AUTORITEIT
PERSOONSGEGEVENS

Richtlijnen voor het recht op dataportabiliteit

Deze tekst is een onofficiële Nederlandse vertaling van Guidelines on the right to data portability van de Artikel 29-werkgroep van Europese privacytoezichthouders. De vertaling is gemaakt in opdracht van de Autoriteit Persoonsgegevens en is daarom niet wettelijk bindend. Mocht de Nederlandse vertaling afwijken van de originele Engelse tekst, dan is de Engelse tekst leidend.

AUTORITEIT
PERSOONSGEGEVENS

Inhoudsopgave

Samenvatting 3

1. Inleiding 4

2. Wat zijn de belangrijkste elementen van dataportabiliteit? 5
2.1 Recht op het ontvangen van persoonsgegevens 5
2.2 Recht op het verzenden van persoonsgegevens van de ene verantwoordelijke naar de ander 5
2.3 Middelen voor dataportabiliteit 6
2.4 Verantwoordelijkheid 6
2.5 Dataportabiliteit vs. andere rechten van betrokkenen 7

3. Wanneer is dataportabiliteit van toepassing? 7
3.1 Welke verwerkingen vallen onder het recht op dataportabiliteit? 7
3.2 Welke persoonsgegevens moeten inbegrepen worden? 8
3.2.1 Eerste voorwaarde: persoonsgegevens over de betrokkene 8
3.2.2 Tweede voorwaarde: door de betrokkene verstrekte gegevens 8
3.2.3 Derde voorwaarde: het recht op dataportabiliteit mag geen afbreuk doen aan de rechten en vrijheden van anderen 10

4. Hoe zijn de algemene regels voor het uitoefenen van privacyrechten van toepassing op dataportabiliteit? 11
4.1 Welke achtergrondinformatie dient aan de betrokkene verstrekt te worden? 11
4.2 Hoe kan de verantwoordelijke de betrokkene identificeren voordat hij aan een verzoek gevolg geeft? 12
4.3 Binnen welke termijn dient aan een dataportabiliteitsverzoek gevolg gegeven te worden? 13
4.4 In welke gevallen kan een verzoek tot dataportabiliteit worden afgewezen of kan er een vergoeding in rekening worden gebracht? 13

5. Hoe dienen de overdraagbare gegevens geleverd te worden? 14
5.1 Wat is het verwachte bestandsformaat? 14
5.2 Hoe om te gaan met een omvangrijke of complexe verzameling van persoonsgegevens? 15
5.3 Hoe kunnen overdraagbare gegevens veiliggesteld worden? 16

Samenvatting

Artikel 20 van de algemene verordening gegevensbescherming (AVG) introduceert een nieuw recht: het recht op dataportabiliteit. Dit nieuwe recht is nauw verbonden met het recht op inzage, maar verschilt hier ook op veel punten van. Het recht op dataportabiliteit (overdraagbaarheid van gegevens) houdt in dat de betrokkene het recht heeft de persoonsgegevens die hij aan een verantwoordelijke heeft verstrekt in een gestructureerde, gangbare en machineleesbare vorm te ontvangen en deze aan een andere verantwoordelijke over te dragen. Het doel van dit nieuwe recht is de positie van betrokkenen te versterken en hun meer controle over hun gegevens te geven.

Aangezien dit directe verzending van persoonsgegevens van de ene verantwoordelijke naar de andere mogelijk maakt, is het recht op dataportabiliteit ook een belangrijk middel in de vrije stroom van persoonsgegevens binnen de EU en werkt het concurrentie tussen verantwoordelijken in de hand. Hierdoor kunnen mensen van dienstverlener veranderen, wat de ontwikkeling van nieuwe diensten binnen de digitale eenheidsmarktstrategie aanmoedigt.

Deze richtlijnen van de Artikel 29-werkgroep van gezamenlijke Europese privacytoezichthouders (WP29) bieden informatie over de interpretatie en implementatie van het recht op dataportabiliteit. Het doel is het recht op dataportabiliteit en het bereik hiervan te bespreken. De richtlijnen verduidelijken de voorwaarden waaronder dit nieuwe recht geldt, met inachtneming van de wettelijke basis van de gegevensverwerking (toestemming van de betrokkene of noodzakelijk om een overeenkomst uit te voeren) en het feit dat dit recht beperkt is tot door de betrokkene verstrekte informatie. Deze richtlijnen bieden tevens concrete voorbeelden en criteria voor de situaties waarin dit recht geldt. In dit geval stelt WP29 dat het recht op dataportabiliteit geldt voor zowel bewust en actief door de betrokkenen verstrekte gegevens als persoonsgegevens die door hun activiteiten gegenereerd worden. Dit nieuwe recht mag niet ondermijnd worden of beperkt worden tot direct door de betrokkene met bijvoorbeeld een webformulier verstrekte informatie.

Als good practice zouden verantwoordelijken moeten beginnen met de ontwikkeling van de middelen die bijdragen aan het voldoen aan verzoeken tot gegevensoverdracht, zoals downloadprogramma's en application programming interfaces (API's). Ze moeten garanderen dat persoonsgegevens in een gestructureerde, gangbare en machineleesbare vorm worden overgedragen en moeten aangemoedigd worden erop toe te zien dat de gebruikte gegevensvorm interoperabel is.

De richtlijnen helpen verantwoordelijken ook hun respectieve verplichtingen goed te begrijpen en raden best practices en middelen aan die helpen om aan het recht op dataportabiliteit te voldoen. Ten slotte raden de richtlijnen aan dat belanghebbenden in de industrie en vakbonden samenwerken aan gezamenlijke interoperabele normen en formats om aan de vereisten van het recht op dataportabiliteit te voldoen.

1. Inleiding

Artikel 20 van de algemene verordening gegevensbescherming (AVG) introduceert het nieuwe recht op dataportabiliteit. Betrokkenen kunnen de persoonsgegevens die zij aan een verantwoordelijke hebben verstrekt in een gestructureerde, gangbare en machineleesbare vorm ontvangen en deze ongehinderd aan een andere verantwoordelijke overdragen. Dit recht, dat onder bepaalde voorwaarden geldt, ondersteunt de vrije keuze en controle van gebruikers en geeft consumenten een sterkere positie.

Wie van zijn recht op inzage (vanuit de Europese privacyrichtlijn 95/46/EC) gebruikmaakte, werd beperkt door de vorm die de verantwoordelijke koos om de gevraagde informatie te leveren. Het nieuwe recht op dataportabiliteit heeft als doel betrokkenen een sterkere positie te geven als het gaat om hun eigen persoonsgegevens, aangezien het hun de mogelijkheid biedt persoonsgegevens eenvoudig van de ene ICT-omgeving naar de andere te verplaatsen, kopiëren of verzenden. Het hoofddoel van dataportabiliteit is dan ook het mogelijk te maken van dienstverlener te wisselen, wat de concurrentie tussen dienstverleners vergroot (door het makkelijker te maken van dienstverlener te wisselen). Daarnaast maakt dit het mogelijk in de context van de digitale eenheidsmarktstrategie nieuwe diensten te ontwikkelen.[1]

Dit recht biedt tevens een kans de relatie tussen betrokkenen en verantwoordelijken opnieuw in evenwicht te brengen doordat het de persoonlijke rechten van personen en hun controle over hun persoonsgegevens bevestigt.

Hoewel dataportabiliteit een nieuw recht is, bestaan er op andere gebieden van wetgeving al andere vormen van overdraagbaarheid of worden deze besproken (bijv. in de context van het opzeggen van overeenkomsten, roaming van communicatiediensten en grensoverschrijdende toegang tot diensten). Tussen deze vormen van overdraagbaarheid kunnen bepaalde synergiën en zelfs voordelen voor mensen ontstaan als deze gezamenlijk aangeboden worden, hoewel met analogieën voorzichtig omgegaan moet worden.

Deze richtlijnen bieden guidance aan verantwoordelijken, zodat deze hun werkwijzen, processen en beleid kunnen aanpassen, en verduidelijken wat dataportabiliteit inhoudt, om betrokkenen in staat te stellen goed van hun nieuwe recht gebruik te maken.

[1] Zie de agenda van de Europese Commissie voor een digitale eenheidsmarkt: https://ec.europa.eu/digital-single-market/en/access-digital-single-market, met name de eerste beleidspijler 'Verbeterde online toegang tot digitale goederen en diensten'.

2. Wat zijn de belangrijkste elementen van dataportabiliteit?

De AVG definieert het recht op dataportabiliteit in Artikel 20(1) als volgt:

De betrokkene heeft het recht zijn persoonsgegevens die hij aan een verantwoordelijke heeft verstrekt in een gestructureerde, gangbare en machineleesbare vorm te verkrijgen en hij heeft het recht die gegevens aan een andere verantwoordelijke over te dragen, zonder daarbij te worden gehinderd door de verantwoordelijke aan wie de persoonsgegevens waren verstrekt [...]

2.1 Recht op het ontvangen van persoonsgegevens

Allereerst is dataportabiliteit een **recht op het ontvangen van persoonsgegevens** die door een verantwoordelijke verwerkt zijn en het recht deze voor nader persoonlijk gebruik op een persoonlijk apparaat op te slaan, zonder het aan een andere verantwoordelijke te verzenden.

In die zin sluit dataportabiliteit aan op het recht op inzage. Eén specifiek kenmerk van dataportabiliteit is het feit dat dit het betrokkenen makkelijk maakt persoonsgegevens zelf te beheren en opnieuw te gebruiken. Deze gegevens dienen "*in een gestructureerde, gangbare en machineleesbare vorm*" te zijn. Zo kan het zijn dat een betrokkene zijn huidige afspeellijst van een streamingdienst voor muziek wil hebben om te kijken hoe vaak hij naar bepaalde nummers geluisterd heeft, om te bepalen welke muziek hij op een ander platform wil kopen. Of misschien wil hij zijn lijst met contactpersonen in zijn webmailapplicatie hebben om een lijst met gasten voor zijn trouwerij op te stellen. Of informatie over zijn aankopen met verschillende klantenkaarten om zijn 'carbon footprint' te bepalen.[2]

2.2 Recht op het verzenden van persoonsgegevens van de ene verantwoordelijke naar de ander

Ten tweede geeft Artikel 20(1) betrokkenen het **recht op het 'ongehinderd' verzenden van persoonsgegevens van de ene verantwoordelijke naar de andere**. Kort gezegd biedt dit onderdeel van dataportabiliteit betrokkenen de mogelijkheid de gegevens die ze verstrekt hebben niet alleen te ontvangen en te gebruiken, maar deze ook aan een andere dienstverlener te verzenden. Dit recht maakt het voor betrokkenen mogelijk de persoonsgegevens eenvoudig te verplaatsen, kopiëren of verzenden. Naast het feit dat dit de positie van consumenten versterkt door het 'insluiten' van gegevens te voorkomen, zal het recht op dataportabiliteit naar verwachting innovatie en het veilig delen van persoonsgegevens tussen verantwoordelijken bevorderen, waarbij de betrokkene de controle heeft.

Het doel van dit recht is het bevorderen van innovatie in het gebruik van gegevens en het aanmoedigen van nieuwe bedrijfsmodellen waarbij meer gegevens gedeeld worden waarbij de betrokkene de controle heeft.[3] Dataportabiliteit kan het gecontroleerd delen van persoonsgegevens tussen organisaties bevorderen en

[2] In deze gevallen valt de verwerking van de gegevens van de betrokkene onder persoonlijk/huishoudelijk gebruik en valt de verwerking daarom niet onder de AVG.
[3] Zie verschillende experimentele applicaties in Europa, zoals MiData [http://www.pcamidata.co.uk/] in het Verenigd Koninkrijk en MesInfos/SelfData [http://mesinfos.fing.org/] van FING in Frankrijk.

daarmee diensten en de ervaringen van de klant verbeteren.[4] Dataportabiliteit kan door de gebruiker gestuurde verzending en hergebruik van persoonsgegevens tussen de verschillende onafhankelijke diensten waarin deze geïnteresseerd is mogelijk maken.

2.3 Middelen voor dataportabiliteit

Qua techniek dienen verantwoordelijken verschillende implementaties van het recht op dataportabiliteit te bieden. Zo **dienen zij de betrokkene de mogelijkheid te bieden de gegevens direct te downloaden, maar tevens de mogelijkheid te bieden deze direct aan een andere verantwoordelijke te verzenden**. Dit kan bereikt worden door een API[5] beschikbaar te stellen. Daarnaast is het mogelijk dat betrokkenen van opslag voor persoonsgegevens gebruik willen maken of een *trusted third party* in willen zetten om hun persoonsgegevens te bewaren en op te slaan en verantwoordelijken vervolgens toestemming geven om de persoonsgegevens waar nodig te raadplegen en verwerken, zodat gegevens eenvoudig van de ene verantwoordelijke naar de ander verzonden kunnen worden.

2.4 Verantwoordelijkheid

Verantwoordelijken die onder Artikel 20 gevolg geven aan verzoeken tot dataportabiliteit, zijn niet verantwoordelijk voor de verwerking door de betrokkene of een ander bedrijf dat de persoonsgegevens ontvangt.

Dataportabiliteit verplicht verantwoordelijken niet om persoonsgegevens langer dan vereist of langer dan gedurende een vooraf bepaalde bewaartermijn te bewaren.[6] Het is belangrijk op te merken dat er geen extra verplichting bestaat om met het bewaren van gegevens te beginnen, louter om aan mogelijke verzoeken tot dataportabiliteit te kunnen voldoen.

Tegelijkertijd dient een ontvangende verantwoordelijke[7] erop toe te zien dat de gegevens die aan hem worden verstrekt relevant zijn en, met het oog op de nieuwe verwerking van gegevens, niet bovenmatig zijn. Zo hoeft, in het geval van de webmaildienst, wanneer het recht op dataportabiliteit wordt gebruikt om e-mails te verkrijgen en de betrokkene besluit deze naar een veilige opslaglocatie te versturen, de nieuwe verantwoordelijke niet de contactgegevens van de correspondenten van de betrokkene te verwerken. Als deze informatie niet relevant is voor het doel van de nieuwe verwerking, dient deze niet bewaard en verwerkt te worden. Dienovereenkomstig hoeft wanneer een betrokkene verzoekt informatie over zijn banktransacties op te sturen naar een dienst die hem helpt met budgetteren, de nieuwe verantwoordelijke niet alle gegevens van de transacties te bewaren als die eenmaal gelabeld zijn.

[4] De zogenoemde 'Quantified Self'- en 'Internet of Things'-markt hebben de voordelen (en risico's) van het verbinden van persoonsgegevens over verschillende aspecten van iemands leven aangetoond, zoals conditie, beweging en de hoeveelheid calorieën die iemand eet, om in één bestand een completer beeld van iemands leven te geven.
[5] Een *application programming interface* (API) bestaat uit subprogramma's, protocollen en middelen voor het maken van software en applicaties. Het verwijst naar de interfaces van applicaties of webdiensten die door verantwoordelijken beschikbaar gesteld worden zodat andere systemen of applicaties verbinding met hun systeem kunnen maken en daarmee kunnen werken.
[6] In het bovengenoemde voorbeeld kunnen, indien de verantwoordelijke niet bijhoudt welke nummers door een gebruiker gespeeld worden, deze persoonsgegevens niet in een verzoek tot dataportabiliteit opgenomen worden.
[7] Diegene die persoonsgegevens ontvangt naar aanleiding van een verzoek tot dataportabiliteit aan een andere verantwoordelijke.

Een 'ontvangende' organisatie wordt een nieuwe verantwoordelijke voor deze persoonsgegevens en dient zich aan de voorwaarden van Artikel 5 van de AVG te houden. Derhalve dient de 'nieuwe' verantwoordelijke voorafgaand een verzoek tot overdracht van gegevens duidelijk en direct het doel van de nieuwe verwerking aan te geven.[8]

2.5 Dataportabiliteit vs. andere rechten van betrokkenen

Wanneer iemand zijn recht op dataportabiliteit (of een ander recht onder de AVG) uitoefent, doet diegene dit onverminderd enig ander recht. Een betrokkene kan zelfs nadat de gegevens overgedragen zijn van de diensten van de verantwoordelijke gebruik blijven maken en daarvan blijven profiteren. Daarnaast kan, als de betrokkene gebruik wil maken van zijn of haar recht op verwijdering van gegevens, dataportabiliteit door de verantwoordelijke niet gebruikt worden als een excuus om dergelijke verwijdering te vertragen of weigeren.

Dataportabiliteit leidt niet automatisch tot de verwijdering van de gegevens uit de systemen van de verantwoordelijke en heeft geen invloed op de oorspronkelijke bewaartermijn die voor de volgens het recht op dataportabiliteit doorgestuurde gegevens geldt. De betrokkene kan zijn rechten uitoefenen zo lang de verantwoordelijke de gegevens verwerkt.

Mocht een betrokkene tot de ontdekking komen dat de vanuit het recht op dataportabiliteit gevraagde gegevens niet volledig aan zijn verzoek voldoen, dan moet met inachtneming van Artikel 15 van de AVG volledig aan een nader verzoek tot inzage voldaan worden.

3. Wanneer is dataportabiliteit van toepassing?

3.1 Welke verwerkingen vallen onder het recht op dataportabiliteit?

Naleving van de AVG vereist van verantwoordelijken dat zij een duidelijke wettelijke basis voor het verwerken van persoonsgegevens hebben.

Onder Artikel 20(1)(a) van de AVG **moeten verwerkingen, om onder dataportabiliteit te vallen, berusten op**:

- **de toestemming van de betrokkene** (op basis van Artikel 6(1)(a), of, voor bijzondere categorieën van gegevens, op basis van Artikel 9(2)(a));
- **een overeenkomst** waarbij de betrokkene partij is, op basis van Artikel 6(1)(b).

De titels van de boeken die iemand in een online boekwinkel gekocht heeft of de nummers waar deze via een muziekstreamingdienst naar geluisterd heeft, zijn andere voorbeelden die over het algemeen onder dataportabiliteit vallen, omdat deze gegevens worden verwerkt om een overeenkomst met de betrokkene uit te voeren.

[8] Daarnaast dient de nieuwe verantwoordelijke persoonsgegevens die niet relevant zijn niet te verwerken en dient de verwerking beperkt te zijn tot wat voor het nieuwe doel vereist is, ook als de persoonsgegevens onderdeel uitmaken van een algemenere set gegevens die de nieuwe verantwoordelijke toegestuurd krijgt. Persoonsgegevens die niet vereist zijn voor het doel van de nieuwe verwerking dienen zo snel mogelijk vernietigd te worden.

De AVG zorgt niet voor een algemeen recht op dataportabiliteit in gevallen waarin de verwerking van persoonsgegevens niet op toestemming of een overeenkomst gebaseerd is.[9]

Daarnaast geldt het recht op dataportabiliteit alleen indien de persoonsgegevens "via geautomatiseerde procedés" worden verwerkt en geldt het daarom niet voor papieren bestanden.

3.2 Welke persoonsgegevens moeten inbegrepen worden?

Volgens Artikel 20(1) dienen gegevens om onder het recht op dataportabiliteit te vallen:

- persoonsgegevens over de betrokkene te zijn, en
- door de betrokkene aan een verantwoordelijke *verstrekt* zijn.

Daarnaast geeft Artikel 20(4) aan dat voldoen aan dit recht geen afbreuk mag doen aan de rechten en vrijheden van anderen.

3.2.1 Eerste voorwaarde: persoonsgegevens over de betrokkene

Onder een verzoek tot dataportabiliteit vallen alleen persoonsgegevens. Daarom vallen anonieme[10] gegevens of gegevens die niet over de betrokkene gaan hier niet onder. Gepseudonimiseerde gegevens die duidelijk aan een betrokkene gekoppeld kunnen worden (doordat deze bijvoorbeeld aanvullende gegevens verstrekt die het mogelijk maken hem te identificeren, vgl. Artikel 11(2)) vallen echter wel onder het recht.

In veel gevallen zullen verantwoordelijken gegevens verwerken waarin de persoonsgegevens van verschillende betrokkenen opgenomen zijn. Waar dit het geval is, dienen verantwoordelijken de zin 'de betrokkene betreffende persoonsgegevens' niet al te strikt op te vatten. Zo kunnen telefoongegevens (in het account van een klant) bijvoorbeeld gegevens van derden bevatten die bij inkomende of uitgaande gesprekken betrokken. Hoewel de administratie daarom persoonsgegevens over meerdere personen bevat, moet het voor klanten mogelijk zijn deze gegevens op grond van een verzoek tot dataportabiliteit te verkrijgen. Als deze gegevens vervolgens echter naar een nieuwe verantwoordelijke gestuurd worden, mag deze nieuwe verantwoordelijke deze niet verwerken voor een doel waarmee afbreuk wordt gedaan aan de rechten en vrijheden van derden (zie hierna: derde voorwaarde).

3.2.2 Tweede voorwaarde: door de betrokkene verstrekte gegevens

De tweede voorwaarde beperkt het toepassingsbereik tot door de betrokkene 'verstrekte' gegevens. Er zijn veel voorbeelden van persoonsgegevens die bewust en actief door de betrokkene 'verstrekt worden', zoals accountgegevens (bijv. e-mailadres, gebruikersnaam, leeftijd) die met webformulieren verstrekt worden. Desondanks **dient de verantwoordelijke bij een verzoek tot dataportabiliteit ook de persoonsgegevens toe**

[9] Zie overweging 68 en Artikel 20(3) van de AVG. Volgens Artikel 20(3) en overweging 68 geldt dataportabiliteit niet wanneer de gegevensverwerking noodzakelijk is voor de vervulling van een taak van algemeen belang of de uitoefening van een openbaar gezag dat aan de verantwoordelijke is verleend, of wanneer een verantwoordelijke zijn openbare taken uitoefent of aan een wettelijke verplichting voldoet. Derhalve zijn de verantwoordelijken in deze gevallen niet verplicht overdraagbaarheid mogelijk te maken. Het is echter wel een good practice om processen te ontwikkelen voor het automatisch beantwoorden van verzoeken tot overdraagbaarheid, door de beginselen van het recht op dataportabiliteit te volgen. Een voorbeeld hiervan is dat een overheidsdienst het mogelijk maakt om eenvoudig inkomstenbelastingaangiften uit het verleden te downloaden. Zie over dataportabiliteit als good practice bij verwerking omdat dit noodzakelijk is voor een gerechtvaardigd belang en voor bestaande vrijwillige programma's pagina's 47 & 48 van de WP29 Opinie 6/2014 over gerechtvaardigde belangen (WP217), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_nl.pdf.

[10] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

te voegen die op basis van de activiteiten van gebruikers gegenereerd en verzameld worden, zoals ruwe gegevens die door een slimme meter gegenereerd worden. Onder deze laatste categorie gegevens vallen geen gegevens die alleen door de verantwoordelijke verwerkt worden, zoals een gebruikersprofiel op basis van een analyse van de ruwe gegevens van de slimme meter.

De verschillende categorieën gegevens kunnen op basis van hun herkomst van elkaar onderscheiden worden om te bepalen of zij onder het recht op dataportabiliteit vallen. De volgende categorieën zijn 'door de betrokkene verstrekte gegevens':

- **De gegevens die actief en bewust door de betrokkene zijn verstrekt vallen onder** het toepassingsbereik van het recht op dataportabiliteit (zoals postadres, gebruikersnaam, leeftijd, etc.)
- **De betreffende gegevens worden door de betrokkene door het gebruik van de dienst of het apparaat 'verstrekt'.** Dit is bijvoorbeeld iemands zoekgeschiedenis, internetverkeer en locatiegegevens. Hieronder vallen mogelijk ook andere ruwe gegevens, zoals de hartslag die door een conditie- of gezondheidsmeter gemeten wordt.

Gededuceerde en afgeleide gegevens worden echter door de verantwoordelijke op basis van de 'door de betrokkene verstrekte' gegevens gecreëerd. Deze persoonsgegevens vallen niet onder het toepassingsbereik van het recht op dataportabiliteit. Zo is de kredietwaardigheid of het resultaat van een beoordeling van de gezondheid van een gebruiker een typisch geval van gededuceerde gegevens. Hoewel zulke gegevens onderdeel kunnen zijn van een door een verantwoordelijke bewaard profiel en deze gegevens op basis van een analyse van door de betrokkene verstrekte gegevens worden gededuceerd en afgeleid (bijvoorbeeld op basis van zijn gedrag), worden deze gegevens doorgaans niet gezien als 'door de betrokkene verstrekt' en vallen deze daarom niet onder dit nieuwe recht.[11]

In het algemeen dient, gezien de doelstelling van het recht op dataportabiliteit, **de term 'door de betrokkene verstrekt' breed opgevat te worden en vallen alleen 'gededuceerde gegevens' en 'afgeleide gegevens' er niet onder**, waaronder mede wordt verstaan persoonsgegevens die door een dienstverlener gegenereerd worden (zoals algoritmen). **Een verantwoordelijke kan deze gededuceerde gegevens uitsluiten, maar dient alle andere persoonsgegevens toe te voegen die de betrokkene met door de verantwoordelijke beschikbaar gestelde middelen verstrekt heeft.**[12]

Daarom vallen persoonsgegevens die betrekking hebben op de activiteiten van de betrokkenen of voortkomen uit de observatie van iemands gedrag onder de term 'verstrekt door', maar gegevens op basis van nadere analyse van dat gedrag niet. Eventuele persoonsgegevens die als onderdeel van de gegevensverwerking door de verantwoordelijke gegenereerd zijn, bijv. door middel van een personalisatie- of aanbevelingsproces, zijn echter van de door de betrokkene verstrekte gegevens gededuceerde of afgeleide gegevens, en vallen niet onder het recht op dataportabiliteit.

[11] Desondanks kan de betrokkene onder Artikel 15 van de AVG (over het recht op inzage) gebruikmaken van zijn "recht om van de verantwoordelijke uitsluitsel te verkrijgen over het al dan niet verwerken van hem betreffende persoonsgegevens en, wanneer dat het geval is, om inzage te verkrijgen in die persoonsgegevens" evenals informatie over "het bestaan van geautomatiseerde besluitvorming, met inbegrip van de in artikel 22, leden 22(1) en (4), bedoelde profilering, en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene".

[12] Hieronder vallen alle gegevens over de betrokkene die worden waargenomen tijdens de activiteiten waarvoor de gegevens verzameld worden, zoals de transactiegeschiedenis of de toegangsgegevens. Gegevens die door het volgen en registreren van de betrokkene verkregen worden (zoals door een app die je hartslag bijhoudt of technologie die wordt gebruikt om internetgedrag te volgen) dienen echter ook als 'door de betrokkene verstrekt' gezien te worden, ook al worden deze niet actief of bewust verzonden.

3.2.3 Derde voorwaarde: het recht op dataportabiliteit mag geen afbreuk doen aan de rechten en vrijheden van anderen

Over persoonsgegevens van andere betrokkenen:
De derde voorwaarde is bedoeld om het ophalen en verzenden van informatie die de persoonsgegevens van andere betrokkenen (die hiervoor geen toestemming gegeven hebben) bevat naar een nieuwe verantwoordelijke te voorkomen wanneer deze gegevens waarschijnlijk zullen worden verwerkt op een manier die afbreuk doet aan de rechten en vrijheden van de andere betrokkenen (Artikel 20(4) van de AVG).[13]

Een dergelijke afbreuk doet zich bijvoorbeeld voor indien de verzending van gegevens van de ene verantwoordelijke naar de andere vanuit het recht van dataportabiliteit derden zou verhinderen hun rechten als betrokkenen onder de AVG uit te oefenen (zoals het recht op informatie, inzage etc.).

De betrokkene die zijn gegevens naar een andere verantwoordelijke laat verzenden, geeft de nieuwe verantwoordelijke toestemming voor de verwerking of gaat een overeenkomst met hem aan. Wanneer de gegevens persoonsgegevens van derden bevatten, dient een andere grondslag voor de rechtmatigheid van de verwerking te worden aangegeven. Zo mag de verantwoordelijke aan wie de gegevens worden verzonden bijvoorbeeld handelen in verband met een gerechtvaardigd belang zoals bedoeld in Artikel 6(1)(f), met name wanneer het doel van de verantwoordelijke is om diensten te leveren aan een betrokkene waardoor deze persoonsgegevens puur voor persoonlijk of huishoudelijk gebruik kan verwerken.

Zo mag een webmaildienst toestaan dat een overzicht aangemaakt wordt van de contactpersonen, vrienden, familieleden, het gezin en de bredere omgeving van een betrokkene. Omdat deze gegevens betrekking hebben op en worden aangemaakt door een identificeerbare persoon die zijn recht op dataportabiliteit wil uitoefenen, dienen verantwoordelijken het gehele overzicht van inkomende en uitgaande e-mails naar de betrokkene te sturen.

Een soortgelijke situatie doet zich voor wanneer een betrokkene zijn of haar recht op dataportabiliteit uitoefent bij zijn bankrekening, aangezien dit persoonsgegevens over de aankopen en transacties van de rekeninghouder zijn, maar ook informatie over transacties die 'verstrekt zijn' door andere mensen die geld naar de rekeninghouder hebben overgemaakt. In deze context is het bij de verzending van webmailgegevens of bankrekeninggegevens onwaarschijnlijk dat er afbreuk gedaan wordt aan de rechten en vrijheden van andere betrokkenen als hun gegevens bij elke verwerking voor hetzelfde doel gebruikt worden, d.w.z. als contactadres dat alleen door de betrokkene gebruikt wordt of als geschiedenis van een van de bankrekeningen van de betrokkene. Daartegenover staat dat hun rechten en vrijheden niet gerespecteerd worden wanneer de nieuwe verantwoordelijke de contactgegevens voor marketingdoeleinden gebruikt.

Derhalve is, om dergelijke negatieve gevolgen voor de betrokken derden te voorkomen, de verwerking van een dergelijk overzicht door een andere verantwoordelijke alleen toegestaan voor zover de gegevens volledig onder controle van de verzoekende gebruiker blijven staan en alleen voor persoonlijke en huishoudelijke doeleinden gebruikt worden. Een ontvangende 'nieuwe' verantwoordelijke (aan wie de gegevens op verzoek van de gebruiker verzonden kunnen worden) mag de verzonden gegevens van derden niet voor eigen doeleinden gebruiken, bijv. voor het promoten van producten en diensten aan die andere

[13] Overweging 68 stelt dat "wanneer het in een bepaalde verzameling persoonsgegevens om meer dan een betrokkene gaat, het recht om de persoonsgegevens te ontvangen de rechten en vrijheden van andere betrokkenen overeenkomstig deze Verordening onverlet moet laten."

betrokkenen. Als ze dit toch doen, is dergelijke verwerking waarschijnlijk onwettig of oneerlijk, vooral als de betreffende derden niet geïnformeerd worden en hun rechten als betrokkenen niet kunnen uitoefenen.

Om de rechten van andere betrokkenen van wie persoonsgegevens worden verzonden verder te beschermen, dienen alle verantwoordelijken (zowel de 'sturende' als de 'ontvangende' partij) middelen te implementeren waarmee betrokkenen de relevante gegevens kunnen selecteren en (waar nodig) gegevens van andere betrokkenen uit kunnen sluiten. Daarnaast dienen zij toestemmingsmechanismen voor andere betrokkenen te implementeren om de gegevensverzending te vergemakkelijken in die gevallen waarin deze partijen toestemming willen geven, bijvoorbeeld omdat zij zelf ook hun gegevens naar een andere verantwoordelijke willen verzenden. Een dergelijke situatie kan zich bijvoorbeeld voordoen bij sociale netwerken.

Over gegevens die onderworpen zijn aan intellectuele eigendomsrechten en beroepsgeheimen:
De rechten en vrijheden van anderen zoals in Artikel 20(4) genoemd kan ook verwijzen naar "*de rechten of vrijheden van anderen, met inbegrip van het zakengeheim of de intellectuele eigendom en met name aan het auteursrecht dat de software beschermt*" waar in overweging 63 over gesproken wordt, om het bedrijfsmodel van verantwoordelijken te beschermen (Artikel 15). Hoewel aan deze rechten gedacht dient te worden voor aan een verzoek tot dataportabiliteit voldaan wordt, "*mogen die overwegingen er echter niet toe leiden dat de betrokkene alle informatie wordt onthouden*".

Het recht op dataportabiliteit geeft iemand niet het recht om de informatie te gebruiken op een manier die als een oneerlijke handeling gezien kan worden of die een overtreding van intellectuele eigendomsrechten inhoudt. **Een potentieel bedrijfsrisico op zich kan echter niet als basis voor het afwijzen van een verzoek tot dataportabiliteit dienen** en verantwoordelijken kunnen door betrokkenen verstrekte persoonsgegevens verstrekken in een vorm waardoor geen informatie bekendgemaakt wordt die onder beroepsgeheim of intellectuele eigendomsrechten vallen.

4. Hoe zijn de algemene regels voor het uitoefenen van privacyrechten van toepassing op dataportabiliteit?

4.1 Welke achtergrondinformatie dient aan de betrokkene verstrekt te worden?

Om aan het nieuwe recht op dataportabiliteit te voldoen, dienen **verantwoordelijken de betrokkenen te informeren over het bestaan van het nieuwe recht op dataportabiliteit**, zoals aangegeven in Artikel 13(2)(b) en 14(2)(c) van de AVG.[14]

Bij het verstrekken van de vereiste duidelijke en complete informatie dienen verantwoordelijken zich ervan te verzekeren dat het recht op dataportabiliteit van andere rechten onderscheiden wordt. Daarom raadt WP29 met name aan dat verantwoordelijken duidelijk het verschil aangeven tussen de soorten

[14] Artikel 12 vereist dat verantwoordelijken "communicatie [...] in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal leveren, in het bijzonder wanneer de informatie specifiek voor een kind bestemd is."
Daarnaast vereist Artikel 12 dat verantwoordelijken "de uitoefening van de rechten van de betrokkene onder artikelen 15 tot en met 22 faciliteert" en "niet weigert gevolg te geven aan het verzoek van de betrokkene" wanneer een dergelijk verzoek ontvangen wordt ("tenzij de verantwoordelijke aantoont dat hij niet in staat is de betrokkene te identificeren").

gegevens die een betrokkene kan ontvangen op grond van het inzagerecht enerzijds en het recht op dataportabiliteit anderzijds.

Daarnaast raadt WP29 verantwoordelijken aan om altijd informatie over het recht op dataportabiliteit te verstrekken voordat een account gesloten wordt. Hierdoor kunnen gebruikers hun persoonsgegevens verzamelen en inzien en de gegevens voorafgaand aan de beëindiging van een overeenkomst eenvoudig naar hun eigen apparaat of aan een andere dienstverlener verzenden.

Tenslotte raadt WP29 als best practice voor 'ontvangende' verantwoordelijken aan dat deze betrokkenen informeren over de aard van de persoonsgegevens die voor het uitvoeren van hun diensten relevant zijn. Hierdoor kunnen gebruikers de risico's voor derden en alle andere onnodige vermenigvuldiging van persoonsgegevens voorkomen, ook waar er geen andere betrokkenen zijn.

4.2 Hoe kan de verantwoordelijke de betrokkene identificeren voordat hij aan een verzoek gevolg geeft?

In de AVG staan geen instructies voor het verifiëren van de identiteit van de betrokkene. Artikel 12(2) van de AVG geeft echter aan dat de verantwoordelijke niet kan weigeren gevolg te geven aan het verzoek van de betrokkene om diens rechten uit te oefenen (met inbegrip van het recht op dataportabiliteit), tenzij deze persoonsgegevens verwerkt voor een doel waarvoor de identificatie van een betrokkene niet vereist is en hij kan aantonen dat hij niet in staat is de betrokkene te identificeren. In een dergelijk geval kan de betrokkene onder Artikel 11(2) echter aanvullende informatie verstrekken op basis waarvan hij geïdentificeerd kan worden. Daarnaast stelt Artikel 12(6) dat wanneer een verantwoordelijke goede redenen heeft om te twijfelen aan de identiteit van de betrokkene, deze om aanvullende informatie kan vragen om de identiteit van de betrokkene te bevestigen. Wanneer een betrokkene geen nadere informatie levert op basis waarvan hij geïdentificeerd kan worden, mag de verantwoordelijke niet weigeren aan het verzoek gevolg te geven. Waar informatie en gegevens die online verzameld worden aan pseudoniemen of unieke identificatiecodes gekoppeld zijn, kunnen verantwoordelijken passende procedures implementeren waarmee iemand een verzoek tot dataportabiliteit kan doen en de gegevens die op hem betrekking hebben kan ontvangen. In elk geval dienen verantwoordelijken een authenticatieprocedure te implementeren om de identiteit van de betrokkene die om zijn persoonsgegevens vraagt of meer in het algemeen zijn rechten onder de AVG uitoefent met sterke zekerheid te identificeren.

In veel gevallen zijn dergelijke identificatieprocedures al geïmplementeerd. Zo worden er vaak gebruikersnamen en wachtwoorden gebruikt om iemand toegang te geven tot de gegevens in zijn e-mailaccounts, accounts op sociale netwerken en accounts die voor verschillende andere diensten worden gebruikt, waarvan sommigen gebruikt worden zonder dat gebruikers hun volledige naam en identiteit opgeven.

Indien de omvang van de door de betrokkene verzochte gegevens zodanig is dat verzending over het internet problematisch is, kan de verantwoordelijke, in plaats van de termijn voor het voldoen aan het verzoek tot het maximum van drie maanden op te laten lopen[15], wellicht een andere manier voor het leveren van de gegevens overwegen, zoals streaming of aanlevering op een cd, dvd of ander fysiek medium, of het mogelijk maken de persoonsgegevens direct aan een andere verantwoordelijke te verzenden (zoals aangegeven in Artikel 20(2) van de AV, waar dit technisch mogelijk is).

[15] Artikel 12(3)

4.3 Binnen welke termijn dient aan een dataportabiliteitsverzoek gevolg gegeven te worden?

Artikel 12(3) vereist dat **de verantwoordelijke de persoonsgegevens "*onverwijld*" en in ieder geval "*binnen een maand na ontvangst van het verzoek*" aan de betrokkene verstrekt** of binnen maximaal drie maanden in complexe gevallen, mits de betrokkene binnen één maand na het oorspronkelijke verzoek van de reden voor de vertraging op de hoogte is gebracht.

Voor verantwoordelijken die informatiemaatschappijdiensten leveren moet het technisch gezien mogelijk zijn binnen een korte termijn aan een verzoek gevolg te geven. Om aan de verwachtingen van de gebruiker te voldoen, is het een good practice om aan te geven binnen welke termijn normaliter aan een verzoek tot dataportabiliteit gevolg gegeven kan worden en dit aan de betrokkenen door te geven.

Indien een verantwoordelijke geen gevolg geeft aan een dataportabiliteitsverzoek van de betrokkene "*deelt hij deze laatste mee waarom het verzoek zonder gevolg is gebleven, en informeert hij hem over de mogelijkheid om een klacht in te dienen bij een toezichthouder en beroep bij de rechter in te stellen*", uiterlijk binnen één maand na ontvangst van het verzoek.

Verantwoordelijken dienen de verplichting om binnen de gegeven termijn te reageren te respecteren, zelfs als de reactie een weigering is. Met andere woorden, de verantwoordelijke mag er, wanneer deze gevraagd wordt aan een verzoek tot dataportabiliteit te voldoen, niet het zwijgen toe doen.

4.4 In welke gevallen kan een verzoek tot dataportabiliteit worden afgewezen of kan er een vergoeding in rekening worden gebracht?

Artikel 12 verbiedt de verantwoordelijke een vergoeding voor de verstrekking van de persoonsgegevens te eisen, tenzij de verantwoordelijke kan aantonen dat de verzoeken kennelijk ongegrond of buitensporig zijn, "*met name vanwege hun repetitieve karakter*". Zelfs wanneer het meerdere verzoeken tot dataportabiliteit betreft, zijn er slechts weinig gevallen waarin de verantwoordelijke een weigering de gevraagde informatie te leveren kan rechtvaardigen. Voor de informatiemaatschappijdiensten of soortgelijke online diensten die gespecialiseerd zijn in het automatisch verwerken van persoonsgegevens, is het zeer onwaarschijnlijk dat het een te grote last is om aan meerdere verzoeken tot dataportabiliteit gevolg te geven.

Daarnaast dienen de kosten van het proces dat wordt ingezet om aan verzoeken tot dataportabiliteit gevolg te geven niet mee te wegen wanneer bepaald wordt of een verzoek buitensporig is. Sterker nog, Artikel 12 van de AVG betreft de verzoeken van één betrokkene en niet het totaal aantal verzoeken dat door de verantwoordelijke ontvangen wordt. Derhalve mogen de algemene implementatiekosten van het systeem niet aan de betrokkenen berekend worden en ook niet gebruikt worden om een verzoek tot dataportabiliteit af te wijzen.

5. Hoe dienen de overdraagbare gegevens geleverd te worden?

5.1 Wat is het verwachte bestandsformaat?

De AVG verplicht verantwoordelijken om **de door mensen verzochte persoonsgegevens aan te leveren in een vorm die hergebruik mogelijk maakt**. Concreet geeft Artikel 20(1) van de AVG aan dat de persoonsgegevens "*in een gestructureerde, gangbare en machineleesbare vorm*" verstrekt dienen te worden. Overweging 68 biedt de verdere uitleg dat deze vorm *interoperabel* dient te zijn, een term die in de EU als volgt gedefinieerd[16] wordt:

> de mogelijkheid voor ongelijksoortige en diverse organisaties om te communiceren teneinde wederzijds voordelige en overeengekomen gemeenschappelijke doelstellingen na te streven, waaronder het delen van informatie en kennis tussen de organisaties, via de bedrijfsprocessen die zij ondersteunen, door middel van de uitwisseling van gegevens tussen hun respectieve ICT-systemen.

De termen 'gestructureerd', 'gangbaar' en 'machineleesbaar' zijn een aantal minimale vereisten die de interoperabiliteit van het door de verantwoordelijke geleverde bestandsformaat mogelijk maakt. In die zin zijn "gestructureerd, gangbaar en machineleesbaar" specificaties voor de middelen, en interoperabiliteit de gewenste uitkomst.

Overweging 21 van Richtlijn 2013/37/EU[17] definieert 'machineleesbaar' als volgt:

> een bestandsformaat met een zodanige structuur dat softwaretoepassingen gemakkelijk specifieke gegevens in het document kunnen identificeren, herkennen en extraheren. Gegevens die zijn gecodeerd in bestanden die in een machinaal leesbaar formaat zijn gestructureerd, zijn machinaal leesbare gegevens. Machinaal leesbare formaten kunnen open of geoctrooieerd zijn; zij kunnen al dan niet formele standaards zijn. Documenten die zijn gecodeerd in een bestandsformaat dat een automatische verwerking beperkt doordat de gegevens niet of niet gemakkelijk uit de documenten kunnen worden gehaald, mogen niet als documenten in een machinaal leesbaar formaat worden beschouwd. In voorkomend geval dienen de lidstaten het gebruik van open, machinaal leesbare formaten aan te moedigen.

Gezien het brede scala aan mogelijk gegevenstypen die door een verantwoordelijke verwerkt kunnen worden, bevat de AVG geen specifieke aanbevelingen voor de vorm van de te leveren persoonsgegevens. De meest passende vorm zal per sector verschillen en er bestaan wellicht al passende vormen, maar het formaat dient altijd zo gekozen te worden dat de gegevens interpreteerbaar zijn. Vormen die aan kostbare licentiebeperkingen onderworpen zijn, zijn niet passend.

[16] Artikel 2 van Besluit nr. 922/2009/EG van het Europees Parlement en de Raad van 16 september 2009 inzake interoperabiliteitsoplossingen voor Europese overheidsdiensten (ISA) OJ L 260, 03.10.2009, p. 20.
[17] tot wijziging van Richtlijn 2003/98/EG inzake het hergebruik van overheidsinformatie.

Overweging 68 verduidelijkt dat "*Het recht van de betrokkene om hem betreffende persoonsgegevens door te zenden of te ontvangen, voor de verantwoordelijke geen verplichting mag doen ontstaan om technisch compatibele systemen voor gegevensverwerking op te zetten of te onderhouden.*" **Derhalve wordt met overdraagbaarheid beoogd dat interoperabele systemen ontstaan, geen compatibele systemen.**[18]

Persoonsgegevens dienen aangeleverd te worden in vormen met een hoge mate van abstractie. Dit betekent dat voor dataportabiliteit een extra laag gegevensverwerking door verantwoordelijken vereist is om gegevens van het platform te halen en daar persoonsgegevens die buiten de overdraagbaarheid vallen (zoals het wachtwoord van de gebruiker, betalingsgegevens, biometrische patronen enz.) uit te filteren. Deze aanvullende gegevensverwerking staat los van de standaard gegevensverwerking, aangezien deze niet voor een nieuw doel van de verantwoordelijke plaatsvindt.

Verantwoordelijken dienen met de gegevens zoveel mogelijk metagegevens mee te sturen, met een zo hoog mogelijke mate van fijnkorreligheid, teneinde de precieze betekenis van de uitgewisselde informatie te behouden. Zo is het leveren van een PDF-versie van een e-mailbox niet voldoende gestructureerd. E-mailgegevens dienen te worden aangeleverd in een formaat waarin alle metagegevens behouden blijven, zodat de gegevens effectief opnieuw gebruikt kunnen worden. Derhalve dient de verantwoordelijke, wanneer deze een gegevensformaat zoekt om de persoonsgegevens in aan te leveren, na te denken over de invloed die dit formaat heeft op het recht van de persoon om de gegevens opnieuw te gebruiken. In gevallen waarin de verantwoordelijke in staat is de betrokkene een keuze te geven wat betreft het formaat, dient een duidelijke uitleg gegeven te worden van de gevolgen van deze keuze. Het verwerken van aanvullende metagegevens uitsluitend omdat men denkt dat deze wellicht nodig zijn of gewenst zijn om aan een verzoek tot dataportabiliteit gevolg te geven, is echter geen legitieme reden voor deze verwerking.

WP29 raadt sterk aan dat belanghebbenden in de industrie en vakbonden samenwerken aan gezamenlijke interoperabele normen en formats, die zullen dienen als vereisten voor het recht op dataportabiliteit. Deze uitdaging is ook door het European Interoperability Framework (EIF) aangepakt. Het EIF heeft 'Een kader voor interoperabiliteit' gecreëerd, een overeengekomen aanpak voor interoperabiliteit voor organisaties die gezamenlijk publieke diensten willen leveren. Binnen het toepassingsbereik geeft het kader een aantal gedeelde elementen zoals woordkeuze, concepten, beginselen, beleid, richtlijnen, aanbevelingen, normen, specificaties en praktijken.[19]

5.2 Hoe om te gaan met een omvangrijke of complexe verzameling van persoonsgegevens?

De AVG legt niet uit hoe men om dient te gaan met de uitdaging van een omvangrijke verzameling van gegevens, een complexe gegevensstructuur of andere technische problemen die tot moeilijkheden voor verantwoordelijken of betrokkenen kunnen leiden.

In alle gevallen is het echter cruciaal dat de betrokkene de definitie, het schema en de structuur van de persoonsgegevens die door de verantwoordelijke verstrekt zouden kunnen worden volledig kan begrijpen. Zo zouden de gegevens eerst in een samenvatting geleverd kunnen worden, met dashboards die de betrokkene in staat stellen onderdelen van de persoonsgegevens op te slaan, in plaats van de gehele catalogus. De verantwoordelijke dient een overzicht in "een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal" te leveren, bij voorkeur (zie Artikel

[18] ISO/IEC 2382-01 definieert interoperabiliteit als volgt: "Het vermogen om te communiceren, programma's uit te voeren of gegevens uit te wisselen tussen verschillende functionele systemen op een wijze waarbij de gebruiker weinig of geen kennis nodig heeft van de typische kenmerken van die systemen."

[19] Bron: http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf

12(1)) van de AVG) zodanig dat de betrokkene software kan gebruiken om specifieke gegevens gemakkelijk te identificeren, te herkennen en te verwerken.

Een van de manieren waarop een verantwoordelijke aan verzoeken tot dataportabiliteit gevolg kan geven is het bieden van een goed beveiligde en gedocumenteerde application programming interface (API). Hierdoor kan iemand met zijn eigen externe software zijn persoonsgegevens opvragen of anderen (inclusief andere verantwoordelijken) toestemming geven dit namens hem te doen, zoals aangegeven in Artikel 20(2) van de AVG. Door via een API toegang tot gegevens te geven, is het wellicht mogelijk een verfijnder toegangssysteem te bieden dat iemand in staat stelt opvolgende verzoeken in te dienen, ofwel in de vorm van een volledige download, of in de vorm van een deltafunctie waarin alleen de wijzigingen sinds de vorige download staan, zonder dat deze aanvullende verzoeken bezwaarlijk zijn voor de verantwoordelijke

5.3 Hoe kunnen overdraagbare gegevens veiliggesteld worden?

Over het algemeen dienen verantwoordelijken volgens Artikel 5(1)(f) te garanderen dat "passende beveiliging van de persoonsgegevens gewaarborgd is en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging ('integriteit en vertrouwelijkheid')".

De verzending van persoonsgegevens aan de betrokkene kan echter ook tot beveiligingsproblemen leiden:

Hoe kan verzekerd worden dat persoonsgegevens veilig bij de juiste persoon afgeleverd worden?

Aangezien het doel van dataportabiliteit is om persoonsgegevens uit het informatiesysteem van de verantwoordelijke te verkrijgen, kan de verzending een gevaar vormen voor die gegevens (met name het gevaar van inbreuk op de gegevens tijdens de verzending). De verantwoordelijke is verantwoordelijk voor het nemen van alle beveiligingsmaatregelen die vereist zijn om te zorgen dat de persoonsgegevens veilig verzonden worden (bijv. door deze te versleutelen) en bij de juiste persoon terechtkomen (bijv. door gebruik van aanvullende authenticatie-informatie). Dergelijke beveiligingsmaatregelen mogen niet belemmerend zijn en niet voorkomen dat gebruikers hun rechten uitoefenen, bijvoorbeeld door aanvullende kosten in rekening te brengen.

Hoe kunnen gebruikers geholpen worden de opgeslagen persoonsgegevens op hun eigen systeem te beveiligen?

Wanneer zij hun persoonsgegevens van een online service halen, bestaat er ook altijd het risico dat gebruikers deze in een minder veilig systeem dan het door de service geboden systeem opslaan. De betrokkene dient hierop gewezen te worden, zodat hij stappen kan ondernemen om de informatie die hij ontvangen heeft te beschermen. De verantwoordelijke kan als best practice ook passende vormen en versleutelingsmethoden aanbevelen om de betrokkene te helpen dit doel te bereiken.

AUTORITEIT
PERSOONSGEGEVENS

Contactgegevens

Bezoekadres

(alleen volgens afspraak)
Bezuidenhoutseweg 30
2594 AV DEN HAAG

Let op: bij bezoek aan de Autoriteit Persoonsgegevens moet u een geldig identiteitsbewijs laten zien.

Postadres

Postbus 93374
2509 AJ DEN HAAG

Telefonisch spreekuur

Op onze website autoriteitpersoonsgegevens.nl vindt u informatie en antwoorden op vragen over de bescherming van persoonsgegevens. Heeft u op deze website geen antwoord op uw vraag gevonden? Dan kunt u contact opnemen met de publieksvoorlichters van de Autoriteit Persoonsgegevens tijdens het telefonisch spreekuur via telefoonnummer **0900-2001 201**. De publieksvoorlichters zijn bereikbaar op maandag, dinsdag, donderdag en vrijdag van 10.00 tot 12.00 uur. (5 cent per minuut, plus de kosten voor het gebruik van uw mobiele of vaste telefoon).

Persvoorlichting

Journalisten en redacteuren kunnen met vragen terecht bij de woordvoerders van de Autoriteit Persoonsgegevens via telefoonnummer **070-8888 555**.

Zakelijke relaties

Bent u een zakelijke relatie van de Autoriteit Persoonsgegevens, zoals een leverancier, dan kunt u ons telefonisch bereiken via telefoonnummer **070-8888 500**.

Over de Autoriteit Persoonsgegevens
Iedereen heeft recht op een zorgvuldige omgang met zijn persoonsgegevens. De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en adviseert over nieuwe regelgeving.