EUROPESE
COMMISSIE

Brussel, 29.5.2019
COM(2019) 250 final

MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT EN DE RAAD

Richtsnoeren over de verordening inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie

Inhoudsopgave

De Europese Commissie heeft dit document louter ter informatie beschikbaar gesteld. Het bevat geen gezaghebbende interpretatie van Verordening (EU) 2018/1807 van het Europees Parlement en de Raad van 14 november 2018 inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie en vormt geen besluit of standpunt van de Europese Commissie. Het doet geen afbreuk aan een dergelijk besluit of standpunt van de Europese Commissie, noch aan de bevoegdheden van het Hof van Justitie van de Europese Unie om de verordening te interpreteren overeenkomstig de EU-verdragen.

1. Inleiding

In een steeds meer gegevensgestuurde economie staan gegevensstromen centraal in bedrijfsprocessen van ondernemingen van alle formaten en in alle sectoren. Nieuwe digitale technologieën bieden nieuwe mogelijkheden voor particulieren, ondernemingen en overheidsdiensten in de Europese Unie (hierna "de EU" genoemd).

Op basis van een voorstel van de Europese Commissie (hierna "de Commissie" genoemd) hebben het Europees Parlement en de Raad in november 2018 Verordening (EU) 2018/1807 inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie[1] (hierna "de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens" genoemd) vastgesteld om de grensoverschrijdende uitwisseling van gegevens verder uit te breiden en de gegevenseconomie te stimuleren. De verordening is van toepassing sinds 28 mei 2019. Het beginsel van vrij verkeer van persoonsgegevens is reeds vastgelegd in Verordening (EU) 2016/679 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 (hierna "de algemene verordening gegevensbescherming" genoemd)[2]. Als gevolg daarvan is er nu een alomvattend kader voor een gemeenschappelijke Europese gegevensruimte en het vrije verkeer van alle gegevens binnen de Europese Unie[3].

De verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens schept rechtszekerheid voor ondernemingen om hun gegevens te verwerken waar zij maar willen in de EU, versterkt het vertrouwen in gegevensverwerkingsdiensten en gaat praktijken die leiden tot afhankelijkheid van één aanbieder tegen. Dit zal de keuze voor de klant vergroten, de efficiëntie verbeteren en het gebruik van cloudtechnologieën stimuleren, wat aanzienlijke besparingen zal opleveren voor ondernemingen in de EU. Uit een studie blijkt dat ondernemingen in de EU 20 tot 50 % van hun IT-kosten kunnen besparen door naar de cloud te migreren[4].

Dankzij de twee verordeningen kunnen gegevens vrij circuleren tussen lidstaten, waardoor gebruikers van gegevensverwerkingsdiensten de op verschillende EU-markten verzamelde gegevens kunnen gebruiken om hun productiviteit te verhogen en hun concurrentievermogen te versterken. Gebruikers kunnen de door de grote EU-markt geboden schaalvoordelen dus ten

---

[1] Verordening (EU) 2018/1807 van het Europees Parlement en de Raad van 14 november 2018 inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie (PB L 303 van 28.11.2018, blz. 59).

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

[3] De algemene verordening gegevensbescherming is ook van toepassing in de Europese Economische Ruimte (EER), waartoe onder meer IJsland, Liechtenstein en Noorwegen behoren. Daarnaast is de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens aangemerkt als relevant voor de EER.

[4] Deloitte: *Measuring the economic impact of cloud computing in Europe* ("Meting van de economische effecten van cloudcomputing in Europa"), SMART 2014/0031, 2016. Online beschikbaar op: http://ec.europa.eu/newsroom/document.cfm?doc_id=41184.

volle benutten, waardoor hun concurrentiepositie in de wereld verbetert en de interconnectiviteit van de Europese gegevenseconomie wordt vergroot.

De verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens heeft drie bijzondere kenmerken:

- Zij verbiedt de lidstaten in de regel om gegevenslokalisatievereisten op te leggen. Uitzonderingen op deze regel kunnen alleen gerechtvaardigd zijn om redenen van openbare veiligheid in overeenstemming met het evenredigheidsbeginsel.
- Zij voorziet in een samenwerkingsmechanisme om ervoor te zorgen dat de bevoegde autoriteiten het recht op toegang tot gegevens die in een andere lidstaat worden verwerkt, kunnen blijven uitoefenen.
- Zij biedt stimulansen voor het bedrijfsleven, met ondersteuning van de Commissie, om zelfregulerende gedragscodes voor het veranderen van dienstverlener en gegevensportabiliteit op te stellen.

Doel van deze richtsnoeren

Met deze richtsnoeren wordt voldaan aan artikel 8, lid 3, van de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens, waarin is bepaald dat de Commissie richtsnoeren moet publiceren over de wisselwerking tussen deze verordening en de algemene verordening gegevensbescherming "wat betreft gegevenssets die bestaan uit zowel persoonsgegevens als niet-persoonsgebonden gegevens".

Deze richtsnoeren zijn bedoeld om gebruikers - met name kleine en middelgrote ondernemingen - inzicht te helpen krijgen in de wisselwerking tussen de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens en de algemene verordening gegevensbescherming[5]. De richtsnoeren zijn daarom met name gericht op: i) de begrippen "niet-persoonsgebonden gegevens" en "persoonsgegevens"; ii) de beginselen van vrij verkeer van gegevens en het verbod op gegevenslokalisatievereisten in het kader van beide verordeningen; en iii) het begrip "gegevensportabiliteit" in het kader van de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens. De richtsnoeren hebben ook betrekking op de vereisten inzake zelfregulering die in de twee verordeningen zijn vastgesteld.

De verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens heeft alleen betrekking op "andere gegevens dan persoonsgegevens" zoals gedefinieerd in de algemene verordening gegevensbescherming. De algemene verordening gegevensbescherming regelt de verwerking van persoonsgegevens, hetgeen een essentieel onderdeel van het EU-kader voor gegevensbescherming vormt[6]. De verordening is op 25 mei 2018 in werking getreden in de

[5] Overweging 37 van Verordening (EU) 2018/1807 van het Europees Parlement en de Raad van 14 november 2018 inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie.

[6]

– Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en

lidstaten. In de verordening zijn geharmoniseerde regels vastgesteld om burgers in de EU/EER te beschermen ten aanzien van de verwerking van hun persoonsgegevens en het vrije verkeer van dergelijke gegevens. De algemene verordening gegevensbescherming: i) specificeert welke gegevens persoonsgegevens zijn; ii) voorziet in wettelijke gronden voor de verwerking ervan; en iii) omschrijft de rechten en verplichtingen die in acht moeten worden genomen bij de verwerking van deze gegevens[7], naast andere bepalingen. Wat het beginsel van vrij verkeer van persoonsgegevens betreft, is in artikel 1, lid 3, van de algemene verordening gegevensbescherming het volgende bepaald: "Het vrije verkeer van persoonsgegevens in de Unie wordt noch beperkt noch verboden om redenen die verband houden met de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens."

In de praktijk is het zeer waarschijnlijk dat een gegevensset in de meeste gevallen zowel persoonsgegevens als niet-persoonsgebonden gegevens bevat. Dit wordt vaak een "gemengde gegevensset" genoemd. In het onderstaande punt 2.2 wordt nader ingegaan op de wisselwerking tussen de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens en de algemene verordening gegevensbescherming op het gebied van gemengde gegevenssets.

---

betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1).

– Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG (PB L 295 van 21.11.2018, blz. 39).

– Richtlijn (EU) 2016/680 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad (PB L 119 van 4.5.2016, blz. 89).

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

[7] Voor nadere richtsnoeren over diverse aspecten van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) en de Europese wetgeving inzake gegevensbescherming, zie de webpagina van het Europees Comité voor gegevensbescherming, dat overeenkomstig artikel 70 van de algemene verordening gegevensbescherming een aantal richtsnoeren heeft uitgebracht, beschikbaar op: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_nl. De desbetreffende webpagina bevat ook verwijzingen naar richtsnoeren, aanbevelingen en andere documenten die zijn verstrekt door de voorganger van het Europees Comité voor gegevensbescherming, de Groep artikel 29. Om burgers en ondernemingen meer bewust te maken van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), heeft de Commissie voorts een mededeling over gegevensbescherming uitgebracht - richtsnoeren voor de directe toepassing van de algemene verordening gegevensbescherming (COM(2018) 43 final), beschikbaar op: https://eur-lex.europa.eu/legal-content/NL/TXT/?qid=1517578296944&uri=CELEX%3A52018DC0043

Voor de duidelijkheid moet worden opgemerkt dat de algemene verordening gegevensbescherming en de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens geen tegenstrijdige verplichtingen bevatten.

2. Wisselwerking tussen de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens en de algemene verordening gegevensbescherming - gemengde gegevenssets

2.1 Het concept "niet-persoonsgebonden gegevens" in het kader van de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens

De verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens[8] heeft tot doel het vrije verkeer van andere gegevens dan persoonsgegevens te waarborgen. In de hele tekst van de verordening wordt de term "gegevens" gebruikt, die moet worden opgevat als "andere gegevens dan persoonsgegevens als gedefinieerd in artikel 4, punt 1, van Verordening (EU) 2016/679 [de algemene verordening gegevensbescherming]"[9]. Dergelijke gegevens, die in dit document ook "**niet-persoonsgebonden gegevens**" worden genoemd, zijn gedefinieerd als tegengesteld (*a contrario*) aan persoonsgegevens, zoals vastgesteld in de algemene verordening gegevensbescherming.

Persoonsgegevens

In de algemene verordening gegevensbescherming is het volgende bepaald: ""persoonsgegevens": alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;"

De definitie van persoonsgegevens is doelbewust ruim geformuleerd en is nagenoeg ongewijzigd gebleven in de algemene verordening gegevensbescherming ten opzichte van de eerdere wetgeving[10]. In Advies 4/2007 van 20 juni 2007 over het begrip persoonsgegevens

[8] Artikel 1 van Verordening (EU) 2018/1807 van het Europees Parlement en de Raad van 14 november 2018 inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie.

[9] Zie artikel 3, lid 1, van Verordening (EU) 2018/1807 van het Europees Parlement en de Raad van 14 november 2018 inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie.

[10] Zie artikel 2, onder a), van Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (einddatum geldigheid: 24 mei 2018, ingetrokken bij de algemene verordening gegevensbescherming). Zie ook de jurisprudentie van het Hof van Justitie inzake de definitie van persoonsgegevens, waarin de ruime interpretatie van een dergelijk begrip wordt erkend, bijvoorbeeld het arrest van het Hof van Justitie van 29 januari 2009, *Productores de Música de España (Promusicae)/Telefónica de España SAU*, C-275/06, ECLI:EU:C:2008:54; het arrest van het Hof van Justitie van 24 november 2011, *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-

(WP 136) is de Groep artikel 29[11] reeds ingegaan op verscheidene aspecten van de definitie van persoonsgegevens, zoals "alle informatie", "over" en "geïdentificeerde of identificeerbare".

Op gebieden zoals onderzoek is het gebruikelijk om persoonsgegevens te pseudonimiseren om iemands identiteit te verhullen. **Pseudonimisering** is de verwerking van persoonsgegevens op zodanige wijze dat deze niet meer aan een specifieke persoon kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt. Deze aanvullende gegevens worden apart bewaard en worden beveiligd door middel van organisatorische of technische maatregelen (bv. versleuteling)[12,13]. Gepseudonimiseerde gegevens worden echter nog steeds als gegevens over een identificeerbare persoon beschouwd indien deze aan de persoon in kwestie kunnen worden gekoppeld door aanvullende gegevens te gebruiken[14]. Dergelijke gegevens **zijn persoonsgegevens** in de zin van de algemene verordening gegevensbescherming.

Niet-persoonsgebonden gegevens

Wanneer de gegevens geen "persoonsgegevens" zijn in de zin van de algemene verordening gegevensbescherming, gaat het om **niet-persoonsgebonden gegevens**. De niet-persoonsgebonden gegevens kunnen aan de hand van hun oorsprong als volgt worden ingedeeld:

- Ten eerste: gegevens die oorspronkelijk geen betrekking hadden op een geïdentificeerde of identificeerbare natuurlijke persoon, zoals gegevens over weersomstandigheden die zijn verkregen door op windturbines geïnstalleerde sensoren of gegevens over de onderhoudsbehoeften van industriële machines.

70/10, ECLI:EU:C:2011:771; het arrest van het Hof van Justitie van 19 oktober 2016, *Patrick Breyer/Bundesrepublik Deutschland*, C-582/14, ECLI:EU:C:2016:779.

[11] De Groep artikel 29 was een adviesorgaan dat de Commissie adviseerde over gegevensbescherming en dat heeft bijgedragen tot de ontwikkeling van een geharmoniseerd beleid op het gebied van gegevensbescherming in de EU. Na de inwerkingtreding van de algemene verordening gegevensbescherming op 25 mei 2018 is de Groep artikel 29 vervangen door het Europees Comité voor gegevensbescherming.

[12] Zie de definitie van "pseudonimisering" in artikel 4, punt 5, van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

[13] In een onderzoek naar de effecten van een nieuw geneesmiddel zou het bijvoorbeeld als pseudonimisering worden aangemerkt indien de persoonsgegevens van de deelnemers aan het onderzoek worden vervangen door unieke aanduidingen (bv. nummer of code) in de onderzoeksdocumentatie en hun persoonsgegevens apart worden bewaard met de toegewezen unieke aanduidingen in een beveiligd document (bv. in een databank met wachtwoordbeveiliging).

[14] Zie overweging 26 van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

- Ten tweede: gegevens die in eerste instantie persoonlijke gegevens waren, maar daarna **anoniem**[15] zijn gemaakt. De "anonimisering" van persoonsgegevens is niet hetzelfde als pseudonimisering (zie hierboven), aangezien naar behoren geanonimiseerde gegevens niet aan een specifieke persoon kunnen worden gekoppeld, zelfs niet door aanvullende gegevens[16] te gebruiken, en derhalve niet-persoonsgebonden gegevens zijn.

Bij de beoordeling of de gegevens naar behoren zijn geanonimiseerd, moet rekening worden gehouden met de specifieke en unieke omstandigheden van elk afzonderlijk geval[17]. Verschillende voorbeelden van heridentificatie van zogenaamd geanonimiseerde gegevenssets hebben aangetoond dat een dergelijke evaluatie een moeilijke opgave kan zijn[18]. Om te bepalen of een persoon identificeerbaar is, moet worden gekeken naar alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door een verwerkingsverantwoordelijke of door een andere persoon om een persoon direct of indirect te identificeren[19].

Voorbeelden van niet-persoonsgebonden gegevens:

- Gegevens die zodanig zijn geaggregeerd dat afzonderlijke gebeurtenissen (zoals afzonderlijke reizen van een persoon naar het buitenland of reispatronen die persoonsgegevens kunnen vormen) niet meer identificeerbaar zijn, kunnen als anonieme gegevens worden aangemerkt[20]. Anonieme gegevens worden bijvoorbeeld

[15] Zie overweging 26 van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), waarin het volgende is bepaald: "De gegevensbeschermingsbeginselen dienen derhalve niet van toepassing te zijn op anonieme gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is."

[16] Zie het arrest van het Hof van Justitie van 19 oktober 2016, *Patrick Breyer*/*Bundesrepublik Deutschland*, C-582/14, ECLI:EU:C:2016:779. Het Hof van Justitie heeft geoordeeld dat dynamische internetprotocoladressen (IP-adressen) persoonsgegevens kunnen vormen, zelfs indien enkel een derde partij (bv. een internetprovider) over aanvullende gegevens beschikt die het mogelijk maken de persoon te identificeren. De mogelijkheid om de persoon te identificeren moet een middel vormen waarvan mag worden aangenomen dat het redelijkerwijs kan worden ingezet om de persoon direct of indirect te identificeren.

[17] Gegevens moeten altijd worden geanonimiseerd aan de hand van de nieuwste geavanceerde anonimiseringstechnieken.

[18] Voor voorbeelden van heridentifcatie van zogenaamd geanonimiseerde gegevens, zie de studie over toekomstige gegevensstromen die voor de Commissie ITRE van het Europees Parlement is uitgevoerd door Blackman, C., Forge, S.: *Data Flows — Future Scenarios: In-Depth Analysis for the ITRE Committee*, 2017, blz. 22, Vak 2. Online beschikbaar op: http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/607362/IPOL_IDA(2017)607362_EN.pdf

[19] Zie overweging 26 van Verordening (EU) 2016/679 van de algemene verordening gegevensbescherming, waarin het volgende is bepaald: "Om uit te maken of van middelen redelijkerwijs valt te verwachten dat zij zullen worden gebruikt om de natuurlijke persoon te identificeren, moet rekening worden gehouden met alle objectieve factoren, zoals de kosten van en de tijd benodigd voor identificatie, met inachtneming van de beschikbare technologie op het tijdstip van verwerking en de technologische ontwikkelingen."

[20] Zie bladzijde 9 van Advies 05/2014 van de Groep artikel 29 over anonimiseringstechnieken (WP 216), goedgekeurd op 10 april 2014: "Alleen als de verwerkingsverantwoordelijke de gegevens zou aggregeren tot een niveau waarop de afzonderlijke gebeurtenissen niet meer identificeerbaar zijn, kan de resulterende gegevensset als anoniem worden aangemerkt. Bijvoorbeeld: indien een organisatie gegevens over afzonderlijke reisbewegingen verzamelt, zouden de afzonderlijke reispatronen op het niveau van de gebeurtenissen nog steeds

voor statistieken of in verkoopverslagen gebruikt (bijvoorbeeld om de populariteit van een product en de kenmerken ervan te beoordelen).

- Met een hoge frequentie verstrekte handelsgegevens in de financiële sector, of gegevens over precisielandbouw die bijdragen tot de monitoring en optimalisering van het gebruik van pesticiden, nutriënten en water.

Wanneer niet-persoonsgebonden gegevens op enigerlei wijze aan een persoon kunnen worden gekoppeld, waardoor ze direct of indirect identificeerbaar zijn, moeten deze gegevens evenwel als persoonsgegevens worden beschouwd.

Als een kwaliteitscontroleverslag over een productielijn het bijvoorbeeld mogelijk maakt de gegevens aan specifieke fabrieksarbeiders te koppelen (bv. de arbeiders die de productieparameters bepalen), worden de gegevens als persoonsgegevens aangemerkt en moet de algemene verordening gegevensbescherming worden toegepast. Dezelfde regels zijn van toepassing wanneer ontwikkelingen op het gebied van technologie en gegevensanalyse het mogelijk maken om geanonimiseerde gegevens om te zetten in persoonsgegevens. [21]

Aangezien naar "natuurlijke personen" wordt verwezen in de definitie van persoonsgegevens, vormen gegevenssets met de namen en contactgegevens van rechtspersonen in beginsel niet-persoonsgebonden gegevens[22]. In bepaalde situaties kan het echter om persoonsgegevens gaan[23]. Dit is bijvoorbeeld het geval wanneer de naam van de rechtspersoon dezelfde is als die van een natuurlijke persoon die eigenaar is van de rechtspersoon of wanneer de informatie betrekking heeft op een geïdentificeerde of identificeerbare natuurlijke persoon[24].

---

worden aangemerkt als persoonsgegevens voor alle partijen, zolang de verwerkingsverantwoordelijke (of andere partij) nog steeds toegang heeft tot de oorspronkelijke ruwe gegevens, zelfs als de directe identificatoren zijn verwijderd van de aan derden verstrekte set. Maar als de verwerkingsverantwoordelijke de ruwe gegevens verwijdert en alleen [op hoog niveau] geaggregeerde statistieken aan derden [...] verstrekt, zoals "op traject X zijn er op maandagen 160 % meer passagiers dan op dinsdagen", zouden deze als anonieme gegevens worden aangemerkt."

[21] Indien persoonsgegevens onrechtmatig worden verwerkt of de verwerking in een ander opzicht in strijd is met de algemene verordening gegevensbescherming, hebben de betrokkenen (natuurlijke personen) krachtens de algemene verordening gegevensbescherming het recht om een klacht in te dienen bij een nationale toezichthoudende autoriteit (gegevensbeschermingsautoriteit) in de EU of om doeltreffende voorziening in rechte in te stellen bij een nationale rechterlijke instantie. De taken, competenties en bevoegdheden van de nationale toezichthoudende autoriteiten zijn geregeld in hoofdstuk VI, afdeling 2, van de algemene verordening gegevensbescherming.

[22] In overweging 14 van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) is het volgende bepaald: "Deze verordening heeft geen betrekking op de verwerking van gegevens over rechtspersonen en met name als rechtspersonen gevestigde ondernemingen, zoals de naam en de rechtsvorm van de rechtspersoon en de contactgegevens van de rechtspersoon." Dit moet evenwel in het licht van de definitie van persoonsgegevens van artikel 4, punt 1, van de algemene verordening gegevensbescherming worden gelezen.

[23] Zie het arrest van het Hof van Justitie van 9 november 2010 in gevoegde zaken *Volker und Markus Schecke GbR*, C-92/09 en *Hartmut Eifert*, C-93/09, /*Land Hessen*, ECLI:EU:C:2010:662, punt 52.

[24] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-data-protection-rules-apply-data-about-company_nl

2.2 Gemengde gegevenssets

De verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens en de algemene verordening gegevensbescherming benaderen het vrije verkeer van gegevens in de EU vanuit twee verschillende hoeken.

De verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens voorziet in een algemeen verbod op gegevenslokalisatievereisten voor niet-persoonsgebonden gegevens. Bij artikel 4, lid 1, van de verordening worden gegevenslokalisatievereisten verboden, tenzij deze gerechtvaardigd zijn om redenen van openbare veiligheid in overeenstemming met het evenredigheidsbeginsel.

De algemene verordening gegevensbescherming garandeert niet alleen een hoog niveau van bescherming van persoonsgegevens, maar zorgt er ook voor dat deze vrij kunnen circuleren. Overeenkomstig artikel 1, lid 3, van de verordening wordt het vrije verkeer van persoonsgegevens "noch beperkt noch verboden om redenen die verband houden met de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens." Samen voorzien de twee verordeningen in het vrije verkeer van "alle" gegevens binnen de EU. In de punten 3.1 en 3.2 wordt nader ingegaan op de specifieke bepalingen.

Een gemengde gegevensset bevat zowel persoonsgegevens als niet-persoonsgebonden gegevens. Het merendeel van de in de gegevenseconomie gebruikte gegevenssets is gemengd. Dergelijke sets komen vaak voor vanwege technologische ontwikkelingen zoals het internet der dingen (d.w.z. voorwerpen digitaal met elkaar verbinden), kunstmatige intelligentie en technologieën die de analyse van big data mogelijk maken.

Voorbeelden van gemengde gegevenssets:

- de fiscale gegevens van een onderneming, met vermelding van de naam en het telefoonnummer van de algemeen directeur van de onderneming;
- gegevenssets van een bank, met name die met informatie over klanten en transactiegegevens, zoals betalingsdiensten (krediet- en debetkaarten), aanvragen in het kader van partnerrelatiebeheer (partner relationship management — PRM) en leningsovereenkomsten, documenten met gemengde gegevens over natuurlijke en rechtspersonen;
- geanonimiseerde statistische gegevens van een onderzoeksinstelling en de aanvankelijk verzamelde ruwe gegevens, zoals de antwoorden van individuele respondenten op vragen in statistische enquêtes;
- de kennisdatabank van een onderneming met daarin IT-problemen en de oplossingen daarvoor op basis van individuele meldingen van IT-incidenten;
- gegevens met betrekking tot het internet der dingen, waarbij op basis van bepaalde gegevens veronderstellingen kunnen worden gemaakt over identificeerbare personen (bv. aanwezigheid op een bepaald adres en gebruikspatronen); en

- analyse van operationele loggegevens van productieapparatuur in de be- en verwerkende industrie.

Voorbeeld: diensten in het kader van klantrelatiebeheer

Sommige banken maken gebruik van door derden geleverde diensten in het kader van klantrelatiebeheer (customer relationship management — CRM), waarvoor de gegevens van een klant beschikbaar moeten worden gesteld in de CRM-omgeving. Tot de gegevens die nodig zijn voor de CRM-dienst behoort alle informatie die nodig is om de interactie met de klant doeltreffend te beheren, zoals hun postadres, e-mailadres, telefoonnummer, de producten en diensten die zij kopen, alsook verkoopverslagen, met inbegrip van geaggregeerde gegevens. Deze gegevens kunnen dus zowel persoonsgegevens als niet-persoonsgebonden gegevens omvatten.

Wat gemengde gegevenssets betreft, is in de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens[25] het volgende bepaald:

"Indien een gegevensset bestaat uit zowel persoonsgegevens als niet-persoonsgebonden gegevens is deze verordening van toepassing op het deel niet-persoonsgebonden gegevens van de gegevensset. Wanneer persoonsgegevens en niet-persoonsgebonden gegevens in een set onlosmakelijk met elkaar verbonden zijn, laat deze verordening de toepassing van Verordening (EU) 2016/679 onverlet."

Wanneer een gegevensset zowel uit persoonsgegevens als niet-persoonsgebonden gegevens bestaat, betekent dit dat:

- de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens van toepassing is op het deel niet-persoonsgebonden gegevens van de gegevensset;
- de bepaling in de algemene verordening gegevensbescherming over vrij verkeer[26] van toepassing is op het deel persoonsgegevens van de gegevensset; en
- indien het deel niet-persoonsgebonden gegevens en het deel persoonsgegevens "onlosmakelijk met elkaar verbonden" zijn, de uit de algemene verordening gegevensbescherming voortvloeiende rechten en verplichtingen inzake gegevensbescherming volledig van toepassing zijn op de volledige gemengde gegevensset, ook wanneer persoonsgegevens slechts een klein deel van de gegevensset uitmaken[27].

[25] Artikel 2, lid 2.

[26] Artikel 1, lid 3, van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming). Zie ook punt 3.2 van de onderhavige tekst.

[27] Zoals vermeld in het werkdocument van de diensten van de Commissie *Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union* ("Effectbeoordeling bij het voorstel

Deze interpretatie is in overeenstemming met het recht op bescherming van persoonsgegevens dat wordt gewaarborgd door het Handvest van de grondrechten van de Europese Unie[28] en met overweging 8 van de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens[29]. Overweging 8 van die verordening luidt als volgt: "Deze verordening doet geen afbreuk aan het rechtskader inzake de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens [...], en met name [de algemene verordening gegevensbescherming] en de Richtlijnen (EU) 2016/680 en 2002/58/EG [...]."

Praktisch voorbeeld:

Een onderneming die binnen de EU actief is, biedt haar diensten aan via een platform. Andere ondernemingen (klanten van die onderneming) uploaden hun documenten, die gemengde gegevenssets bevatten, op het platform. De ondernemingen die de documenten uploaden, moeten er als "verwerkingsverantwoordelijken" voor zorgen dat de verwerking voldoet aan de algemene verordening gegevensbescherming. Door de gegevensset namens de verwerkingsverantwoordelijken te verwerken, moet de onderneming die de diensten aanbiedt (de "verwerker") de gegevens opslaan en verwerken overeenkomstig de algemene verordening gegevensbescherming, bijvoorbeeld om ervoor te zorgen dat een passend beveiligingsniveau met betrekking tot gegevens wordt gewaarborgd, onder meer door middel van versleuteling.

Het begrip "onlosmakelijk met elkaar verbonden" is in geen van beide verordeningen gedefinieerd[30]. Concreet kan dit begrip naar een situatie verwijzen waarin een gegevensset zowel persoonsgegevens als niet-persoonsgebonden gegevens bevat en het scheiden van deze gegevens ofwel onmogelijk is, ofwel economisch inefficiënt of technisch onhaalbaar wordt geacht door de verwerkingsverantwoordelijke. Wanneer bijvoorbeeld systemen voor CRM en verkoopverslagen worden aangekocht, zou de onderneming dubbel moeten betalen voor software door aparte software aan te kopen voor CRM (persoonsgegevens) en systemen voor verkoopverslagen (geaggregeerde/niet-persoonsgebonden gegevens) op basis van de CRM-gegevens.

Een gegevensset zal waarschijnlijk ook aanzienlijk minder waarde hebben als deze wordt gescheiden. Door de veranderende aard van gegevens (zie punt 2.1) wordt het bovendien moeilijker om een duidelijk onderscheid te maken tussen verschillende categorieën gegevens, waardoor het ook moeilijker wordt om deze van elkaar te scheiden.

---

voor een verordening van het Europees Parlement en de Raad inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie") (SWD(2017) 304 final), deel 1/2, blz. 3, moet de algemene verordening gegevensbescherming volledig in acht worden genomen wat betreft het deel persoonsgegevens van de set, ongeacht hoeveel persoonsgegevens de gemengde gegevenssets bevatten.

[28] Handvest van de grondrechten van de Europese Unie (PB C 362 van 26.10.2012, blz. 391).

[29] Overweging 8.

[30] De verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens en de algemene verordening gegevensbescherming.

Belangrijk is dat geen van beide verordeningen ondernemingen verplicht om de door hen beheerde of verwerkte gegevenssets te scheiden.

Bijgevolg is een gemengde gegevensset over het algemeen aan de verplichtingen van verwerkingsverantwoordelijken en verwerkers onderworpen en moeten de uit de algemene verordening gegevensbescherming voortvloeiende rechten van de betrokkenen in acht worden genomen.

Verwerking van gezondheidsgegevens

Gezondheidsgegevens kunnen deel uitmaken van een gemengde gegevensset. Voorbeelden hiervan zijn elektronische patiëntendossiers, klinische proeven of gegevenssets die worden verzameld door diverse mobiele gezondheids- en welzijnsapps (zoals apps om onze gezondheidstoestand te meten, om ons eraan te herinneren dat we onze medicatie moeten innemen of om de vorderingen van onze conditie te volgen)[31]. Door de technologische ontwikkelingen wordt de exacte scheiding tussen persoonsgegevens en niet-persoonsgebonden gegevens in deze gegevenssets steeds vager. Bijgevolg moet de verwerking ervan in overeenstemming zijn met de algemene verordening gegevensbescherming, met name (aangezien gezondheidsgegevens een bijzondere categorie gegevens vormen overeenkomstig de verordening) met artikel 9, dat een algemeen verbod op de verwerking van bijzondere categorieën gegevens oplegt en in uitzonderingen op dit verbod voorziet.

De gegevens in gemengde gegevenssets die gezondheidsgegevens bevatten, kunnen een waardevolle bron van informatie zijn, bijvoorbeeld voor nader medisch onderzoek, voor het in kaart brengen van bijwerkingen van een voorgeschreven geneesmiddel, voor doeleinden op het gebied van statistieken over ziekten of voor de ontwikkeling van nieuwe gezondheidsdiensten of behandelingen. Bij de uitvoering van de eerste en daaropvolgende gegevensverwerkingsactiviteiten moet echter worden voldaan aan de voorschriften van de algemene verordening gegevensbescherming. Daarom moet een dergelijke verwerking van gezondheidsgegevens een geldige rechtsgrondslag[32] hebben en naar behoren worden gerechtvaardigd, beveiligd zijn en voldoende waarborgen bieden.

Tot slot is het voor particulieren en ondernemingen van essentieel belang om rechtszekerheid en vertrouwen in de verwerking van gegevens te hebben. Dit is ook cruciaal voor de gegevenseconomie. Beide verordeningen garanderen dit en streven er tegelijk ook naar het vrije verkeer van gegevens ongemoeid te laten.

---

[31] Voor de ontwikkeling en het gebruik van mobiele gezondheidsapps moeten de regels van de algemene verordening gegevensbescherming strikt worden nageleefd. Deze eisen zullen nader worden gespecificeerd in de gedragscode voor de bescherming van de persoonlijke levenssfeer op het gebied van mobiele gezondheidsapps, die momenteel wordt uitgewerkt. Voor meer informatie over de stand van zaken van de uitwerking, zie: https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps

[32] Zie artikel 6, lid 1, van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

3. Vrij verkeer van gegevens en intrekking van gegevenslokalisatievereisten

In dit punt wordt nader ingegaan op het begrip "gegevenslokalisatievereisten" in het kader van de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens en op het beginsel van vrij verkeer in de algemene verordening gegevensbescherming. Hoewel deze bepalingen voornamelijk voor de lidstaten zijn bedoeld, kan het nuttig zijn voor ondernemingen om een nauwkeuriger beeld te krijgen van de manier waarop deze twee verordeningen bijdragen tot het vrije verkeer van alle gegevens binnen de EU.

3.1 Vrij verkeer van niet-persoonsgebonden gegevens

In de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens[33] is het volgende bepaald: "Gegevenslokalisatievereisten zijn verboden, behalve wanneer zij in overeenstemming met het evenredigheidsbeginsel om redenen van openbare veiligheid gerechtvaardigd zijn."

Gegevenslokalisatievereisten worden gedefinieerd[34] als "elke verplichting, verbodsbepaling, voorwaarde, beperking die of ander vereiste dat is vastgelegd in de wettelijke en bestuursrechtelijke bepalingen van een lidstaat of voortvloeit uit een algemene en vaste publiekrechtelijke praktijk in een lidstaat en binnen publiekrechtelijke instellingen, ook op het gebied van overheidsopdrachten, onverminderd Richtlijn 2014/24/EU, die gegevensverwerking op het grondgebied van een welbepaalde lidstaat verplicht stelt of die gegevensverwerking in een andere lidstaat belemmert"[35].

De definitie toont aan dat de maatregelen die het vrije verkeer van gegevens binnen de EU beperken, verschillende vormen kunnen aannemen. Deze kunnen in wettelijke en bestuursrechtelijke bepalingen zijn vastgesteld of zelfs uit een algemene en vaste publiekrechtelijke praktijk voortvloeien. Bovendien geldt het verbod op gegevenslokalisatievereisten voor zowel directe als indirecte maatregelen die het vrije verkeer van niet-persoonsgebonden gegevens zouden beperken.

Bij **directe gegevenslokalisatievereisten** kan het bijvoorbeeld gaan om een verplichting om gegevens op een specifieke geografische locatie op te slaan (bv. servers moeten zich in een bepaalde lidstaat bevinden) of een verplichting om aan unieke nationale technische vereisten te voldoen (bv. gegevens verplicht in specifieke nationale formaten).

Indirecte gegevenslokalisatievereisten, die de verwerking van niet-persoonsgebonden gegevens in een andere lidstaat zouden belemmeren, kunnen verschillende vormen aannemen.

---

33 Artikel 4, lid 1.

34 Artikel 3, lid 5, van Verordening (EU) 2018/1807 van het Europees Parlement en de Raad van 14 november 2018 inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie.

35 Merk op dat de keuzevrijheid van marktdeelnemers en de overheid inzake de plaats waar gegevens worden verwerkt, verder wordt ingeperkt door rechtsonzekerheid over de reikwijdte van al dan niet legitieme gegevenslokalisatievereisten (zie overweging 4 van Verordening (EU) 2018/1807 van het Europees Parlement en de Raad van 14 november 2018 inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie).

Hierbij kan het gaan om vereisten inzake het verplicht gebruik van technologische voorzieningen die in een bepaalde lidstaat zijn gecertificeerd of goedgekeurd of andere vereisten die tot gevolg hebben dat het moeilijker wordt om gegevens buiten een specifiek geografisch gebied of grondgebied binnen de Europese Unie te verwerken[36,37].

Bij de beoordeling of een specifieke maatregel een indirecte gegevenslokalisatievereiste vormt, moet rekening worden gehouden met de specifieke omstandigheden van elk geval.

In de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens[38] wordt verwezen naar het begrip "**openbare veiligheid**" zoals uiteengezet in de jurisprudentie van het Hof van Justitie van de Europese Unie. De openbare veiligheid "omvat zowel de interne als de externe veiligheid van een lidstaat[39], alsmede vraagstukken in verband met de openbare veiligheid, met name om ruimte te bieden voor onderzoek, opsporing en vervolging van strafbare feiten. Het veronderstelt dat er sprake is van een reële en voldoende ernstige bedreiging voor een van de fundamentele belangen van de samenleving[40], zoals een bedreiging voor het functioneren van de instellingen en de essentiële openbare diensten en voor het overleven van de bevolking, het risico van een ernstige verstoring van de externe betrekkingen of van de vreedzame co-existentie van de volkeren, alsook de aantasting van militaire belangen."

Daarnaast moet een om redenen van openbare veiligheid gerechtvaardigde gegevenslokalisatievereiste evenredig zijn. Volgens de jurisprudentie van het Hof van Justitie van de Europese Unie vereist het evenredigheidsbeginsel dat de getroffen maatregelen geschikt zijn om de nagestreefde doelstelling te verwezenlijken en niet verder gaan dan voor dat doel nodig is[41].

---

[36] Overweging 4 van Verordening (EU) 2018/1807 van het Europees Parlement en de Raad van 14 november 2018 inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie.

[37] Zie twee studies over gegevenslokalisatievereisten die zijn uitgevoerd vóór de vaststelling van de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens: 1) Godel, M. et al.: *Facilitating cross border data flows in the Digital Single Market* ("Grensoverschrijdende gegevensstromen in de digitale eengemaakte markt vergemakkelijken"), SMART-nummer 2015/2016. Online beschikbaar op: http://ec.europa.eu/newsroom/document.cfm?doc_id=41185 en 2) Time.lex, Spark Legal Network en Tech4i2: *Cross-border data flow in the digital single market: study on data localisation restrictions* ("Grensoverschrijdende gegevensstromen in de digitale eengemaakte markt: studie over gegevenslokalisatiebeperkingen"). SMART-nummer 2015/0054. Online beschikbaar op: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=46695

[38] Overweging 19.

[39] Zie bijvoorbeeld het arrest van het Hof van Justitie van 23 november 2010, *Land Baden-Württemberg/Tsakouridis*, C-145/09, ECLI:EU:C:2010:708, punt 43 en het arrest van 4 april 2017, *Sahar Fahimian/Bundesrepublik Deutschland*, C-544/15, ECLI:EU:C:2017:225, punt 39.

[40] Zie bijvoorbeeld het arrest van het Hof van Justitie van 22 december 2008, *Commissie van de Europese Gemeenschappen/Republiek Oostenrijk*, C-161/07, ECLI:EU:C:2008:759, punt 35 en de daarin aangehaalde jurisprudentie en het arrest van 26 maart 2009, *Commissie van de Europese Gemeenschappen/Italiaanse Republiek*, C-326/07, ECLI:EC:C:2009:193, punt 70 en de daarin aangehaalde jurisprudentie.

[41] Zie bijvoorbeeld het arrest van het Hof van Justitie van 8 juli 2010, *Afton Chemical Limited/Secretary of State for Transport*, C-343/09, ECLI:EU:C:2010:419, punt 45 en de daarin aangehaalde jurisprudentie.

Voor de duidelijkheid moet worden opgemerkt dat het verbod op gegevenslokalisatievereisten geen afbreuk doet aan reeds bestaande beperkingen waarin het EU-recht voorziet[42].

Bovendien voorziet de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens niet in verplichtingen voor ondernemingen of legt deze geen beperkingen op aan hun contractuele vrijheid om te beslissen waar hun gegevens zullen worden verwerkt.

De lidstaten moeten de details van de gegevenslokalisatievereisten die op hun grondgebied van toepassing zijn voor het publiek beschikbaar maken door middel van een **centraal nationaal online-informatiepunt** (nationale websites). Zij moeten dit punt actueel houden of een overeenkomstig een andere Uniehandeling ingesteld centraal informatiepunt van actuele informatie voorzien[43]. De Commissie zal links naar deze informatiepunten op het Uw Europa-portaal[44] publiceren om ervoor te zorgen dat ondernemingen gemakkelijk toegang hebben tot relevante informatie in de hele EU.

3.2 Vrij verkeer van persoonsgegevens

In de algemene verordening gegevensbescherming[45] is het volgende bepaald: "Het vrije verkeer van persoonsgegevens in de Unie wordt noch beperkt noch verboden om redenen die verband houden met de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens."

Wanneer een lidstaat lokalisatievereisten oplegt aan persoonsgegevens om andere redenen dan de bescherming van persoonsgegevens, moeten deze redenen worden getoetst aan de bepalingen inzake de fundamentele vrijheden en de toegestane gronden om van die vrijheden af te wijken in het Verdrag betreffende de werking van de Europese Unie[46,47] en de

---

[42] Zie bijvoorbeeld artikel 245, lid 2, van Richtlijn 2006/112/EG van 28 november 2006 betreffende het gemeenschappelijke stelsel van belasting over de toegevoegde waarde, waarin het volgende is bepaald: "De lidstaten kunnen de op hun grondgebied gevestigde belastingplichtigen verplichten tot kennisgeving van de plaats van bewaring wanneer deze buiten hun grondgebied gelegen is." Deze vereiste moet echter in samenhang met artikel 249 worden gelezen, waarin het volgende is bepaald: "Wanneer een belastingplichtige de door hem verzonden of ontvangen facturen elektronisch bewaart waarbij een on-linetoegang tot de gegevens wordt gewaarborgd, en de plaats van bewaring in een andere lidstaat gelegen is dan de lidstaat waar hij is gevestigd, hebben de bevoegde autoriteiten van de lidstaat waar deze belastingplichtige gevestigd is met het oog op de toepassing van deze richtlijn het recht van elektronische toegang tot alsmede downloading en gebruik van deze facturen binnen de grenzen bepaald bij de regelgeving van de lidstaat van vestiging van de belastingplichtige, en voor zover deze lidstaat de facturen nodig heeft voor controledoeleinden."

[43] Artikel 4, lid 4, van Verordening (EU) 2018/1807 van het Europees Parlement en de Raad van 14 november 2018 inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie.

[44] https://europa.eu/youreurope/index.htm

[45] Artikel 1, lid 3, van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

[46] Geconsolideerde versie van het Verdrag betreffende de werking van de Europese Unie (PB C 326 van 26.10.2012, blz. 47).

[47] Zie ook het arrest van het Hof van Justitie van 19 juni 2008, *Commissie van de Europese Gemeenschappen*/*Groothertogdom Luxemburg*, C-319/06, ECLI:EU:C:2008:350, punten 90-91: het Hof heeft geoordeeld dat een verplichting om bepaalde documenten ter beschikking te houden en te bewaren in een bepaalde lidstaat een beperking van het vrij verrichten van diensten vormt; een rechtvaardiging dat "de

desbetreffende EU-wetgeving, zoals de dienstenrichtlijn[48] en de richtlijn inzake elektronische handel[49].

Voorbeeld:

In een nationale wet is bepaald dat salarisrekeningen zich in een bepaalde lidstaat moeten bevinden om redenen in verband met de controle op de naleving van de regelgeving, bijvoorbeeld door de nationale belastingdienst. Een dergelijke nationale bepaling zou buiten het toepassingsgebied van artikel 1, lid 3, van de algemene verordening gegevensbescherming vallen omdat het om andere redenen dan de bescherming van persoonsgegevens gaat. In plaats daarvan zou deze vereiste moeten worden getoetst aan de bepalingen inzake de fundamentele vrijheden en de toegestane gronden om van die vrijheden af te wijken in het Verdrag betreffende de werking van de Europese Unie.

In de algemene verordening gegevensbescherming[50] wordt erkend dat de lidstaten voorwaarden, waaronder beperkingen, kunnen opleggen ten aanzien van de verwerking van genetische gegevens, biometrische gegevens of gezondheidsgegevens. Zoals aangegeven in overweging 53 mogen dergelijke nationale beperkingen evenwel geen belemmering vormen voor het vrije verkeer van persoonsgegevens binnen de EU wanneer deze voorwaarden van toepassing zijn op de grensoverschrijdende verwerking van deze gegevens. Dit is in overeenstemming met artikel 16 van het Verdrag betreffende de werking van de Europese Unie, dat de rechtsgrondslag vormt voor de vaststelling van voorschriften betreffende het recht op bescherming van persoonsgegevens en de voorschriften betreffende het vrij verkeer van die gegevens.

3.3 Toepassingsgebied van de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens

Zoals reeds vermeld heeft de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens tot doel het vrije verkeer van niet-persoonsgebonden gegevens "binnen de Unie" te waarborgen[51]. De verordening is derhalve niet van toepassing op verwerkingsactiviteiten die

vervulling van de toezichthoudende taak van de autoriteiten in het algemeen wordt vergemakkelijkt" is niet voldoende.

[48] Richtlijn 2006/123/EG van het Europees Parlement en de Raad van 12 december 2006 betreffende diensten op de interne markt (PB L 376 van 27.12.2006, blz. 36).

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

[50] Artikel 9, lid 4, van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

[51] Zie artikel 1 van Verordening (EU) 2018/1807 van het Europees Parlement en de Raad van 14 november 2018 inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie.

buiten de EU worden verricht en evenmin op de met die verwerking verband houdende gegevenslokalisatievereisten[52,53].

Overeenkomstig artikel 2, lid 1, is het toepassingsgebied van de verordening derhalve beperkt tot de verwerking van elektronische niet-persoonsgebonden gegevens in de EU die:

(a) als dienst wordt verleend aan gebruikers die in de EU verblijven of er een vestiging hebben, ongeacht of de dienstverlener in de EU is gevestigd, of
(b) wordt verricht door een natuurlijke persoon of een rechtspersoon die in de EU verblijft of er een vestiging heeft, voor eigen intern gebruik.

Voorbeelden:

Artikel 2, lid 1, onder a), van de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens:

- Een in de VS gevestigde verlener van clouddiensten verleent zijn verwerkingsdiensten aan in de EU verblijvende of gevestigde klanten. De verlener van clouddiensten verricht zijn activiteiten via servers die zich op het grondgebied van de EU bevinden, waarop de gegevens van zijn Europese klanten worden opgeslagen of anderszins verwerkt. De verlener van clouddiensten hoeft geen in de EU gevestigde infrastructuur te bezitten, maar kan bijvoorbeeld ook serverruimte in de EU huren. De verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens is van toepassing op dergelijke gegevensverwerking.
- Een in Japan gevestigde verlener van clouddiensten biedt zijn diensten aan Europese klanten aan. De verwerkingscapaciteiten van de verlener bevinden zich in Japan en alle verwerkingsactiviteiten worden daar verricht. De verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens is niet van toepassing in dit geval omdat alle verwerkingsactiviteiten buiten de EU worden verricht[54].

[52] Zie overweging 15 van Verordening (EU) 2018/1807 van het Europees Parlement en de Raad van 14 november 2018 inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie.

[53] De term "verwerking" is ruim gedefinieerd (artikel 3, lid 2, van Verordening (EU) 2018/1807 van het Europees Parlement en de Raad van 14 november 2018 inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie) en, zoals benadrukt in overweging 17, moet de verordening van toepassing zijn op verwerking in de ruimst mogelijke zin en het gebruik van alle soorten IT-systemen omvatten.

[54] Merk op dat Verordening (EU) 2018/1807 van het Europees Parlement en de Raad van 14 november 2018 inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie geen betrekking heeft op door de lidstaten opgelegde gegevenslokalisatievereisten inzake de opslag van niet-persoonsgebonden gegevens in derde landen en dat deze vereisten in nationale wetgeving kunnen zijn opgenomen. Voor de duidelijkheid moet worden opgemerkt dat de algemene verordening gegevensbescherming van toepassing is op de verwerking van persoonsgegevens van betrokkenen die zich in de EU bevinden, door een niet in de EU gevestigde verwerkingsverantwoordelijke of verwerker, wanneer de verwerkingsactiviteiten verband houden met: a) het aanbieden van goederen of diensten aan deze betrokkenen in de Unie, ongeacht of een betaling door de betrokkenen is vereist; of b) het monitoren van hun gedrag, voor zover dit gedrag in de Unie plaatsvindt (zie artikel 3, lid 2, van de algemene verordening gegevensbescherming).

Artikel 2, lid 1, onder b), van de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens:

- Een kleine Europese start-up uit lidstaat A besluit om zijn activiteiten uit te breiden door een vestiging te openen in lidstaat B. Om de kosten zo laag mogelijk te houden, kiest deze start-up ervoor de gegevensopslag en -verwerking van de nieuwe vestiging te centraliseren op zijn server die zich in lidstaat A bevindt. De lidstaten mogen dergelijke inspanningen om IT te centraliseren niet verbieden, behalve wanneer dit gerechtvaardigd is om redenen van openbare veiligheid in overeenstemming met het evenredigheidsbeginsel.

Hoewel de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens niet van toepassing is wanneer alle verwerkingsactiviteiten voor niet-persoonsgebonden gegevens buiten de EU worden verricht, moet de algemene verordening gegevensbescherming worden nageleefd wanneer persoonsgegevens deel uitmaken van de gegevensset. Met name de regels voor de doorgifte van persoonsgegevens aan derde landen of internationale organisaties in het kader van de algemene verordening gegevensbescherming moeten te allen tijde worden nageleefd[55].

3.4 Activiteiten in verband met de interne organisatie van de lidstaten

De verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens verplicht de lidstaten niet om de verlening van diensten met betrekking tot niet-persoonsgebonden gegevens die zij zelf willen verlenen, uit te besteden of anders dan via overheidsopdrachten te regelen[56].

Artikel 2, lid 3, tweede alinea, van de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens luidt als volgt:

"Deze verordening doet geen afbreuk aan de wettelijke en bestuursrechtelijke bepalingen die verband houden met **de interne organisatie** van de lidstaten, waarbij de bevoegdheden en verantwoordelijkheden voor **gegevensverwerking** worden verdeeld onder of toegekend aan overheidsinstanties of publiekrechtelijke instellingen als gedefinieerd in artikel 2, lid 1, punt 4, van Richtlijn 2014/24/EU[57] **zonder contractuele vergoeding van particuliere**

[55] Voor informatie over de doorgifte van persoonsgegevens aan derde landen, zie de website van de Commissie: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_nl en de *Mededeling van de Commissie aan het Europees Parlement en de Raad — Uitwisseling en bescherming van persoonsgegevens in een geglobaliseerde wereld*, COM(2017) 7 final, beschikbaar op: https://eur-lex.europa.eu/legal-content/NL/ALL/?uri=CELEX:52017DC0007. Op 23 januari 2019 heeft de Commissie het adequaatheidsbesluit met betrekking tot Japan vastgesteld. Daardoor kunnen persoonsgegevens, beschermd door sterke waarborgen, vrij tussen de EU en Japan worden uitgewisseld.

[56] Overweging 14 van Verordening (EU) 2018/1807 van het Europees Parlement en de Raad van 14 november 2018 inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie.

[57] Artikel 2, lid 1, punt 4, van Richtlijn 2014/24/EU van het Europees Parlement en de Raad van 26 februari 2014 betreffende het plaatsen van overheidsopdrachten en tot intrekking van Richtlijn 2004/18/EG (PB L 94 van 28.3.2014, blz. 65) luidt als volgt: ""publiekrechtelijke instellingen": instellingen die voldoen aan

partijen, en doet evenmin afbreuk aan de wettelijke en bestuursrechtelijke bepalingen van de lidstaten die voorzien in de toepassing van die bevoegdheden en verantwoordelijkheden."[58]

Er kunnen legitieme redenen zijn om ervoor te kiezen gegevensverwerkingsdiensten zelf te verlenen, onder meer door middel van "inbesteding" of onderlinge afspraken tussen overheidsdiensten. Typische voorbeelden zijn het gebruik van een "overheidscloud" of een overheid die een centraal IT-agentschap aanstelt om gegevensverwerkingsdiensten te verlenen voor overheidsinstellingen en -organen.

In de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens worden de lidstaten evenwel aangespoord om de economische efficiëntie en andere voordelen van uitbesteding aan externe dienstverleners in overweging te nemen[59,60]. Zodra de nationale autoriteiten beginnen met de "uitbesteding" van gegevensverwerking waarbij de prestaties van particuliere partijen contractueel worden vergoed en de verwerking in de EU plaatsvindt, valt deze verwerking onder de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens, wat betekent dat het beginsel van vrij verkeer van niet-persoonsgebonden gegevens van toepassing is op de algemene en publiekrechtelijke praktijken van de nationale autoriteiten. Zij mogen met name geen gegevenslokalisatiebeperkingen opleggen, bijvoorbeeld in aanbestedingen voor overheidsopdrachten[61].

4. Zelfreguleringsbenaderingen die het vrije verkeer van gegevens ondersteunen

Zelfregulering draagt bij tot innovatie en versterkt het vertrouwen van marktdeelnemers. Daarnaast kan hiermee beter worden ingespeeld op marktontwikkelingen. Dit punt biedt een overzicht van zelfreguleringsinitiatieven voor de verwerking van zowel persoonsgegevens als niet-persoonsgebonden gegevens.

---

alle volgende kenmerken: a) zij zijn opgericht voor het specifieke doel te voorzien in andere behoeften van algemeen belang dan die van industriële of commerciële aard; b) zij bezitten rechtspersoonlijkheid, en c) zij worden merendeels door de staats-, regionale of lokale overheidsinstanties of andere publiekrechtelijke lichamen gefinancierd, of hun beheer staat onder toezicht van deze instanties of lichamen, of zij hebben een bestuurs-, leidinggevend of toezichthoudend orgaan waarvan de leden voor meer dan de helft door de staat, de regionale of lokale overheidsinstanties of andere publiekrechtelijke instellingen zijn aangewezen;".

[58] In overweging 13 van Verordening (EU) 2018/1807 van het Europees Parlement en de Raad van 14 november 2018 inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie wordt erop gewezen dat de verordening geen afbreuk doet aan Richtlijn 2014/24/EU.

[59] Overweging 14 van Verordening (EU) 2018/1807 van het Europees Parlement en de Raad van 14 november 2018 inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie.

[60] Een externe dienstverlener is een entiteit die geen "publiekrechtelijke instelling" is in de zin van artikel 2, lid 1, punt 4, van Richtlijn 2014/24/EU van het Europees Parlement en de Raad van 26 februari 2014 betreffende het plaatsen van overheidsopdrachten en tot intrekking van Richtlijn 2004/18/EG (PB L 94 van 28.3.2014, blz. 65).

[61] Overweging 13 van Verordening (EU) 2018/1807 van het Europees Parlement en de Raad van 14 november 2018 inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie.

4.1 Gegevens overdragen en van verlener van clouddiensten veranderen

De verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens heeft onder meer tot doel praktijken die leiden tot afhankelijkheid van één aanbieder te voorkomen. Er is sprake van dergelijke praktijken wanneer gebruikers niet van dienstverlener kunnen veranderen omdat hun gegevens "geblokkeerd" zijn in het systeem van de aanbieder, bijvoorbeeld als gevolg van een specifiek gegevensformaat of contractuele regelingen, en niet buiten het IT-systeem van de verlener kunnen worden overgedragen. Gegevens overdragen zonder belemmeringen is belangrijk om gebruikers in staat te stellen vrij te kiezen tussen verleners van gegevensverwerkingsdiensten en aldus voor daadwerkelijke concurrentie op de markt te zorgen.

Gegevensoverdraagbaarheid (ook gegevensportabiliteit genoemd) tussen ondernemingen wordt steeds belangrijker voor een breed scala aan digitale sectoren, waaronder clouddiensten.

Volgens artikel 6 van de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens moet de Commissie het opstellen van zelfregulerende gedragscodes op EU-niveau ("gedragscodes") bevorderen en faciliteren, om bij te dragen aan een concurrerende gegevenseconomie. Het artikel biedt het bedrijfsleven de basis voor de ontwikkeling van zelfregulerende gedragscodes voor het veranderen van dienstverlener en het overdragen van gegevens tussen verschillende IT-systemen.

Bij de ontwikkeling van dergelijke gedragscodes voor het overdragen van gegevens moet rekening worden gehouden met een aantal aspecten, met name:

- **beste praktijken** ter vergemakkelijking van het veranderen van dienstverlener en gegevensportabiliteit in een gestructureerde, algemeen gangbare en machineleesbare vorm;
- **minimale informatievereisten** om ervoor te zorgen dat professionele gebruikers voor de sluiting van een overeenkomst voldoende gedetailleerde en duidelijke informatie krijgen over de toepasselijke processen, technische vereisten, termijnen en kosten wanneer professionele gebruikers van dienstverlener willen veranderen of gegevens terug naar hun eigen IT-systemen willen overdragen;
- **benaderingen van certificeringsregelingen** om clouddiensten beter met elkaar te vergelijken; en
- **stappenplannen voor communicatie** teneinde de gedragscodes onder de aandacht te brengen.

Op de markt voor clouddiensten is de Commissie begonnen met het vergemakkelijken van de werkzaamheden van de werkgroepen van belanghebbenden uit de sector van clouddiensten in de digitale eengemaakte markt, waarin deskundigen op het gebied van clouddiensten en professionele gebruikers, met inbegrip van kleine en middelgrote ondernemingen, zijn samengebracht. In dit stadium is een subgroep bezig met de ontwikkeling van zelfregulerende gedragscodes voor het overdragen van gegevens en het veranderen van verlener van

clouddiensten (werkgroep SWIPO)[62] en werkt een andere subgroep aan de ontwikkeling van cloudbeveiligingscertificering (werkgroep CSPCERT)[63].

De werkgroep SWIPO is bezig met de ontwikkeling van gedragscodes voor het hele spectrum van clouddiensten, namelijk Infrastructuur als dienst (Infrastructure as a Service — IaaS), Platform als dienst (Platform as a Service — PaaS) en Software als dienst (Software as a Service — SaaS).

De Commissie verwacht dat de verschillende gedragscodes zullen worden aangevuld met **contractuele modelbepalingen**[64]. Dit zal voldoende technische en juridische specificiteit bieden bij de praktische uitvoering en toepassing van de gedragscodes, hetgeen van bijzonder belang zal zijn voor kleine en middelgrote ondernemingen. Volgens de planning zullen de contractuele modelbepalingen worden opgesteld nadat de gedragscodes zijn ontwikkeld (hetgeen uiterlijk op 29 november 2019 moet zijn afgerond).

Overeenkomstig artikel 8 van de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens zal de Commissie de tenuitvoerlegging van de verordening uiterlijk op 29 november 2022 evalueren. Dit zal het mogelijk maken de volgende punten te beoordelen: i) het effect op het vrije verkeer van gegevens in Europa; ii) de toepassing van de verordening, met name wat gemengde gegevenssets betreft; iii) de mate waarin de lidstaten bestaande, ongerechtvaardigde gegevenslokalisatiebeperkingen daadwerkelijk hebben ingetrokken; en iv) de markteffectiviteit van gedragscodes op het gebied van gegevensoverdracht en het veranderen van verlener van clouddiensten.

Het begrip "overdraagbaarheid" (ook portabiliteit genoemd) en de wisselwerking met de algemene verordening gegevensbescherming

In beide verordeningen[65] wordt verwezen naar gegevensoverdraagbaarheid en de doelstelling om het gemakkelijker te maken om gegevens van de ene IT-omgeving naar de andere over te dragen, d.w.z. naar de systemen van een andere aanbieder of naar systemen ter plaatse. Hiermee wordt de afhankelijkheid van één aanbieder voorkomen en wordt de concurrentie tussen dienstverleners bevorderd. De verordeningen hanteren echter een verschillende benadering ten aanzien van overdraagbaarheid als het gaat om de verhouding tussen de doelgroepen van belanghebbenden en de juridische aard van de bepalingen.

62 De werkgroep voor het veranderen van verlener van clouddiensten en het overdragen van gegevens.

63 De werkgroep voor de Europese certificering van verleners van clouddiensten. Zie ook punt 4.3.

64 Zie overweging 30 van Verordening (EU) 2018/1807 van het Europees Parlement en de Raad van 14 november 2018 inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie.

65 Artikel 6 van Verordening (EU) 2018/1807 van het Europees Parlement en de Raad van 14 november 2018 inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie en artikel 20 van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

Het recht op overdraagbaarheid van persoonsgegevens uit hoofde van artikel 20 van de algemene verordening gegevensbescherming is gericht op de verhouding tussen de betrokkene en de verwerkingsverantwoordelijke. Het gaat om het recht van de betrokkene om de persoonsgegevens die hij of zij aan een verwerkingsverantwoordelijke heeft verstrekt, in een gestructureerde, gangbare en machineleesbare vorm te verkrijgen, en het recht die gegevens aan een andere verwerkingsverantwoordelijke over te dragen, zonder daarbij te worden gehinderd door de verwerkingsverantwoordelijke aan wie de persoonsgegevens waren verstrekt[66]. De betrokkenen in deze verhouding zijn doorgaans consumenten van diverse onlinediensten die van dienstverlener willen veranderen.

Artikel 6 van de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens verleent het recht op gegevensportabiliteit niet aan professionele gebruikers, maar hanteert een zelfreguleringsbenadering, met vrijwillige gedragscodes voor het bedrijfsleven. Tegelijkertijd is het gericht op een situatie waarin een professionele gebruiker de verwerking van zijn gegevens heeft uitbesteed aan een derde die een gegevensverwerkingsdienst aanbiedt[67]. Overeenkomstig artikel 3, lid 8, van de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens kan het bij een "professionele gebruiker" gaan om "een natuurlijke of rechtspersoon, met inbegrip van een openbaar lichaam of een publiekrechtelijke instelling, die gebruikmaakt van of verzoekt om een gegevensverwerkingsdienst voor zijn handel, bedrijf, ambacht, beroep of taak."

In de praktijk gaat het bij de portabiliteit uit hoofde van artikel 6 van de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens om business-to-business-interacties tussen een professionele gebruiker (die overeenkomstig de algemene verordening gegevensbescherming als "verwerkingsverantwoordelijke" kan worden aangemerkt in gevallen waarin persoonsgegevens worden verwerkt) en een dienstverlener (die in sommige gevallen evenzo als "verwerker" kan worden aangemerkt).

Ondanks de verschillen kunnen zich situaties voordoen waarin de overdracht van gegevens zowel onder de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens als de algemene verordening gegevensbescherming zou vallen wat gemengde gegevenssets betreft.

Voorbeeld:

Een onderneming die gebruikmaakt van een clouddienst besluit om van verlener van clouddiensten te veranderen en alle gegevens over te dragen naar een nieuwe verlener. Het veranderen van dienstverlener en de overdracht van gegevens worden geregeld in het contract

[66] Zie de richtsnoeren van Groep artikel 29 over het recht op overdraagbaarheid van gegevens (WP 242 rev.01) (*Guidelines on the right to data portability*), aangenomen op 13 december 2016, zoals laatstelijk herzien en aangenomen op 5 april 2017.

[67] Overweging 29 van Verordening (EU) 2018/1807 van het Europees Parlement en de Raad van 14 november 2018 inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie vermeldt: "Terwijl individuele consumenten beter zijn geworden van het bestaande Unierecht [d.w.z. de algemene verordening gegevensbescherming], is het voor zakelijke of professionele gebruikers niet gemakkelijker om van dienstverlener te veranderen."

tussen de klant en de verlener van clouddiensten. Als de oude verlener van clouddiensten zich aan de gedragscodes houdt die in het kader van de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens zijn ontwikkeld, moeten de gegevens overeenkomstig de daarin gespecificeerde vereisten worden overgedragen.

Indien de persoonsgegevens ook deel uitmaken van de overgedragen gegevenssets, moet de overdracht aan alle relevante bepalingen van de algemene verordening gegevensbescherming voldoen, met name door ervoor te zorgen dat de nieuwe verlener van clouddiensten voldoet aan de toepasselijke vereisten, zoals beveiliging[68].

Voorbeeld:

Wanneer een bank besluit om van verlener van klantrelatiebeheer (customer relationship management — CRM) te veranderen, is het mogelijk dat bepaalde gegevens (persoonsgegevens en niet-persoonsgebonden gegevens) van de oude aanbieder naar de nieuwe moeten worden overgedragen. In dat geval zullen deze gegevens aan verschillende wettelijke voorschriften zijn onderworpen, waarvan sommige uit hoofde van de algemene verordening gegevensbescherming en andere uit hoofde van de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens.

4.2 Gedragscodes en certificeringsregelingen voor de bescherming van persoonsgegevens

Om aan te tonen dat is voldaan aan de verplichtingen van de algemene verordening gegevensbescherming (zie artikel 24, lid 3, en artikel 28, lid 5) kan gebruik worden gemaakt van gedragscodes en certificeringsregelingen.

Overeenkomstig artikel 40, lid 1, en artikel 42, lid 1, van de algemene verordening gegevensbescherming moeten de lidstaten, de toezichthoudende autoriteiten, het Europees Comité voor gegevensbescherming en de Commissie het bedrijfsleven aanmoedigen om gedragscodes op te stellen en certificeringsmechanismen voor gegevensbescherming in te voeren.

Verenigingen of andere instanties die een specifieke categorie van verwerkingsverantwoordelijken of verwerkers vertegenwoordigen, kunnen een gedragscode opstellen voor hun specifieke sector. Een ontwerp van de gedragscode moet ter goedkeuring worden voorgelegd aan de respectieve bevoegde toezichthoudende autoriteit[69]. Indien de ontwerpgedragscode betrekking heeft op verwerkingsactiviteiten in verschillende lidstaten,

[68] Zie Advies 05/2012 van Groep artikel 29 over cloudcomputing (WP196) (*Opinion 05/2012 on Cloud Computing*), aangenomen op 1 juli 2012, waarin de positie en verplichtingen van cloudgebruikers en verleners van clouddiensten ten aanzien van de verwerking van persoonsgegevens nader worden gespecificeerd.

[69] Zie artikel 40, lid 5, en artikel 55 van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

moet de toezichthoudende autoriteit deze vóór goedkeuring ervan aan het Europees Comité voor gegevensbescherming voorleggen. Vervolgens zal het Comité zich uitspreken over de vraag of de ontwerpgedragscode in overeenstemming is met de algemene verordening gegevensbescherming.

Het Europees Comité voor gegevensbescherming heeft haar richtsnoeren (nr. 1/2019) over gedragscodes en toezichthoudende organen in het kader van de algemene verordening gegevensbescherming gepubliceerd[70]. De richtsnoeren bevatten informatie over het opstellen van gedragscodes, criteria voor de goedkeuring ervan en andere nuttige informatie. Evenzo bevatten de richtsnoeren van het Europees Comité voor gegevensbescherming (nr. 1/2018) over certificering en het vaststellen van certificeringscriteria overeenkomstig de artikelen 42 en 43 van de algemene verordening gegevensbescherming informatie over certificering in het kader van deze verordening en de ontwikkeling en goedkeuring van certificeringscriteria[71].

Voorbeelden van door de cloudsector ontwikkelde gedragscodes:

De EU Cloud Code of Conduct, die met ondersteuning van de Commissie is ontwikkeld, is in samenwerking met de Cloud Select Industry Group (C-SIG) opgesteld op basis van de gegevensbeschermingsrichtlijn[72] en vervolgens op basis van de algemene verordening gegevensbescherming. De EU Cloud Code of Conduct bestrijkt het hele spectrum van clouddiensten, namelijk Software als dienst (Software as a Service — SaaS), Platform als dienst (Platform as a Service — PaaS) en Infrastructuur als dienst (Infrastructure as a Service — IaaS)[73].

De gedragscode van de verleners van cloudinfrastructuurdiensten in Europa (Cloud Infrastructure Services Providers in Europe — CISPE)[74] is gericht op verleners van IaaS-diensten. De gedragscode van CISPE bestaat uit vereisten ten aanzien van verleners van IaaS-diensten die als gegevensverwerkers optreden in het kader van de algemene verordening gegevensbescherming. Het bevat ook bepalingen over de governancestructuur voor de uitvoering en toepassing van de gedragscode.

[70] Europees Comité voor gegevensbescherming: *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679* (Richtsnoeren nr. 1/2019 over gedragscodes en toezichthoudende organen in het kader van Verordening (EU) 2016/679), aangenomen op 12 februari 2019, versie voor openbare raadpleging, online beschikbaar op: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-under_nl

[71] Europees Comité voor gegevensbescherming: *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679* (Richtsnoeren nr. 1/2018 over certificering en het vaststellen van certificeringscriteria overeenkomstig de artikelen 42 en 43 van Verordening (EU) 2016/679), aangenomen op 23 januari 2019, online beschikbaar op: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_en

[72] Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (einddatum geldigheid: 24 mei 2018).

[73] Voor meer informatie over de EU Cloud Code of Conduct, zie: https://eucoc.cloud/en/home.html

[74] Voor meer informatie over de gedragscode van CISPE, zie: https://cispe.cloud/code-of-conduct/

De gedragscode van de Cloud Security Alliance voor de naleving van de algemene verordening gegevensbescherming is gericht op alle belanghebbenden in het kader van cloudcomputing en de Europese wetgeving inzake persoonsgegevens, zoals verleners, gebruikers, potentiële gebruikers, auditors en makelaars van clouddiensten. De gedragscode bestrijkt het hele spectrum van verleners van clouddiensten[75].

4.3 Het vertrouwen in grensoverschrijdende gegevensverwerking vergroten – beveiligingscertificering

Zoals vermeld in overweging 33 van de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens moet het vergroten van het vertrouwen in de beveiliging van grensoverschrijdende gegevensverwerking de neiging van marktdeelnemers en de overheid om gegevenslokalisatie als substituut voor gegevensbeveiliging te gebruiken, verminderen. Naast het cyberbeveiligingspakket dat de Commissie in 2017 heeft voorgesteld[76], ontwikkelt de werkgroep CSPCERT aanbevelingen met het oog op een Europese cloudcertificeringsregeling die aan de Commissie zal worden gepresenteerd. Een dergelijke regeling kan het vrije verkeer van gegevens vergemakkelijken, de onderlinge vergelijkbaarheid van clouddiensten verbeteren en het gebruik van clouddiensten bevorderen. De Commissie kan Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging) verzoeken een potentiële regeling voor te bereiden overeenkomstig de desbetreffende bepalingen van de cyberbeveiligingsverordening[77]. Een dergelijke regeling kan zowel persoonsgegevens als niet-persoonsgebonden gegevens betreffen. Naast de cyberbeveiligingsverordening en zoals benadrukt in punt 4.2, kan de algemene verordening gegevensbescherming ook worden gebruikt om aan te tonen dat er sprake is van passende waarborgen inzake gegevensbeveiliging[78].

Slotopmerkingen

Rechtszekerheid en vertrouwen in de verwerking van gegevens zijn van essentieel belang voor de EU om gegevens optimaal te benutten, waarbij waardeketens zich over sectoren en grenzen heen kunnen ontwikkelen. Beide verordeningen garanderen dit en streven tegelijk ook naar het vrije verkeer van gegevens. Met de verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens en de algemene verordening gegevensbescherming wordt de grondslag gelegd voor het vrije verkeer van alle gegevens binnen de Europese Unie en een sterk concurrerende Europese gegevenseconomie.

---

[75] Voor meer informatie over de gedragscode van de Cloud Security Alliance, zie: https://gdpr.cloudsecurityalliance.org/

[76] Zie voor meer informatie: https://ec.europa.eu/digital-single-market/en/cyber-security

[77] Verordening van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening).

[78] Zie overweging 74 van de cyberbeveiligingsverordening.