen mogen **niet** gebeld worden, tenzij zij anders hebben aangegeven; • In ieder telefonisch gesprek moet de betrokkene gewezen worden op het Bel-Me-Niet Register en het recht van verzet. **Cookies** • Voor cookies is voorafgaande toestemming vereist (*opt-in*); • De website moet toestemming vragen voor het plaatsen van cookies. Deze toestemming mag afgeleid worden uit bepaalde handelingen, zoals het doorgaan van het bekijken van de website nadat betrokkene geïnformeerd is over de cookies; • De website is verplicht het doel te melden waarvoor de cookies worden geplaatst of gelezen; • Iedere gebruiker moet volledig, gebruiksvriendelijk en duidelijk worden geïnformeerd.[xx]	
Notabene: daarnaast geldt ook de volgende regel uit de AVG: A) Voor toestemming moet gekeken worden naar art. 4 lid 1 sub 11 jo. art. 7 AVG.	
Concluderend: ***Voor zowel de Tw als de ePV geldt dat toestemming de eisen van art. 4 lid 1 sub 11 jo. art. 7 AVG moet volgen. Wat nieuw is onder de ePV, is dat onder toestemming gegeven door de eindgebruiker ook verstaan mag worden toestemming gegeven door de eindapparatuur.***	
Art. 11.1 lid 2 Tw De aanbieder van een openbaar elektronisch communicatienetwerk en de aanbieder van een openbare elektronische communicatiedienst onthouden zich van het	Art. 6b (oud 6(2)) – Toegestane verwerking van elektronische communicatiegegevens. Beschermt zowel de inhoud als de metadata die aan elektronische communicatie gehecht is. Metadata zijn gegevens die aan bepaalde inhoudelijke communicatie kleven, zoals

Geldend recht ePR/Tw	Voorgesteld ePV
aftappen, afluisteren of anderszins onderscheppen of controleren van de communicatie via een openbaar elektronisch communicatienetwerk of openbare elektronische communicatiedienst en de daarmee verband houdende gegevens tenzij en voor zover: a) De betrokken abonnee voor deze handelingen zijn uitdrukkelijke toestemming heeft gegeven; b) Deze handelingen noodzakelijk zijn om de integriteit en de veiligheid van de netwerken en diensten van de betrokken aanbieder te waarborgen; c) Deze handelingen noodzakelijk zijn voor het overbrengen van informatie via de netwerken en diensten van de betrokken aanbieder, of d) Deze handelingen noodzakelijk zijn ter uitvoering van een wettelijk voorschrift of rechterlijk bevel.	datum, exacte tijdstip en identiteit afzender en ontvanger. Aanbieders van elektronische-communicatie netwerken en services mogen enkel elektronische-communicatiemetadata verwerken als: • De eindgebruiker toestemming heeft gegeven; • Het noodzakelijk is voor de uitvoering van het contract (omtrent elektronische-communicatieservices) met de eindgebruiker; • Het noodzakelijk is voor de bescherming van het vitaal belang van een natuurlijk persoon; • Het is noodzakelijk voor statistische meetdoeleinden van elektronische communicatiemetagegevens die locatiegegevens vormen, op voorwaarden dat: - Dergelijke gegevens worden gepseudonimiseerd; - De verwerking niet kon worden uitgevoerd door geanonimiseerde informatie te verwerken en dat locatiegegevens zijn gewist of geanonimiseerd wanneer ze niet langer nodig zijn voor het vooropgestelde doel; - De locatiegegevens worden niet gebruikt om de aard en/of kenmerken van een eindgebruiker te kennen en/of een profiel van de eindgebruiker op te stellen. • Het is noodzakelijk voor statistische doeleinden, anders dan op basis van elektronische informatie communicatiemetagegevens die locatiegegevens vormen of voor wetenschappelijke onderzoeksdoeleinden gelden.

Geldend recht ePR/Tw	Voorgesteld ePV
	Voordat eerdergenoemde metadata, welke geanonimiseerd is, gedeeld mag worden met derden dient het volgende te gebeuren: • Er moet een assessment worden uitgevoerd om de impact op de vertrouwelijkheid van de communicatie en de privacy van de eindgebruiker te bepalen; ▪ De eindgebruiker informeren over de voorgestelde verwerking en de rechten die eindgebruiker heeft; ▪ Toepasselijke technische en organisatorische maatregelen implementeren. De EDPB is bij dit artikel van oordeel dat de ePV niet kan afwijken van het Handvest van de grondrechten van de Europese Unie (Handvest) en hetgeen hierover recent in jurisprudentie is bepaald. *'Het verschaffen van een rechtsgrondslag voor andere doeleinden dan gerichte bewaring met het oog op de rechtshandhaving en de bescherming van de nationale veiligheid is op grond van het Handvest derhalve niet toegestaan en zou in ieder geval moeten zijn onderworpen aan strikte temporele en materiële beperkingen en aan toetsing door een rechtbank of een onafhankelijke instantie.'* Als de Commissie, het Parlement en de Raad zich hierin kunnen vinden, zal de tekst van dit artikel hoogst waarschijnlijk worden aangepast.
Notabene: daarnaast gelden ook de volgende regels uit de AVG: A) Voor de speciale categorieën van persoonsgegevens zal er gekeken moeten worden naar art. 9 AVG. B) Het assessment dat uitgevoerd moet worden vindt zijn oorsprong in art. 35 AVG. Art. 36 AVG regelt in welke gevallen er voorafgaande raadpleging vereist is.	
Concluderend: ***De ePV stemt de grondslagen voor een verwerking van elektronische-communicatiegegevens af op de grondslagen die we ook vanuit de AVG kennen. Daarmee wordt er meer ruimte gecreëerd om te verwerken dan nu onder de Tw.***	

<table>
<tr><th>Geldend recht ePR/Tw</th><th>Voorgesteld ePV</th></tr>
<tr><td><u>Hoofdstuk 13 Tw.</u>
Aanbieders van openbare telecommunicatienetwerken en -diensten zijn verplicht gegevens met betrekking tot een bijzondere last te beveiligen tegen kennisneming door onbevoegden alsmede geheimhouding te betrachten met betrekking tot deze gegevens.

Aanbieders van openbare telecommunicatienetwerken en –diensten nemen met betrekking tot de gegevens … passende technische en organisatorische maatregelen teneinde:

• De gegevens te beveiligen tegen vernietiging, verlies of wijziging en niet toegelaten opslag, verwerking, toegang of openbaarmaking;
• Te waarborgen dat toegang tot de gegevens slechts geschiedt door speciaal daartoe bevoegde personen;
• De gegevens te kunnen vernietigen na afloop van de periode van:
a. Twaalf maanden voor gegevens in verband met telefonie over een vast of mobiel netwerk,
a. Zes maanden voor gegevens in verband met internettoegang, e-mail over het internet en internettelefonie.</td><td><u>Art. 7 – Opslag en wissing van elektronische-communicatiegegevens.</u>
Elektronische-communicatiegegevens dienen gewist of geanonimiseerd te worden op het moment dat ze niet langer nodig zijn voor het doel van de verwerking.

De aanbieder van elektronische-communicatie services dient metadata te wissen of te anonimiseren op het moment dat het niet meer nodig is voor de verzending of communicatie.

Op het moment dat metadata wordt gebruikt voor facturering dan mag deze data bewaard worden tot het moment dat de termijn om bezwaar te maken verlopen is of er via gerechtelijke weg betaling kan worden afgedwongen.

Zoals bij het vorige artikel, is ook over deze tekst het laatste woord nog niet gezegd. Als de partijen met het oordeel van de EDPB meegaan, is het bewaren van metadata niet toegestaan, anders dan voor rechtshandhaving of bescherming van de nationale veiligheid. Facturering valt hier niet onder.</td></tr>
<tr><td colspan="2"><u>Notabene: daarnaast geldt ook de volgende regel uit de AVG:</u>
A) De doelbinding van de gegevensverwerking vindt zijn grondslag in art. 5 lid 1 sub b AVG.</td></tr>
<tr><td colspan="2">Concluderend: Onder de Tw kennen we al de verplichting om te zorgen voor passende technische en organisatorische maatregelen om gegevens te beveiligen, toegang te beperken en te wissen. De Tw had ook een vastgestelde retentieperiode voor bepaalde gegevens. Onder de ePV wordt er teruggevallen op het bewaartermijnenbeleid van de AVG, namelijk dat dergelijke gegevens verwijderd moeten worden op het moment dat ze niet langer nodig zijn voor het doel van de verwerking.</td></tr>
<tr><td><u>Artikel 11.7a Tw.</u>
Het via een elektronisch communicatienetwerk opslaan van of toegang verkrijgen tot informatie in de</td><td><u>Art. 8 – Bescherming van eindapparatuur van eindgebruikers.</u>
Het gebruik van verwerkings- en opslagcapaciteit van eindapparatuur en het</td></tr>
</table>

Geldend recht ePR/Tw	Voorgesteld ePV
randapparatuur van een gebruiker, is alleen toegestaan op voorwaarde dat de betrokken gebruiker: • Is voorzien van duidelijke en volledige informatie overeenkomstig de AVG, in ieder geval over de doeleinden waarvoor deze informatie wordt gebruikt, en; • Daarvoor toestemming heeft verleend. Deze vereisten zijn ook van toepassing indien op een andere wijze dan door middel van een elektronisch communicatienetwerk informatie wordt opgeslagen of toegang wordt verleend op het randapparaat opgeslagen informatie. De bovenstaande punten zijn niet van toepassing indien het de opslag of toegang betreft: • Met als uitsluitend doel de communicatie over een elektronisch communicatienetwerk uit te voeren; • Die strikt noodzakelijk is om de door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij te leveren of – mits dit geen of geringe gevolgen heeft voor de persoonlijke levenssfeer van de betrokken abonnee of gebruiker – om informatie te verkrijgen over de kwaliteit of effectiviteit van een geleverde dienst van de informatiemaatschappij. Het toestemmingsvereiste uit art. 11.7a TW moet voldoen aan een toestemming van een betrokkene als bedoeld in art. 4, onderdeel 11, AVG.	verzamelen van gegevens uit eindapparatuur van eindgebruikers is verboden behalve in de volgende gevallen: • Het is noodzakelijk voor de overdracht van elektronische communicatie over een elektronisch-communicatienetwerk; • De eindgebruiker heeft toestemming gegeven; • Het is noodzakelijk voor het aanbieden van een, specifiek door de eindgebruiker, aangevraagde dienst; • Het is noodzakelijk om de omvang van het publiek te meten, mits deze meting door de aanbieder van de door de eindgebruiker aangevraagde dienst van of derde partij wordt verricht; • Het noodzakelijk is om de veiligheid van diensten of eindapparatuur van de eind binnen de informatiemaatschappij te behouden of te herstellen, fraude te voorkomen of technische storingen te detecteren; • Het is noodzakelijk voor een software update op voorwaarde dat: - De updates noodzakelijk zijn voor de veiligheid en deze de gekozen privacysettings niet wijzigt; - De eindgebruiker vooraf geïnformeerd is; - De eindgebruiker de mogelijkheid heeft gekregen de update naar een later moment te verschuiven of uit te stellen; • Het is noodzakelijk om de eindapparatuur te lokaliseren in het geval de eindgebruiker een noodoproep maakt; • Het noodzakelijk is voor een ander doel dan waarvoor de informatie is bedoeld op grond van deze Verordening. Wanneer deze

Geldend recht ePR/Tw	Voorgesteld ePV
	verwerking niet gebaseerd is op de eindgebruikers toestemming of op Unie- of lidstatelijk recht (...), moet de verwerkingsverantwoordelijke rekening houden met: - Elk verband tussen de doeleinden waarvoor de verwerking en opslagmogelijkheden zijn gebruikt en de doeleinden van de verdere verwerking; - De context waarin de verwerkings- en opslagmogelijkheden zijn geweest, in het bijzonder met betrekking tot de relatie tussen betrokken eindgebruikers en aanbieder; - De aard van de verwerkings- en opslagmogelijkheden of van het verzamelen ervan; - De mogelijke gevolgen van de beoogde verdere verwerking voor eindgebruikers; - Het bestaan van passende waarborgen, zoals pseudonimisering en versleuteling. • Een dergelijke verdere verwerking, zoals hierboven beschreven, mag alleen plaatsvinden mits: - De informatie wordt gewist of wordt geanonimiseerd zodra deze niet langer meer nodig is voor het doel; - De verwerking is beperkt tot informatie welke is gepseudonimiseerd; - De informatie niet wordt gebruik om de aard of kenmerken van een eindgebruiker of om een profiel van een eindgebruiker op te bouwen.

Geldend recht ePR/Tw	Voorgesteld ePV
	Voordat eerdergenoemde geanonimiseerde metadata gedeeld mag worden met derden dient het volgende te gebeuren: • Er moet een assessment worden uitgevoerd om de impact op de vertrouwelijkheid van de communicatie en de privacy van de eindgebruiker te bepalen; • De eindgebruiker informeren over de voorgestelde verwerking en de rechten die eindgebruiker heeft; • Toepasselijke technische en organisatorische maatregelen implementeren. Het verzamelen van gegevens uit eindapparatuur om een aansluiting op andere apparatuur en/of netwerkuitrusting mogelijk te maken, is verboden tenzij: • Het uitsluitend plaatsvindt met het doel en gedurende de tijd die nodig is om een aansluiting tot stand te brengen of te onderhouden; • De eindgebruiker toestemming heeft gegeven; • Het is noodzakelijk voor het meten van statistische doeleinden mits verbonden aan een tijds- en ruimtelimiet en waarna de data geanonimiseerd of gewist wordt; • Het is noodzakelijk om service verzoeken van de eindgebruiker uit te voeren. Hier heeft de EDPB opgemerkt dat de regels omtrent toestemming, zoals opgenomen in de AVG, ook van toepassing zijn op de e-privacyregels. Dat betekent dat moet worden voorkomen dat dienstverleners oneerlijke praktijken toepassen, zoals bijvoorbeeld een cookiewall. Het afhankelijk stellen van toegang tot diensten en functies van

<table>
<tr><th>Geldend recht ePR/Tw</th><th>Voorgesteld ePV</th></tr>
<tr><td></td><td>toestemming van een gebruiker, moet worden verboden. De EDPB ziet graag een expliciete bepaling waarin dit verbod is opgenomen.</td></tr>
<tr><td colspan="2"><u>Notabene: daarnaast gelden ook de volgende regels uit de AVG:</u>
A) De eisen voor het gebruik van een verwerker dan wel in geval van gezamenlijke verwerkingsverantwoordelijkheid zijn neergelegd in art. 28 respectievelijk 26 AVG.
B) Voor de speciale categorieën van persoonsgegevens zal er gekeken moeten worden naar art. 9 AVG.
C) Het assessment dat uitgevoerd moet worden vindt zijn oorsprong in art. 35 AVG. Art. 36 AVG regelt in welke gevallen er voorafgaande raadpleging vereist is.
D) De eisen die gelden voor de informatieplicht zijn terug te vinden in art. 13 AVG. Voor de te nemen veiligheidsmaatregelen zal er gekeken moeten worden naar art. 32 AVG.</td></tr>
<tr><td colspan="2">Concluderend: Onder de ePV zijn er meer mogelijkheden om voorbij te gaan aan het in art. 8 genoemde verbod dan voorheen in de Tw. Daarnaast worden er een aantal eisen gesteld aan het delen van dergelijke gegevens met derden, deze eisen zijn vergelijkbaar met die uit de AVG.</td></tr>
<tr><td><u>Artikel 11.11 Tw</u>
Een abonnee die last heeft van hinderlijke of kwaadwillige oproepen, waarbij de verstrekking van het nummer van het oproepende netwerkaansluitpunt is geblokkeerd, kan aan de aanbieder van een openbaar elektronisch communicatienetwerk of van een openbare elektronische communicatiedienst verzoeken om het nummer van de oproepende abonnee en de beschikbare daarop betrekking hebbende naam-, adres-, postcode- en woonplaatsgegevens, te verstrekken.

Een verzoek als bedoeld in het eerste lid voldoet aan de volgende vereisten:

a. het verzoek is schriftelijk en bevat de naam-, adres-, postcode- en woonplaatsgegevens van de verzoeker alsmede het nummer waarop de oproepen betrekking hebben, en

b. het verzoek bevat een indicatie van de data en tijdstippen waarop de desbetreffende oproepen hebben plaatsgevonden.</td><td><u>Art. 14 – Ongewenste, kwaadaardige en vervelende oproepen.</u>
Aanbieders van openbaar beschikbare, nummer gebaseerde, persoonlijke communicatiediensten moeten geavanceerde maatregelen om de ontvangst van ongewenste, kwaadaardige en vervelende oproepen door eindgebruikers te beperken.

Daarnaast verstrekken aanbieders van persoonlijke, op nummer gebaseerde, communicatiediensten de opgeroepen eindgebruiker eveneens kosteloos de volgende mogelijkheden om
• Binnenkomende oproepen van specifieke nummers, uit anonieme bronnen of nummers die gebruik maken van een specifieke code of voorvoegsel, waar technisch mogelijk, te blokkeren;
• De automatische doorschakeling van oproepen door een derde naar de eindapparatuur van de eindgebruiker te beëindigen.</td></tr>
</table>

Geldend recht ePR/Tw	Voorgesteld ePV
De verzoeker informeert de aanbieder onverwijld omtrent hinderlijke of kwaadwillige oproepen, die plaats hebben gevonden na indiening van het verzoek. De aanbieder stelt naar aanleiding van het verzoek een onderzoek in, teneinde vast te stellen of tot verstrekking van de gegevens, dient te worden overgegaan. Indien bij het onderzoek blijkt dat het oproepende nummer toebehoort aan een abonnee van een andere aanbieder, verleent de desbetreffende aanbieder op een daartoe strekkend verzoek van de met het onderzoek belaste aanbieder medewerking aan het onderzoek en verstrekt, indien het onderzoek daartoe aanleiding geeft, de beschikbare op het oproepende nummer betrekking hebbende naam-, adres-, postcode- en woonplaatsgegevens aan de aanbieder die met het onderzoek belast is. Van de gegevensverstrekking aan een verzoeker wordt door de aanbieder mededeling gedaan aan de abonnee, wiens gegevens het betreft.	
Concluderend: ***Wat nieuw is onder de ePV is dat aanbieders actief vooraf maatregelen moeten nemen om hinderlijke, ongewenste en kwaadaardige oproepen tegen te gaan dan wel te beperken. Het is niet langer voldoende dit achteraf voor een eindgebruiker te doen.***	
<u>Art. 11.7 lid 3 Tw</u> Een ieder die elektronische contactgegevens voor elektronische berichten heeft verkregen in het kader van de verkoop van zijn product of dienst mag deze gegevens gebruiken voor het overbrengen van communicatie voor commerciële, ideële of charitatieve doeleinden met betrekking tot eigen gelijksoortige producten of diensten, mits bij de verkrijging van de contactgegevens aan de klant duidelijk en uitdrukkelijk de gelegenheid is geboden om kosteloos en op gemakkelijke wijze verzet aan te tekenen tegen het gebruik van die elektronische contactgegevens, en, indien de klant hiervan geen gebruik heeft	<u>Art. 16 – Ongevraagde en direct marketing communicaties.</u> Natuurlijke of rechtspersonen zijn niet toegestaan om gebruik te maken van elektronische- communicatiediensten voor de verzending van direct marketing berichten aan eindgebruikers die natuurlijke personen zijn, tenzij die hun toestemming hebben gegeven. Op het moment dat een natuurlijke- of rechtspersoon contactgegevens voor elektronische berichten verzameld in het kader van een aankoop van een product of service dan mogen deze gegevens wel gebruikt worden voor direct marketing van

Geldend recht ePR/Tw	Voorgesteld ePV
gemaakt, hem bij elke overgebrachte communicatie de mogelijkheid wordt geboden om onder dezelfde voorwaarden verzet aan te tekenen tegen het verder gebruik van zijn elektronische contactgegevens. Artikel 12, derde lid, van de Algemene verordening gegevensbescherming is van overeenkomstige toepassing. Art. 12 lid 3 AVG regelt dat de betrokkene binnen één maand (mits niet verlengd) uitsluitsel moet krijgen over het gevolg dat aan zijn of haar verzoek is gegeven.	eigen vergelijkbare producten of services mits de eindgebruikers de kans hebben gekregen/krijgen om hier bezwaar tegen te maken. Lidstaten kunnen aan bovenstaande een tijdslimiet stellen. Natuurlijke of rechtspersonen die gebruikmaken van elektronische-communicatiediensten voor de doeleinden van direct marketing verstrekken de identiteit van een lijn waarop contact met hen kan worden opgenomen. Lidstaten mogen eisen dat een natuurlijke of rechtspersonen die gebruikmaken van elektronische-communicatiediensten voor de doeleinden van direct marketing gebruik maken van een specifieke code of voorvoegsel zodat te herkennen is dat de oproep een direct marketing oproep is. Elke natuurlijke of rechtspersoon die gebruik maakt van elektronische-communicatiediensten voor de verzending van direct marketing berichten moet: • Zijn of haar identiteit prijsgeven en een contactadres of nummer gebruiken; • De eindgebruiker informeren over de marktering aard van de communicatie en de identiteit van de rechts- of natuurlijke persoon van wie het afkomstig is; • De eindgebruiker duidelijk de mogelijkheid geven om zijn of haar toestemming voor direct marketing gratis, op elk moment en makkelijk in te trekken.
Notabene: daarnaast geldt ook de volgende regel uit de AVG: A) Art. 21 AVG regelt alles omtrent het bezwaar dat gemaakt kan worden tegen de verwerking, in casu de direct marketing.	

Geldend recht ePR/Tw	Voorgesteld ePV
Concluderend: ***In de Tw bestaat, net als in de ePV, het recht om gegevens te gebruiken voor direct marketing. Daarbij geldt, onder beiden, dat dit enkel mag indien de eindgebruiker vooraf, dan wel achteraf, de mogelijkheid heeft om bezwaar te maken tegen een dergelijke verwerking. Wat nieuw is onder de ePV, is dat diegene die contact opneemt zijn of haar identiteit moet prijsgeven. Anonieme direct marketing is daarmee verboden.***	
<u>Er bestaat geen recht op schadevergoeding op basis van de Tw.</u> <u>Art. 82 AVG</u> Eenieder die materiële of immateriële schade heeft geleden ten gevolge van een inbreuk op deze verordening, heeft het recht op van de verwerkingsverantwoordelijke of de verwerker schadevergoeding te ontvangen voor de geleden schade.	<u>Art. 22 – Recht op schadevergoeding en aansprakelijkheid.</u> Elke persoon 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.
Concluderend: ***Op basis van de voorgestelde regels heeft een betrokkene recht op schadevergoeding ten gevolge van een inbreuk hierop. Dit is een wijziging ten opzichte van het huidige recht.***	
<u>Art. 11.3 jo. Art. 11.3a Tw</u> De aanbieder van een openbare elektronische communicatiedienst stelt de Autoriteit Persoonsgegevens (AP) onverwijld in kennis van een inbreuk op de beveiliging, als bedoeld in art. 11.3, die nadelige gevolgen heeft voor de bescherming van persoonsgegevens die zijn verwerkt in verband met de levering van een openbare elektronische communicatiedienst in de EU.[xxi] Op grond van Verordening 611/2013 is de meldtermijn datalekken voor een openbare elektronische communicatiedienst 24 uur in plaats van 72 uur in de AVG.[xxii]	Verordening 611/2013 blijft naast de ePV gelden. De meldtermijn datalekken voor een openbare elektronische communicatiedienst blijft 24 uur.[xxiii]

Recente ontwikkelingen en opinies

Opinie Europese privacy toezichthouders (EDPB)
De EDPB is het gezamenlijke orgaan van de nationale privacy toezichthouders. De EDPB ziet de huidige herziening van de ePR door middel van een ePV als een belangrijke, noodzakelijke en dringende stap.[xxiv] De EDPB *"staat volledig achter de aanpak van de voorgestelde Verordening, die gebaseerd is op ruime verbodsbepalingen, beperkte uitzonderingen en het gebruik van toestemming"*. Volgens de EDPB moet de ePV iedere mogelijkheid uitsluiten om inhoud en metadata van elektronische communicatie te verwerken op basis van open gronden, zoals het 'gerechtvaardigd belang', nu deze verder gaan dan wat nodig is voor de levering van een elektronische communicatiedienst. De EDPB is daarnaast van mening dat de ePV iedere mogelijkheid moet uitsluiten om metagegevens van elektronische communicatie te verwerken met het oog op de uitvoering van een overeenkomst, er mag dus geen uitzondering worden gemaakt op basis van het algemene doel een overeenkomst uit te voeren. Metagegevens van elektronische communicatie mogen volgens de EDPB nog steeds zonder toestemming worden verwerkt, mits de gegevens eerst zijn geanonimiseerd.

Volgens de EDPB is voor de vertrouwelijkheid van elektronische communicatie specifieke bescherming vereist die verder gaat dan de AVG. De vertrouwelijkheid van communicatie is een grondrecht dat wordt beschermd op basis van art. 7 van het Handvest van de grondrechten van de EU, waaraan de huidige ePR uitvoering geeft. Dit grondrecht moet volgens de EDPB gelden voor iedere vorm van elektronische communicatie, ongeacht de wijze waarop door de betrokkene gegevens van de verzender naar de ontvanger worden verstuurd. Daarnaast moet in ieder geval de integriteit van de eindapparatuur van iedere betrokkene worden beschermd. Gezien het ruime gebruik van elektronische communicatie in dit digitale tijdperk is het waarschijnlijk dat deze, vanwege de combinatie van inhoud of metadata, bijzondere categorieën van persoonsgegevens bevat waardoor zeer nauwkeurige conclusies over het privéleven van de betrokken personen kunnen worden getrokken.

De EDPB benadrukt daarnaast dat *"de uitbreiding van het toepassingsgebied van de ePV tot functioneel gelijkwaardige diensten, waaronder 'over-the-top diensten' vallen, een essentieel onderdeel van de hervorming uitmaakt."*[xxv] Met de toestemming die krachtens de ePV moet worden verkregen, wordt hetzelfde bedoeld als in de AVG. Volgens de EDPB zal met name de eis dat de toestemming vrijelijk moet worden verleend voorkomen dat aanbieders van diensten een cookiewall voor hun gebruikers gaan opwerpen.

In het kort, volgens de EDPB:

- *"Mag de ePV het niveau van bescherming dat wordt geboden door de huidige ePR niet verlagen;*
- *De ePV moet daarnaast voorzien in technologie-neutrale bescherming voor alle soorten elektronische communicatie, dus ook voor OTT-diensten;*
- *De toestemming van de gebruiker moet op een technisch haalbare en afdwingbare manier systematisch worden verkregen voordat de*

- *elektronische communicatiegegevens worden verwerkt of voordat gebruik wordt gemaakt van de opslag- of verwerkingscapaciteit van de gebruiker;*
- *Doeltreffende manieren worden vastgesteld om toestemming te verkrijgen voor websites en mobiele applicaties;*
- *Iedere ad-hoc uitzondering die wetgevers overwegen moeten toegevoegd worden in de ontwerpteksten van de Commissie en het Parlement welke met de grootste zorgvuldigheid moet worden onderzocht;*
- *Om te zorgen dat toestemming vrijelijk wordt verleend overeenkomstig de AVG, mag de toegang tot diensten en functies niet afhankelijk worden gesteld van de toestemming van een gebruiker voor de verwerking van persoonsgegevens of de verwerking van informatie met betrekking tot of verwerkt door de eindapparatuur, waardoor cookiewalls uitdrukkelijk verboden moeten worden;*
- *Het gebruik van daadwerkelijk geanonimiseerde elektronische communicatiegegevens moet worden aangemoedigd;*
- *De privacy van de eindgebruikers moeten in iedere relevante context worden bescherming en concurrentieverstoringen moeten worden voorkomen."*[xxvi]

Opinies verschillende EU-landen nader toelichten

Tijdens de telecomraad op 3 december 2019 is het niet gelukt om onder leiding van het Finse Voorzitterschap, wat liep van 1 juli 2019 tot 31 december 2019, samen met alle EU-lidstaten tot een algemene oriëntatie met betrekking tot de voorgestelde versie van de ePV te komen.[xxvii] De meeste EU-lidstaten ondersteunen de algemene doelen van de ePV. De problemen lagen meer op het gebied van de toekomstbestendigheid, de impact en innovatie en de link met de AVG.[xxviii]

Het stokje werd op 1 januari 2020 overgedragen aan Kroatië welke tot 30 juni 2020 het voorzitterschap van de Raad van de Europese Unie vervulde. Kroatië had begin 2020 veel aan te merken op de toentertijd voorgestelde versie van de ePV. Vandaar dat het land in maart 2020 zelf met een compleet nieuw cookievoorstel is gekomen welke tot grote wijzigingen heeft geleid die nu ter discussie staan.[xxix] In dit voorstel zijn de gronden voor het verwerken van persoonsgegevens die verzameld worden via cookies uitgebreid. Kroatië is verder van mening dat persoonsgegevens via cookies ook verzameld mogen worden op grond van een gerechtvaardigd belang van de verwerkingsverantwoordelijke, en dus zonder toestemming van de betrokkene, tenzij de betrokkene een groter privacybelang heeft. Daarbij dient de verwerkingsverantwoordelijke op nauwkeurige en zorgvuldige wijze te beoordelen of een gerechtvaardigd belang aanwezig is. Ook lijkt het voorstel meer ruimte te bieden voor een cookiewall.

In het nieuwe conceptvoorstel van de ePV dat is opgesteld door Kroatië staat in de artikelen 6b en 8 het gerechtvaardigd belang verwerkt. Op basis van het voorgestelde art. 6b zou het mogelijk zijn metadata van elektronische communicatie te verwerken op grond van een gerechtvaardigd belang. Art. 8 biedt vervolgens de mogelijkheid, ook op basis
van het gerechtvaardigd belang, toegang te verkrijgen via een elektronisch communicatienetwerk tot informatie in de randapparatuur van een gebruiker of deze op te slaan. Op basis hiervan kunnen dus ook cookies worden geplaatst op basis van de grondslag

'gerechtvaardigd belang'. Metadata mag wel puur geanonimiseerd met derden worden gedeeld, de eindgebruikers moeten worden geïnformeerd over de gegevensverwerking en zij mogen hiertegen bezwaar maken en bij iedere verwerking moet een assessment uitgevoerd worden. Daarnaast beschrijft het nieuwe conceptvoorstel dat het gerechtvaardigd belang niet als grondslag gebruikt mag worden indien de fundamentele rechten en vrijheden van eindgebruikers zwaarder wegen dan de verwerking zelf, zoals het geval is wanneer bijzondere persoonsgegevens worden verwerkt.[xxx]

Het voorstel van Kroatië wordt door sommigen de 'Kroatische Kronkel' genoemd, aangezien het voorstel weinig nieuwe mogelijkheden biedt.[xxxi] De verkregen gegevens mogen namelijk niet met derden worden gedeeld en er moet een assessment voor uitgevoerd worden. Maar ook een aantal Lidstaten zijn tegenstander van de gerechtvaardigd belang grondslag. Deze Lidstaten hebben liever een vaste lijst met verwerkingsgronden. Daarnaast zijn er Lidstaten die vinden dat de ePV verder in lijn moet worden gebracht met de AVG en dat zij grote zorgen hebben omtrent de rechten en belangen van providers en eindgebruikers.[xxxii]

Duitsland behoort tot de groep van Lidstaten die graag de bestaande bepalingen uit de ePV meer in overeenstemming wil brengen met de AVG.[xxxiii]. In november 2020 heeft de Raad van de EU een nieuwe conceptverordening gepubliceerd waarin de lidstaten verschillende aanvullende wijzigingen hebben voorgesteld.[xxxiv] Eén van de belangrijkste wijzigingen is dat het 'gerechtvaardigd belang' als grondslag voor het plaatsen van cookies, zoals voorgesteld door het Kroatische Voorzitterschap, in het nieuwe conceptvoorstel is weggehaald nu sommige lidstaten dit een te brede grondslag vinden. Ook het verwerken van metadata en elektronische communicatie is volgens dit voorstel niet meer mogelijk op grond van het gerechtvaardigd belang.

Daarnaast bevat het nieuwe conceptvoorstel ook een bepaling met betrekking tot het toestaan van verwerkingen van metadata wanneer dit noodzakelijk is voor de bescherming van vitale belangen van een natuurlijke persoon. Door de huidige COVID-19 pandemie hebben de lidstaten deze wijziging anders dan voorheen beoordeeld waardoor er is gekozen voor een bredere reikwijdte. Hierdoor verandert de focus van enkel en alleen de eindgebruiker, naar het belang van natuurlijke personen. Een ander belangrijk punt is dat het standpunt omtrent de cookiewalls weer is gewijzigd. Door het Kroatische Voorzitterschap is voorgesteld dat door middel van cookiewalls in bepaalde situaties vrijelijk toestemming kan worden gegeven, namelijk om een gelijksoortige website te bezoeken van dezelfde provider. Uit het nieuwe conceptvoorstel volgt dat dit ook het geval is wanneer gelijksoortige websites zonder cookiewalls worden aangeboden door *andere* providers.

Maar ook het Duitse voorstel is er niet doorheen gekomen. Inmiddels heeft Portugal het voorzitterschap overgenomen en ook al een nieuw ePV voorstel gepubliceerd. Portugal wil de Verordening vooral vereenvoudigd en meer in lijn met de AVG hebben.[xxxv] Zo heeft Portugal de territoriale reikwijdte van de ePV veranderd, waardoor ook niet-Europese organisaties aan de ePV zullen moeten voldoen.

De grondslag ‘gerechtvaardigd belang’, die door het Duitse Voorzitterschap is verwijderd, is ook door Portugal niet opgenomen in haar conceptvoorstel. Daarnaast is de verenigbare verwerking voor metadata en data zoals die verkregen worden uit cookies, wél opnieuw toegevoegd. Ook al is de verenigbare verwerking voor metadata en data uit cookies terug te vinden in het nieuwe conceptvoorstel, deze benadering sluit nog steeds de mogelijkheid uit om gegevens verder te verwerken voor profileringsdoeleinden. Door deze toevoeging wordt dit ePV voorstel wel dichter in lijn gebracht met de huidige AVG.

Het Portugese voorstel bevat geen bepaling meer die vereist dat bij een cookiewall sprake moet zijn van een “cookieloos” vergelijkbaar aanbod bij dezelfde aanbieder. Aanbieders van websites mogen dus ook een cookiewall instellen indien andere aanbieder een vergelijkbaar aanbod heeft. Daarnaast is ook de periode van inwerkingtreding en toepasselijkheid veranderd van twee naar één jaar. Hierdoor hebben organisaties minder tijd om de Verordening te implementeren.

Om het allemaal nog spannender te maken heeft de EDPB recent haar zorgen geuit over de voortdurende discussie over de bevoegde toezichthouder. De EPDB uitte haar bezorgdheid over alle nieuwe oriëntaties met betrekking tot de handhaving van de ePV, welke zouden kunnen leiden tot een gefragmenteerd toezicht, procedurele complexiteit en een gebrek aan consistentie en rechtszekerheid voor individuen en bedrijven.[xxxvi] De EDPB is namelijk voor één toezichthouder voor zowel de ePV als de AVG, maar een grote groep lidstaten pleit ervoor dat deze keuze binnen de lidstaten zelf ligt, en dus ook dat er meerdere toezichthouders aangesteld kunnen worden.

Wat verandert de komst van de ePV voor mijn organisatie?

Er zijn organisaties die de komst van de ePV vrezen doordat nieuwe regels impact zullen hebben op bestaande direct marketing. Kanttekening bij deze vrees is dat de toestemmingsvereisten al zijn aangescherpt met de komst van de AVG en jurisprudentie van het Europese Hof van Justitie.[xxxvii] Uit recente rechtspraak blijkt bijvoorbeeld dat je nooit een rechtmatige toestemming kunt verkrijgen door middel van een standaard vooraf aangevinkt selectievakje voor het plaatsen van cookies en je dus altijd een actieve toestemming van internetgebruikers moet verkrijgen.[xxxviii] Ook zonder de ePV moeten organisaties dus nu al hoge prioriteit geven aan naleving van de huidige regels op het gebied van cookies en marketing.[xxxix] Bovendien kennen wij in Nederland al langer één van de meest strenge cookiebepalingen van de EU met art. 11.7a Tw.[xl]

Desalniettemin kan de ePV alsnog een forse impact hebben op organisaties die zich bezighouden met digitale direct marketing als deze organisaties nog niet aantoonbaar compliant zijn met de Tw en de AVG. Ook zullen nieuwe partijen zoals browsers, die onder de AVG (nog) geen verwerkingsverantwoordelijkheden zijn, worden geraakt door de ePV.[xli] Tevens vallen onder de ePV nieuwe aanbieders die online communicatiediensten aanbieden, zoals Facebook, Twitter, Whatsapp, Skype, IMessage en Gmail zodat organisaties die dit soort diensten hebben ingebed in hun websites, ook zwaardere compliance verplichtingen zullen hebben.[xlii]

De komst van de ePV zal ook veranderingen met zich meebrengen op het gebied van het markttoezicht. Momenteel is het toezicht op de naleving van de ePR deels belegd bij de Autoriteit Persoonsgegevens (AP) en deels bij de Autoriteit Consument en Markt (ACM).[xliii] Het toezicht is

hierdoor versnipperd waardoor onduidelijkheid kan bestaan over de uitleg van e-privacy regels. Met de komst van de ePV zal het toezicht hierop hoogstwaarschijnlijk bij de AP worden neergelegd. Ook zal er, net als bij de AVG, de mogelijkheid geïntroduceerd worden om boetes op te leggen door de AP.[xliv]

Op dit moment verschillen de AP en de ACM nog wel eens van beleid. Zo is de AP namelijk van mening dat een cookiewall in geen enkel geval is toegestaan, omdat de AVG bepaalde eisen stelt aan de benodigde toestemming voor het plaatsen van tracking cookies. Dat komt omdat je met een cookiewall geen toestemming kunt krijgen van gebruikers voor het plaatsen van tracking cookies.[xlv] De ACM hanteert de beleidsregels dat een cookiewall, ondanks dat het niet erg gebruiksvriendelijk is, in de meeste gevallen is toegestaan ook al druist dit in tegen de geest van de wet. *"De cookiebepaling beoogt namelijk de gebruiker een keuze te geven ten aanzien van zijn privacy en het gebruik van zijn persoonsgegevens op het internet. Als websites gebruikers alleen toegang geven indien alle cookies worden geaccepteerd, wordt de gebruiker beperkt in zijn keuze."*[xlvi] Een cookiewall is niet toegestaan voor (semi-) overheidswebsites, waaronder ook de publieke omroepen vallen. Op grond van art. 11.7a lid 5 Tw mogen rechtspersonen, die bij of krachtens het publiekrecht zijn ingesteld, namelijk de toegang tot de website niet ontzeggen aan gebruikers die geen toestemming geven voor het plaatsen of uitlezen van gegevens. Hieruit kan geconcludeerd worden dat de AP er principiëler in lijkt te staan dan de ACM, waardoor de verwachting is dat met de ePV, principiëler toezicht wordt gehouden.

Wij zouden organisaties, en marketingbedrijven in het bijzonder, aanraden om een Data Protection Impact Assessment (DPIA) uit te voeren. In onze factsheet van augustus 2023 kan je lezen hoe je als organisatie een DPIA kunt uitvoeren. Door het uitvoeren van een DPIA breng je als organisatie in kaart welke privacy risico's de verwerking van online communicatie met zich mee kunnen brengen en hoe vertrouwelijke digitale communicatie beschermd kan worden binnen jouw organisatie. Dit is niet verplicht onder de AVG, tenzij de verwerking een groot risico voor betrokkenen met zich meebrengt. Het doel is om er op die manier voor te zorgen dat je de ePV zo goed mogelijk binnen de organisatie implementeert om klachten of erger te voorkomen. Hoewel de ePV niet, zoals de AVG, een apart artikel omtrent het uitvoeren van een assessment kent, komt deze verplichting wel in een aantal andere artikelen terug. Art. 6a lid 2 jo lid 1 sub b bijvoorbeeld stelt dat er een assessment uitgevoerd moet worden in het geval dat consent gebruikt wordt als grondslag voor de verwerking van elektronische communicatiegegevens. Er zal onder art. 6b en 8 van de ePV ook een assessment moeten worden uitgevoerd voordat dergelijke data met derden wordt gedeeld. Ook als het uitvoeren van een DPIA niet voor jou als organisatie verplicht is, kan het je helpen om duidelijk te krijgen welke gegevens jouw organisatie online verwerkt en hoe daarmee om wordt gegaan.[xlvii]

Met de komst van de AVG waren veel organisaties ook bang voor de nieuwe verplichtingen die dit met zich meebracht op het gebied van dataprotectie. Met de komst van de ePV is er geen reden voor extra paniek, als je als organisatie al goed bezig bent met AVG-compliant te zijn en te blijven en de regels uit de ePR en AVG naleeft.[xlviii]

Stappenplan voor wat nu al te doen

1. Voer een GAP-analyse uit met als norm de huidige Tw en AVG

**Indien dit nog niet door de organisatie is uitgevoerd.*

2. Tref (alsnog) de vereiste maatregelen om aantoonbaar compliant te worden aan de huidige Tw en AVG

**Gelet op de recente ontwikkelingen, zoals het wegvallen van het EU-VS Privacy Shield, en de zware compliance eisen die naar alle waarschijnlijkheid zullen voortvloeien uit de ePV, voorkom je het treffen van ad hoc maatregelen. Daarnaast kun je tijdig rekening houden met de beginselen van Privacy by Design & Default.*

3. Monitor de ontwikkelingen rondom de ePV nauwkeurig en analyseer tijdig of er nieuwe maatregelen moeten worden getroffen om compliant te worden aan de ePV

**Door eventuele achterstallige compliance met de Tw en de AVG nu aan te pakken ben je als organisatie beter voorbereid op de maatregelen die voortkomen uit de ePV. Indien je als organisatie niet compliant bent met de Tw en de AVG op het moment van inwerkingtreding van de ePV, is de impact vele malen groter.*

4. Voer alvast assessments uit op verwerkingsprocessen waarbij elektronische communicatiegegevens worden verwerkt of met derden worden gedeeld

Conclusie

Hoewel het nog even op zich kan laten wachten voordat de ePV er daadwerkelijk is en tal van wijzigingen nog doorgevoerd kunnen gaan worden, zouden we willen meegeven om binnen jouw organisatie alvast de eerste stappen te maken. Het is aan te raden om als organisatie goed de ontwikkelingen met betrekking tot de komst van de ePV in de gaten te houden en te anticiperen op de komende nieuwe regels en verplichtingen. Zoals gezegd, gelden er met de komst van de AVG en recente rechtspraak al strengere eisen met betrekking tot cookies. Het is daarom verstandig om de cookiebanners op je website alvast te controleren om te bekijken of deze in orde zijn. Kom je er niet uit of heb je momenteel geen capaciteit? L2P kan je op basis van onze praktijkervaringen bijstaan bij diverse werkzaamheden zoals het opstellen van een cookiestatement, het vormgeven van een cookiebanner of het uitvoeren van een GAP-analyse.

Gezonde groet,
L2P
+31 (0) 26 848 3118
info@l2p.nl

Geraadpleegde bronnen:

[i] 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).
[ii] 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), Publicatieblad Nr. L 201 van 31/07/2002 blz. 0037 – 0047.
[iii] Louwers advocaten, '*De e-privacy verordening: komt hij er dan toch?*, 18 februari 2021 *Louwersadvocaten.nl*
[iv] 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), COM/2017/010 final - 2017/03 (COD).
[v] Art. 1.1 Tw.
[vi] J. Goes, '*De belangenstrijd rond de ePrivacy Verordening*', 15 augustus 2018 *Ictrecht.nl*.
[vii] Art. 2 AVG.
[viii] B. Schermer, '*De e-Privacy Verordening, een korte update*', *Considerati.com*.
[ix] J. Goes, '*De belangenstrijd rond de ePrivacy Verordening*', 15 augustus 2018, *Ictrecht.nl*.
[x] S. Nas, '*De ePrivacy Verordening: dit staat er nu al op het spel*', 21 januari 2020, *IIR Whitepaper*.
[xi] Redactie IIR, Trainingen en Conferenties, '*Wat is ePrivacy Verordening*?', 22 november 2018 *IIR.nl*; 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),COM/2017/010 final - 2017/03 (COD).
[xii] 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), COM/2017/010 final - 2017/03 (COD).
[xiii] Louwers advocaten, '*De e-privacy verordening: stand van zaken in 2020*', 21 april 2020 *Louwersadvocaten.nl*.
[xiv] S. Nas, '*De ePrivacy Verordening: dit staat er nu al op het spel*', 21 januari 2020 *IIR Whitepaper*.
[xv] Louwers advocaten, '*De e-privacy verordening: stand van zaken in 2020*', 21 april 2020 *Louwersadvocaten.nl*.
[xvi] 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), COM/6543/20 final – 6543/20 (COD); Louwers advocaten, '*De e-privacy verordening: stand van zaken in 2020*', 21 april 2020 *Louwersadvocaten.nl*.
[xvii] EDPB, 'Verklaring 3/2021 over de e-privacyverordening', 9 maart 2021.
Eerste Kamer E170003 – '*Voorstel voor een verordening betreffende privacy en elektronische communicatie*', 26 augustus 2020.
[xviii] B. Schermer, 'De e-Privacy Verordening, een korte update', *Considerati.com*.
[xix] Kamerstuk, Tweede Kamer der Staten-Generaal, 25522, nr. 3, 23 september 1997.
[xx] DMCC, 'Telecommunicatiewet', 2020.
[xxi] F.J. Zuiderveen Borgesius, '*De meldplicht voor datalekken in de Telecommunicatiewet*', PPMG_T2_Computerrecht, augustus 2011.
[xxii] Art. 2 lid 2 Verordening (EU) Nr. 611/2013 van de Commissie van 24 juni 2013 betreffende maatregelen voor het melden van inbreuken in verband met persoonsgegevens op grond van Richtlijn 2002/58/EG van het Europees Parlement en de Raad betreffende privacy en elektronische communicatie.
[xxiii] Art. 2 lid 2 Verordening (EU) Nr. 611/2013 van de Commissie van 24 juni 2013 betreffende maatregelen voor het melden van inbreuken in verband met persoonsgegevens op grond van Richtlijn 2002/58/EG van het Europees Parlement en de Raad betreffende privacy en elektronische communicatie.

[xxiv] European Data Protection Board, '*Verklaring van het Europees Comité voor gegevensbescherming over herziening van de ePrivacy Verordening en de gevolgen daarvan voor de bescherming van personen in verband met privacy en de vertrouwelijkheid van hun communicatie'*, 2018.
[xxv] Idem.
[xxvi] Idem.
[xxvii] Eerste Kamer E170003 – '*Voorstel voor een verordening betreffende privacy en elektronische communicatie*', 26 augustus 2020.
[xxviii] Verslag bijeenkomst Raad voor Vervoer, Telecommunicatie en Energie van 3 december 2019, zie: https://www.eerstekamer.nl/eu/behandeling/20191220/brief_regering_verslag_van_de
[xxix] 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), COM/6543/20 final – 6543/20 (COD).
[xxx] E. Troll, '*De ePrivacyverordening: een stand van zaken'*, Privacyweb, 22 juni 2020.
[xxxi] DMCC, J. va Doodewaerd, '*e-Privacy: Kroatië komt met nieuw cookievoorstel*', 3 maart 2020.
[xxxii] E. Troll, '*De ePrivacyverordening: een stand van zaken'*, Privacyweb, 22 juni 2020.
[xxxiii] European Counsel of the European Union, '*The presidency of the counsel of the EU'*, 202.
[xxxiv] Council of the European Union, *'Proposal for a Regulation of the European Parliament and the Council concering the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation of Privacy and Electronic Communications),* 9931/20, Brussels 4 November 2020, zie: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_9931_2020_INIT&from=EN.
[xxxv] Council of the European Union, *'Proposal for a Regulation of the European Parliament and the Council concering the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation of Privacy and Electronic Communications),* 9931/20, Brussels 5 januari 2021.
[xxxvi] EDPB Press Release 2020_19, '*European Data Protection Board – 42nd Plenary session: Presentation of two new sets of SCCs & EDPB adopts statement on ePrivacy Regulation',* 20 november 2020.
[xxxvii] S. Nas, '*De ePrivacy Verordening: dit staat er nu al op het spel*', 21 januari 2020 *IIR Whitepaper*.
[xxxviii] Hof van Justitie van de Europese Unie zaak C-673/17 1 oktober 2019.
[xxxix] S. Nas, '*De ePrivacy Verordening: dit staat er nu al op het spel*', 21 januari 2020 *IIR Whitepaper*.
[xl] M. de Bruyne, '*Uitspraak Plant49 Zaak: zó mag je geen toestemming meer vragen voor cookies*', 7 oktober 2019 *DDMA.nl.*
[xli] S. Nas, '*ePrivacy verordening: geen reden voor paniek'*, 2 juli 2018 *IIR.nl*.
[xlii] J. Goes, '*De belangenstrijd rond de ePrivacy Verordening'*, 15 augustus 2018 *Ictrecht.nl*.
[xliii] S. Nas, '*ePrivacy verordening: geen reden voor paniek'*, 2 juli 2018 *IIR.nl*.
[xliv] S. Nas, '*ePrivacy verordening: geen reden voor paniek'*, 2 juli 2018 *IIR.nl*.
[xlv] Autoriteit Persoonsgegevens, '*Cookies*', 2020.
[xlvi] Autoriteit Consument & Markt, Beleidsregels inzake cookies, versie november 2016.
[xlvii] Redactie IIR, Trainingen en Conferenties, '*Wat gaat de ePrivacy Verordening betekenen voor marketeers*?', 11 december 2018 *IIR.nl.*
[xlviii] S. Nas, '*ePrivacy verordening: geen reden voor paniek'*, 2 juli 2018 *IIR.nl*.