

Verklaring



Translations proofread by EDPB Members.
This language version has not yet been proofread.

Verklaring 3/2021 over de e-privacyverordening Vastgesteld op 9 maart 2021

Het Europees Comité voor gegevensbescherming heeft de volgende verklaring vastgesteld:

De EDPB beschouwt het door de Raad vastgestelde onderhandelingsmandaat over de bescherming van de privacy en de vertrouwelijkheid bij het gebruik van elektronische-communicatiediensten (“het standpunt van de Raad”) als een positieve stap in de richting van een nieuwe e-privacyverordening. Het is van het grootste belang dat het algemene gegevensbeschermingskader van de EU snel wordt aangevuld met geharmoniseerde regels voor elektronische communicatie.

Zoals al herhaaldelijk is verklaard¹, mag de e-privacyverordening in geen geval het beschermingsniveau van de huidige e-privacyrichtlijn verlagen, maar moet zij een aanvulling vormen op de algemene verordening gegevensbescherming (AVG) door bijkomende sterke garanties te bieden voor de vertrouwelijkheid en de bescherming van alle soorten elektronische communicatie. De e-privacyverordening kan op geen enkele manier worden gebruikt om de AVG feitelijk te wijzigen. In dit verband geeft het standpunt van de Raad op enkele punten aanleiding tot bezorgdheid en de EDPB wil wijzen op een aantal kwesties die bij de komende onderhandelingen aan de orde moeten worden gesteld.

Deze verklaring staat los van een mogelijke toekomstige verklaring of advies van de EDPB waarin nader wordt ingegaan op de standpunten van de medewetgevers.

¹ Zie de complete lijst van documenten over de e-privacyregels van de EDPB en de Groep gegevensbescherming artikel 29 als bijlage bij deze verklaring.

Bezorgdheid over de verwerking en bewaring van elektronische-communicatiegegevens met het oog op de rechtshandhaving en de bescherming van de nationale veiligheid

Met betrekking tot artikel 6, lid 1, punt d), en artikel 7, lid 4, herhaalt de EDPB dat wetgevende maatregelen op grond waarvan aanbieders van elektronische-communicatiediensten verplicht zijn elektronische-communicatiegegevens te bewaren, moeten voldoen aan:

-) artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie (hierna: Handvest);
-) de meest recente jurisprudentie van het Hof van Justitie van de Europese Unie (hierna: Hof)²; en
-) artikel 8 van het Europees Verdrag voor de rechten van de mens.

De EDPB is van oordeel dat de e-privacyverordening niet kan afwijken van de toepassing van de meest recente jurisprudentie van het HvJ-EU, waarin met name is bepaald dat de artikelen 7, 8, 11 en 52, lid 1, van het Handvest aldus moeten worden uitgelegd dat zij zich verzetten tegen wetgevende maatregelen die, als preventieve maatregel, zouden voorzien in de algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens. 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.

Met betrekking tot de uitsluiting van het toepassingsgebied van de verordening van door aanbieders verrichte verwerkingsactiviteiten is de EDPB van oordeel dat een dergelijke uitsluiting indruist tegen het uitgangspunt van een consistent EU-kader voor gegevensbescherming. In geval van uitsluiting benadrukt de EDPB evenwel dat de AVG van toepassing is.

De vertrouwelijkheid van elektronische communicatie vereist specifieke bescherming (artikelen 6, 6 bis, 6 ter en 6 quater)

Het vertrouwelijke karakter van communicatie is een grondrecht dat wordt beschermd door artikel 7 van het Handvest, dat reeds is uitgevoerd door de e-privacyrichtlijn. Dit recht op vertrouwelijkheid moet gelden voor alle vormen van elektronische communicatie, ongeacht de wijze waarop de betrokken gegevens — in rust of in doorvoer — van de verzender naar de ontvanger worden verstuurd, en moet tevens de integriteit van de eindapparatuur van elke gebruiker beschermen.

Algemene verbodsbepalingen met kleine uitzonderingen voor de verwerking van persoonsgegevens

De EDPB staat volledig achter de aanpak op basis van algemene verbodsbepalingen met kleine, specifieke en duidelijk omschreven (doelgerichte) uitzonderingen.

De EDPB is bezorgd dat enkele door de Raad opgenomen uitzonderingen (met name artikel 6, lid 1, punt c), artikel 6 ter, lid 1, punt e), artikel 6 ter, lid 1, punt f), en artikel 6 quater) zeer uitgebreide vormen van verwerking mogelijk lijken te maken, en herinnert eraan dat die uitzonderingen moeten worden beperkt tot specifieke en duidelijk omschreven doeleinden. In elk geval moeten die specifieke doeleinden uitdrukkelijk worden vermeld om de rechtszekerheid en het hoogst mogelijke niveau van bescherming te garanderen.

Voorts kunnen de uitzonderingen van artikel 6, lid 1, punt b), artikel 6, lid 1, punt c), en artikel 6, lid 1, punt d), op grond waarvan toegang tot elektronische-communicatiegegevens, met inbegrip van

² Hof, gevoegde zaken C-511/18, C-512/18 en C-520/18, zaak C-623/17.

inhoudelijke gegevens, mogelijk is om de netwerkbeveiliging en de beveiliging van de apparatuur van eindgebruikers te waarborgen, ertoe leiden dat aanbieders van elektronische-communicatiediensten of hun verwerkers volledige toegang krijgen tot de inhoud van alle communicatie van eindgebruikers. Aangezien dit het recht op vertrouwelijkheid en de privacyverwachtingen van de eindgebruiker zou kunnen ondermijnen, moet de toegang proportioneel zijn en ten minste worden beperkt om eraan te herinneren dat stelselmatig toezicht op de inhoud van elektronische communicatie niet toelaatbaar is en dat aanbieders of verwerkers de encryptiemaatregelen niet mogen omzeilen.

Ten slotte moet in de verordening het belang van anonimisering worden benadrukt als fundamentele garantie die stelselmatig de voorkeur moet krijgen wanneer het gaat om het gebruik van elektronische-communicatiegegevens.

De beschikbaarheid van sterke en betrouwbare encryptie is een noodzaak in de moderne digitale wereld

Sterke, moderne encryptietechnologie moet de algemene regel zijn om een veilige, vrije en betrouwbare gegevensstroom tussen burgers, bedrijven en overheden te waarborgen, en is van cruciaal belang om ervoor te zorgen dat de beveiligingsverplichting van de AVG, bijvoorbeeld voor gezondheidsgegevens, wordt nageleefd en IT-systemen worden beschermd in een context van toenemende bedreigingen. End-to-endencryptie, van de verzender tot de ontvanger, is ook de enige manier om een volledige bescherming van de verstuurd gegevens te waarborgen. Eventuele maatregelen om de encryptie te verzwakken, zelfs voor doeleinden zoals de nationale veiligheid, zouden door mogelijk onrechtmatig gebruik die beschermingsmechanismen volstrekt nutteloos maken. De encryptie moet gestandaardiseerd, sterk en efficiënt blijven³.

De nieuwe verordening moet het geven van toestemming voor cookies en soortgelijke technologieën afdwingen en moet dienstverleners technische instrumenten ter beschikking stellen waarmee zij die toestemming gemakkelijk kunnen verkrijgen (artikel 8⁴)

De behoefte aan een privacybeschermende aanpak met betrekking tot “graag of niet”-oplossingen

Er zij aan herinnerd dat bepalingen inzake toestemming op grond van de AVG van toepassing zijn in het kader van de e-privacyregels. De EDPB is dan ook van oordeel dat de noodzaak om echte en vrijelijk gegeven toestemming te verkrijgen, moet voorkomen dat dienstverleners oneerlijke praktijken toepassen, zoals “graag of niet”-oplossingen, waarbij de toegang tot diensten en functies afhankelijk wordt gesteld van de toestemming van een gebruiker voor het opslaan van informatie, of dat zij toegang krijgen tot informatie die reeds is opgeslagen op de eindapparatuur van een gebruiker (de zogeheten “cookiemuren”)⁵.

De EDPB benadrukt dat er een expliciete bepaling in de e-privacyverordening moet worden opgenomen om dit verbod te verankeren teneinde gebruikers in staat te stellen profilering te aanvaarden of te weigeren. Dezelfde dienstverleners moeten gebruikers derhalve eerlijke alternatieven bieden. Dergelijke beginselen moeten zonder onderscheid gelden voor alle

³ Verklaring van de Groep gegevensbescherming artikel 29 over encryptie en de gevolgen ervan voor de bescherming van personen met betrekking tot de verwerking van hun persoonsgegevens in de EU, 11 april 2018, beschikbaar op: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622229

⁴ Evenals de bijbehorende overwegingen (20aaaa en 21aa van het standpunt van de Raad).

⁵ Zoals de EDPB eerder heeft vermeld in de verklaring over de herziening van de e-privacyverordening, aangenomen op 25 mei 2018, beschikbaar op: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_nl.pdf en in de EDPB-richtsnoeren 5/2019 inzake toestemming overeenkomstig Verordening 2016/679, punt 39, beschikbaar op: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_nl.pdf

dienstverleners, ongeacht hun sector of hun huidige financieringsmodel (zie overweging 21aa van het standpunt van de Raad).

De publieksmeting is beperkt tot niet-intrusieve methoden die waarschijnlijk geen privacyrisico voor de gebruikers vormen

Het standpunt van de Raad voorziet in een nieuwe uitzondering voor publieksmeting zoals voorgesteld door de Groep gegevensbescherming artikel 29⁶. De door de Raad voorgestelde afwijking voor publieksmeting is echter te breed geformuleerd en zou kunnen leiden tot een overdreven brede interpretatie van wat onder de werkingssfeer van de afwijking zou kunnen vallen en daarmee tot een verlaging van het beschermingsniveau van de eindapparatuur van eindgebruikers.

De EDPB benadrukt derhalve dat de afwijking voor publieksmeting moet worden beperkt tot een analyse op laag niveau die nodig is om de verrichting van de door de gebruiker gevraagde dienst te analyseren en tot louter het verstrekken van statistische gegevens aan de aanbieder van de dienst. De analyse moet worden uitgevoerd door de aanbieder of diens verwerkers. Deze verwerking kan, op zichzelf of in combinatie met andere traceringsoplossingen, voor de aanbieder of andere verwerkingsverantwoordelijken dan ook geen aanleiding zijn om bepaalde gebruikers eruit te pikken of te profileren. Bovendien mag de publieksmetingsdienst niet toelaten dat navigatie-informatie over gebruikers wordt verzameld op verschillende websites/applicaties en moet deze een gebruikersvriendelijk mechanisme omvatten om af te zien van het verzamelen van gegevens.

Doeltreffende manier om toestemming voor websites en mobiele applicaties te verkrijgen (artikel 4 bis)

De EDPB is van oordeel dat de e-privacyverordening de huidige situatie moet verbeteren door de zeggenschap aan de gebruikers terug te geven en de “toestemmingsmoeheid” aan te pakken. Artikel 4 bis moet verder gaan en een verplichting bevatten om in browsers en besturingssystemen een gebruikersvriendelijk en effectief mechanisme op te nemen waarmee verwerkingsverantwoordelijken toestemming kunnen verkrijgen om een gelijk speelveld te creëren voor alle actoren. Het toepassingsgebied van de verordening moet ook uitdrukkelijk aanbieders van browsers en besturingssystemen omvatten.

De privacyinstellingen moeten het recht op bescherming van persoonsgegevens en de integriteit van de eindapparatuur van gebruikers standaard waarborgen en moeten het de gebruiker gemakkelijker maken om op vlotte, bindende en ten aanzien van alle partijen afdwingbare wijze toestemming te verlenen of in te trekken .

Verdere verwerking voor verenigbare doeleinden (artikel 6 quater en artikel 8, lid 1, punt g))

Met betrekking tot lopende besprekingen over de verdere verwerking van elektronische-communicatiemetagegevens/gegevens die via cookies en soortgelijke technologieën zijn verzameld, spreekt de EDPB nogmaals zijn steun uit voor de benadering van de e-privacyverordening zoals oorspronkelijk voorgesteld door de Europese Commissie en gevolgd door het Europees Parlement, waarbij wordt uitgegaan van een algemeen verbod, met beperkte uitzonderingen op basis van toestemming. Verdere verwerking voor verenigbare doeleinden brengt het risico met zich mee dat de door de e-privacyverordening geboden bescherming, met name voor de verwerking van elektronische-communicatiemetagegevens, wordt ondermijnd door verwerking toe te staan voor elk

⁶ Zie ook Advies 4/2012 over ontheffing van de toestemmingsverplichting voor cookies (WP 194), blz. 10-11. Beschikbaar op: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_nl.pdf

doel dat volgens de dienstverlener voldoet aan de “verenigbaarheidsclausule”, terwijl de wetgever duidelijk beoogde het gebruik ervan bij gebreke van toestemming te beperken tot specifieke doeleinden. De EDPB wenst te benadrukken dat de bovengenoemde gegevens nog verder kunnen worden verwerkt zonder toestemming en zonder risico’s voor de gebruikers nadat zij zijn geanonimiseerd.

Toekomstige rol van toezichthoudende autoriteiten, de EDPB en het samenwerkingsmechanisme (artikelen 18 tot en met 20)

De EDPB herinnert eraan dat om een gelijk speelveld op de digitale interne markt te garanderen, het van essentieel belang is om een geharmoniseerde interpretatie en handhaving van alle gegevensverwerkingsbepalingen van de e-privacyverordening in de hele EU te waarborgen.

Het toezicht op de privacybepalingen van de e-privacyverordening moet aan de bevoegde toezichthoudende autoriteiten in het kader van de AVG worden toevertrouwd ter verdere ondersteuning van de consistentie

De EDPB wil eraan herinneren dat er een duidelijke onderlinge koppeling van bevoegdheden is tussen nationale autoriteiten die op grond van de huidige e-privacyrichtlijn bevoegd zijn en gegevensbeschermingsautoriteiten. De bepalingen van de toekomstige e-privacyverordening in verband met de bescherming van de privacy mogen niet afzonderlijk worden toegepast, aangezien zij zijn verweven met de verwerking van persoonsgegevens en de AVG.

Om een hoog niveau van bescherming van persoonsgegevens en juridische en procedurele zekerheid met elkaar te verzoenen, moeten de voor de handhaving van de AVG verantwoordelijke nationale autoriteiten worden belast met het toezicht op de bepalingen van de toekomstige e-privacyverordening in verband met de verwerking van persoonsgegevens, zoals oorspronkelijk voorgesteld door de Europese Commissie⁷.

De EDPB merkt op dat, anders dan in het oorspronkelijke voorstel van de Europese Commissie, alle verwijzingen naar de samenwerkings- en consistentiemechanismen van hoofdstuk VII van de AVG in het standpunt van de Raad zijn verwijderd. Om de hierboven genoemde redenen herhaalt de EDPB dat alleen met een perfecte afstemming op het samenwerkings- en consistentiekader van de AVG de doelstellingen van de e-privacyverordening kunnen worden bereikt, fragmentatie bij de handhaving en toepassing van de verordening kan worden voorkomen en de last voor de aanbieders, die zich anders mogelijk tot meer dan 27 toezichthoudende autoriteiten zouden moeten wenden, beperkt kan worden gehouden.

Wanneer nationale bevoegde autoriteiten die geen lid zijn van de EDPB contact zouden moeten onderhouden met de EDPB, zoals momenteel is voorzien in het standpunt van de Raad, dan zou hun vermogen om tijdig bij te dragen aan een consistente toepassing van de e-privacyverordening worden aangetast ten nadele van zowel de digitale economie als de bescherming van de grondrechten.

Voor het Europees Comité voor gegevensbescherming

⁷ Voorstel van de Europese Commissie 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), 10 januari 2017, beschikbaar op: <https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A52017PC0010>, en het bijbehorende advies van de Groep gegevensbescherming artikel 29, beschikbaar op: https://ec.europa.eu/newsroom/document.cfm?doc_id=44103

De voorzitter

(Andrea Jelinek)

BIJLAGE: Lijst van eerdere documenten van de EDPB en de Groep gegevensbescherming artikel 29

-) Advies 1/2009 over de voorstellen tot wijziging van Richtlijn 2002/58/EG betreffende privacy en elektronische communicatie (e-privacyrichtlijn), beschikbaar op: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp159_nl.pdf
-) Advies 4/2012 over ontheffing van de toestemmingsverplichting voor cookies (WP 194), beschikbaar op: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_nl.pdf
-) Advies 3/2016 over de evaluatie en herziening van de e-privacyrichtlijn (WP 240), beschikbaar op https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=645254
-) Advies van de Groep gegevensbescherming artikel 29 over het 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), beschikbaar op: https://ec.europa.eu/newsroom/document.cfm?doc_id=44103
-) Verklaring van de Groep gegevensbescherming artikel 29 over encryptie en de gevolgen daarvan voor de bescherming van personen met betrekking tot de verwerking van hun persoonsgegevens in de EU, Brussel, 11 april 2018, beschikbaar op: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622229
-) Verklaring van de EDPB over de herziening van de e-privacyverordening en de gevolgen daarvan voor de bescherming van personen in verband met de privacy en de vertrouwelijkheid van hun communicatie, aangenomen op 25 mei 2018, beschikbaar op: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_nl.pdf
-) Verklaring 3/2019 van de EDPB over een e-privacyverordening, aangenomen op 13 maart 2019, beschikbaar op: https://edpb.europa.eu/sites/edpb/files/files/file1/201903_edpb_statement_eprivacyregulation_nl_0.pdf
-) Verklaring van de EDPB over de e-privacyverordening en de toekomstige rol van toezichhoudende autoriteiten en de EDPB, aangenomen op 19 november 2020, beschikbaar op: https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-eprivacy-regulation-and-future-role-supervisory_nl