

De AVG en IoT-data onder de Data Act: een gelukkig huwelijk?

Computerrecht 2025/3

Met de lancering in 2020 van de Europese Datastrategie² heeft de Europese Commissie een verschuiving bewerkstelligd van het beschermen van data naar het delen van data. Waar de Algemene verordening gegevensbescherming (AVG) en de Databankenrichtlijn bescherming bieden aan persoonsgegevens en databanken, brengen de Data Governance Act (DGA),³ de Data Act (Dataverordening)⁴ en European Data Spaces⁵ kaders met zich mee voor het uitwisselen van data.

In Computerrecht is de (concept) Data Act al meerdere keren behandeld, onder andere in relatie tot de DGA⁶ en ook in relatie tot de AVG.⁷ In dit artikel onderzoek ik in het bijzonder hoe de AVG en de in de Data Act geregelde uitwisseling van data via internet-of-things (IoT) producten (in de Data Act 'verbonden producten' genoemd)⁸ samengaan. Kunnen we spreken van een gelukkig huwelijk tussen hoofdstuk II van de Data Act en de AVG?

1. Wat is de Data Act?

De Data Act is een Europese verordening die in diverse hoofdstukken verschillende aspecten van de uitwisseling van data reguleert.

De hoofdstukken die naar verwachting de meeste invloed op de praktijk zullen hebben, zijn hoofdstuk II over de uitwisseling van IoT-data en hoofdstuk VI over het *switchen* van *cloud provider*. Voor partijen die betrokken zijn bij verbonden producten geldt samengevat dat zij gebruikers

van die producten toegang moeten geven tot hun IoT-data en deze op hun verzoek moeten uitwisselen met andere partijen. Cloud-aanbieders moeten het samengevat voor hun klanten mogelijk maken om met hun data naar een andere cloud provider over te stappen (te *switchen*).

Verder geeft de Data Act kaders voor de vergoedingen die in rekening mogen worden gebracht voor het beschikbaar stellen van data tussen ondernemingen en voor geschillenbeslechting ten aanzien van de uitwisseling van data. Ook bevat de Data Act een regeling voor onredelijke contractuele bepalingen in datacontracten tussen ondernemingen, met een 'zwarte lijst' met verboden bepalingen en een 'grijze lijst' met bepalingen die worden vermoed onredelijk te zijn. Tot slot geeft het voorschriften voor interoperabiliteitsnormen en slimme contracten met betrekking tot de uitwisseling van data en schrijft het regels voor ten aanzien van het opvragen van data door Europese en niet-Europese overheidsinstanties.

Er valt genoeg te zeggen (en te schrijven) over de Data Act, maar in dit artikel richt ik mij specifiek op de relatie tussen de Data Act en de AVG, en nog meer specifiek op de uitwisseling van IoT-data.

2. De relatie tussen de Data Act en de AVG

De Data Act en de AVG blijven naast elkaar bestaan, maar zij verschillen (in ieder geval) in hun toepassingsbereik en hun normadressaten.

In artikel 1 lid 5 benadrukt de Data Act dat die verordening geen afbreuk doet aan unie- en nationale wetgeving met betrekking tot de bescherming van persoonsgegevens, de persoonlijke levenssfeer en de vertrouwelijkheid van communicatie en de integriteit van eindapparatuur, waaronder de AVG. Dat artikel bepaalt ook dat bij tegenstrijdigheid met de Data Act de unie- en nationale wetgeving met betrekking tot de bescherming van persoonsgegevens voor gaat.

2.1 Toepassingsbereik Data Act en AVG

Waar de AVG alleen betrekking heeft op persoonsgegevens⁹ heeft de Data Act betrekking op digitale gegevens.¹⁰ Digitale gegevens bestaan volgens artikel 2 lid 1 Data Act uit elke digitale weergave van handelingen, feiten of informatie en elke compilatie van dergelijke handelingen, feiten of informatie, ook in de vorm van geluids-, visuele of audiovisuele opnamen. Hier vallen dus allerlei soorten digitale gegevens onder zoals technische data, gegevens over verbonden objecten zoals gebouwen, machines en

1 Bienenke Braat is advocaat bij Bit Legal en auteur van het boek *Kun je eigenaar zijn van data?*

2 Europese Commissie, Een Europese datastrategie (mededeling), 19 februari 2020, COM (2020) 66 final, zie ook https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_nl

3 Verordening (EU) 2022/868 van het Europees Parlement en de Raad van 30 mei 2022 betreffende Europese datagovernance en tot wijziging van Verordening (EU) 2018/1724 (Datagovernanceverordening).

4 Verordening (EU) 2023/2854 van het Europees Parlement en de Raad van 13 december 2023 betreffende geharmoniseerde regels inzake eerlijke toegang tot en eerlijk gebruik van data en tot wijziging van Verordening (EU) 2017/2394 en Richtlijn (EU) 2020/1828 (Dataverordening).

5 Waarvan de eerste, de European Health Data Space momenteel wordt afgerond, OM (2022) 197 final 2022/0140 (COD) Voorstel voor een Verordening van het Europees Parlement en de Raad betreffende de Europese ruimte voor gezondheidsgegevens. Zie ook https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en.

6 E. Valgaeren en S. Depreeuw, 'Data Governance Act en Data Act: naar een nieuw datarecht?', *Computerrecht* 2023/113.

7 L. Deschuyteneer en A. Van de Meulebroucke, 'Interacties tussen de Data Governance Act, de Data Act en de Algemene Verordening Gegevensbescherming: een nieuwe koers of een geëffend pad?', *Computerrecht* 2023/115.

8 Data uit verbonden producten noem ik hierna ook 'IoT-data'.

9 Zijnde informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (artikel 4 lid 1 AVG).

10 In de Data Act worden dit verder 'gegevens' genoemd.

andere gebruiksvoorwerpen, financiële gegevens, bedrijfsinformatie, communicatiedata, gegevens die op infrastructuur van cloud-aanbieders staan.

Het begrip 'digitale gegevens' onder de Data Act is daarmee breder dan het begrip 'persoonsgegevens' uit de AVG. Als de digitale gegevens betrekking hebben op natuurlijke personen, zijn zij aan te merken als persoonsgegevens onder de AVG en anders niet. Het hangt dus af van de kwalificatie van de digitale gegevens als persoonsgegevens of de bepalingen van de AVG in een gegeven geval van toepassing zijn naast die van de Data Act. In paragraaf 3.3 wordt ten aanzien van IoT-data verder uitgewerkt wanneer die data zijn aan te merken als persoonsgegevens.

2.2 Normadressaten in de Data Act en de AVG

De Data Act en de AVG hebben andere normadressaten. De AVG is van toepassing op verwerkingsverantwoordelijken en verwerkers (artikel 3 lid 1 AVG). Daarbij maakt het niet uit wat voor een soort organisatie de verwerkingsverantwoordelijke of verwerker is: de AVG is van toepassing op de verwerking van persoonsgegevens door een verwerkingsverantwoordelijke of door een verwerker, ongeacht in welke branche deze opereert, welke diensten deze verleent, of het een overheidsinstantie is of een bedrijf.

De Data Act daarentegen richt zich tot verschillende normadressaten. De centrale normadreesaat is de gegevenshouder, maar daarnaast zijn er verplichtingen voor fabrikanten van verbonden producten en verkopers, verhuurders en lessors daarvan, aanbieders van gerelateerde diensten, aanbieders van clouddiensten, slimme contracten en ondernemingen in het algemeen.

Eenzijds is het toepassingsbereik van de AVG dus beperkter dan dat van de Data Act omdat die verordening alleen betrekking heeft op persoonsgegevens en niet op digitale gegevens in het algemeen. Anderzijds is het toepassingsbereik breder in die zin dat alle soorten organisaties die persoonsgegevens verwerken onder de AVG vallen, terwijl de Data Act zich richt op bepaalde soorten (rechts)personen die te maken hebben met digitale gegevens.

3. Enkele begrippen met betrekking tot IoT-data

De Data Act regelt de uitwisseling van data in hoofdstuk II. De kern van dit hoofdstuk is dat gebruikers van verbonden producten toegang moeten krijgen tot hun IoT-data en deze naar hun keuze moeten kunnen overdragen aan een derde. Als de fabrikant het verbonden product niet zo aanbiedt dat de gebruiker rechtstreeks toegang heeft tot de IoT-data,¹¹ is het de gegevenshouder die de IoT-data beschikbaar moet stellen en het voor de gebruiker mogelijk

moet maken deze aan een derde over te dragen (artikel 4 en artikel 5 Data Act).

3.1 Wat zijn verbonden producten?

Van belang is om te weten wat verbonden producten zijn. Dit zijn blijkens artikel 2 lid 5 Data Act (samengevat) goederen die data genereren, waarbij de data via het internet kunnen worden uitgelezen en kunnen worden doorgegeven.

Een korte zijstap over de uitdrukking 'goed'¹² in artikel 2 lid 5 Data Act. Goederen zijn zaken en vermogensrechten (artikel 3:1 BW). Er zijn niet veel andere goederen denkbaar dan zaken die IoT-data kunnen genereren, vermogensrechten kunnen dat niet. Software en artificial intelligence kunnen ook data genereren, maar de goederenrechtelijke status daarvan is op dit moment niet duidelijk. Het begrip 'goed' uit de Data Act valt – naar de huidige stand van zaken – dus samen met het begrip 'zaak' (artikel 3:2 BW), zijnde voor menselijke beheersing vatbare stoffelijke objecten.

Verbonden producten zijn dus, naar de huidige stand van zaken, zaken die data genereren, waarbij de data via het internet kunnen worden uitgelezen en worden doorgegeven.

3.2 Wie is een gebruiker?

Ook van belang is om te weten wie een gebruiker is onder de Data Act, deze heeft immers de rechten op grond van hoofdstuk II Data Act. Een gebruiker is een natuurlijke- of rechtspersoon die een verbonden product in eigendom heeft, of aan wie contractueel tijdelijke rechten zijn overgedragen om dat verbonden product te gebruiken, of die gerelateerde diensten ontvangt (artikel 2 lid 12 Data Act). Gebruikers zijn dus in ieder geval natuurlijke- of rechtspersonen die het product in eigendom hebben. Bijvoorbeeld de consument die een connected consumentenproduct koopt, of het bedrijf dat een zakelijk verbonden product koopt.

Het zijn ook in ieder geval natuurlijke- of rechtspersonen die gebruikmaken van gerelateerde diensten. Blijkens artikel 2 lid 6 Data Act is een gerelateerde dienst een digitale dienst (anders dan een elektronische communicatiedienst zoals Whatsapp), waaronder software, die op het moment van aankoop, huur of lease, ofwel zodanig met het product verbonden is dat de afwezigheid ervan het product zou beletten om een of meer functies uit te voeren, ofwel die vervolgens wordt verbonden met het product om daar functies aan toe te voegen, ofwel de functies van het verbonden product te updaten of aan te passen. In de praktijk zijn dit vaak mobiele apps die samen met het verbonden product kunnen worden gebruikt, of online applicaties waarmee de verbonden producten kunnen worden beheerd.

En wie zijn dan aan te merken als natuurlijke- of rechtspersonen 'aan wie contractueel tijdelijke rechten zijn

¹¹ De fabrikant is hiertoe niet verplicht en mag het product ook zo ontwerpen dat de data alleen indirect, via een andere partij (de gegevenshouder) toegankelijk is. Zie ook antwoord op vraag 19 in Frequently Asked Questions, Data Act, 15 september 2024, versie 1.1: <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act>.

¹² De Engelse uitdrukking is 'item'.

overgedragen om dat product te gebruiken? Zijn dat huurders? Lessees? Personen die het verbonden product in bruikleen hebben? Naar mijn mening volgt uit de Data Act dat gebruikers niet alleen eigenaren, huurders of lessees zijn, maar dat gebruikers ook natuurlijke personen of rechtspersonen kunnen zijn aan wie verbonden producten op een andere contractuele basis beschikbaar zijn gesteld.¹³

In het eerste concept van de Data Act¹⁴ was de definitie van gebruiker beperkt tot 'een natuurlijke of rechtspersoon die een product in eigendom heeft, *huurt of least* ontvangt'. De cursieve tekst is aangepast naar 'aan wie contractueel tijdelijke rechten zijn overgedragen om dat verbonden product te gebruiken'. In overweging 18 licht de Data Act toe dat tijdelijke rechten *bijvoorbeeld* rechten kunnen zijn die zijn verleend uit hoofde van een huur- of een leaseovereenkomst.¹⁵ Het begrip 'tijdelijke rechten' omvat dus kennelijk meer dan alleen het recht om het verbonden product te huren of te leasen, zoals nog wel limitatief stond in het eerdere concept van de Data Act. Gezien deze wetgeschiedenis heeft de wetgever de definitie van gebruiker kennelijk breder willen maken dan alleen een (rechts)persoon die het product heeft gekocht, huurt of leaset.

Hieruit volgt m.i. dat de tijdelijke rechten ook moeten kunnen bestaan uit andere soorten rechten om het verbonden product te gebruiken. Bijvoorbeeld als een werkgever op grond van een (bruikleen)contract verbonden producten beschikbaar stelt aan een werknemer, een uitzendorganisatie aan diens uitzendkrachten, of een vrijwilligersorganisatie aan vrijwilligers. Dit punt is echter alleen relevant als dit soort personen geen gerelateerde dienst gebruiken. Immers, als zij dat wel doen zijn zij hoe dan ook aan te merken als gebruikers.

Tot slot is de vraag hoe het begrip gebruiker uit de Data Act zich verhoudt tot de AVG. Wanneer het verbonden product of de gerelateerde dienst wordt gebruikt door een natuurlijke persoon en de IoT-data zijn aan te merken als diens persoonsgegevens (zie daarover de volgende paragraaf), valt het begrip gebruiker samen met het begrip 'betrokkene' onder de AVG.

3.3 Wanneer zijn IoT-data aan te merken als persoonsgegevens?

Om te weten wanneer IoT-data zijn aan te merken als persoonsgegevens moet eerst worden gekeken naar wat in de Data Act wordt verstaan onder 'IoT-data'. Daarin wordt niet de uitdrukking 'IoT-data' gebruikt, maar de uitdrukking 'eenvoudig beschikbare gegevens, alsook de relevante metagegevens die nodig zijn om die gegevens te interpreteren en te gebruiken' (Artikel 4 lid 1 Data Act en artikel 5 lid 1 Data Act).

Eenvoudig beschikbare gegevens zijn 'productgegevens' en 'gegevens van een gerelateerde dienst' die een gegevenshouder rechtmatig verkrijgt of rechtmatig kan verkrijgen van het verbonden product of de gerelateerde dienst, zonder daarvoor een onevenredig grote inspanning te moeten leveren die verder zou gaan dan een eenvoudige handeling (artikel 2 lid 17 Data Act). 'Productgegevens' zijn op hun beurt gegevens die door het gebruik van het verbonden product worden gegenereerd en die zodanig door de fabrikant zijn ontworpen dat ze via het internet kunnen worden opgevraagd door een gebruiker, gegevenshouder, derde of de fabrikant (artikel 2 lid 15 Data Act). En 'gegevens van een gerelateerde dienst' zijn volgens artikel 2 lid 16 Data Act gegevens die de digitalisering vertegenwoordigen van handelingen van de gebruiker of van gebeurtenissen die gerelateerd zijn aan het verbonden product, die intentioneel door de gebruiker zijn geregistreerd of als een bijproduct van de handeling van de gebruiker zijn gegenereerd tijdens het verlenen van de gerelateerde dienst door de aanbieder.

Samengevat zijn IoT-data dus: opvraagbare data die worden gegenereerd door het gebruik van het verbonden product, data die worden vastgelegd door het gebruik van de software (zoals een mobiele app of online applicatie) die nodig is om het verbonden product te gebruiken, en de daarmee samenhangende metadata. Enkele voorbeelden zijn: temperatuur, druk, audio, pH-waarde, positie, versnelling, snelheid, maar ook gebruiksdata zoals moment van aan- en uitzetten, andere handelingen met het verbonden product, de duur van het gebruik van het verbonden product en de locatie van het product.

Zijn dat soort data dan altijd aan te merken als persoonsgegevens? Dat kan niet zo absoluut worden gesteld. Zolang de gebruiker-natuurlijke persoon niet direct of indirect te identificeren is, zijn de IoT-data geen persoonsgegevens. Er zijn echter niet veel situaties denkbaar waarin data uit verbonden producten die door natuurlijke personen worden gebruikt volledig anoniem zullen blijven.

Bij verbonden producten die puur zakelijk worden gebruikt zullen de IoT-data weliswaar niet noodzakelijkerwijs als persoonsgegevens worden aangemerkt, maar ook die producten kunnen worden gebruikt door natuurlijke personen en worden gekoppeld aan geïdentificeerde of identificeerbare personen – bijvoorbeeld aan werknemers via een ID-pas.

Elektronische *identifiers* zoals IP-adressen en MAC-adressen die uit de verbonden producten worden uitgelezen

13 De Europese Commissie is hier zelf niet consistent in. Op deze webpagina 'Data Act explained': <https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained> geeft de Europese Commissie een limitatieve opsomming: '(i.e. any legal or natural person who owns, rents or leases a connected product)'. Echter in de FAQ's bij vraag 11 geeft de EC aan: "This implies that the user has a stable right on the connected product, e.g. ownership, or a right from a rent or lease contract."

14 2022/0047, Voorstel voor een Verordening van het Europese Parlement en de Raad betreffende geharmoniseerde regels inzake eerlijke toegang tot en eerlijk gebruik van data (Dataverordening).

15 Met 'dienst' werd in dit concept het huidige begrip 'gerelateerde dienst' bedoeld.

16 De tekst uit het hiervoor genoemde online document 'Data Act explained' die luidt: 'i.e. any legal or natural person who owns, rents or leases a connected product' is niet consistent met de tekst "A data holder must have a contract with the user (e.g. sales contract, rental contract, related service contract, etc.) defining the rights regarding the access, use and sharing of the data that is generated by the connected product or related service".

kúnnen op zichzelf persoonsgegevens zijn, hoewel dat afhangt van de feitelijke situatie en de middelen die de gegevenshouder heeft om de gebruiker te identificeren.¹⁷ Echter, hoe dan ook vloeit uit de verplichting in de Data Act om de IoT-data toegankelijk te maken voor de gebruiker voort dat de gebruiker in enige mate moet worden geïdentificeerd. De gebruiker moet immers toegang hebben tot diens eigen IoT-data.¹⁸ Daarbij wordt in de regel gebruikgemaakt van accounts die de gebruiker in de gerelateerde dienst aanmaakt waarbij deze een gebruikersnaam of een e-mailadres invoert. Als dat account van een natuurlijke persoon is, kan de gebruiker aan de hand van de gebruikersnaam of het e-mailadres al worden geïdentificeerd.¹⁹ Wanneer een natuurlijke persoon het verbonden product gebruikt, leiden de verplichtingen van de Data Act dus in feite tot de noodzaak om van de IoT-data persoonsgegevens te 'maken'.

Als het eenmaal om een geïdentificeerde of identificeerbare natuurlijke persoon gaat, zullen veel van de IoT-data zijn aan te merken als persoonsgegevens. Denk bij bijvoorbeeld een slimme tandenborstel aan het aantal keren dat het op een dag is gebruikt, hoe lang, hoe hard er is gepoetst, hoe vaak er is ingelogd op de app et cetera. Dit is allemaal informatie betreffende de gebruiker, dus persoonsgegevens.

Het onderscheid wordt echter meer diffuus bij meer algemene IoT-data die niet betrekking hebben op een specifieke gebruiker. Een slimme plafondlamp die bijvoorbeeld zo wordt ingesteld dat hij iedere dag op een bepaald tijdstip aan- en uitgaat, hoeft niet per se informatie te geven over de persoon die de lamp gebruikt, ook als de naam of het e-mailadres van die persoon bekend zijn. Maar een nachtlamp die precies registreert wanneer dezelfde bewoner de lamp aan- en uitzet kan informatie geven over het slaappatroon van die bewoner: wanneer deze opstaat en naar bed gaat of deze 's nachts vaak wakker wordt. Dat zijn wel persoonsgegevens.

Het voorgaande maakt duidelijk dat van geval tot geval moet worden bekeken welk soort gebruiker het verbonden product gebruikt en welke IoT-data er precies worden uitgelezen, om na te gaan of de IoT-data als persoonsgegevens kwalificeren.

4. AVG-rollen van bij de uitwisseling IoT-data betrokken (rechts)personen

De volgende vraag die ik behandel is welke (rechts)personen zijn aan te merken als verwerkingsverantwoordelijken ten aanzien van de IoT-data die persoonsgegevens

zijn. Is dat de verkoper, verhuurder of lessor van het verbonden product? De aanbieder van de gerelateerde dienst? De partij die het verbonden product op een andere contractuele basis aan natuurlijke personen beschikbaar stelt? De Data Act geeft hier geen antwoord op, maar al deze partijen kunnen m.i. worden aangemerkt als verwerkingsverantwoordelijken.

4.1 Verwerkingsverantwoordelijke en verwerker

Wie verwerkingsverantwoordelijke is, hangt af van het antwoord op de feitelijke vraag welke (rechts)persoon het doel en de middelen van de verwerking van de persoonsgegevens bepaalt (artikel 4 lid 7 AVG). Daarbij gaat het er om welke beslissende invloed de (rechts)persoon uitoefent over die doeleinden en de middelen.²⁰

Waar persoonsgegevens worden verwerkt en de AVG van toepassing is²¹ kunnen (rechts)personen die de persoonsgegevens verwerken maar één van twee rollen hebben: die van verwerkingsverantwoordelijke (al dan niet gezamenlijk met een andere verwerkingsverantwoordelijke) of die van verwerker.

In overweging 22 van de Data Act staat dat verwerkers niet worden geacht als gegevenshouders op te treden. Dit is een logische overweging. Immers, de verwerker dient op grond van de AVG alleen de instructies van de verwerkingsverantwoordelijke op te volgen (artikel 28 lid 3 sub a AVG). De verwerker kan dus niet bepalen wat er met de persoonsgegevens gebeurt, dat kan alleen de verwerkingsverantwoordelijke. De verwerker kan dus ook niet als gegevenshouder bepalen wat er met de IoT-data gebeurt, en of de gebruiker daar toegang toe krijgt of niet.

4.2 Gegevenshouder onder de Data Act

Zijn gegevenshouders dan altijd verwerkingsverantwoordelijken?

Een gegevenshouder is een natuurlijke of rechtspersoon die op grond van de Data Act, het unierecht of nationale recht verplicht is gegevens te gebruiken en deze ter beschikking te stellen (artikel 2 lid 13 Data Act). De definitie omvat een cirkelredenering: de verplichting om data beschikbaar te maken rust op de gegevenshouder en de gegevenshouder is de (rechts)persoon die op grond van de Data Act, het unierecht of het nationale recht een verplichting heeft om data beschikbaar te stellen.²² Daarom is dit een ongelukkige definitie.

De overwegingen van de Data Act geven geen houvast op dit punt, dus is het zinvol te kijken naar de begrippen 'eenvoudig beschikbare gegevens' en 'productgegevens'.

17 HvJ EU 19 oktober 2016, C-582/14, ECLI:EU:C:2016:779, r.o. 49 (*Breyer*) en HvJ EU 17 juni 2021, C-597/19, ECLI:EU:C:2021:492, r.o. 102 (*Mircom*).

18 Artikel 4 lid 5 Data Act geeft in dit verband aan dat een gegevenshouder, om na te gaan of een natuurlijke of rechtspersoon een gebruiker is, niet van deze personen kan verlangen dat zij meer informatie verstrekken dan nodig is.

19 De discussie over het gebruik van aliases of nep-emailadressen daargelaten.

20 Vlg. HvJ EU 10 juli 2018, C-25/17, ECLI:EU:C:2018:551, r.o. 66 (*Jehova getuigen*) en HvJ EU 29 juli 2019, C-40/17, ECLI:EU:C:2019:629, r.o. 78 (*Fashion ID*).

21 Ingevolge artikel 2 AVG (materiaal toepassingsgebied) en artikel 3 (territoriaal toepassingsgebied). De AVG is bijvoorbeeld niet van toepassing bij verwerking door een natuurlijke persoon bij de uitoefening van zuiver persoonlijke of huishoudelijke activiteiten (artikel 2 lid 2 sub c AVG).

22 Zo wordt ook gesignaleerd door P. Wolters, *De invloed van de Data Act op de verschuivende balans tussen gegevensbescherming en het vrije verkeer van data*, Ars Aequi januari 2023, p. 31.

Zoals hiervoor aangegeven zijn eenvoudig beschikbare gegevens aan te merken als productgegevens en gegevens van een gerelateerde dienst die een gegevenshouder *rechtmatig verkrijgt of rechtmatig kan verkrijgen* van het verbonden product of de gerelateerde dienst, zonder daarvoor een onevenredig grote inspanning te moeten leveren die verder zou gaan dan een eenvoudige handeling (artikel 2 lid 17 Data Act). Productgegevens zijn op hun beurt gegevens die door het gebruik van het verbonden product worden gegenereerd en die zodanig door de fabrikant zijn ontworpen *dat ze via het internet kunnen worden opgevraagd* door een gebruiker, *gegevenshouder*, derde of de fabrikant (artikel 2 lid 15 Data Act). Voorts bepaalt artikel 4 lid 1 Data Act dat de gegevenshouder de IoT-data ter beschikking moet stellen aan de gebruiker 'met dezelfde kwaliteit als de voor de gegevenshouder *beschikbare* gegevens.'

Hieruit kan worden gedistilleerd dat een gegevenshouder is aan te merken als de natuurlijke- of rechtspersoon die de IoT-data rechtmatig verkrijgt of kan verkrijgen en die over de middelen beschikt om de data op te vragen. Ik zou dat willen samenvatten als: de natuurlijke- of rechtspersoon die rechtmatig over de IoT-data beschikt of kan beschikken.²³ Immers, een natuurlijke- of rechtspersoon die niet in feitelijke of juridische zin over de data beschikt, kan ook niet verplicht worden die data beschikbaar te stellen aan de gebruiker. Dit strookt ook met het gebruik van de uitdrukking 'gegevenshouder'.

De begrippen gegevenshouder en verwerkingsverantwoordelijke zijn echter niet synoniem. Een verwerkingsverantwoordelijke hoeft niet noodzakelijkerwijs toegang te hebben tot de persoonsgegevens of daar feitelijk over te beschikken om aan te worden gemerkt als verwerkingsverantwoordelijke.²⁴ Voldoende is dat de (rechts)persoon het doel en de middelen van de verwerking bepaalt. De gegevenshouder daarentegen, zo blijkt uit de voorgaande analyse, moet wel over de IoT-data (kunnen) beschikken om als gegevenshouder te worden aangemerkt.

Een partij die over IoT-data beschikt die tevens persoonsgegevens zijn en die verwerker is, wordt, zoals eerder aangegeven, niet aangemerkt als gegevenshouder. Dat betekent dat een gegevenshouder die over dat soort IoT-data beschikt moet worden aangemerkt als verwerkingsverantwoordelijke, al dan niet gezamenlijk met een andere verwerkingsverantwoordelijke. Die gegevenshouder kan immers alleen de rol van verwerker of van (gezamenlijk) verwerkingsverantwoordelijke hebben.

4.3 Verschillende AVG-scenario's met IoT-data

Er zijn bij het verwerken van IoT-data die persoonsgegevens zijn meerdere scenario's denkbaar, hierna noem ik er – niet limitatief – een aantal. Het scenario onder d. is geba-

seerd op de hiervoor verdedigde stelling dat een gebruiker-natuurlijke persoon ook een persoon kan zijn die het verbonden product in gebruik heeft anders dan als eigenaar, huurder of lessee.

- a) Een consument koopt een slimme ijskast. De fabrikant levert daarbij een mobiele app om de temperatuur van de ijskast op afstand aan te passen. De consument maakt met een e-mailadres een account in de app. Via de mobiele app krijgt de consument ook te zien wanneer de ijskast leeg begint te raken en er weer boodschappen moeten worden gedaan. Wanneer deze informatie een patroon weergeeft over de gebruiker van de ijskast gaat het ook om persoonsgegevens. De fabrikant is aan te merken als verwerkingsverantwoordelijke van de IoT-data.
- b) Dezelfde fabrikant maakt het mogelijk om via een applicatie van een derde partij toegang te krijgen tot de IoT-data, de fabrikant heeft zelf niet die toegang, slaat ze ook niet op en bepaalt ook niet wat er met de IoT-data gebeurt. De derde partij die de applicatie aanbiedt is aan te merken als verwerkingsverantwoordelijke, de fabrikant niet.
- c) Een consument huurt een verbonden fiets. De verhuurder levert een mobiele app mee die het mogelijk maakt om het fietsslot te activeren. De app geeft ook toegang tot de IoT-data die de fiets genereert. Daarmee kan de huurder alle ritten bekijken, inclusief de gps-locaties. De mobiele app-aanbieder verwerkt de IoT-data als verwerker. De verhuurder heeft inzicht in de door de fietsen gegenereerde data. De fabrikant van de fiets heeft geen toegang tot de data en bepaalt ook niet wat daarmee gebeurt. De verhuurder is aan te merken als verwerkingsverantwoordelijke, de fabrikant niet.
- d) Een werkgever stelt verbonden gereedschap beschikbaar aan diens werknemers, het gereedschap wordt via een persoonlijke code van de werknemers aan hen gekoppeld. De werkgever heeft via een eigen dashboard inzicht in de IoT-data die uit de producten wordt gelezen, zoals op welke tijdstippen op de dag de werknemer het gereedschap gebruikt en hoe lang en daarin wordt het gereedschap ook op afstand beheerd. Het dashboard wordt geleverd door de fabrikant van het gereedschap, de fabrikant verwerkt de IoT-data alleen in opdracht van de werkgever. De werkgever is aan te merken als verwerkingsverantwoordelijke en de fabrikant als verwerker.
- e) Een fabrikant verkoopt verbonden auto's aan een leasemaatschappij. De fabrikant verzamelt data uit de auto's voor eigen doeleinden en maakt deze ook beschikbaar voor de leasemaatschappij. Zowel de fabrikant als de leasemaatschappij zijn aan te merken als verwerkingsverantwoordelijken.
- f) Een fabrikant verkoopt verbonden tandenborstels. De fabrikant leest de IoT-data uit en stelt deze ter beschikking aan een aanbieder van een mobiele app. Die aanbieder biedt een app aan waarmee verbonden

²³ Wolters verwoordt dit als een partij die de data onder zich 'houdt' en 'feitelijk of rechtens controle heeft over de data', p. 31. De Europese Commissie gebruikt in de FAQ's de bewoordingen 'who controls access to the readily available data', p. 14.

²⁴ HvJ EU 10 juli 2018, ECLI:EU:C:2018:551 (*Jehovan todistajat*), r.o. 75.

producten van verschillende fabrikanten kunnen worden uitgelezen en beheerd, waaronder de IoT-data uit de tandenborstels. De fabrikant is aan te merken als verwerkingsverantwoordelijke en de aanbieder van de app ook.

De gebruikers van de betreffende verbonden producten moeten zich op grond van de Data Act richten tot de verwerkingsverantwoordelijken-gegevenshouders om hun rechten op grond van de Data Act en de AVG in te roepen.

4.4 Kunnen (zakelijke) gebruikers ook gegevenshouders zijn?

Kunnen zakelijke partijen die de verbonden producten aan andere gebruikers in gebruik geven en daarbij als gegevenshouder IoT-data verwerken zelf ook worden aangemerkt als gebruikers? Dit zou wel moeten volgen uit de Data Act. Immers, dit soort partijen heeft de verbonden producten in eigendom of kan die zelf huren of leasen, daarmee vallen zij onder de definitie van gebruiker. De Europese Commissie denkt daar echter anders over. Bij vraag 31 van de FAQ's over de Data Act, namelijk of een bedrijf tegelijkertijd zowel gebruiker als datahouder kan zijn, stelt de Europese Commissie dat dit niet zo kan zijn voor dezelfde IoT-data.²⁵

Mogelijk heeft de Europese Commissie hier bedoeld te zeggen dat de zakelijke gebruiker niet *op precies hetzelfde moment ('tegelijkertijd')* voor dezelfde soort IoT-data ook gebruiker kan zijn. Bij verwerkingen die elkaar opvolgen zou een zakelijke gebruiker namelijk wel zowel gebruiker als gegevenshouder moeten kunnen zijn.

In het voorbeeld van de verhuurder van de verbonden fietsen is de verhuurder als eigenaar de zakelijke gebruiker en zijn de huurders ook gebruikers, want deze huren de fietsen. De fietsen genereren IoT-data die 'van' de huurders zijn. Diezelfde data krijgt de verhuurder ook te zien in een eigen dashboard. Kunnen de huurders zich dan niet tot de verhuurder – als bedrijf dat ook gebruiker is – wenden voor overdracht van hun IoT-data? Ik denk dat de zakelijke gebruiker in zo'n geval ook gegevenshouder kan zijn.

In overweging 34 van de Data Act staat namelijk uitdrukkelijk dat een gebruiker ook een gegevenshouder kan zijn. Daarin staat:

“Wanneer de gegevenshouder en de gebruiker gezamenlijke verwerkingsverantwoordelijken zijn in de zin van artikel 26 van Verordening (EU) 2016/679, zijn zij verplicht om door middel van een onderlinge regeling op transparante wijze hun respectieve verantwoordelijkheden voor de naleving van die verordening vast te stellen. *Het moet duidelijk zijn dat een dergelijke gebruiker, zodra gegevens beschikbaar zijn gesteld, op zijn beurt gegevenshouder kan worden*, indien die gebruiker voldoet aan de criteria van deze verordening en dus onderworpen wordt aan de verplichtingen om gegevens beschikbaar te stellen uit hoofde van deze verordening.”

Blijkens deze overweging kan een gebruiker dus voor dezelfde set IoT-data ook gegevenshouder zijn, als deze gezamenlijk verwerkingsverantwoordelijke is met de datahouder. Geldt dat ook als de verwerkingsverantwoordelijke niet *gezamenlijk* verantwoordelijke is, maar zelfstandig verantwoordelijke? De Data Act sluit deze mogelijkheid m.i. niet uit.

Als de stellingname zou worden gevolgd dat een bedrijf niet tegelijkertijd zowel gebruiker als gegevenshouder kan zijn, dan zou dat in de praktijk tot – vermoedelijk vaak voorkomende – situaties leiden waarin de gebruiker-betrokkene diens rechten onder de Data Act niet kan doen gelden, omdat er geen gegevenshouder kan worden geïdentificeerd.

De Commissie onderkent in het antwoord op vraag 31 van de FAQ's dat de Data Act situaties toestaat waarin een persoon een gebruiker kan zijn zonder dat er een gegevenshouder is. Daarbij geeft de Commissie als voorbeeld de situatie waarin een natuurlijke persoon een verbonden product heeft gekocht en daarop direct toegang heeft tot de data, maar de fabrikant geen toegang heeft en dus geen gegevenshouder is. De natuurlijke persoon heeft in dit scenario direct toegang tot de data, dan is het minder bezwaarlijk dat er geen gegevenshouder is. De Data Act geeft de fabrikant echter de vrijheid producten ook zo te ontwerpen dat de data niet direct (rechtstreeks) toegankelijk zijn, maar alleen indirect.²⁶ Dat laatste is wat in de praktijk het meest gebeurt bij IoT-producten.

Het zal niet zelden gebeuren dat een bedrijf de verbonden producten verhuurt, leaset of anderszins in gebruik geeft, de fabrikant geen toegang heeft tot de data en de aanbieder van de gerelateerde dienst is aan te merken als verwerker. In dat geval heeft de gebruiker-betrokkene, als de zakelijke gebruiker niet ook gegevenshouder kan zijn, geen rechten onder de Data Act.

Ter illustratie kan het scenario van de verhuurder van de fietsen weer worden gebruikt. De fabrikant heeft geen toegang tot de data in de app, die is dus niet gegevenshouder. De verhuurder is onder de Data Act gebruiker, want deze heeft de fietsen in eigendom en heeft ook toegang tot de data. De huurder van de fiets is ook gebruiker, want deze huurt de fiets. De verhuurder is aan te merken als verwerkingsverantwoordelijke en de huurder als betrokkene. De aanbieder van de app is in dit geval verwerker, dus geen gegevenshouder. Als de verhuurder-gebruiker geen gegevenshouder kan zijn, is er geen gegevenshouder waar de huurder-gebruiker zich tot kan wenden onder de Data Act. Deze heeft dan alleen rechten ten aanzien van de IoT-data die zijn aan te merken als persoonsgegevens maar niet ten aanzien van niet-persoonsgegevens op grond van de Data Act. Los van de tekst in overweging 31 kun je je afvragen of dit een gevolg is dat de wetgever voor ogen heeft gehad.

²⁵ Frequently Asked Questions, Data Act, 15 september 2024, versie 1.1, p. 21.

²⁶ Artikel 3 lid 1 Data Act, zie ook de Frequently Asked Questions, Data Act, 15 september 2024, versie 1.1, antwoord op vraag 19, p. 21.

4.5 Tussenconclusie

Het voorgaande laat zien dat gegevenshouders van IoT-data die persoonsgegevens zijn, zijn aan te merken als verwerkingsverantwoordelijken onder de AVG. Verwerkers kunnen dat niet zijn. Daarbij is m.i. niet uit te sluiten dat gebruikers zelf ook kunnen worden aangemerkt als gegevenshouders wanneer zij verbonden producten verhuren, leasen of op een andere contractuele basis ter beschikking stellen aan andere gebruikers.

5. De rechtsgronden voor het delen van IoT-data

Een andere vraag die relevant is, is wat de rechtsgrond is bij de verwerking van IoT-data. Om rechtsgeldig persoonsgegevens te verwerken is altijd een rechtsgrond nodig op grond van artikel 6 lid 1 AVG. De toepasselijke rechtsgrond hangt af van de feitelijke situatie. Daarbij kunnen voor verschillende soorten verwerkingen en doeleinden verschillende rechtsgronden gelden.

De verschillende verwerkingen van IoT-data kunnen, en zullen vaak, verschillende rechtsgronden hebben. De 'bronverwerking' is de registratie van de IoT-data via het verbonden product en de verwerking daarvan via de gerelateerde dienst. De toegang tot de IoT-data door de gebruiker-betrokkene zelf en het overdragen daarvan aan een derde op verzoek van de gebruiker is ook een verwerking, evenals het gebruik daarvan door de gebruiker die niet een betrokkene is, bijvoorbeeld het bedrijf dat verbonden producten heeft gekocht en die aan gebruikers die natuurlijke personen zijn ter beschikking stelt. Dat geldt ook voor het gebruik van de IoT-data door de fabrikant en de aanbieder van de gerelateerde dienst voor hun eigen doeleinden. Tot slot is het ontvangen van de IoT-data door de derde op verzoek van de gebruiker – dit kan de zakelijke gebruiker zijn, maar ook de gebruiker-betrokkene – ook een verwerking waar een rechtsgrond voor moet zijn.

De Data Act geeft in artikel 4 lid 12 en artikel 5 lid 7 aan dat als de gebruiker niet een betrokkene²⁷ is – en dus een rechtspersoon-gebruiker is – de gegevenshouder de IoT-data die persoonsgegevens zijn alleen beschikbaar stelt aan een dergelijke gebruiker als daar een rechtsgrond voor is, en als het om bijzondere persoonsgegevens gaat, als wordt voldaan aan artikel 9 AVG en daarnaast aan artikel 5 lid 3 van de e-Privacyrichtlijn²⁸ (geïmplementeerd in artikel 11.7a Telecommunicatiewet (Tw)).

Deze artikelen hebben op zich niet veel toegevoegde waarde. Immers, voor *elke* verwerking van persoonsgegevens moet een rechtsgrond zijn – dus niet alleen wanneer de gebruiker niet een betrokkene is, maar ook wanneer de gebruiker dat wel is – en bijzondere persoonsgegevens mogen überhaupt alleen worden verwerkt als daar een

uitzonderingsgrond voor bestaat onder artikel 9 AVG. Maar de verwijzing naar artikel 5 lid 3 van de e-Privacyrichtlijn, dat er waarschijnlijk op advies van de toezicht-houders (EDPB en EDPS) in is gekomen,²⁹ is wel nuttig.

5.1 Artikel 11.7a Telecommunicatiewet

Het is de moeite waard om eerst te kijken naar de rol van artikel 11.7a Tw bij verbonden producten. In artikel 11.7a Tw zijn regels vastgelegd die ook wel de cookie-regels worden genoemd. Die bepalingen hebben echter niet alleen betrekking op cookies, maar op het via een elektronisch communicatienetwerk opslaan van informatie of het toegang verkrijgen tot informatie op randapparaat van een gebruiker,³⁰ al dan niet via software die daarop is geïnstalleerd. Wanneer de IoT-data uit een verbonden product worden uitgelezen en dat product kan worden aangemerkt als randapparatuur, valt die situatie dus onder artikel 11.7a Tw.

Onder randapparatuur moet, samengevat, worden verstaan apparaten die voor het overbrengen, verwerken of ontvangen van informatie direct of indirect op een telecommunicatienetwerk zijn aangesloten.³¹ Overweging 36 van de Data Act benoemt dat IoT-apparaten als randapparatuur beschouwd worden als deze direct of indirect verbonden zijn met een openbaar communicatienetwerk. Voorbeelden van randapparatuur zijn smartphones, smart-tv's en vergelijkbare IoT-apparaten en laptops, connected auto's, medische apparaten, connected tv's, smart-brillen.³² Veel verbonden producten zijn aan te

²⁷ In de Nederlandse tekst van de Data Act staat 'data subject' maar daar zal 'betrokkene' mee bedoeld zijn.

²⁸ Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie).

²⁹ Gezamenlijke opinie van de European Data Protection Board en European Data Protection Supervisor over de Data Act (2/2022, 4 mei 2022), randnummer 43.

³⁰ Artikel 11.7a Tw geldt ten aanzien van gebruikers en niet ten opzichte van abonnees (van telecommunicatiediensten). Onder het begrip 'gebruiker van randapparatuur' worden zowel de abonnee die gebruiker is verstaan als de gebruiker die geen abonnee is, zie G.J. Zwenne, *Tekst en Commentaar Privacy en Gegevensbeschermingsrecht*, Kluwer, Deventer, 2022, commentaar bij artikel 11.7a, nummer 2.

³¹ De definitie in artikel 1 a), Richtlijn 2008/63/EG van de commissie van 20 juni 2008 betreffende de mededinging op de markten van telecommunicatie-eindapparatuur luidt: 'De apparaten die voor overbrenging, verwerking of ontvangst van informatie direct of indirect op de interface van een openbaar telecommunicatienet zijn aangesloten; in beide gevallen, direct of indirect, kan de aansluiting geschieden per draad, per optische vezel of via elektromagnetische golven; een aansluiting is indirect wanneer een apparaat geplaatst is tussen het eindapparaat en de interface van het net.'

³² FAQ's Data Act, p. 7. Zie tevens EDPB Guidelines 02/2021 over *virtual voice assistants*, randnummer 25 en EDPB Guidelines 2/2023 on *Technical Scope of Art. 5(3) of e-Privacy Directive*, randnummer 16 en 17 alsook 28, waar de toezichthouders aangeven dat de bescherming van vertrouwelijkheid van de informatie niet beperkt is tot de persoonlijke levenssfeer of natuurlijke personen, maar ook het recht op respect voor hun correspondentie of de gerechtvaardigde belangen van rechtspersonen kan betreffen en dat randapparatuur die toestaat dat dergelijke correspondentie en gerechtvaardigde belangen worden uitgevoerd zijn beschermd op grond van artikel 5 lid 3 e-Privacyrichtlijn.

merken als randapparatuur zoals bedoeld in de e-Privacy-richtlijn.³³

Als artikel 11.7a Tw van toepassing is moet de gebruiker van het verbonden product toestemming geven voor het uitlezen van de IoT-data (artikel 11.7a lid 1 sub b Tw) en moet deze worden voorzien van duidelijke en volledige informatie conform de AVG (artikel 11.7a lid 1 sub a Tw). Dit hoeft echter niet als de opslag van, of de toegang tot de IoT-data uitsluitend tot doel heeft de communicatie over het communicatienetwerk uit te voeren (artikel 11.7a lid 3 sub a Tw). Dat hoeft ook niet als dat strikt noodzakelijk is om de door de gebruiker gevraagde dienst van de informatiemaatschappij te leveren (artikel 11.7a lid 3 sub b Tw).

Een gerelateerde dienst (bijvoorbeeld mobiele app) kan worden aangemerkt als een door de gebruiker gevraagde dienst van de informatiemaatschappij. Zonder de toegang tot de IoT-data kan die gerelateerde dienst niet worden verleend. Het komt mij dus voor dat de actie van de toegang tot de IoT-data om te zorgen dat de gebruiker-betrokkene de gerelateerde dienst kan gebruiken onder de uitzondering van lid 3 sub b van artikel 11.7a Tw valt en dat *daar* geen toestemming voor nodig is.

Dat is anders in de in de artikelen 4 lid 12 en artikel 5 lid 7 Data Act genoemde gevallen waarin een *andere* gebruiker dan de gebruiker-natuurlijke persoon toegang krijgt tot de IoT-data. Bijvoorbeeld de in de scenario's hiervoor genoemde verhuurder, lessor of andere partij die het verbonden product beschikbaar stelt. En ook in het geval dat een ander, zoals de fabrikant of de aanbieder van de gerelateerde dienst, toegang heeft tot de IoT-data voor eigen doeleinden. Het gaat dan immers niet om een door de gebruiker-betrokkene gevraagde dienst en ook niet uitsluitend om de communicatie over het elektronische communicatienetwerk. De uitzonderingen in lid 3 van artikel 11.7a Tw zijn dan dus niet van toepassing. Dit betekent dat de gebruiker toestemming moet geven voordat dergelijke derden toegang kunnen krijgen tot de IoT-data (voor eigen doeleinden).

Hoewel de toestemming die vereist is op grond van artikel 11.7a Tw aan de eisen moet voldoen van toestemming uit de AVG,³⁴ betekent dat niet noodzakelijkerwijs dat de verdere verwerking van de IoT-data alleen maar op toestemming kan worden gebaseerd. Hoewel toestemming de meest toepasselijke en waarschijnlijke rechtsgrond is voor het verder verwerken van de IoT-data,³⁵ is m.i. niet uit te sluiten dat verdere verwerkingen ook gebaseerd kunnen

worden op de andere rechtsgronden van artikel 6 lid 1 AVG.³⁶ Een strikte uitleg dat toestemming nodig is voor *alle* opvolgende verwerkingshandelingen volgt niet uit de AVG, noch uit artikel 5 lid 3 van de e-Privacyrichtlijn. Bovendien zou dan niet in artikelen 4 lid 12 en 5 lid 7 van de Data Act hebben gestaan dat wanneer de IoT-data aan een rechtspersoon-gebruiker ter beschikking worden gesteld daar *een* rechtsgrond voor moet zijn. Dan zou daar hebben gestaan dat dit alleen op de rechtsgrond toestemming kan. Hierna zal ik dan ook de rechtsgronden uit artikel 6 lid 1 AVG afzonderlijk bespreken om na te gaan of de verwerking van de IoT-data die persoonsgegevens zijn (hierna ook alleen 'IoT-data' genoemd) daarop kan worden gebaseerd. Daarbij laat ik de vitaal belang rechtsgrond uit artikel 6 lid 1 sub d AVG buiten beschouwing.

5.2 De wettelijke verplichting

De Data Act geeft in overweging 7 aan dat die verordening zelf geen rechtsgrond vormt voor het verwerken van persoonsgegevens. Ook de verplichting van de gegevenshouder om de gebruiker toegang te geven tot de IoT-data en die op verzoek aan een derde over te dragen vormt blijkens deze overweging niet de rechtsgrond voor het verwerken van die persoonsgegevens. Artikel 6 lid 1 sub c AVG vormt in samenhang met de Data Act zelf dus niet de rechtsgrond voor de verwerking van die persoonsgegevens.³⁷

De verwerking van IoT-data zou wel eventueel op een andere wettelijke verplichting kunnen worden gebaseerd. Een voorbeeld van zo'n wettelijke verplichting is de zogenaamde automatische eCall naar het noodnummer 112 als zich een serieus ongeluk voordoet met een connected auto.³⁸ Het is zeker niet uit te sluiten dat in de toekomst meer van dit soort rechtstreekse wettelijke verplichtingen komen om IoT-data uit verbonden producten te verwerken.

Ook kunnen IoT-data door een bevoegde overheidsinstantie worden opgevraagd op grond van een wettelijke verplichting, bijvoorbeeld de Belastingdienst die bepaalde IoT-data opvraagt in het kader van een onderzoek. Voor het doorgeven van die data is de rechtsgrond dan artikel 6 lid 1 sub c AVG.

5.3 Uitvoering van de overeenkomst

De rechtsgrond van artikel 6 lid 1 sub b AVG, inhoudende dat de verwerking van persoonsgegevens noodzakelijk is

33 De European Data Protection Board en European Data Protection Supervisor geven in hun gezamenlijke opinie over de Data Act (2/2022, mei 2022) aan dat het begrip randapparatuur deels overlapt met de definitie van (connected) product, randnummers 40 en 41, onder verwijzing naar de EDPB Guidelines 02/2021 over *virtual voice assistants*. Zie daarnaast de EDPB Guidelines 1/2020 over verwerking van persoonsgegevens in de context van *connected vehicles* en *mobility related applications*, randnummer 13.

34 Artikel 11.1 onder g Tw.

35 Gezamenlijke opinie EDPB en EDPS over de Data Act, randnummer 44 en EDPB Guidelines 02/2021 over *virtual voice assistants*, randnummer 27.

36 Dit volgt in ieder geval uit de EDPB Guidelines 1/2020 over verwerking van persoonsgegevens in de context van *connected vehicles* en *mobility related applications* randnummers 14, 106, 131 waar andere rechtsgronden dan toestemming worden genoemd. En hoewel de EDPB wegblijft van de rechtsgrond van het gerechtvaardigd belang (artikel 6 lid 1 sub f AVG), is niet in te zien waarom de verdere verwerking niet op die rechtsgrond zou kunnen worden gebaseerd.

37 Dit geldt overigens ook voor het verplicht overhandigen van persoonsgegevens aan overheidsinstanties op grond van hoofdstuk V Data Act, zie ook overweging 69 Data Act.

38 EDPB Guidelines 1/2020 over verwerking van persoonsgegevens in de context van *connected vehicles* en *mobility related applications* randnummers 128-131.

voor het uitvoeren van een overeenkomst met de betrokkene, of het treffen van precontractuele maatregelen, moet beperkt worden uitgelegd. De verwerking moet objectief onontbeerlijk zijn om een doel te bereiken dat integreerend deel uitmaakt van de aan de betrokkene te leveren contractuele prestatie. Die verwerking moet essentieel zijn voor de correcte uitvoering van de tussen de verwerkingsverantwoordelijke en betrokkene gesloten overeenkomst.³⁹

Dat is m.i. het geval bij de verwerking van de IoT-data via een mobiele applicatie (gerelateerde dienst) die de gebruiker-betrokkene gebruikt. De overeenkomst voor het gebruik van die applicatie kan niet correct worden uitgevoerd zonder de IoT-data via die app beschikbaar te maken.

Ook kan dat m.i. gezegd worden als de gebruiker-betrokkene de gegevenshouder verzoekt diens IoT-data over te dragen aan een derde op grond van artikel 5 lid 1 Data Act. Dit kan worden gezien als een overeenkomst tussen de gebruiker-betrokkene en de derde.⁴⁰ De verwerkingshandeling van het delen van de IoT-data met de derde kan (of moet) dus worden gebaseerd op artikel 6 lid 1 sub b AVG, zowel voor de verzender als de ontvanger.

In het eerder genoemde scenario van de verhuur van de verbonden fietsen, is de vraag of de verhuurder de IoT-data verwerkt omdat dit *noodzakelijk* is voor de uitvoering van de huurovereenkomst zelf. Zeker niet alle IoT-data zullen daarvoor noodzakelijk zijn. Als de verhuurder de gps-locaties van de fietsen registreert om de fietsen weer te kunnen revindiceren, is dat niet noodzakelijk voor de uitvoering van die overeenkomst, maar voor het gerechtvaardigd belang van de verhuurder. Als de gps-locatie wordt geregistreerd zodat de huurder tijdens de fietstocht zelf kan zien waar deze is, dan kan m.i. wel gezegd worden dat de locatie noodzakelijk is voor het uitvoeren van de overeenkomst. En stel dat de verhuurder het mogelijk maakt om via self-service de gehuurde producten op te halen. De IoT-data uit het gehuurde product geven aan wanneer het product is meegenomen en weer is teruggebracht en op basis daarvan stelt de verhuurder vast hoeveel de huurder moet betalen. In dit geval zou het verwerken van die gegevens m.i. ook als noodzakelijk voor de uitvoering van de overeenkomst kunnen worden aangemerkt.

En wat als de gegevenshouder de IoT-data voor doeleinden wil gebruiken die helemaal losstaan van de overeenkomst met de gebruiker? Bijvoorbeeld de fabrikant die IoT-data uit alle apparaten wil aggregeren tot data die inzicht geven in hoeveel apparaten zich in welke landen bevinden? Staat de Data Act daaraan in de weg? Als het gaat om persoonsgegevens, staat de Data Act daar niet aan in

de weg en laat het dit over aan de AVG.⁴¹ Daarvoor moet worden gekeken naar de andere rechtsgronden uit artikel 6 lid 1 AVG.

5.4 *Gerechtvaardigd belang*

De rechtsgrond die voor veel organisaties in aanmerking komt om de IoT-data te verwerken, buiten wat noodzakelijk is voor de uitvoering van de overeenkomst met de gebruiker-betrokkene, is artikel 6 lid 1 sub f AVG: de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de gegevenshouder-verwerkingsverantwoordelijke of een derde.

Bij het gebruik van IoT-data door bedrijven op grond van het gerechtvaardigd belang zal het vaak gaan om commerciële belangen. Het Hof van Justitie bevestigde onlangs dat commerciële belangen ook in aanmerking komen als gerechtvaardigde belangen op grond van artikel 6 lid 1 sub f AVG.⁴² Voorwaarde is wel, net als bij iedere andere verwerking van persoonsgegevens op basis van het gerechtvaardigd belang, dat de verwerking noodzakelijk is voor de nagestreefde gerechtvaardigde belangen en dat de belangen van de gebruiker-betrokkene niet zwaarder wegen (slot artikel 6 lid 1 sub f AVG). Getoetst moet worden of de verwerking valt binnen de redelijke verwachting van de gebruiker-betrokkene, rekening houdend met diens relatie tot de verwerkingsverantwoordelijke.⁴³

Het is bepaald niet ondenkbaar dat bijvoorbeeld de aanbieder van een gerelateerde dienst (mobiele app) die toets niet zou halen als deze de IoT-data – als persoonsgegevens – zou doorverkopen. Die toets zou echter waarschijnlijk wel kunnen worden gehaald als de gegevenshouder de IoT-data volledig zou aggregeren (ook een verwerkingshandeling) en de geaggregeerde gegevens zou delen met derden, of die data zou gebruiken voor het analyseren van het gebruik van de verbonden producten om zo de eigen dienstverlening te verbeteren. Dat geldt ook in het hiervoor omschreven scenario waarin de werkgever gereedschap beschikbaar stelt aan werknemers en de IoT-data zou gebruiken voor diens gerechtvaardigde belangen om te weten hoe lang dat gereedschap is gebruikt en wanneer het toe is aan onderhoud of vervanging.

In het kader van de noodzakelijkheidstoets moet worden gekeken naar welke persoonsgegevens noodzakelijk zijn voor de behartiging van de gerechtvaardigde belangen. Dit kan met zich meebrengen dat niet alle IoT-data die uit het verbonden product worden uitgelezen ook kunnen worden verwerkt voor die gerechtvaardigde belangen, want niet alle IoT-data zullen daar altijd *noodzakelijk* voor zijn.

39 HvJ EU 4 juli 2023, C-252/21, ECLI:EU:C:2023:537, r.o. 98, 99 (*Meta Platforms/Bundelskartellant*).

40 Dit wordt onderstreept door artikel 6 lid 1 Data Act, waarin staat dat de derde deze gegevens uitsluitend verwerkt voor de doeleinden en onder de voorwaarden die met de gebruiker zijn overeengekomen.

41 Artikelen 4 lid 13 en 14 Data Act bevatten beperkingen op wat een gegevenshouder mag doen met gegevens die *geen* persoonsgegevens zijn (in de Data Act wordt de uitdrukking 'gegevens die niet persoonsgebonden gegevens zijn' gebruikt) maar geen beperkingen op gegevens die wel persoonsgegevens zijn.

42 HvJ EU, 4 oktober 2024, C -621/22 (*Koninklijke Nederlandse Lawn Tennisbond vs Autoriteit Persoonsgegevens*), r.o. 49.

43 Overweging 47 AVG alsmede HvJ EU *Meta Platforms/Bundelskartellant*, r.o. 116 en HvJ EU *KNLTB/AP*, r.o. 54.

Dit is een afweging die op een case-by-case basis moet worden gemaakt.

5.5 Taak van algemeen belang

Kunnen overheidsinstanties zich voor de verwerking van IoT-data baseren op de rechtsgrond in artikel 6 lid 1 sub e AVG, namelijk dat de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang of een taak in het kader van de uitoefening van het openbare gezag dat aan de gegevenshouder is opgedragen?

Overheidsinstanties *kunnen* in ieder geval gegevenshouders zijn, zo geeft de Data Act aan. In overweging 63 staat: 'Hoewel overheidsinstanties doorgaans niet onder het begrip 'gegevenshouder' vallen, kunnen overheidsondernemingen daar wel onder vallen.'

Overheidsinstanties zouden bijvoorbeeld verbonden producten kunnen inzetten die hen ondersteunen bij de vervulling van hun publieke taken. Daarbij kunnen IoT-data worden verwerkt die tevens zijn aan te merken als persoonsgegevens. Bijvoorbeeld een gemeentelijk onderdeel dat verbonden veegwagens inzet en de IoT-data koppelt aan de medewerkers die de veegwagens gebruiken. De overheidsinstantie moet dan onderbouwen dat de verwerking van die persoonsgegevens noodzakelijk is voor het vervullen van de publieke taak. Daarnaast moet zijn voldaan aan de eisen die artikel 6 lid 3 AVG stelt aan deze rechtsgrond.

In dit verband merk ik nog op dat het slot van artikel 6 lid 1 sub f AVG bepaalt dat de rechtsgrond van het gerechtvaardigd belang niet geldt voor de verwerking van persoonsgegevens door overheidsinstanties in het kader van de uitoefening van hun taken. Als verbonden producten voor publieke taken worden ingezet en daarbij IoT-data worden verwerkt die tevens persoonsgegevens zijn, kan de rechtsgrond dus niet het gerechtvaardigd belang van de overheidsinstantie zijn.

5.6 Toestemming

Dan de rechtsgrond van de toestemming (artikel 6 lid 1 a AVG).

Op voorhand is moeilijk te zeggen in welke situaties bij IoT-data (extra) toestemming moet worden gevraagd.⁴⁴ De toezichthouders merken op dat het voor de hand ligt om toestemming te vragen voor het delen van IoT-data met derde partijen (anders dan verwerkers).⁴⁵ Dat ligt inderdaad voor de hand, maar het zal niet in alle gevallen nodig zijn. Wanneer het delen van de IoT-data met derden noodzakelijk is voor de uitvoering van de overeenkomst met de betrokkene, of wanneer het delen met derden in de gege-

ven omstandigheden binnen de redelijke verwachting van de gebruiker-betrokkene valt, hoeft de rechtsgrond niet toestemming te zijn.

Als de IoT-data ook bijzondere persoonsgegevens zijn en toestemming de enige manier is om die te verwerken – omdat geen beroep kan worden gedaan op een andere uitzonderingsgrond in de AVG of UAVG – is toestemming ook de rechtsgrond voor de verwerking van die bijzondere persoonsgegevens.

Bij toestemming moet altijd worden bedacht dat deze ook weer op ieder moment moet kunnen worden ingetrokken (artikel 7 lid 3 AVG). De gegevenshouder-verwerkingsverantwoordelijke moet dus maatregelen treffen om te zorgen dat de IoT-data niet verder worden verwerkt als de gebruiker-betrokkene diens toestemming intrekt.

5.7 Vitaal belang

Artikel 6 lid d AVG bevat de rechtsgrond dat de verwerking noodzakelijk is om de vitale belangen van de betrokkene of van andere personen te beschermen. Deze rechtsgrond is alleen van toepassing in uitzonderlijke situaties, als dat noodzakelijk is voor de bescherming van een belang dat essentieel is voor het leven van de betrokkene of dat van een andere natuurlijke persoon (overweging 46 AVG).

Hoewel dit niet een rechtsgrond is die voor gebruikelijke verwerkingen van IoT-data kan worden gebruikt, is niet uit te sluiten dat het in levensbedreigende situaties noodzakelijk zou kunnen zijn om IoT-data te verwerken. Bijvoorbeeld als een wandelaar in de bergen vermist raakt die een gps-tracker bij zich heeft.

5.8 Tussenconclusie

Op grond van artikel 11.7a Tw moet toestemming worden gevraagd voor het uitlezen van IoT-data uit een verbonden product dat is aan te merken als randapparatuur. M.i. kunnen de daaropvolgende verwerkingen van de IoT-data worden gebaseerd op de andere rechtsgronden uit artikel 6 AVG.

6. Uitoefening rechten gebruiker-betrokkene in de Data Act en de AVG

6.1 Algemeen

Een aandachtspunt bij de relatie tussen de AVG en IoT-data, is hoe de rechten van de gebruiker-betrokkene onder de Data Act zich verhouden tot de rechten onder de AVG. De gebruiker heeft onder de Data Act recht op toegang tot diens IoT-data en het recht die aan een derde over te laten dragen. Deze rechten zijn vergelijkbaar met de rechten van de gebruiker-betrokkene op inzage in diens persoonsgegevens (artikel 15 AVG) en het recht op gegevensoverdraagbaarheid (artikel 20 AVG). De Data Act geeft in artikel 1 lid 5 expliciet aan dat de rechten uit hoofdstuk II van de Data Act een aanvulling vormen op het recht van inzage en overdraagbaarheid uit hoofde van de artikelen 15 en 20 AVG.

⁴⁴ Wanneer er op grond van artikel 11.7a Tw toestemming wordt gevraagd voor het plaatsen van *tracking cookies* dan wordt over het algemeen aangenomen dat de enige rechtsgrond voor het verwerken van persoonsgegevens die met dat soort cookies worden verwerkt (opgebouwde profielen), de toestemming is. Zie bijvoorbeeld J.A.N. Baas, *JBP* 2023, nr. 158, p. 1328. Gezien de gevolgen van het verwerken van dat soort persoonsgegevens is dat m.i. terecht.

⁴⁵ EDPB Guidelines over *connected vehicles*, randnummer 95.

Ten aanzien van het recht op gegevensoverdraagbaarheid van artikel 20 AVG kan worden opgemerkt dat dit een andere strekking heeft dan het recht uit de Data Act om de IoT-data over te dragen aan een derde partij naar keuze van de gebruiker-betrokkene. De rechten uit artikel 20 AVG zijn beperkt tot de situatie waarin de rechtsgrond de toestemming is (artikel 6 lid 1 sub a AVG), of artikel 6 lid 1 sub b AVG (uitvoering van de overeenkomst). De Data Act bevat niet dergelijke beperkingen. Zoals hiervoor betoogd, kan de verwerking van de IoT-data in de gerelateerde dienst die wordt gebruikt door de gebruiker-betrokkene zelf worden gebaseerd op artikel 6 lid 1 sub b AVG. In dat geval valt het recht op overdraagbaarheid samen met dat recht uit de Data Act.

De vraag is echter in hoeverre artikel 20 AVG van toepassing is op IoT-data. Dat artikel beperkt zich tot persoonsgegevens die de betrokkene aan de verantwoordelijke heeft *verstrekt*. Volgens de toezichthouders omvat het begrip ‘verstrekken’ niet alleen het actief verstrekken van de gegevens door de betrokkene, maar ook situaties waarin de verantwoordelijke over de gegevens beschikt door het observeren van de activiteiten van de betrokkenen.⁴⁶ Daarbij worden voorbeelden gegeven zoals gegevens uit een slimme meter en gegevens van een hartslag die met een draagbaar apparaat worden geregistreerd. Niet iedereen is het eens met deze ruime uitleg van het begrip ‘verstrekken’.⁴⁷

Wordt de ruime uitleg van de toezichthouders gevolgd, dan vallen de meeste IoT-data onder de strekking van artikel 20 AVG. IoT-data die bestaan uit productgegevens zijn data die het verbonden product genereert. Gegevens van een gerelateerde dienst zijn gegevens die worden gegenereerd door de handelingen van de gebruiker in een gerelateerde dienst of daaraan gerelateerde gebeurtenissen die intentioneel door de gebruiker worden geregistreerd óf als bijproduct van die handelingen worden geregistreerd. Dit zijn in de ruime uitleg allemaal gegevens die onder het begrip ‘verstrekken’ vallen.

Bij een beperkte uitleg waarin artikel 20 AVG alleen ziet op gegevens (IoT-data) die de gebruiker *actief* verstrekt, vallen veel IoT-data niet onder artikel 20 AVG. In de beperkte opvatting zijn alleen gegevens van een gerelateerde dienst die *intentioneel* door de gebruiker worden *geregistreerd* aan te merken als persoonsgegevens die onder de strekking van artikel 20 AVG vallen.

Hieruit blijkt dat bij zowel de beperkte als de ruime uitleg van het begrip ‘verstrekken’ uit artikel 20 AVG sprake is van IoT-data die onder dat artikel vallen.

6.2 *Beperkingen Data Act versus beperkingen onder de AVG*

De rechten van de gebruiker uit de Data Act op toegang tot, en overdracht van de IoT-data kunnen op andere gronden worden beperkt dan in de AVG.

Het recht op een kopie van de persoonsgegevens kan onder omstandigheden worden beperkt op grond van artikel 15 AVG zelf. Artikel 15 lid 4 AVG bepaalt dat het in lid 3 bedoelde recht op een kopie van de persoonsgegevens geen afbreuk doet aan de rechten en vrijheden van anderen. Dat geldt ook voor het recht op gegevensoverdraagbaarheid van artikel 20 AVG (zie lid 4). Artikel 23 AVG jo. artikel 41 Uitvoeringswet AVG bevat daarnaast meerdere situaties op grond waarvan de rechten uit de AVG kunnen worden beperkt.

Vergelijkbare beperkingen zijn niet te vinden in de Data Act. In de Data Act staat wel (artikel 4 lid 2) dat de gegevenshouder en de gebruiker de toegang tot de gegevens of het gebruik of verder delen daarvan contractueel kunnen beperken of verbieden als dat de beveiligingsvereisten van het product – zoals wettelijk vastgesteld – kan ondermijnen op een manier die ernstige negatieve gevolgen heeft voor de gezondheid, veiligheid of beveiliging van natuurlijke personen. Hier staat weliswaar dat gebruiker en gegevenshouder dit ‘overeen kunnen komen’, maar in de praktijk zal dit naar verwachting worden opgenomen in eenzijdig opgelegde voorwaarden van de gegevenshouder. Daarnaast mag de gegevenshouder op grond van artikel 4 lid 7 Data Act het delen van IoT-data die zijn aan te merken als bedrijfsgeheimen tegenhouden of opschorten, als met de gebruiker geen afspraken kunnen worden gemaakt over geheimhouding daarvan of de gebruiker de geheimhouding schendt.⁴⁸ Op grond van lid 8 van artikel 4 Data Act kan de gegevenshouder per geval zelfs de toegang tot de IoT-data weigeren. Dat kan in uitzonderlijke omstandigheden, namelijk als deze door bekendmaking van de bedrijfsgeheimen zeer waarschijnlijk ernstige economische schade zal lijden.

Omdat de Data Act expliciet aangeeft dat de AVG in geval van tegenstrijdigheid voor gaat, is de vraag of de gegevenshouder deze beperkingen uit de Data Act kan opleggen als de gebruiker-betrokkene een beroep doet op diens AVG-rechten.⁴⁹ Kan de gegevenshouder de beperkingen uit de AVG dan gebruiken om de beperkingen uit de Data Act af te dwingen?

6.3 *Beperkingen in de Data Act en het recht op een kopie onder de AVG*

Artikel 4 lid 2 Data Act geeft de gegevenshouder de mogelijkheid de *toegang* of het *delen* van de IoT-data te beperken of te verbieden, als de wettelijk vastgestelde beveili-

⁴⁶ Article 29 Working Party, WP242, *On the right to data portability*, p. 10.

⁴⁷ Zie bijvoorbeeld Kranenburg en Verhey, *De Algemene Verordening gegevensbescherming in Europees en Nederlands perspectief*, Wolters Kluwer, Deventer, 2024, p. 296; onder verwijzing naar Rechtbank Amsterdam, 11 maart 2021, ECLI:NL:RBAMS:2021:1020, r.o. 4.75.

⁴⁸ De gegevenshouder moet in zo'n geval wel de toezichthouder van deze acties op de hoogte brengen.

⁴⁹ Als de IoT-data persoonsgegevens zijn zullen ze wellicht minder snel kunnen worden aangemerkt als bedrijfsgeheim, maar uitgesloten is dit niet.

gingseisen van het verbonden product daardoor in gevaar zouden kunnen komen.

Als de gebruiker de toegang tot diens IoT-data wordt ontzegd op grond van dit artikel, wordt in feite ook het recht van de gebruiker-betrokkene op een kopie van die persoonsgegevens op grond van de AVG ontzegd. Kan de gegevenshouder, om dit te rechtvaardigen, een beroep doen op artikel 15 lid 4 AVG, waarin staat dat het recht op een kopie geen afbreuk doet aan de rechten en vrijheden van anderen? De gegevenshouder kan zelf namelijk ook een dergelijke 'andere' zijn.⁵⁰ M.i. is verdedigbaar dat de gegevenshouder-verwerkingsverantwoordelijke artikel 15 lid 4 AVG kan invoeren als de gebruiker-betrokkene een kopie vraagt van de IoT-data en de gegevenshouder kan aantonen dat aan de voorwaarden van artikel 4 lid 2 Data Act is voldaan.

De gegevenshouder zou m.i. ook artikel 15 lid 4 AVG naar voren kunnen brengen als de gebruiker-betrokkene om een kopie van diens IoT-data vraagt en de gegevenshouder een beroep kan doen op artikel 4 lid 8 Data Act. Op basis van dat artikel mag de gegevenshouder toegang tot de IoT-data weigeren, als die data bedrijfsgeheimen zijn en de gegevenshouder ondanks genomen maatregelen om die bedrijfsgeheimen te beschermen, zeer waarschijnlijk ernstige economische schade zou lijden.⁵¹

6.4 *Beperkingen Data Act en het recht op gegevensoverdraagbaarheid onder de AVG*

Geldt dit ook als de gebruiker-betrokkene vraagt om diens IoT-data te *delen* met een derde?

Een gegevenshouder kan ook het delen van de IoT-data op grond van artikel 4 lid 2 Data Act beperken of verbieden en als de IoT-data bedrijfsgeheimen zijn dat tegenhouden of opschorten op grond van artikel 4 lid 7 Data Act. Artikel 20 AVG lid 4 kent eenzelfde bepaling als artikel 15 lid 4 AVG: daarin staat ook dat het recht op gegevensoverdraagbaarheid geen afbreuk doet aan de rechten en vrijheden van anderen. Het is m.i. verdedigbaar dat de gegevenshouder-verwerkingsverantwoordelijke een beroep kan doen op dit lid 4, als deze kan aantonen dat er sprake is van een situatie zoals omschreven in artikel 4 lid 2 respectievelijk lid 7 Data Act.

6.5 *Beperkingen ten aanzien van overdracht aan poortwachters*

Een vergelijkbare situatie als hiervoor doet zich voor bij de beperking die artikel 5 lid 3 Data Act oplegt. Op grond van dit artikel mogen derden die zijn aan te merken als poortwachters op grond van de Digital Markets Act (DMA)⁵² geen IoT-data ontvangen op verzoek van de gebruiker. De

gedachte achter dit verbod is dat dit soort partijen al over zoveel data beschikken dat het niet wenselijk is om hen ook IoT-data te verstrekken.⁵³

Artikel 20 AVG geeft de gebruiker-betrokkene echter het recht diens IoT-data over te laten dragen aan *een* andere verwerkingsverantwoordelijke, zonder daarbij te mogen worden gehinderd door de verwerkingsverantwoordelijke. Dit conflicteert met artikel 5 lid 3 Data Act, aangezien de IoT-data niet aan poortwachters mogen worden overgedragen.

Kan dit conflict worden opgelost met een beroep op artikel 20 lid 4 AVG? Moet het algemene belang dat artikel 5 lid 3 Data Act probeert na te streven, namelijk om poortwachters niet te veel 'datamacht' te geven, worden aangemerkt als een belang dat de rechten en vrijheden van anderen beschermt? Het is niet duidelijk of de wetgever dit voor ogen heeft gehad, maar ik denk dat niet is uit te sluiten dat artikel 20 lid 4 AVG een grond kan bieden voor een gegevenshouder om te weigeren de IoT-data aan een poortwachter over te dragen.

Eventueel zou ook artikel 23 AVG jo. 41 lid 1 sub e UAVG soelaas kunnen bieden. Dat artikellid staat het beperken van de AVG-rechten toe als dat noodzakelijk is voor een belangrijke doelstelling van algemeen belang van de EU of van de lidstaat. De gegevenshouder moet blijkens de aanhef van artikel 23 AVG dan wel onderbouwen dat sprake is van een beperking die de wezenlijke inhoud van de grondrechten en de fundamentele vrijheden onverlet laat en in een democratische samenleving een noodzakelijke en evenredige maatregel vormt.⁵⁴

Als de gegevenshouder geen beperkingen uit de AVG zou kunnen invoeren tegen een verzoek van de betrokkene om de IoT-data aan een poortwachter over te dragen, zou de gegevenshouder moeten kiezen tussen overtreding van artikel 20 van de AVG (weigeren over te dragen aan *een* andere verwerkingsverantwoordelijke) en overtreding van artikel 5 lid 3 Data Act (in strijd met het verbod overdragen aan een poortwachter).⁵⁵ Dat is niet de bedoeling geweest van de wetgever, die in de Data Act heeft opgenomen dat de AVG bij tegenstrijdigheid voorgaat. Een alternatieve route voor de gegevenshouder is om te stellen dat de AVG in dit geval vóór gaat en dat er toch moet worden overgedragen aan een poortwachter als de gebruiker-betrokkene dat vraagt. Hoe dan ook is dit geen benijdenswaardige positie en het laatste woord is hier vermoedelijk niet over gezegd.

⁵⁰ Richtlijnen EDPB on data subject rights, 01/2022, versie 2.1, nummer 171.

⁵¹ De gegevenshouder moet de toezichthouder van een dergelijke weigering op de hoogte brengen, zie artikel 4 lid 8 Data Act.

⁵² Verordening (EU) 2022/1925 van het Europees Parlement en de Raad van 14 september 2022 over betwistbare en eerlijke markten in de digitale sector, en tot wijziging van Richtlijnen (EU) 2019/1937 en (EU) 2020/1828 (digitalemarktenverordening).

⁵³ Overweging 40 Data Act.

⁵⁴ Hierbij laat ik de discussie over de juistheid van de implementatie van artikel 23 AVG in de UAVG buiten beschouwing.

⁵⁵ Ook de derde aan wie de IoT-data worden overgedragen heeft op grond van artikel 6 Data Act te maken met beperkingen op wat de derde met die data mag doen. Deze mag de IoT-data ook niet aan een poortwachter overdragen (lid 2 sub d), mag deze niet met een derde delen om een product te ontwikkelen dat concurreert met het verbonden product waar de IoT-data uit zijn gehaald (lid 2 sub e), mag de IoT-data alleen aan derden ter beschikking stellen op grond van een overeenkomst met de gebruiker en op voorwaarde dat de andere derde alle met de (oorspronkelijke) gegevenshouder overeengekomen maatregelen in acht neemt om eventuele bedrijfsgeheimen te beschermen (lid 2 sub c).

6.6 Tussenconclusie

Als de IoT-data persoonsgegevens zijn valt het recht uit de Data Act op toegang tot de IoT-data samen met het recht op inzage (op een kopie) uit de AVG. Het in de Data Act vastgelegde recht op overdracht van de IoT-data aan een derde valt samen met het recht op gegevensoverdraagbaarheid als is voldaan aan de voorwaarden van artikel 20 AVG. Wil de gegevenshouder de beperkingen in kunnen roepen die de Data Act toestaat, zal deze moeten onderbouwen dit te doen ter bescherming van diens rechten en vrijheden op grond van artikel 15 en 20 lid 4 AVG. Bij het verbod op overdracht van IoT-data aan een poortwachter kan er conflict ontstaan met artikel 20 AVG. Niet duidelijk is of dat kan worden opgelost met een beroep op artikel 20 lid 4 AVG, of 23 AVG jo. 41 lid 1 sub e UAVG.

7. Conclusie

Er valt, zoals eerder aangegeven, genoeg te zeggen over de Data Act, ook in verhouding tot de AVG. In dit artikel heb ik specifiek de relatie onderzocht tussen de AVG en de verwerking van IoT-data onder de Data Act.

Daaruit komt naar voren dat IoT-data uit verbonden producten die door natuurlijke personen worden gebruikt al snel persoonsgegevens zijn, omdat de gebruiker in enige mate moet worden geïdentificeerd. Niet alle IoT-data zullen echter persoonsgegevens zijn, als het data zijn die niet betrekking hebben op natuurlijke personen, dan zijn het geen persoonsgegevens.

Het begrip 'gegevenshouder' verdient, door de cirkeldefinitie, verduidelijking. Ook het begrip 'gebruiker' zou, als het gaat om de vraag wat precies moet worden verstaan onder gebruikers aan wie 'contractueel tijdelijke rechten zijn overgedragen' kunnen worden verduidelijkt. Door deze onduidelijkheid kan bijvoorbeeld discussie ontstaan over de vraag of zakelijke gebruikers (bedrijven) ook kunnen worden aangemerkt als gegevenshouders. Naar mijn mening luidt het antwoord hierop 'ja'.

Alle partijen die IoT-data verwerken die tevens persoonsgegevens zijn hebben rollen onder de AVG, ofwel als (gezamenlijk) verwerkingsverantwoordelijke of als verwerker. Welke rol zij hebben, hangt af van de situatie. Een verwerker wordt niet geacht gegevenshouder te zijn.

De toestemmingseis van artikel 11.7a van de Telecommunicatiewet is van toepassing op het uitlezen van IoT-data uit verbonden producten die kunnen worden aangemerkt als randapparatuur. Toestemming hoeft niet te worden gevraagd als het gaat om een dienst die aan de gebruiker wordt geleverd, zoals de gerelateerde dienst (de mobiele app) die bij het verbonden product wordt geleverd. Daarbuiten geldt die toestemmingseis wel. Opvolgende verwerkingen van de IoT-data kunnen m.i., afhankelijk van de situatie, worden gebaseerd op de verschillende rechtsgronden uit de AVG.

Bij het toegang geven tot de IoT-data en het verstrekken daarvan aan derden, kan de gegevenshouder aanlopen tegen de beperkingen die de Data Act toestaat en oplegt. M.i.

zou de gegevenshouder ofwel een beroep moeten kunnen doen op de relevante beperkingen uit de AVG, ofwel naar voren moeten kunnen brengen dat de AVG voorgaat.

Concluderend kun je van een ongelukkig huwelijk tussen hoofdstuk II van de Data Act en de AVG niet spreken, maar helemaal zonder spanningen is deze echtverbintenis niet.