



**Richtlijnen inzake het recht op gegevensoverdraagbaarheid**

**Goedgekeurd op dinsdag 13 december 2016  
Laatstelijk herzien en goedgekeurd op 5 april 2017**

De Groep is opgericht op grond van artikel 29 van Richtlijn 95/46/EG. Zij is een onafhankelijk Europees adviesorgaan inzake gegevensbescherming en de persoonlijke levenssfeer. De taken zijn omschreven in artikel 30 van Richtlijn 95/46/EG en in artikel 15 van Richtlijn 2002/58/EG.

Het secretariaat wordt verzorgd door directoraat C (Grondrechten en rechtsstatelijkheid) van het directoraat-generaal Justitie en Consumenten van de Europese Commissie, 1049 Brussel, België, kamer MO59 05/35.

Website: [http://ec.europa.eu/justice/data-protection/index\\_en.htm](http://ec.europa.eu/justice/data-protection/index_en.htm)

## INHOUDSOPGAVE

<b>Samenvatting .....</b>	<b>3</b>
<b>I. Inleiding .....</b>	<b>4</b>
<b>II. Wat zijn de belangrijkste elementen van gegevensoverdraagbaarheid?.....</b>	<b>5</b>
<b>III. Wanneer is gegevensoverdraagbaarheid van toepassing? .....</b>	<b>9</b>
<b>IV. Hoe zijn de algemene regels inzake de uitoefening van de rechten van betrokkenen op gegevensoverdraagbaarheid van toepassing?.....</b>	<b>15</b>
<b>V. Hoe moeten de overdraagbare gegevens worden geleverd? .....</b>	<b>18</b>

## **Samenvatting**

In artikel 20 van de algemene verordening gegevensbescherming wordt een nieuw recht op gegevensoverdraagbaarheid geïntroduceerd, dat nauw verbonden is met het recht op inzage, maar er ook op veel punten van verschilt. Dit recht houdt in dat betrokkenen de persoonsgegevens die ze aan een verwerkingsverantwoordelijke hebben verstrekt, in een gestructureerd, gangbaar en machineleesbaar formaat kunnen ontvangen en deze aan een andere verwerkingsverantwoordelijke kunnen overdragen. Dit nieuwe recht heeft als doel de positie van de betrokkene te versterken en hem/haar meer controle over zijn/haar gegevens te geven.

Aangezien dit de rechtstreekse verzending van persoonsgegevens van de ene verwerkingsverantwoordelijke naar de andere mogelijk maakt, is het recht op gegevensoverdraagbaarheid ook een belangrijk hulpmiddel ter ondersteuning van de vrije stroom van persoonsgegevens binnen de EU en werkt het concurrentie tussen verwerkingsverantwoordelijken in de hand. Hierdoor kunnen mensen van dienstverlener veranderen, wat de ontwikkeling van nieuwe diensten in het kader van de digitale eenheidsmarktstrategie bevordert.

Dit advies vormt een richtsnoer voor de interpretatie en implementatie van het recht op gegevensoverdraagbaarheid, dat via de algemene verordening gegevensbescherming werd geïntroduceerd. Het is de bedoeling het recht op gegevensoverdraagbaarheid en het bereik ervan 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 noodzaak om een overeenkomst uit te voeren) en het feit dat dit recht beperkt is tot de door de betrokkene verstrekte persoonsgegevens. Het advies biedt tevens concrete voorbeelden en criteria ter toelichting van de situaties waarin dit recht geldt. In dat verband stelt de WP29 dat het recht op gegevensoverdraagbaarheid geldt voor zowel bewust en actief door de betrokkene verstrekte gegevens als voor persoonsgegevens die door diens activiteiten gegenereerd worden. Dit nieuwe recht mag niet worden ondermijnd en beperkt tot direct door de betrokkene verstrekte persoonsgegevens, bijvoorbeeld via een onlineformulier.

Een goede praktijk zou erin bestaan dat verwerkingsverantwoordelijken starten met de ontwikkeling van middelen die bijdragen tot het voldoen aan verzoeken tot gegevensoverdraagbaarheid, zoals downloadprogramma's en applicatieprogramma-interfaces. Ze zouden moeten garanderen dat persoonsgegevens in een gestructureerd, gangbaar en machineleesbaar formaat worden overgedragen, en moeten worden aangemoedigd om de interoperabiliteit te verzekeren van het gegevensformaat dat bij een verzoek tot gegevensoverdraagbaarheid wordt gebruikt.

Het advies helpt verwerkingsverantwoordelijken ook hun respectieve verplichtingen duidelijk te begrijpen en raadt beste praktijken en middelen aan die helpen om het recht op gegevensoverdraagbaarheid na te leven. Tot slot wordt in het advies belanghebbenden uit de sector en beroepsverenigingen aangeraden samen aan een algemene reeks interoperabele normen en formaten te werken zodat aan de eisen van het recht op gegevensoverdraagbaarheid kan worden voldaan.

## **I. Inleiding**

In artikel 20 van de algemene verordening gegevensbescherming wordt een nieuw recht op gegevensoverdraagbaarheid geïntroduceerd. Dit recht houdt in dat betrokkenen de persoonsgegevens die ze aan een verwerkingsverantwoordelijke hebben verstrekt, in een gestructureerd, gangbaar en machineleesbaar formaat kunnen ontvangen en deze ongestoord aan een andere verwerkingsverantwoordelijke kunnen overdragen. Dit recht, dat onverminderd bepaalde voorwaarden wordt toegepast, helpt de gebruiker om keuzes te maken, controle te krijgen en zijn positie te versterken.

Wie in het verleden van zijn recht op inzage krachtens de Europese privacyrichtlijn 95/46/EG gebruik maakte, werd beperkt door het formaat waarin de verwerkingsverantwoordelijke de gevraagde informatie bezorgde. **Het nieuwe recht op gegevensoverdraagbaarheid is bedoeld om de positie van betrokkenen met betrekking tot hun eigen persoonsgegevens te versterken; het biedt hen immers de mogelijkheid om persoonsgegevens vlot van de ene IT-omgeving naar de andere te verplaatsen, te kopiëren of door te sturen** (ongeacht of het daarbij gaat om hun eigen systemen, de systemen van vertrouwde derden of die van nieuwe verwerkingsverantwoordelijken).

Door te bevestigen dat individuen persoonlijke rechten hebben, alsook controle over de hen betreffende persoonsgegevens, vormt gegevensoverdraagbaarheid ook een mogelijkheid om de relatie tussen betrokkenen en verwerkingsverantwoordelijken "opnieuw in evenwicht te brengen"<sup>1</sup>.

Hoewel het recht op overdraagbaarheid van persoonsgegevens tot meer concurrentie tussen diensten kan leiden (door het makkelijker te maken om van dienstverlener te wisselen), reguleert de algemene verordening gegevensbescherming de persoonsgegevens en niet de concurrentie. Zo worden overdraagbare gegevens met name in artikel 20 niet beperkt tot de gegevens die noodzakelijk of nuttig zijn om van dienstverlener te wisselen<sup>2</sup>.

Hoewel gegevensoverdraagbaarheid een nieuw recht is, bestaan er op andere gebieden van wetgeving al andere vormen van overdraagbaarheid of worden deze besproken (bv. in de context van het opzeggen van overeenkomsten, roaming van communicatiediensten en grensoverschrijdende toegang tot diensten<sup>3</sup>). Tussen deze verschillende vormen van overdraagbaarheid kunnen bepaalde synergieën en zelfs voordelen voor personen ontstaan als ze gezamenlijk worden aangeboden, hoewel met analogieën voorzichtig moet worden omgegaan.

Dit advies begeleidt verwerkingsverantwoordelijken bij het bijwerken van hun praktijken, processen en beleidslijnen en verduidelijkt de betekenis van het concept gegevensoverdraagbaarheid zodat betrokkenen hun nieuw recht efficiënt kunnen toepassen.

---

<sup>1</sup> De belangrijkste doelstelling van gegevensoverdraagbaarheid is ervoor te zorgen dat het individu meer controle krijgt over zijn/haar persoonsgegevens, alsook dat hij/zij een actieve rol speelt in het ecosysteem van de gegevens.

<sup>2</sup> Dit recht kan bijvoorbeeld banken de mogelijkheid bieden om aan de hand van persoonsgegevens die initieel in het kader van een energievoorzieningsdienst werden verzameld, extra diensten aan te bieden waarover de gebruiker controle heeft.

<sup>3</sup> Zie de agenda van de Europese Commissie voor een digitale eenheidsmarkt: <https://ec.europa.eu/digital-agenda/en/digital-single-market>, in het bijzonder de eerste beleidspijler "Betere onlinetoegang tot digitale goederen en diensten".

## **II. Wat zijn de belangrijkste elementen van gegevensoverdraagbaarheid?**

Het recht op gegevensoverdraagbaarheid wordt in artikel 20, lid 1, van de algemene verordening gegevensbescherming gedefinieerd.

*De betrokkene heeft het recht de hem betreffende persoonsgegevens, die hij aan een verwerkingsverantwoordelijke heeft verstrekt, in een gestructureerde, gangbare en machineleesbare vorm te verkrijgen, en hij heeft 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 [...]*

### **- Een recht om persoonsgegevens te verkrijgen**

Gevensoverdraagbaarheid is in eerste instantie een **recht van de betrokkene om een subset te ontvangen van persoonsgegevens** over hem of haar die door een verwerkingsverantwoordelijke werden verwerkt, en om die gegevens voor later persoonlijk gebruik op te slaan. Die gegevens kunnen op een eigen apparaat of in een eigen cloud worden opgeslagen, zonder dat ze daarbij naar een andere verwerkingsverantwoordelijke moeten worden verzonden.

In dat opzicht vult gegevensoverdraagbaarheid het recht op inzage aan. Een specifiek kenmerk van gegevensoverdraagbaarheid is dat het betrokkenen een manier biedt om hun persoonsgegevens zelf makkelijk te beheren en opnieuw te gebruiken. Deze gegevens moeten "in een gestructureerd, gangbaar en machineleesbaar formaat" worden verkregen. Bijvoorbeeld: een betrokkene kan zijn huidige afspeellijst (of een historiek van beluisterde nummers) van een muziekstreamingdienst willen opvragen om te kijken hoeveel keer hij bepaalde nummers heeft beluisterd of om te bepalen welke muziek hij op een ander platform wil aankopen of beluisteren. Tegelijkertijd wil hij misschien ook zijn contactenlijst van zijn webmailapplicatie opvragen om bijvoorbeeld een lijst met gasten voor zijn huwelijk op te stellen, of informatie krijgen over aankopen met verschillende klantenkaarten of zijn koolstofvoetafdruk bepalen<sup>4</sup>.

### **- Een recht om persoonsgegevens van de ene aan een andere verwerkingsverantwoordelijke over te dragen**

Ten tweede wordt in artikel 20, lid 1, bepaald dat betrokkenen het **recht hebben om persoonsgegevens van de ene aan een andere verwerkingsverantwoordelijke over te dragen**, en dit "zonder daarbij te worden gehinderd". Gegevens kunnen ook direct van de ene aan een andere verwerkingsverantwoordelijke worden overgedragen op verzoek van de betrokkene en waar dat technisch haalbaar is (artikel 20, lid 2). In dat verband worden

---

<sup>4</sup> In deze gevallen kan de verwerking van de door de betrokkene bezorgde gegevens binnen het toepassingsgebied van huishoudelijke activiteiten vallen, op voorwaarde dat de betrokkene volledige en exclusieve controle heeft over de verwerking, of ze kan namens de betrokkene door een andere partij worden uitgevoerd. In dit laatste geval moet de andere partij als een verwerkingsverantwoordelijke worden beschouwd, ook al gaat het enkel over opslag van persoonsgegevens, en moet deze de principes en verplichtingen zoals in de algemene verordening gegevensbescherming vastgelegd naleven.

verwerkingsverantwoordelijken in overweging 68 aangemoedigd om interoperabele formaten te ontwikkelen die gegevensoverdraagbaarheid mogelijk maken,<sup>5</sup> maar zonder de verwerkingsverantwoordelijken daarbij te verplichten te kiezen voor of te blijven werken met technisch compatibele verwerkingssystemen<sup>6</sup>. In de algemene verordening gegevensbescherming wordt het verwerkingsverantwoordelijken echter verboden de verzending te beperken.

In principe biedt dit aspect van gegevensoverdraagbaarheid betrokkenen de mogelijkheid om de gegevens die ze aan een andere dienstverlener (in hetzelfde of in een ander activiteitengebied) hebben bezorgd, niet alleen te verkrijgen en opnieuw te gebruiken, maar ze ook te verzenden. Naast het feit dat de consument weerbaar wordt gemaakt door "lock-in" te voorkomen, wordt verwacht dat door het recht op gegevensoverdraagbaarheid ook opportuniteiten worden bevorderd op het vlak van innovatie en het veilig en beveiligd delen van persoonsgegevens tussen verwerkingsverantwoordelijken onder toezicht van de betrokkene<sup>7</sup>. Gegevensoverdraagbaarheid kan het gecontroleerd en beperkt delen door gebruikers van persoonsgegevens tussen organisaties bevorderen en aldus diensten en klantervaringen verrijken<sup>8</sup>. Gegevensoverdraagbaarheid kan verzending en hergebruik van persoonsgegevens van gebruikers tussen de diverse diensten waarin ze geïnteresseerd zijn mogelijk maken.

---

<sup>5</sup> Zie ook punt V.

<sup>6</sup> Bijgevolg moet speciale aandacht worden besteed aan het formaat van de verzonden gegevens ter garantie dat deze zonder al te veel moeite door de betrokken of door een andere verwerkingsverantwoordelijke opnieuw kunnen worden gebruikt. Zie ook punt V.

<sup>7</sup> Zie diverse experimentele toepassingen in Europa, bv. [MiData](#) in het Verenigd Koninkrijk, [MesInfos / SelfData](#) door FING in Frankrijk.

<sup>8</sup> De zogenaamde Quantified Self en IoT-sectoren hebben aangetoond welke voordelen (en risico's) er zijn wanneer persoonsgegevens uit verschillende aspecten van het dagelijks leven van een persoon zoals conditie, beweging en calorieopname met elkaar worden gelinkt om in één enkel bestand een alomvattend beeld te krijgen van het leven van die persoon.

## - Verantwoordelijkheid

Gegevensoverdraagbaarheid garandeert het recht om persoonsgegevens te ontvangen en te verwerken overeenkomstig de wensen van de betrokkene<sup>9</sup>.

Verwerkingsverantwoordelijken die krachtens de voorwaarden vermeld in artikel 20 op verzoeken tot gegevensoverdraagbaarheid ingaan, zijn niet verantwoordelijk voor de verwerking door de betrokkene of door een andere onderneming die persoonsgegevens ontvangt. Ze handelen namens de betrokkene, ook wanneer de persoonsgegevens rechtstreeks naar een andere verwerkingsverantwoordelijke worden doorgestuurd. In dat opzicht is de verwerkingsverantwoordelijke niet aansprakelijk voor de naleving van de wetgeving inzake gegevensbescherming door de ontvangende verwerkingsverantwoordelijke, aangezien deze niet door de verzendende verwerkingsverantwoordelijke wordt gekozen. Tegelijkertijd moet de verwerkingsverantwoordelijke de nodige waarborgen voorzien om te verzekeren dat ze ook echt namens de betrokkene handelen. Zo kan hij bijvoorbeeld procedures instellen om te verzekeren dat het soort persoonsgegevens dat verzonden wordt, ook effectief overeenstemt met datgene wat de betrokkene wil verzenden. Dat kan door de nodige bevestiging van de betrokkene op te vragen, hetzij vóór de verzending, hetzij op een eerder tijdstip, wanneer voor het eerst met de verwerking werd ingestemd of het contract daartoe werd gefinaliseerd.

Verwerkingsverantwoordelijken die aan een verzoek tot gegevensoverdraagbaarheid voldoen, zijn niet specifiek verplicht om de kwaliteit van de gegevens voorafgaand aan de verzending te controleren. Uiteraard zouden deze gegevens al correct en actueel moeten zijn, in overeenstemming met de principes vermeld in artikel 5, lid 1, van de algemene verordening gegevensbescherming. Daarenboven impliceert gegevensoverdraagbaarheid geen verplichting voor de verwerkingsverantwoordelijke om persoonsgegevens langer dan nodig of langer dan een gespecificeerde bewaringstermijn te bewaren<sup>10</sup>. Het is belangrijk dat er geen extra verplichting bestaat om gegevens langer dan de geldende bewaartermijnen te bewaren, louter om aan eventuele latere verzoeken tot gegevensoverdraagbaarheid te kunnen voldoen.

Wanneer de opgevraagde persoonsgegevens door een gegevensverwerker zijn verwerkt, moet het krachtens artikel 28 van de algemene verordening gegevensbescherming afgesloten contract de verplichting opnemen om "de verwerkingsverantwoordelijke via de nodige technische en organisatorische maatregelen (...) te helpen zodat hij aan verzoeken tot uitvoering van de rechten van de betrokkene kan voldoen". De verwerkingsverantwoordelijke moet in samenwerking met zijn gegevensverwerkers dan ook specifieke procedures implementeren om aan verzoeken tot gegevensoverdraagbaarheid te kunnen voldoen. Bij gezamenlijke verantwoordelijkheid moeten de verantwoordelijkheden met betrekking tot de verwerking van verzoeken tot gegevensoverdraagbaarheid in een contract duidelijk aan iedere verwerkingsverantwoordelijke toegewezen worden.

Verder moet een ontvangende verwerkingsverantwoordelijke<sup>11</sup> er ook op toezien dat de geleverde overdraagbare gegevens relevant en niet buitensporig zijn met het oog op de nieuwe

---

<sup>9</sup> Het recht op gegevensoverdraagbaarheid beperkt zich niet tot persoonsgegevens die nuttig en relevant zijn voor gelijkaardige diensten verleend door concurrenten van de verwerkingsverantwoordelijke.

<sup>10</sup> Als de verwerkingsverantwoordelijke uit het bovenstaande voorbeeld geen gegevens over de door een gebruiker beluisterde nummers bijhoudt, kunnen deze persoonsgegevens niet in een verzoek tot gegevensoverdraagbaarheid worden opgenomen.

<sup>11</sup> m.a.w. die persoonsgegevens ontvangt na een verzoek tot gegevensoverdraagbaarheid door de betrokkene bij een andere verwerkingsverantwoordelijke.

gegevensverwerking. Bijvoorbeeld: bij een verzoek tot gegevensoverdraagbaarheid aan een webmaildienst, waarbij het de bedoeling is van de betrokkene om e-mails te ontvangen en op een beveiligd archiefplatform op te slaan, is het niet nodig dat de nieuwe verwerkingsverantwoordelijke de contactgegevens van de correspondenten van de betrokkene verwerkt. Als deze informatie niet relevant is voor de nieuwe verwerking, moet ze niet worden bewaard en verwerkt. In ieder geval zijn ontvangende verwerkingsverantwoordelijken niet verplicht om na een verzoek tot gegevensoverdraagbaarheid verzonden persoonsgegevens te aanvaarden en te verwerken. Een gelijkaardig voorbeeld: wanneer een betrokkene vraagt om gegevens van zijn of haar banktransacties te verzenden naar een dienst die hem/haar met budgetbeheer helpt, moet de ontvangende verwerkingsverantwoordelijke niet alle gegevens aanvaarden of alle gegevens van de transacties bewaren zodra ze met het oog op de nieuwe dienst zijn gelabeld. Met andere woorden: alleen de gegevens die noodzakelijk en relevant zijn voor de door de ontvangende verwerkingsverantwoordelijke geleverde dienst, moeten worden aanvaard en bewaard.

Een "ontvangende" organisatie wordt voor deze persoonsgegevens een nieuwe verwerkingsverantwoordelijke en moet de principes vastgelegd in artikel 5 van de algemene verordening gegevensbescherming naleven. Daartoe moet de "nieuwe" ontvangende verwerkingsverantwoordelijke voorafgaand aan een verzoek tot verzending van de overdraagbare gegevens duidelijk en direct het doel van de nieuwe verwerking vastleggen in overeenstemming met de eisen inzake transparantie vermeld in artikel 14<sup>12</sup>. Net als bij elke andere gegevensverwerking die onder zijn verantwoordelijkheid wordt uitgevoerd, moet de verwerkingsverantwoordelijke de principes vermeld in artikel 5 toepassen. Deze principes hebben o.a. betrekking op rechtmatigheid, redelijkheid en transparantie, doelbeperking, gegevensminimalisering, accuraatheid, integriteit en vertrouwelijkheid, opslagbeperking en verantwoordingsplicht<sup>13</sup>.

Verwerkingsverantwoordelijken die persoonsgegevens bijhouden, moeten bereid zijn om het recht op gegevensoverdraagbaarheid van hun betrokkene mogelijk te maken. Verwerkingsverantwoordelijken kunnen er ook voor kiezen om gegevens van een betrokkene te aanvaarden, zonder dat ze daartoe verplicht zijn.

#### **- Gevensoverdraagbaarheid versus andere rechten van betrokkenen**

**Wanneer iemand zijn/haar recht op gegevensoverdraagbaarheid uitoefent, is dat onverminderd enig ander recht (zoals ook het geval is bij alle andere rechten in de algemene verordening gegevensbescherming).** Een betrokkene kan gebruik blijven maken en blijven profiteren van de dienstverlening van de verwerkingsverantwoordelijke, zelfs nadat de gegevens overgedragen zijn. Gevensoverdraagbaarheid leidt niet automatisch tot het

---

<sup>12</sup> Daarenboven mag de nieuwe verwerkingsverantwoordelijke geen persoonsgegevens verwerken die niet relevant zijn, en moet de verwerking worden beperkt tot wat voor de nieuwe doeleinden nodig is, ook als de persoonsgegevens deel uitmaken van een meer algemene dataset die via een overdraagbaarheidsproces is verzonden. Persoonsgegevens die niet noodzakelijk zijn om het doel van de nieuwe verwerking te bereiken, moeten zo snel mogelijk worden gewist.

<sup>13</sup> Na ontvangst door de verwerkingsverantwoordelijke kunnen de persoonsgegevens die in het kader van het recht op gegevensoverdraagbaarheid werden verzonden, door de betrokkene als "geleverd door" worden beschouwd en conform het recht op gegevensoverdraagbaarheid opnieuw worden doorgestuurd, voor zover is voldaan aan de andere voorwaarden die op dit recht van toepassing zijn (met name de wettelijke basis van de verwerking ...).



wissen van de gegevens<sup>14</sup> uit de systemen van de verwerkingsverantwoordelijke en heeft geen impact op de originele bewaringstermijn die van toepassing is op de doorgestuurde gegevens. De betrokkene kan zijn/haar rechten uitoefenen zolang de verwerkingsverantwoordelijke de gegevens nog verwerkt.

Als de betrokkene zijn/haar recht op wissing wil uitoefenen ("recht op vergetelheid" krachtens artikel 17), kan gegevensoverdraagbaarheid niet door een verwerkingsverantwoordelijke worden gebruikt om die wissing te vertragen of te weigeren.

Indien een betrokkene ontdekt dat persoonsgegevens die conform het recht op gegevensoverdraagbaarheid werden aangevraagd, niet volledig met zijn/haar verzoek overeenstemmen, moet aan elk volgend verzoek om persoonsgegevens in het kader van het recht op inzage volledig worden voldaan, krachtens artikel 15 van de algemene verordening gegevensbescherming.

Wanneer in een specifieke Europese wet of wet van een lidstaat over een ander onderwerp ook een vorm van overdraagbaarheid van de betreffende gegevens wordt voorzien, moet bovendien ook met de voorwaarden in deze specifieke wetgeving rekening worden gehouden wanneer aan een verzoek tot gegevensoverdraagbaarheid krachtens de algemene verordening gegevensbescherming wordt voldaan. Ten eerste: als uit het verzoek van de betrokkene duidelijk blijkt dat het niet meteen zijn/haar bedoeling is om rechten krachtens de algemene verordening gegevensbescherming uit te oefenen, maar eerder alleen rechten krachtens sectorale wetgeving, zijn de bepalingen inzake gegevensoverdraagbaarheid van de algemene verordening gegevensbescherming niet op dit verzoek van toepassing<sup>15</sup>. Als het verzoek daarentegen overdraagbaarheid krachtens de algemene verordening gegevensbescherming beoogt, zal het bestaan van dergelijke specifieke wetgeving de verwerkingsverantwoordelijken niet ontslaan van de algemene toepassing van het principe van gegevensoverdraagbaarheid, zoals bepaald in de algemene verordening gegevensbescherming. In de plaats daarvan moet per geval worden beoordeeld hoe een dergelijke specifieke wetgeving (als die al bestaat) het recht op gegevensoverdraagbaarheid kan beïnvloeden.

### **III. Wanneer is gegevensoverdraagbaarheid van toepassing?**

- **Welke verwerkingsactiviteiten vallen onder het recht op gegevensoverdraagbaarheid?**

Naleving van de algemene verordening gegevensbescherming vereist van verwerkingsverantwoordelijken dat zij over een duidelijke wettelijke basis voor het verwerken van persoonsgegevens beschikken.

---

<sup>14</sup> zoals gedefinieerd in artikel 17 van de algemene verordening gegevensbescherming

<sup>15</sup> Bijvoorbeeld: als het verzoek van de betrokkene specifiek bedoeld is om een leverancier van rekeninginformatiediensten inzage in zijn/haar bankrekeninghistoriek te geven, zoals in de Richtlijn Betalingsdiensten 2 (PSD2) vermeld, moet die inzage conform de bepalingen van deze richtlijn worden toegestaan.

Krachtens artikel 20, lid 1, onder a), van de algemene verordening gegevensbescherming moeten verwerkingsactiviteiten, **om onder het recht op gegevensoverdraagbaarheid te vallen**, berusten op:

- hetzij op de toestemming van de betrokkene (uit hoofde van artikel 6, lid 1, onder a), of artikel 9, lid 2, onder a), wanneer het gaat om speciale categorieën van persoonsgegevens);
- hetzij op een contract waarin de betrokkene een partij is uit hoofde van artikel 6, lid 1, onder b).

De titels van boeken die iemand in een online boekwinkel heeft gekocht of de nummers waarnaar via een muziekstreamingdienst wordt geluisterd, zijn enkele voorbeelden van persoonsgegevens die doorgaans onder de gegevensoverdraagbaarheid vallen, omdat ze worden verwerkt op basis van de uitvoering van een contract waarin de betrokkene een partij is.

De algemene verordening gegevensbescherming biedt geen algemeen recht op gegevensoverdraagbaarheid in gevallen waarin de verwerking van persoonsgegevens niet op toestemming of een contract berust<sup>16</sup>. Zo bestaat er bijvoorbeeld geen verplichting voor financiële instellingen om aan een verzoek tot gegevensoverdraagbaarheid te voldoen wanneer het gaat om persoonsgegevens die worden verwerkt in het kader van hun verplichtingen tot preventie en detectie van witwaspraktijken en andere financiële misdrijven; en zo geldt gegevensoverdraagbaarheid ook niet voor professionele contactgegevens die in het kader van een B2B-relatie worden verwerkt wanneer die verwerking zich niet baseert op de toestemming van de betrokkene, noch op een contract waarin hij of zij een partij is.

Bij gegevens over werknemers geldt het recht op gegevensoverdraagbaarheid doorgaans alleen als de verwerking zich baseert op een contract waarin de betrokkene een partij is. In veel gevallen zal er niet van worden uitgegaan dat in deze context vrijwillig toestemming is gegeven, gezien de ongelijke machtsverhouding tussen werkgever en werknemer<sup>17</sup>. Sommige HR-verwerkingen daarentegen vinden hun wettelijke motivering in het rechtmatig belang, of zijn noodzakelijk om aan specifieke wettelijke verplichtingen op het vlak van tewerkstelling te kunnen voldoen. In de praktijk zal het recht op gegevensoverdraagbaarheid in een HR-context ongetwijfeld voor bepaalde verwerkingsactiviteiten gelden (zoals betalings- en vergoedingsdiensten, interne rekrutering), maar in heel wat andere gevallen zal steeds geval

---

<sup>16</sup> Zie overweging 68 en artikel 20, lid 3, van de algemene verordening gegevensbescherming. In artikel 20, lid 3, en in overweging 68 wordt bepaald dat gegevensoverdraagbaarheid niet van toepassing is wanneer de gegevensverwerking noodzakelijk is voor de uitvoering van een taak die het openbaar belang dient, of bij uitvoering van de officiële autoriteit die de verwerkingsverantwoordelijke bekleedt, of wanneer een verwerkingsverantwoordelijke zijn openbare taken uitvoert of een wettelijke verplichting naleeft. Bijgevolg zijn verwerkingsverantwoordelijken dan ook niet verplicht om in die gevallen gegevensoverdraagbaarheid mogelijk te maken. Het behoort echter tot de goede praktijken om processen te ontwikkelen teneinde automatisch aan verzoeken tot gegevensoverdraagbaarheid te kunnen voldoen, door de principes met betrekking tot het recht op gegevensoverdraagbaarheid na te leven. Een mogelijk voorbeeld hiervan is een overheidsdienst die de mogelijkheid biedt om inkomstenbelastingaangiften uit het verleden te downloaden. Voor gegevensoverdraagbaarheid als goede praktijk bij verwerking op basis van de wettelijk vastgelegde noodzaak voor een rechtmatig belang en voor bestaande vrijwillige regelingen: zie pagina's 47 & 48 van Advies 6/2014 van de WP29 over rechtmatige belangen (WP217).

<sup>17</sup> Zoals door de WP29 beschreven in haar Advies 8/2001 van 13 september 2001 (WP48).

per geval moeten worden nagaan of aan alle voorwaarden met betrekking tot het recht op gegevensoverdraagbaarheid is voldaan.

Tot slot geldt het recht op gegevensoverdraagbaarheid alleen als de gegevens "geautomatiseerd worden verwerkt" en geldt het bijgevolg niet voor papieren bestanden.

**- Welke persoonsgegevens moeten worden opgenomen?**

Krachtens artikel 20, lid 1, moeten gegevens, om onder het recht op gegevensoverdraagbaarheid te vallen:

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

In artikel 20, lid 4, wordt ook bepaald dat naleving van dit recht geen afbreuk mag doen aan de rechten en vrijheden van anderen.

Eerste voorwaarde: persoonsgegevens over de betrokkene

Alleen persoonsgegevens vallen onder het verzoek tot gegevensoverdraagbaarheid. Dus anonieme gegevens<sup>18</sup> of gegevens die niets met de betrokkene te maken hebben, vallen daar niet onder. Gegevens over een pseudoniem dat duidelijk aan een betrokkene kan worden gelinkt (bv. omdat hij of zij de nodige informatie bezorgt voor de respectieve identificatie, zie artikel 11, lid 2), vallen hier echter wel onder.

In veel gevallen zullen verwerkingsverantwoordelijken gegevens verwerken waarin de persoonsgegevens van verschillende betrokkenen opgenomen zijn. In dat geval dienen verwerkingsverantwoordelijken de zin "persoonsgegevens over de betrokkene" niet al te strikt op te vatten. Zo kunnen gegevens van telefoongesprekken, persoonlijke berichten of VoIP-communicaties (in de accounthistoriek van de klant) bijvoorbeeld informatie bevatten van derden die bij inkomende en uitgaande gesprekken betrokken zijn. Maar ook al bevatten die geregistreerde gegevens dan persoonsgegevens over meerdere personen, toch moeten de klanten deze gegevens op grond van een verzoek tot gegevensoverdraagbaarheid kunnen verkrijgen, want ze betreffen (ook) de betrokkene zelf. Maar als deze gegevens daarna naar een nieuwe verwerkingsverantwoordelijke gestuurd worden, mag deze nieuwe verwerkingsverantwoordelijke ze niet verwerken voor een doel waarbij afbreuk wordt gedaan aan de rechten en vrijheden van derden (zie hierna: derde voorwaarde).

Tweede voorwaarde: gegevens verstrekt door de betrokkene

De tweede voorwaarde beperkt het toepassingsbereik tot gegevens die door de betrokkene zijn "verstrekt".

Er zijn heel wat voorbeelden van persoonsgegevens die bewust en actief door de betrokkene worden "verstrekt" zoals accountgegevens (bv. e-mailadres, gebruikersnaam, leeftijd) die via onlineformulieren worden voorgelegd. Maar door de betrokkene "verstrekte" gegevens kunnen ook voortvloeien uit het observeren van diens activiteiten. Bijgevolg is de WP29 van mening dat dit nieuwe recht pas volwaardig kan worden genoemd als onder "verstrekt" ook de

---

<sup>18</sup> [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf)

persoonsgegevens wordt verstaan die uit de activiteiten van gebruikers kunnen worden opgemaakt, zoals ruwe gegevens die door een slimme meter of andere soorten verbonden apparaten worden verwerkt<sup>19</sup>, logbestanden van activiteiten, een historiek van internetgebruik of zoekopdrachten.

In deze laatste categorie gegevens vinden we niet de gegevens die door de verwerkingsverantwoordelijke zijn gecreëerd (op basis van de geobserveerde gegevens of direct ontvangen via invoer) zoals een gebruikersprofiel gecreëerd op basis van een analyse van de verzamelde ruwe gegevens van een slimme meter.

In functie van hun herkomst kan een onderscheid worden gemaakt tussen verschillende categorieën van gegevens om te bepalen of ze al dan niet onder het recht op gegevensoverdraagbaarheid vallen. De volgende categorieën kunnen worden gekwalificeerd als "door de betrokkene verstrekt":

- **Gegevens die actief en bewust door de betrokkene zijn verstrekt** (bv. e-mailadres, gebruikersnaam, leeftijd enz.)
- **Observatiegegevens die door de betrokkene zijn verstrekt door het gebruik van de dienst of het apparaat.** Daarbij kan het bijvoorbeeld gaan om iemands zoekhistoriek, internetverkeer en locatiegegevens. Maar ook andere ruwe gegevens zoals de hartslag die door een draagbaar toestel wordt gemeten, vallen daaronder.

Gededuceerde en afgeleide gegevens worden daarentegen door de verwerkingsverantwoordelijke op basis van de "door de betrokkene verstrekte" gegevens gecreëerd. Zo kan bijvoorbeeld het resultaat van een beoordeling van de gezondheid van een gebruiker of het profiel dat in het kader van risicobeheer en financiële regelingen wordt gecreëerd (bv. om een kredietwaardigheid toe te kennen of aan regels inzake witwaspraktijken te voldoen) op zich niet als "door de betrokkene verstrekt" worden beschouwd. Ook al maken dergelijke gegevens deel uit van een profiel dat door een verwerkingsverantwoordelijke wordt bewaard en worden ze uit de analyse van door de betrokkene verstrekte gegevens (bv. via zijn activiteiten) gededuceerd of afgeleid, toch zullen ze doorgaans niet als "door de betrokkene verstrekt" worden beschouwd en bijgevolg niet binnen het toepassingsgebied van dit nieuwe recht vallen<sup>20</sup>.

Gezien de beleidsdoelstellingen van het recht op gegevensoverdraagbaarheid, moet de term "door de betrokkene verstrekt" algemeen genomen ruim worden opgevat zodat "gededuceerde gegevens" en "afgeleide gegevens", waaronder ook persoonsgegevens die door een dienstverlener worden gegenereerd (zoals resultaten op basis van algoritmen), daar niet onder

---

<sup>19</sup> Door gegevens te kunnen opvragen die voortvloeien uit het observeren van diens activiteiten, zal de betrokkene ook een beter beeld kunnen krijgen van de implementatiekeuzes die de verwerkingsverantwoordelijke maakt met betrekking tot het toepassingsgebied van de geobserveerde gegevens. En bovendien zal de betrokkene hierdoor ook zelf beter kunnen kiezen welke gegevens hij of zij bereid is te verstrekken om een gelijkaardige dienst te krijgen, en zich bewust zijn van de mate waarin zijn/haar recht op privacy wordt gerespecteerd.

<sup>20</sup> Toch kan de betrokkene nog steeds gebruikmaken van zijn/haar "recht om van de verwerkingsverantwoordelijke bevestiging te krijgen over het feit of er al dan niet hem/haar betreffende persoonsgegevens worden verwerkt en, wanneer dat zo is, om inzage te krijgen in die gegevens", evenals informatie over "het bestaan van geautomatiseerde besluitvorming, met inbegrip van profilering waarnaar verwezen wordt in artikel 22, lid 1 en lid 4, en, tenminste in die gevallen, nuttige informatie over de daarbij gebruikte logica, alsook het belang en de verwachte gevolgen van een dergelijke verwerking voor de betrokkene", in overeenstemming met artikel 15 van de algemene verordening gegevensbescherming (waarin naar het recht van inzage wordt verwezen).

vallen. Een verwerkingsverantwoordelijke kan deze gededuceerde gegevens uitsluiten, maar moet alle andere persoonsgegevens die de betrokkene via door de verwerkingsverantwoordelijke beschikbaar gestelde middelen heeft verstrekt, opnemen<sup>21</sup>.

Bijgevolg omvat de term "verstrekt door" persoonsgegevens die met de activiteit van de betrokkene te maken hebben of uit de observatie van iemands gedrag voortvloeien, maar geen gegevens die uit de daaropvolgende analyse van dat gedrag kunnen worden opgemaakt. Anderzijds zijn persoonsgegevens die door de verwerkingsverantwoordelijke in het kader van de gegevensverwerking worden gecreëerd, bv. via een personalisatie- of aanbevelingsproces, of door categorisering of profilering van een gebruiker, gegevens die afgeleid of gededuceerd zijn uit de persoonsgegevens die de betrokkene zelf heeft verstrekt; bijgevolg vallen deze gegevens niet onder het recht op gegevensoverdraagbaarheid.

Derde voorwaarde: het recht op gegevensoverdraagbaarheid doet geen afbreuk aan de rechten en vrijheden van anderen

### **Met betrekking tot persoonsgegevens over andere betrokkenen**

De derde voorwaarde is bedoeld om te vermijden dat gegevens die persoonsgegevens van andere betrokkenen (die hiervoor geen toestemming hebben gegeven) bevatten, worden opgehaald en naar een nieuwe verwerkingsverantwoordelijke worden verzonden wanneer deze gegevens naar alle waarschijnlijkheid zullen worden verwerkt op een manier die afbreuk doet aan de rechten en vrijheden van die andere betrokkenen (artikel 20, lid 4, van de algemene verordening gegevensbescherming)<sup>22</sup>.

Een dergelijk negatief gevolg zou zich bijvoorbeeld kunnen voordoen als derden, door de verzending van gegevens van de ene verwerkingsverantwoordelijke naar de andere, hun rechten als betrokkenen krachtens de algemene verordening gegevensbescherming niet zouden kunnen uitoefenen (zoals het recht op informatie, van inzage enz.).

De betrokkene die het initiatief neemt om zijn/haar gegevens naar een andere verwerkingsverantwoordelijke te verzenden, geeft toestemming aan de nieuwe verwerkingsverantwoordelijke om die gegevens te verwerken of sluit een contract met die verwerkingsverantwoordelijke af. Wanneer de dataset ook persoonsgegevens van derden omvat, moet een andere wettelijke basis voor de verwerking worden vastgelegd. Zo kan de verwerkingsverantwoordelijke bijvoorbeeld een rechtmatig belang nastreven krachtens artikel 6, lid 1, onder f), vooral wanneer de verwerkingsverantwoordelijke tot doel heeft aan de betrokkene een dienst te leveren die deze laatste in staat stelt persoonsgegevens om puur persoonlijke of huishoudelijke redenen te verwerken. De verwerkingsactiviteiten van de betrokkene in het kader van een persoonlijke activiteit die op een derde betrekking hebben en gevolgen voor die derde kunnen hebben, vallen steeds onder de verantwoordelijkheid van die

---

<sup>21</sup> Dit omvat alle geobserveerde gegevens over de betrokkene tijdens de activiteiten waarvoor de gegevens specifiek worden verzameld, zoals een historiek van transacties of een toegangsllog. Gegevens die worden verzameld door de betrokkene te volgen en te registreren (zoals met een app die de hartslag meet of technologie waarmee het surfgedrag wordt gevolgd), moeten ook als "door de betrokkene verstrekt" worden beschouwd, zelfs als dat niet actief of bewust gebeurt.

<sup>22</sup> In Overweging 68 staat: "wanneer het in een bepaalde reeks persoonsgegevens om meer dan één betrokkene gaat, moet het recht om de persoonsgegevens te ontvangen de rechten en vrijheden van andere betrokkenen overeenkomstig deze verordening onverlet laten".

betrokkene, voor zover op geen enkele manier door de verwerkingsverantwoordelijke tot de verwerking werd besloten.

Bijvoorbeeld: bij een webmaildienst kan een lijst worden aangemaakt met contacten, vrienden, kennissen, familieleden en de ruimere omgeving van de betrokkene. Aangezien deze gegevens betrekking hebben op de identificeerbare persoon die zijn recht op gegevensoverdraagbaarheid wil uitoefenen (en door die persoon werden gecreëerd), moeten verwerkingsverantwoordelijken de volledige lijst met inkomende en uitgaande e-mails van die betrokkene bezorgen.

Op dezelfde manier kan de bankrekening van een betrokkene persoonsgegevens bevatten die betrekking hebben op transacties van niet alleen de rekeninghouder, maar ook andere personen (die bv. geld naar de rekeninghouder hebben overgeschreven). Aan de rechten en vrijheden van die derden wordt allicht geen afbreuk gedaan wanneer de bankrekeninginformatie na een verzoek tot gegevensoverdraagbaarheid aan de rekeninghouder wordt gestuurd, op voorwaarde dat in beide voorbeelden de gegevens voor hetzelfde doel worden gebruikt (m.a.w. contactadres alleen gebruikt door de betrokkene of een historiek van de bankrekening van de betrokkene).

Anderzijds worden de rechten en vrijheden van derden niet gerespecteerd als de nieuwe verwerkingsverantwoordelijke de persoonsgegevens voor andere doeleinden gebruikt, bv. als de ontvangende verwerkingsverantwoordelijke persoonsgegevens van andere personen uit de contactlijst van de betrokkene voor marketingdoeleinden gebruikt.

Om eventuele inbreuken op de betrokken derden dan ook te vermijden, is de verwerking van dergelijke persoonsgegevens door een andere verwerkingsverantwoordelijke slechts toegestaan wanneer de gegevens onder de exclusieve controle van de verzoekende gebruiker blijven en alleen voor puur persoonlijke of huishoudelijke doeleinden worden beheerd. Een ontvangende "nieuwe" verwerkingsverantwoordelijke (aan wie de gegevens op verzoek van de gebruiker kunnen worden verzonden) mag de verzonden gegevens over derden niet voor eigen doeleinden gebruiken, bv. om aan die andere derde betrokkenen marketingproducten en -diensten voor te stellen. Zo mag deze informatie bijvoorbeeld niet worden gebruikt om het profiel van de derde betrokkene aan te vullen en zijn sociale omgeving zonder medeweten en toestemming te hervormen<sup>23</sup>. En kan ze ook niet worden gebruikt om informatie over deze derden op te vragen en specifieke profielen te creëren, ook al beschikt de verwerkingsverantwoordelijke al over hun persoonsgegevens. Anders is een dergelijke verwerking naar alle waarschijnlijkheid onwettig en oneerlijk, vooral als de betreffende derden niet werden geïnformeerd en hun rechten als betrokkenen niet kunnen uitoefenen.

Bovendien behoort het tot de goede praktijken voor alle verwerkingsverantwoordelijken (zowel de "verzender" als de ontvangende" partijen) om middelen te implementeren waarmee betrokkenen de relevante gegevens die ze willen ontvangen en verzenden kunnen selecteren en, waar mogelijk, gegevens van andere personen kunnen uitsluiten. Dit kan helpen om de risico's verder te beperken voor derden waarvan de persoonsgegevens kunnen worden overgedragen.

---

<sup>23</sup> Een sociale netwerkdienst mag het profiel van zijn leden niet aanvullen aan de hand van persoonsgegevens die door een betrokkene werden verzonden in het kader van zijn recht op gegevensoverdraagbaarheid, zonder daarbij het transparantiebeginsel te respecteren en er ook voor te zorgen dat ze zich op een gepaste wettelijke basis inzake deze specifieke verwerking kunnen beroepen.

Aanvullend moeten de verwerkingsverantwoordelijken toestemmingssystemen voor andere betreffende betrokkenen invoeren zodat gegevens in gevallen waarbij de partijen hun akkoord verlenen (bv. als ze hun gegevens ook naar een andere verwerkingsverantwoordelijke willen verplaatsen) vlot verzonden kunnen worden. Een dergelijke situatie kan zich bijvoorbeeld bij sociale netwerken voordoen, maar het is aan de verwerkingsverantwoordelijken om te beslissen welke primaire praktijk ze volgen.

#### **Met betrekking tot gegevens die onder intellectuele eigendom en bedrijfsgeheimen vallen**

De rechten en vrijheden van anderen worden vermeld in artikel 20, lid 4. Aangezien dit niet direct te maken heeft met overdraagbaarheid, kan dit worden beschouwd als "met inbegrip van bedrijfsgeheimen of intellectuele eigendom, en in het bijzonder het auteursrecht dat software beschermt". Maar ook al zou met deze rechten rekening moeten worden gehouden voordat aan een verzoek tot gegevensoverdraagbaarheid wordt voldaan, "toch zouden die overwegingen niet leiden tot een weigering om alle gegevens over de betrokkene te verstrekken". Daarenboven mag de verwerkingsverantwoordelijke geen verzoek tot gegevensoverdraagbaarheid afwijzen op basis van een inbreuk op een ander contractueel recht (bv. een uitstaande schuld of een zakelijk conflict met de betrokkene).

Het recht op gegevensoverdraagbaarheid geeft een individu niet het recht om de bekomen informatie te misbruiken op een manier die als een oneerlijke praktijk gekwalificeerd kan worden of die een inbreuk op intellectuele eigendomsrechten vormt.

Een mogelijk bedrijfsrisico kan echter op zich geen basis vormen voor een weigering om aan het verzoek tot overdraagbaarheid te voldoen, en verwerkingsverantwoordelijken kunnen de door betrokkenen verstrekte persoonsgegevens zo verzenden dat er geen informatie wordt vrijgegeven die onder bedrijfsgeheimen of intellectuele eigendomsrechten valt.

#### **IV. Hoe zijn de algemene regels inzake de uitoefening van de rechten van betrokkenen op gegevensoverdraagbaarheid van toepassing?**

##### **- Welke voorafgaande informatie moet aan de betrokkene worden bezorgd?**

Om aan het nieuwe recht op gegevensoverdraagbaarheid te voldoen, moeten verwerkingsverantwoordelijken betrokkenen over het bestaan van het nieuwe recht op overdraagbaarheid informeren. Wanneer de respectieve persoonsgegevens direct bij de betrokkene worden gehaald, moet dat gebeuren "op het ogenblik waarop de gegevens worden verkregen". Als de persoonsgegevens niet van de betrokkene zijn verkregen, moet de verwerkingsverantwoordelijke de conform artikelen 13, lid 2, onder b), en 14, lid 2, onder c), vereiste informatie verstrekken.

"Wanneer de persoonsgegevens niet van de betrokkene zijn verkregen, moet de krachtens artikel 14, lid 3, vereiste informatie binnen een redelijke termijn van maximaal één maand na het verkrijgen van de gegevens worden verstrekt, bij de eerste communicatie met de betrokkene of wanneer de gegevens aan derden worden bekendgemaakt<sup>24</sup>.

Bij het verstrekken van de vereiste informatie moeten verwerkingsverantwoordelijken ervoor zorgen dat ze een onderscheid maken tussen het recht op gegevensoverdraagbaarheid en

---

<sup>24</sup> In artikel 12 wordt bepaald dat verwerkingsverantwoordelijken "de communicatie [...] in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal verstrekken, in het bijzonder wanneer de informatie specifiek voor een kind bestemd is".

andere rechten. Daarom raadt de WP29 met name aan dat verwerkingsverantwoordelijken duidelijk het verschil uitleggen tussen de soorten gegevens die een betrokkene via het recht op inzage en het recht op gegevensoverdraagbaarheid kan ontvangen.

Verder raadt de werkgroep verwerkingsverantwoordelijken aan om altijd de nodige informatie over het recht op gegevensoverdraagbaarheid te verstrekken voordat betrokkenen een eventuele account sluiten. Hierdoor kunnen gebruikers hun persoonsgegevens overlopen en deze gemakkelijk naar hun eigen toestel of naar een andere dienstverlener doorsturen voordat een contract wordt beëindigd.

Tot slot raadt de WP29 als beste praktijk voor "ontvangende" verwerkingsverantwoordelijken aan dat betrokkenen alle nodige informatie krijgen over het soort persoonsgegevens dat relevant is voor de prestaties van hun diensten. Naast het feit dat hierdoor een eerlijke verwerking wordt verzekerd, stelt dit gebruikers ook in staat om de risico's voor derden te beperken, alsook elke andere onnodige reproductie van persoonsgegevens, zelfs wanneer er geen andere betrokkenen zijn.

**- Hoe kan de verwerkingsverantwoordelijke de betrokkene identificeren alvorens op diens verzoek in te gaan?**

In de algemene verordening gegevensbescherming zijn geen opgelegde vereisten te vinden over hoe de betrokkene moet worden geauthenticeerd. In artikel 12, lid 2, van de algemene verordening gegevensbescherming wordt echter gesteld dat de verwerkingsverantwoordelijke niet mag weigeren om op het verzoek van een betrokkene tot uitoefening van diens rechten (met inbegrip van het recht op gegevensoverdraagbaarheid) in te gaan, tenzij er persoonsgegevens worden verwerkt voor een doeleinde waarbij geen identificatie van een betrokkene vereist is en kan worden aangetoond dat de betrokkene op geen enkele manier kan worden geïdentificeerd. Maar in hoofde van artikel 11, lid 2, kan de betrokkene in die omstandigheden meer informatie geven om zijn/haar identificatie mogelijk te maken. Aanvullend wordt in artikel 12, lid 6, bepaald dat wanneer een verwerkingsverantwoordelijke redelijke twijfels heeft over de identiteit van een betrokkene, bijkomende informatie kan worden aangevraagd om de identiteit van de betrokkene te bevestigen. Wanneer een betrokkene aanvullende informatie verleent om zijn/haar identificatie mogelijk te maken, mag de verwerkingsverantwoordelijke niet weigeren om op het verzoek in te gaan. Wanneer informatie en online verzamelde gegevens aan pseudoniemen of unieke identificatiegegevens zijn gelinkt, kunnen verwerkingsverantwoordelijken aangepaste procedures implementeren zodat iemand een verzoek tot gegevensoverdraagbaarheid kan indienen en de hem/haar betreffende gegevens kan ontvangen. In ieder geval moeten verwerkingsverantwoordelijken een authenticatieprocedure implementeren zodat ze met zekerheid de identiteit kunnen achterhalen van de betrokkene die zijn of haar persoonsgegevens opvraagt of, meer algemeen, de hem of haar krachtens de algemene verordening gegevensbescherming verleende rechten uitoefent.

Deze procedures bestaan vaak al. De identificatie van de betrokkenen is vaak al door de verwerkingsverantwoordelijke gerealiseerd voordat een contract wordt afgesloten of zijn/haar toestemming voor verwerking wordt verkregen. Hierdoor kunnen de persoonsgegevens gebruikt voor de registratie van de betrokkene wiens gegevens worden verwerkt ook als



bewijs worden gebruikt om de betrokkene met het oog op overdraagbaarheid te identificeren<sup>25</sup>.

Terwijl de voorafgaande identificatie van betrokkenen in deze gevallen een verzoek tot bewijs van hun wettelijke identiteit kan vereisen, is een dergelijke verificatie niet relevant om de link tussen de gegevens en de respectieve persoon te evalueren; want een dergelijke link is niet gelinkt aan de officiële of wettelijke identiteit. In principe kan het feit dat de verwerkingsverantwoordelijke bijkomende informatie kan opvragen om iemands identiteit te beoordelen, niet leiden tot buitensporige aanvragen en tot het verzamelen van persoonsgegevens die niet relevant of noodzakelijk zijn om de link tussen de persoon en de aangevraagde persoonsgegevens te bevestigen.

In veel gevallen bestaan dergelijke authenticatieprocedures al. Bijvoorbeeld: gebruiksnamen en wachtwoorden worden vaak gebruikt om personen toegang te verlenen tot de gegevens in hun e-mailaccounts, socialenetwerkaccounts en accounts voor diverse andere diensten, waarvan personen soms gebruik willen maken zonder hun volledige naam en identiteit kenbaar te maken.

Als het volume van de door de betrokkene aangevraagde gegevens verzending via het internet bemoeilijkt, kan de verwerkingsverantwoordelijke, in plaats van eventueel gedurende een verlengde periode van maximaal drie maanden toestemming te geven om aan het verzoek te beantwoorden<sup>26</sup>, ook alternatieve middelen voor de levering van de gegevens moeten overwegen zoals het gebruik van streaming of opslag op een cd, dvd of een andere fysieke gegevensdrager, of toelaten dat de persoonsgegevens direct naar een andere verwerkingsverantwoordelijke worden verzonden (krachtens artikel 20, lid 2, van de algemene verordening gegevensbescherming, waar technisch haalbaar).

**- Binnen welke termijn moet op een verzoek tot overdraagbaarheid worden gereageerd?**

In artikel 12, lid 3, wordt bepaald dat de verwerkingsverantwoordelijke "onverwijld" en in ieder geval "binnen een maand na ontvangst van het verzoek" "informatie over het gegeven gevolg" aan de betrokkene verstrekt. Deze periode van één maand kan bij complexe gevallen tot maximaal drie maanden worden verlengd, op voorwaarde dat de betrokkene binnen één maand na het originele verzoek over de redenen voor dit uitstel is geïnformeerd.

Verwerkingsverantwoordelijken die diensten van de informatiemaatschappij leveren, zijn wellicht beter gesitueerd om op erg korte termijn aan verzoeken te kunnen voldoen. Om aan de verwachtingen van de gebruiker te beantwoorden, behoort het tot de goede praktijken om het tijdsbestek te definiëren waarin een verzoek tot gegevensoverdraagbaarheid doorgaans kan worden beantwoord en dit aan betrokkenen mee te delen.

Verwerkingsverantwoordelijken die weigeren om op een verzoek tot gegevensoverdraagbaarheid in te gaan, moeten uit hoofde van artikel 12, lid 4, de betrokkene binnen één maand na ontvangst van het verzoek informeren "waarom het verzoek zonder

---

<sup>25</sup> Bijvoorbeeld: wanneer de gegevensverwerking aan een gebruikersaccount gelinkt is, kan het invoeren van inlogcode en wachtwoord eventueel volstaan om de betrokkene te identificeren.

<sup>26</sup> Artikel 12, lid 3: "De verwerkingsverantwoordelijke verstrekt informatie over het gevolg dat aan het verzoek is gegeven."

gevolg is gebleven, en [...] over de mogelijkheid om klacht in te dienen bij een toezichthoudende autoriteit en beroep bij de rechter in te stellen".

**Verwerkingsverantwoordelijken moeten de verplichting om binnen de gegeven termijnen te antwoorden respecteren, zelfs bij een weigering. Met andere woorden: de verwerkingsverantwoordelijke mag niet stil blijven wanneer hem gevraagd wordt op een verzoek tot gegevensoverdraagbaarheid in te gaan.**

- **In welke situaties kan een verzoek tot gegevensoverdraagbaarheid worden verworpen of kan een vergoeding worden aangerekend?**

Artikel 12 verbiedt de verwerkingsverantwoordelijke een vergoeding te vragen voor de levering van persoonsgegevens, tenzij de verwerkingsverantwoordelijke kan aantonen dat de verzoeken duidelijk ongegrond of buitensporig zijn, "met name vanwege hun repetitieve karakter". Voor diensten van de informatiemaatschappij die in geautomatiseerde verwerking van persoonsgegevens gespecialiseerd zijn, kan de implementatie van geautomatiseerde systemen zoals applicatieprogramma-interfaces (API's)<sup>27</sup> de uitwisselingen met de betrokkene vereenvoudigen, en zelfs de mogelijke last voortvloeiend uit repetitieve verzoeken verminderen. Bijgevolg zullen er erg weinig situaties zijn waarbij de verwerkingsverantwoordelijke een weigering tot het leveren van de gevraagde informatie kan rechtvaardigen, zelfs wanneer het gaat om meerdere verzoeken tot gegevensoverdraagbaarheid.

Verder zou met de totale kostprijs van de processen die worden ontwikkeld om aan verzoeken tot gegevensoverdraagbaarheid te voldoen, geen rekening mogen worden gehouden om de buitensporigheid van een verzoek te bepalen. Artikel 12 van de algemene verordening gegevensbescherming is met name gericht op de verzoeken van één enkele betrokkene en niet op het totale aantal verzoeken dat door een verwerkingsverantwoordelijke wordt ontvangen. Bijgevolg mag de totale kostprijs voor de implementatie van het systeem niet aan de betrokkenen worden aangerekend, noch worden gebruikt om een weigering van een verzoek tot gegevensoverdraagbaarheid te motiveren.

## **V. Hoe moeten de overdraagbare gegevens worden geleverd?**

- **Welke verwachte middelen moet de verwerkingsverantwoordelijke implementeren om gegevens te kunnen leveren?**

In artikel 20, lid 1, van de algemene verordening gegevensbescherming wordt bepaald dat betrokkenen het recht hebben om de gegevens naar een andere verwerkingsverantwoordelijke te sturen zonder daarbij gehinderd te worden door de verwerkingsverantwoordelijke aan wie de persoonsgegevens werden verstrekt.

Dergelijke hinder kan omschreven worden als elke door de verwerkingsverantwoordelijke ingestelde wettelijke, technische of financiële belemmering bedoeld om inzage, verzending of hergebruik door de betrokkene of door een andere verwerkingsverantwoordelijke te ontzeggen of te vertragen. Enkele voorbeelden van dergelijke hinder zijn: gevraagde vergoedingen voor het leveren van gegevens, gebrekkige interoperabiliteit van of toegang tot

---

<sup>27</sup> Een applicatieprogramma-interface (API) staat voor de interfaces van applicaties of webdiensten die door verwerkingsverantwoordelijken beschikbaar worden gesteld om ervoor te zorgen dat andere systemen of applicaties met hun systemen kunnen worden verbonden en kunnen werken.

een gegevensformaat, API of het voorziene formaat, buitensporige vertraging of complexiteit om de volledige dataset op te halen, opzettelijk knoeien met de dataset, of specifieke en onnodige of buitensporige eisen inzake sectorale standaardisatie of accreditatie<sup>28</sup>.

In artikel 20, lid 2, worden verwerkingsverantwoordelijken ook verplichtingen opgelegd om de overdraagbare gegevens rechtstreeks naar andere verwerkingsverantwoordelijken door te sturen "indien dit technisch mogelijk is".

De technische haalbaarheid om gegevens van de ene verwerkingsverantwoordelijke naar de andere te sturen onder toezicht van de betrokkene, moet geval per geval worden beoordeeld. In overweging 68 worden de beperkingen voor wat "technisch haalbaar" is verder verduidelijkt, en daarbij wordt aangegeven dat "het voor de verwerkingsverantwoordelijke geen verplichting mag doen ontstaan om technisch compatibele systemen voor gegevensverwerking op te zetten of te houden".

Van verwerkingsverantwoordelijken wordt verwacht dat ze persoonsgegevens in een interoperabel formaat verzenden, ook al creëert dat geen verplichtingen voor andere verwerkingsverantwoordelijken om deze formaten te ondersteunen. De directe verzending van de ene verwerkingsverantwoordelijke naar de andere kan dan ook plaatsvinden wanneer communicatie tussen twee systemen op een veilige manier mogelijk is<sup>29</sup>, en wanneer het ontvangende systeem technisch in staat is om de inkomende gegevens te ontvangen. Als de rechtstreekse verzending door technische belemmeringen wordt verhinderd, moet de verwerkingsverantwoordelijke deze belemmeringen aan de betrokkenen uitleggen; doet hij dan niet, dan heeft zijn beslissing nagenoeg hetzelfde effect als een weigering om in te gaan op het verzoek van een betrokkene (artikel 12, lid 4).

Op technisch vlak moeten verwerkingsverantwoordelijken twee verschillende en aanvullende trajecten onderzoeken en evalueren om overdraagbare gegevens beschikbaar te maken aan de betrokkenen of aan andere verwerkingsverantwoordelijken:

- rechtstreekse verzending van de volledige dataset van overdraagbare gegevens (of meerdere extracten met delen van de volledige dataset);
- een geautomatiseerd programma voor extractie van relevante gegevens.

Verwerkingsverantwoordelijken zullen doorgaans de tweede methode kiezen wanneer het gaat om complexe en omvangrijke datasets, aangezien op die manier extractie mogelijk is van eender welk deel van de dataset dat voor de betrokkene relevant is in het kader van zijn/haar verzoek. Verder kan hierdoor ook het risico worden geminimaliseerd en kunnen mogelijk systemen voor synchronisatie van gegevens worden gebruikt<sup>30</sup> (bv. bij regelmatige communicatie tussen verwerkingsverantwoordelijken). Dit kan een betere manier zijn om naleving door de "nieuwe" verwerkingsverantwoordelijke te verzekeren, en kan ook een

---

<sup>28</sup> Er kunnen zich wel enkele rechtmatige belemmeringen voordoen, zoals wanneer het gaat om de rechten en vrijheden van derden vermeld in artikel 20, lid 4, of wanneer het gaat om de beveiliging van de eigen systemen van de verwerkingsverantwoordelijken. In dat geval behoort het tot de verantwoordelijkheid van de verwerkingsverantwoordelijke om te rechtvaardigen waarom dergelijke belemmeringen rechtmatig zijn en geen hinder vormen zoals bedoeld in artikel 20, lid 1.

<sup>29</sup> Via een geauthenticeerde communicatie met het vereiste niveau van gegevenscodering.

<sup>30</sup> Een synchronisatiemechanisme kan helpen om aan de verplichtingen in hoofde van artikel 5 van de algemene verordening gegevensbescherming, waarin wordt bepaald dat "persoonsgegevens moeten (...) juist zijn en zo nodig worden geactualiseerd", te voldoen.

goede praktijk zijn om risico's inzake privacy vanwege de initiële verwerkingsverantwoordelijke te beperken.

Deze twee verschillende en mogelijk aanvullende manieren om relevante overdraagbare gegevens te bezorgen, kan worden geïmplementeerd door gegevens op verschillende manieren beschikbaar te stellen, bijvoorbeeld via beveiligde berichten, een SFTP-server, een beveiligde WebAPI of WebPortal. Aan betrokkenen moet de mogelijkheid worden geboden om gebruik te maken van een persoonlijke gegevensopslag, een systeem voor het beheer van persoonsgegevens<sup>31</sup> of andere soorten vertrouwde derden voor het bewaren en opslaan van de persoonsgegevens en het verlenen van toestemming aan verwerkingsverantwoordelijken om de persoonsgegevens voor zover nodig in te zien en te verwerken.

- **Welk gegevensformaat kunnen we verwachten?**

In de algemene verordening gegevensbescherming wordt van verwerkingsverantwoordelijken geëist dat ze de door de persoon aangevraagde persoonsgegevens aanleveren in een formaat dat hergebruik mogelijk maakt. Specifiek wordt in artikel 20, lid 1, van de algemene verordening gegevensbescherming vastgelegd dat de persoonsgegevens "in een gestructureerd, gangbaar en machineleesbaar formaat" moeten worden geleverd. In overweging 68 wordt verder toegelicht dat dit formaat interoperabel moet zijn, een term die<sup>32</sup> in de EU als volgt wordt gedefinieerd:

*de mogelijkheid voor ongelijksoortige en diverse organisaties om te interageren 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 enkele minimale eisen die de interoperabiliteit van het door de verwerkingsverantwoordelijke geleverde gegevensformaat moeten vereenvoudigen. Bijgevolg staat "in een gestructureerd, gangbaar en machineleesbaar formaat" voor de specificaties voor de middelen, terwijl de interoperabiliteit het gewenste resultaat is.

In overweging 21 van Richtlijn 2013/37/EU<sup>33,34</sup> wordt "machineleesbaar" als volgt gedefinieerd:

*een bestandsformaat met een zodanige structuur dat softwaretoepassingen gemakkelijk specifieke gegevens, met inbegrip van individuele feitelijke beweringen, kunnen identificeren, herkennen en extraheren. Gegevens die zijn gecodeerd in*

---

<sup>31</sup> Voor meer informatie over managementsystemen voor persoonsgegevens (PIMS) verwijzen we bijvoorbeeld naar Advies 9/2016 van de Europese Toezichthouder voor gegevensbescherming, dat u terugvindt op [https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-10-20\\_PIMS\\_opinion\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-10-20_PIMS_opinion_EN.pdf)

<sup>32</sup> Artikel 2 van Besluit nr. 922/2009/EG van het Europees Parlement en de Raad van woensdag 16 september 2009 inzake interoperabiliteitsoplossingen voor Europese overheidsdiensten (ISA) (PB L 260 van 03.10.2009, blz. 20)

<sup>33</sup> Tot wijziging van Richtlijn 2003/98/EG inzake het hergebruik van overheidsinformatie.

<sup>34</sup> Het EU glossarium (<http://eur-lex.europa.eu/eli-register/glossary.html>) biedt verdere verduidelijking van de verwachtingen met betrekking tot de in deze richtlijn gebruikte begrippen zoals *machineleesbaar*, *interoperabiliteit*, *open formaat*, *standaard*, *metagegevens*.

*bestanden die in een machinaal leesbaar formaat zijn gestructureerd, zijn machinaal leesbare gegevens. Machinaal leesbare formaten kunnen open of propriëtair 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 grote aantal mogelijke soorten gegevens dat door een verwerkingsverantwoordelijke verwerkt kan worden, legt de algemene verordening gegevensbescherming geen specifieke aanbevelingen op voor het formaat van de te leveren persoonsgegevens. Het meest aangepaste formaat zal verschillen in functie van de diverse sectoren, en er kunnen bovendien al aangepaste formaten bestaan, maar het uiteindelijke formaat moet altijd worden gekozen met als doel interpreteerbaar te zijn en de betrokkene een zo groot mogelijke mate van gegevensoverdraagbaarheid te bieden. Bijgevolg worden formaten waarvoor dure licenties moeten worden aangekocht, niet als geschikt beschouwd.

In overweging 68 wordt verduidelijkt dat "*Het recht van de betrokkene om hem/haar betreffende persoonsgegevens door te zenden of te ontvangen, mag voor de verwerkingsverantwoordelijke geen verplichting doen ontstaan om technisch compatibele systemen voor gegevensverwerking op te zetten of te houden. Bijgevolg is overdraagbaarheid bedoeld om interoperabele systemen te ontwikkelen, geen compatibele systemen*"<sup>35</sup>.

Men gaat ervan uit dat persoonsgegevens worden geleverd in formaten waarbij van een eventueel intern of propriëtair formaat zoveel mogelijk abstractie is gemaakt. Hierdoor impliceert gegevensoverdraagbaarheid een bijkomend niveau van gegevensverwerking door verwerkingsverantwoordelijken om gegevens van het platform te halen en persoonsgegevens die niet onder het recht op overdraagbaarheid vallen, zoals gededuceerde gegevens of gegevens over beveiliging van systemen, uit te filteren. Hierdoor worden verwerkingsverantwoordelijken aangemoedigd om gegevens in hun eigen systemen die binnen het toepassingsbereik van de wet op overdraagbaarheid vallen, vooraf te identificeren. Deze bijkomende gegevensverwerking wordt beschouwd als een nevenactiviteit van de primaire gegevensverwerking, aangezien ze niet wordt uitgevoerd om aan een nieuw door de verwerkingsverantwoordelijke gedefinieerd doeleinde te beantwoorden.

Wanneer in een bepaalde bedrijfstak of gegeven context geen specifieke formaten gangbaar zijn, **dienen verwerkingsverantwoordelijken de persoonsgegevens te leveren in gangbare open formaten (bv. XML, JSON, CSV ...) samen met nuttige metagegevens met een zo hoog mogelijke mate van gedetailleerdheid**, en tegelijkertijd een hoge mate van abstractie te behouden. Bijgevolg moeten geschikte metagegevens worden gebruikt om de betekenis van uitgewisselde informatie zo accuraat mogelijk te beschrijven. Hierdoor zouden metagegevens moeten volstaan om de functie en het hergebruik van de gegevens mogelijk te maken, maar uiteraard zonder dat daarbij bedrijfsgeheimen worden onthuld. Het is dan ook onwaarschijnlijk dat een persoon zijn postbus met inkomende e-mails in pdf-versie leveren

---

<sup>35</sup> In ISO/IEC 2382-01 wordt interoperabiliteit als volgt gedefinieerd: "De mogelijkheid om te communiceren, programma's uit te voeren of gegevens over te dragen tussen verschillende functie-eenheden op een manier die van de gebruiker weinig of geen kennis van de unieke kenmerken van die eenheden vereist."

voldoende gestructureerd of beschrijvend zal zijn om de gegevens van het Postvak IN makkelijk opnieuw te kunnen gebruiken. In de plaats daarvan moeten de e-mailgegevens worden geleverd in een formaat waarin alle metagegevens behouden blijven, zodat de gegevens efficiënt opnieuw kunnen worden gebruikt. Dus bij de keuze van een gegevensformaat voor de levering van de persoonsgegevens moet de verwerkingsverantwoordelijke nagaan hoe dit formaat het recht van het individu om de gegevens opnieuw te gebruiken, kan beïnvloeden of hinderen. Wanneer de verwerkingsverantwoordelijke de betrokkene voor het gewenste formaat van de persoonsgegevens meerdere opties kan voorleggen, dient hij de impact van de keuze duidelijk toe te lichten. De verwerking van bijkomende metagegevens met als enige doel dat ze nodig of gewenst kunnen zijn om aan een verzoek tot gegevensoverdraagbaarheid te voldoen, is echter geen legitieme reden voor een dergelijke verwerking.

**De WP29 spoort belanghebbenden uit de sector en beroepsverenigingen sterk aan om samen aan een algemene reeks interoperabele normen en formaten te werken om aan de eisen van het recht op gegevensoverdraagbaarheid te voldoen.** Dit probleem is ook onderzocht door het Europees Interoperabiliteitskader (EIF), dat een goedgekeurde methode heeft ontwikkeld voor interoperabiliteit voor organisaties die gezamenlijk openbare diensten willen leveren. Binnen zijn toepassingsgebied specificeert dit kader een reeks algemene aspecten zoals woordenschat, begrippen, principes, beleidslijnen, richtlijnen, aanbevelingen, standaarden, specificaties en praktijken<sup>36</sup>.

**- Hoe omgaan met een omvangrijke of complexe verzameling van persoonsgegevens?**

In de algemene verordening gegevensbescherming wordt niet uitgelegd hoe er moet worden gereageerd bij een omvangrijke gegevensverzameling, een complexe gegevensstructuur of andere technische problemen die verwerkingsverantwoordelijken of betrokkenen voor problemen kunnen stellen.

In alle gevallen is het echter wel cruciaal dat het individu de definitie, het schema en de structuur van de persoonsgegevens die de verwerkingsverantwoordelijke kan leveren, ten volle kan begrijpen. Zo kunnen gegevens bijvoorbeeld eerst in een samengevatte vorm worden aangeleverd via dashboards die de betrokkene de mogelijkheid bieden om subsets van de persoonsgegevens op te slaan, en niet meteen alle gegevens. De verwerkingsverantwoordelijke moet een overzicht geven "in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal" (zie artikel 12, lid 1, van de algemene verordening gegevensbescherming) zodat de betrokkene altijd duidelijk weet welke gegevens hij/zij voor een bepaald doel aan een andere verwerkingsverantwoordelijke moet downloaden of verzenden. Zo moeten betrokkenen in staat zijn om met behulp van softwareapplicaties specifieke gegevens makkelijk te identificeren, te herkennen en te verwerken.

Zoals hierboven al vermeld, kan het aanbieden van een passend beveiligde en gedocumenteerde API een praktische manier zijn voor een verwerkingsverantwoordelijke om op verzoeken tot gegevensoverdraagbaarheid in te gaan. Hierdoor kunnen individuen verzoeken met betrekking tot hun persoonsgegevens aan de verwerkingsverantwoordelijke bezorgen via hun eigen of derde software, of anderen (met inbegrip van een andere

---

<sup>36</sup> Bron: [http://ec.europa.eu/isa/documents/isa\\_annex\\_ii\\_eif\\_en.pdf](http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf)

verwerkingsverantwoordelijke) toestemming verlenen om dit in hun naam uit te voeren, zoals in artikel 20, lid 2, van de algemene verordening gegevensbescherming gespecificeerd. Door toegang te verlenen tot gegevens via een extern toegankelijke API, kan ook een meer gesofisticeerd toegangssysteem worden aangeboden dat individuen in staat stelt om opeenvolgende verzoeken voor gegevens in te dienen, hetzij als volledige download, hetzij als een delta-functie met enkele wijzigingen sinds de meest recente download, zonder dat deze bijkomende verzoeken de verwerkingsverantwoordelijke nog meer werk bezorgen.

#### **- Hoe kunnen overdraagbare gegevens worden beveiligd?**

Verwerkingsverantwoordelijken moeten algemeen genomen garanderen dat gegevens "door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging" krachtens artikel 5, lid 1, onder f), van de algemene verordening gegevensbescherming.

Maar ook bij de verzending van persoonsgegevens naar de betrokkene kunnen zich enkele veiligheidsproblemen stellen:

#### Hoe kunnen verwerkingsverantwoordelijken verzekeren dat persoonsgegevens veilig aan de juiste persoon worden geleverd?

Aangezien met gegevensoverdraagbaarheid ernaar wordt gestreefd om persoonsgegevens uit het informatiesysteem van de verwerkingsverantwoordelijke te verkrijgen, kan de verzending een mogelijke bron van risico's voor die gegevens worden (met name bij inbreuken op de gegevens tijdens de verzending). De verwerkingsverantwoordelijke is verantwoordelijk voor alle veiligheidsmaatregelen die nodig zijn om te verzekeren dat persoonsgegevens niet alleen veilig worden verzonden (via end-to-end of gegevenscodering) naar de juiste bestemming (met behulp van strikte authenticatiemaatregelen), maar ook dat de persoonsgegevens die in hun systemen blijven zitten, blijvend beschermd worden, alsook voor transparante procedures voor het behandelen van mogelijke inbreuken op de gegevens<sup>37</sup>. Verwerkingsverantwoordelijken moeten dan ook de specifieke risico's die met gegevensoverdraagbaarheid gepaard gaan beoordelen en de nodige maatregelen nemen om de risico's te beperken.

Hierna enkele maatregelen ter beperking van de risico's: als de betrokkene al moet worden geïdentificeerd aan de hand van bijkomende authenticatiegegevens zoals een gedeeld geheim of een andere authenticatiefactor zoals een eenmalig wachtwoord; de verzending opschorten of bevriezen bij enig vermoeden dat de account gecompromitteerd is; bij directe verzending van de ene naar de andere verwerkingsverantwoordelijke moet authenticatie via mandaat zoals authenticaties op basis van tokens worden gebruikt.

Dergelijke beveiligingsmaatregelen mogen niet hinderlijk zijn en mogen gebruikers er niet van weerhouden om hun rechten uit te oefenen, bv. door het opleggen van bijkomende kosten.

#### Hoe gebruikers helpen om de opslag van hun persoonsgegevens in hun eigen systemen te beveiligen?

---

<sup>37</sup> In overeenstemming met Richtlijn (EU) 2016/1148 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie.

Door hun persoonsgegevens via een onlinedienst op te halen, bestaat er altijd een risico dat gebruikers ze op een minder beveiligd systeem opslaan dan het systeem dat door de dienst werd voorzien. De betrokkene die de gegevens opvraagt, is verantwoordelijk voor het nemen van de juiste maatregelen om persoonsgegevens in zijn eigen systeem te beveiligen. Maar hij/zij moet hiervan ook bewust worden gemaakt zodat hij/zij de nodige stappen onderneemt om de ontvangen informatie te beveiligen. Als een voorbeeld van goede praktijk kunnen verwerkingsverantwoordelijken ook een aangepast formaat/aangepaste formaten, coderingsprogramma's en andere veiligheidsmaatregelen aanraden om de betrokkene te helpen bij het bereiken van deze doelstelling.

\* \* \*

Gedaan te Brussel, 13 december 2016

*Namens de werkgroep*  
*De voorzitter*  
*Isabelle FALQUE-PIERROTIN*

Laatstelijk herzien en goedgekeurd op 5 april  
2017

*Namens de werkgroep*  
*De voorzitter*  
*Isabelle FALQUE-PIERROTIN*