

Memorie van toelichting (Uitvoeringswet dataverordening)

I. Algemeen

1. Inleiding

Dit wetsvoorstel (hierna: de Uitvoeringswet) strekt tot uitvoering van 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) (hierna: de verordening).

De verordening is van toepassing vanaf 12 september 2025 en moet dan uitvoerbaar zijn in Nederland door middel van wet- en regelgeving of feitelijk handelen. De verordening is alleen van toepassing op het grondgebied van Nederland binnen de Europese Unie en heeft geen gevolgen voor Bonaire, Sint-Eustatius en Saba.

De beleidsverantwoordelijkheid voor de onderwerpen uit de verordening en de Uitvoeringswet ligt bij de Minister van Economische Zaken en Klimaat, de Minister voor Rechtsbescherming en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties. In paragraaf vier wordt hier nader op ingegaan.

In paragraaf twee wordt de Nederlandse en Europese beleidscontext geschetst. In paragraaf drie worden de hoofdlijnen van de verordening uiteengezet. In paragraaf vier wordt nader ingegaan op het onderhavige wetsvoorstel. In paragraaf vijf wordt stilgestaan bij de verhouding tot ander recht. In paragraaf zes worden de gevolgen, zoals voor regeldruk, beschreven. In paragraaf zeven wordt ingegaan op de evaluatie van de verordening. In paragraaf acht worden de uitkomsten van de toetsen en consultaties gedeeld. In paragraaf negen wordt ingegaan op de inwerkingtreding en het overgangsrecht.

2. Beleidscontext

Gegevens zijn steeds belangrijker in onze economie en maatschappij. De Nederlandse Kabinetsvisie op datadeling tussen bedrijven (2019)¹ stelt dat het delen van gegevens tussen bedrijven maatschappelijke en economische kansen biedt. De visie schetst ook verschillende redenen waarom partijen gegevens nu nog niet willen, kunnen of mogen delen, waaronder potentiële marktmacht als gevolg van dataconcentraties en een gebrek aan onderling vertrouwen. Het kabinet heeft drie uitgangspunten voor beleidsontwikkeling gericht op datadeling tussen bedrijven benoemd: datadeling is bij voorkeur vrijwillig, datadeling komt zo nodig verplicht tot stand en burgers en bedrijven houden grip op hun gegevens.

Ook in de Nederlandse Strategie Digitale Economie² (SDE; 2022) is aandacht voor de noodzaak om op een nieuwe en bewuste manier om te gaan met het gebruik van gegevens. De verordening draagt in lijn met de Nederlandse inzet in de SDE bij aan het gebruik van gegevens door middelgrote en kleine bedrijven (mkb), biedt nieuwe mogelijkheden tot innovatie en draagt bij aan een eerlijkere, transparantere markt voor gegevens waarin consumenten en bedrijven meer grip hebben op hun gegevens en het gebruik ervan. Vertrouwen hebben in de digitale wereld en regie hebben op het digitale leven zijn bovendien twee kernwaarden in de Werkagenda Waardengedreven Digitaliseren (2022). Het toegang hebben tot gegevens is van essentieel belang om regie te hebben. Waar het gaat om datadeling moet dat op een verantwoorde manier gebeuren, waarbij de burger zelf grip kan houden op zijn of haar gegevens en de bescherming van persoonsgegevens geborgd is.

De Europese Commissie heeft in 2020 een Europese Datastrategie gepubliceerd. De Commissie stelt dat gegevens een groot potentieel hebben. Door het (her)gebruik en beheer van gegevens te verbeteren kunnen ondernemingen economische waarde creëren en bijdragen aan maatschappelijke vraagstukken zoals verduurzaming, mobiliteit of gezondheidszorg. Er worden door de Commissie verschillende uitdagingen geconstateerd: de versnippering van gegevens tussen lidstaten, beperkte

¹ Kamerstukken II 2018/19, 26643, nr. 594.

² Kamerstukken II 2022/23, 26643, nr. 941.

beschikbaarheid van gegevens voor (her)gebruik en ongelijke marktmacht in de gegevens- en cloudmarkt.

In de strategie schetst de Commissie een toekomstvisie voor één Europese gegevensmarkt, waar gezamenlijke regels en effectieve handhaving ervoor zorgen dat gegevens binnen de EU en tussen sectoren kunnen stromen en waar de regels over datatoegang, datakwaliteit en datagebruik eerlijk, praktisch en duidelijk zijn. Hiermee verbindt de strategie de bescherming van fundamentele rechten zoals privacy en gegevensbescherming, veiligheid en ethische normen met de bevordering van waardecreatie uit gegevens.

Onzekerheid over de rechten en plichten met betrekking tot gegevens staan het gebruik van gegevens in het belang van de samenleving in de weg. Daarom heeft de Commissie voorstellen gedaan voor een Datagovernanceverordening en een Dataverordening. De Europese regels over privacy, gegevensbescherming en mededinging worden volledig in acht genomen. De Algemene Verordening Gegevensbescherming³ (hierna: AVG) is voor privacy en gegevensbescherming een belangrijke pijler. In paragraaf vijf wordt hier verder op ingegaan.

In aanloop naar de publicatie van de verordening heeft het kabinet in een non-paper⁴ aangegeven wat de verordening zou moeten bereiken, waarbij voortgebouwd is op de uitgangspunten uit de Kabinetsvisie op datadelen tussen bedrijven. Het non-paper stelt dat een beperkte groep bedrijven gegevens verzamelt en hier waarde mee creëert. Personen en organisaties die door het gebruik van een product of dienst bijdragen aan de creatie van gegevens hebben vaak geen toegang tot zulke 'co-gegenereerde' gegevens. Het non-paper stelt daarom dat personen en organisaties meer controle moeten krijgen over het gebruik van co-gegenereerde gegevens zodat ook zij kunnen profiteren van de waarde van deze gegevens. Het bevorderen van de portabiliteit (het overdragen van gegevens van het ene naar het andere systeem) en interoperabiliteit (dat verschillende systemen technisch in staat zijn samen te werken, bijvoorbeeld om gegevens te delen) van gegevens en applicaties, met name bij dataverwerkingsdiensten, is van groot belang. Dit zou ook de concurrentie en innovatie bij datagedreven producten en diensten moeten bevorderen. In lijn met de kabinetsinzet versterkt het voorstel de controle van gebruikers van producten en diensten over hun gegevens. Ook vergroot het voorstel de concurrentie, keuzevrijheid en interoperabiliteit in de markt voor clouddiensten. Daarmee stimuleert het voorstel de data-economie en draagt het bij aan het gelijkwaardiger verdelen van de waarde van data.

3. Dataverordening

De verordening heeft tot doel om geharmoniseerde regels voor een eerlijke toegang tot en eerlijk gebruik van gegevens vast te stellen. De verordening heeft zowel betrekking op persoonsgegevens als niet-persoonsgebonden gegevens. De Europese Commissie heeft geconstateerd dat een aantal factoren de Europese economie momenteel verhindert om gegevens ten volle te benutten. Belangrijke knelpunten zijn onder andere het gebrek aan duidelijkheid over wie gebruik mag maken van gegevens van met het internet verbonden producten (ook wel 'slimme producten' of 'internet-of-things producten' genoemd) en het feit dat als gevolg van ongelijke marktmacht mkb vaak geen evenwichtige data-uitwisselingscontracten met sterkere marktspelers kunnen sluiten. Bovendien zijn er in de interne markt obstakels om over te stappen naar concurrerende en betrouwbare dataverwerkingsdiensten en beperkte mogelijkheden om gegevens uit verschillende sectoren te combineren. Dit heeft invloed op diverse economische sectoren en leidt ertoe dat gegevens in de EU te weinig worden benut, met negatieve gevolgen voor de keuzevrijheid van consumenten, innovatie en openbare dienstverlening. De verordening beoogt obstakels voor de toegang tot gegevens weg te nemen en de rechten om gegevens te gebruiken evenwichtiger te verdelen, zowel voor private als publieke partijen. Dit stimuleert het gebruik van gegevens, door de controle die bedrijven en consumenten over hun gegevens hebben op evenwichtige wijze te organiseren.

³ Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119).

⁴ Kamerstukken II 2021/22, 21501-33, nr. 875.

In het effectbeoordelingsverslag zijn door de Europese Commissie alternatieve maatregelen onderzocht.⁵ Een minimale interventie met niet bindende maatregelen bestaande uit het ondersteunen van goede voorbeelden en zelfregulering werd niet afdoende geacht om efficiëntere en eerlijke datatoegang en gebruik tot stand te brengen.

Een optie om verdergaande maatregelen te nemen, bijvoorbeeld door technische eisen, zou substantieel hogere kosten voor datahouders opleveren en investeringen in verbonden producten negatief beïnvloeden.

De verordening beoogt een kader te stellen voor onder andere de volgende situaties, met verschillende reikwijdtes, actoren, soorten gegevens en type maatregelen (zie ook artikel 1 van de verordening):

- het beschikbaar stellen van productgegevens en gegevens van gerelateerde diensten aan de gebruiker van het verbonden product of gerelateerde dienst (hoofdstuk II);
- het beschikbaar stellen van gegevens door gegevenshouders aan gegevensontvangers (hoofdstuk III);
- oneerlijke contractuele bedingen met betrekking tot de toegang tot en het gebruik van gegevens tussen ondernemingen (hoofdstuk IV);
- het beschikbaar stellen van gegevens door gegevenshouders aan overheidsinstanties, de Commissie, de Europese Centrale Bank en organen van de Unie, indien er sprake is van een uitzonderlijke noodzaak aan die gegevens voor de uitvoering van een specifieke taak in het algemeen belang (hoofdstuk V);
- het vergemakkelijken van het overstappen tussen dataverwerkingsdiensten (hoofdstuk VI);
- het invoeren van waarborgen tegen ongeoorloofde toegang van derden tot niet-persoonsgebonden gegevens (hoofdstuk VII);
- de ontwikkeling van interoperabiliteitsnormen voor dataruimten, dataverwerkingsdiensten en slimme contracten (hoofdstuk VIII).

Om ervoor te zorgen dat deze regels datadelen in de hele Unie mogelijk maken zonder al te grote belemmeringen voor de interne markt, en de regels en het toezicht in de interne markt uniform zijn, is er gekozen voor een verordening.

Deze hoofdstukken worden hierna verder toegelicht. **Hoofdstuk I** over algemene bepalingen bevat artikelen over het onderwerp, toepassingsgebied en de definities uit de verordening en wordt niet apart behandeld. Waar nodig wordt de inhoud van dit hoofdstuk besproken bij de andere hoofdstukken waar het mee samenhangt. **Hoofdstuk XI** over slotbepalingen bevat onder meer artikelen met betrekking tot overgangsrecht, evaluatie en inwerkingtreding. Die onderwerpen komen terug in paragrafen 7 en 9 van het algemene deel van de toelichting.

3.1 Delen van gegevens tussen bedrijven en consumenten en tussen bedrijven onderling

Hoofdstuk II van de verordening reguleert het gebruik van gegevens die door (het gebruik van) verbonden producten of gerelateerde diensten worden gegenereerd. De gegevens die verbonden producten genereren kunnen op verschillende manieren van waarde zijn. De aanbieder van een product kan de gegevens bijvoorbeeld gebruiken om het product zelf te verbeteren. De gebruiker van een product of dienst kan de gegevens gebruiken om inzichten over het eigen handelen of de omgeving op te doen. Aanbieders van een product en derde partijen kunnen de gegevens gebruiken om aftermarketdiensten, zoals onderhoud en reparatie, of andere diensten aan te bieden.

Aanbieders van producten hebben vaak toegang tot de gegenereerde gegevens en kunnen deze binnen de kaders van de wet gebruiken of delen. Gebruikers van verbonden producten zijn afhankelijk van de aanbieder voor toegang tot de gegenereerde gegevens. Hierdoor hebben ze vaak maar beperkt toegang tot de gegevens, terwijl zij door hun gebruik wel bijdragen aan de creatie hiervan. De verordening geeft gebruikers van een verbonden product of gerelateerde dienst het recht op toegang tot de gegevens die door hun gebruik worden gegenereerd en het recht deze gegevens te delen met derde partijen. Dit geeft gebruikers controle over het gebruik van de gegevens uit hun producten en stelt ze in staat de gegevens te gebruiken op een voor hun waardevolle manier. Zo zou

⁵ [Effectbeoordelingsverslag en ondersteunende studies bij het voorstel voor een dataverordening | Shaping Europe's digital future \(europa.eu\)](#).

de gebruiker van een landbouwapparaat gegevens moeten kunnen delen met een partij naar keuze voor onderhoud of reparatie en kan de gebruiker van een industriële machine de door de machine gegenereerde gegevens gebruiken om haar bedrijfsprocessen te (laten) optimaliseren. Hiermee beoogt de verordening ook de innovatie en concurrentie bij aftermarketdiensten en de ontwikkeling van nieuwe diensten die gebruik maken van productgegevens te stimuleren.

Verbonden producten en gerelateerde diensten

Hoofdstuk II heeft betrekking op verbonden producten en gerelateerde diensten. Onder verbonden producten worden producten verstaan die gegevens over hun prestaties, gebruik of omgeving genereren of verzamelen, bijvoorbeeld door middel van een sensor, en deze gegevens via een netwerk kunnen communiceren. Een breed scala aan producten kan hieronder vallen; consumentengoederen zoals koelkasten, en horloges, medische apparatuur en industriële machines. Voor diverse productgroepen wordt het in toenemende mate de norm dat ze verbonden producten zijn. Bijvoorbeeld voor thermostaten is het steeds gebruikelijker dat ze gegevens verzamelen en communiceren over onder andere temperatuur en energieverbruik. Voor productgroepen zoals voertuigen en landbouwapparatuur geldt ook dat ze steeds vaker als verbonden producten worden geproduceerd en aangeboden. Producten die hoofdzakelijk gegevens opslaan, verwerken of doorgeven namens anderen dan de gebruiker, zoals servers, vallen niet onder definitie van verbonden producten. Gerelateerde diensten zijn diensten, zoals software, die noodzakelijk zijn voor een product om één of meer van zijn functies uit te voeren. Dit kan bijvoorbeeld het besturingssysteem van een verbonden product zijn. Ook virtuele assistenten vallen onder dit hoofdstuk, maar alleen wanneer zij interacteren met een verbonden product of gerelateerde dienst. Gegevens die virtuele assistenten genereren die niets te maken hebben met het gebruik van een verbonden product of gerelateerde dienst vallen niet onder dit hoofdstuk.

Om de administratieve lasten voor het mkb te beperken is dit hoofdstuk niet van toepassing op de gegevens uit verbonden producten en diensten die door micro- of kleine bedrijven⁶ worden gemaakt of geleverd. Middelgrote ondernemingen⁷ krijgen bovendien tijd om hun producten of diensten aan de verordening aan te passen. Hiertoe is in het eerste jaar dat bedrijven kwalificeren als middelgrote ondernemingen de verordening niet van toepassing op gegevens gegenereerd door het gebruik van verbonden producten die zij maken en gerelateerde diensten die zij verlenen. Ook vallen producten die middelgrote ondernemingen maken in het eerste jaar dat zij in de markt zijn geplaatst buiten de toepassing van de verordening.

Betrokken partijen

Om gegevensdeling uit verbonden producten en gerelateerde diensten te faciliteren definieert de verordening verschillende rollen: gebruikers, aanbieders, gegevenshouders en derde partijen. De gebruiker is de natuurlijke of rechtspersoon die een verbonden product in eigendom heeft, huurt of leaset, of die gerelateerde diensten ontvangt. Onder de verordening zal de gebruiker eenvoudig en kosteloos toegang moeten krijgen tot de gegevens die verbonden producten en gerelateerde diensten genereren. Daarnaast krijgt de gebruiker het recht een derde partij toegang tot de gegevens te verlenen. Ondernemingen die onder de Digitalemarktenverordening (DMA) als poortwachter zijn aangewezen mogen onder dit onderdeel van de verordening niet als derde partij gegevens ontvangen, dit wordt in paragraaf 5.2 van deze memorie van toelichting verder toegelicht.

Om te verzekeren dat gebruikers toegang tot gegevens kunnen krijgen en verlenen moeten gegevens die verbonden producten genereren gemakkelijk, veilig en kosteloos toegankelijk zijn voor de gebruiker. Dit kan zowel direct (bijvoorbeeld via het display van het product) als indirect (bijvoorbeeld via een (web)applicatie) worden gefaciliteerd. Daarnaast verplicht de verordening aanbieders van zowel verbonden producten als gerelateerde diensten om voordat zij een product of dienst verkopen, leasen of verhuren aan bepaalde transparantieplichtingen te voldoen. Aanbieders moeten onder andere aan gebruikers communiceren welke gegevens een product of dienst kan genereren en hoe gebruikers deze gegevens kunnen raadplegen. De gegevenshouder, de partij die controle heeft over de toegang tot gegevens, moet vervolgens de gebruiker en derde partijen op verzoek van de gebruiker toegang tot de gegevens verlenen. De gegevenshouder en de aanbieder van een product of gerelateerde dienst kunnen in de praktijk dezelfde partij zijn.

Reikwijdte gegevens

De verordening bakent de gegevens die binnen de reikwijdte van hoofdstuk II vallen op verschillende manieren af. De verordening heeft betrekking op de gegevens die worden gegenereerd door het

⁶ Zoals aangemerkt in artikel 3 van de bijlage bij Aanbeveling 2003/361/EG.

⁷ Zoals aangemerkt in artikel 3 van de bijlage bij Aanbeveling 2003/361/EG.

gebruik van het verbonden product en de gerelateerde dienst. Hieronder vallen zowel gegevens die de gebruiker bewust registreert als alle gegevens die het product als gevolg van het gebruik registreert. Voorbeelden hiervan zijn gegevens die sensoren registreren en gegevens die door interactie met de gebruikersinterface worden geregistreerd. Via verbonden producten kunnen in sommige gevallen ook niet-gerelateerde diensten of apps, waaronder onlinediensten of videodiensten, worden geraadpleegd en tekst-, audio- of audiovisuele inhoud worden gecreëerd of afgespeeld. Deze inhoud, die doorgaans wordt beschermd door intellectuele eigendomsrechten, en de gegevens gecreëerd door het gebruik van niet-gerelateerde diensten vallen niet onder deze verordening. Voor een smartphone vallen bijvoorbeeld de gegevens over het gebruik van het product zelf zoals de batterij en GPS wel binnen hoofdstuk II, maar de gegevens gegenereerd door het gebruik van een tekstverwerkapplicatie, internetbrowser en een videostreamingdienst niet.

Gegevenshouders hoeven alleen gegevens beschikbaar te stellen waar zij zelf toegang toe hebben of met een eenvoudige handeling toegang toe kunnen verkrijgen. Om te verzekeren dat de gegevens bruikbaar zijn voor gebruikers en derde partijen wordt de gegevenshouder geacht toegang te geven tot gegevens met dezelfde kwaliteit als de gegevenshouder zelf heeft. De gegevens moeten in primaire, maar bruikbare vorm beschikbaar worden. Hiermee gaat het om ruwe gegevens, inclusief metagegevens, die automatisch worden gegenereerd en eventueel zijn voorbereid om ze begrijpelijk en bruikbaar te maken, bijvoorbeeld door ze te sorteren of om te zetten in een eenheid als graden Celsius of kilometers. Wanneer de gegevenshouder boven op het voorbereiden van gegevens extra investeringen doet om nieuwe waarden of inzichten aan gegevens te koppelen valt deze informatie buiten de reikwijdte van hoofdstuk II. Deze informatie hoeft dus niet verplicht te worden gedeeld. Dit gaat met name om informatie die wordt opgedaan door de toepassing van complexe, eventueel door intellectuele eigendomsrechten beschermde, algoritmen.

Beschermen van rechten en belangen van betrokken partijen

Om gegevensdeling uit verbonden producten te faciliteren is het belangrijk dat alle betrokken partijen erop kunnen vertrouwen dat hun rechten en belangen ten aanzien van de informatie die uit gegevens kan worden verkregen geborgd zijn. De verordening bevat verschillende bepalingen om de rechten en belangen van de betrokken partijen te borgen.

Sommige verbonden producten of gerelateerde diensten zullen op basis van hun gebruik persoonsgegevens genereren over de gebruiker of derden (bijvoorbeeld huisgenoten). In zulke gevallen is het belangrijk dat de gegevensbeschermingsrechten van de betreffende betrokkene in de zin van de AVG geborgd blijven, zeker als het datasubject niet de gebruiker zelf is. De verordening doet geen enkele afbreuk aan het gegevensbeschermingsrecht. Elke verwerking van persoonsgegevens onder de verordening moet onverminderd voldoen aan alle relevante gegevensbeschermingswetgeving (zie ook paragraaf 5.1 van het algemeen deel van de toelichting). Het recht van de gebruiker om gegevens te delen met derde partijen mag dus ook geen afbreuk doen aan de gegevensbeschermingsrechten van anderen.

Gebruikers kunnen behalve rechten als betrokkenen ook andere rechten en belangen hebben. De gegevens die verbonden producten en gerelateerde diensten genereren kunnen inzicht geven in de economische situatie of het gedrag van de gebruiker. Daarom moet het geven van toegang tot gegevens onder hoofdstuk II net zo makkelijk zijn als het intrekken van deze toegang. Ook mogen gegevenshouders en derde partijen de beschikbare gegevens niet gebruiken om inzichten in de economische situatie van de gebruiker te verwerven of om de commerciële positie van de gebruiker te ondermijnen.

De verordening verplicht gegevenshouders bepaalde gegevens te verstrekken aan gebruikers of door de gebruiker gekozen derden, ook als die gegevens in aanmerking komen voor bescherming als bedrijfsgeheim. De bescherming uit hoofde van de Richtlijn bescherming bedrijfsgeheimen blijft echter verzekerd waardoor gegevenshouders en aanbieders van verbonden producten en gerelateerde diensten erop kunnen vertrouwen dat hun bedrijfsgeheimen gewaarborgd blijven en hun economische positie niet onevenredig wordt geschaad. Gegevens die bedrijfsgeheimen bevatten, mogen alleen worden gedeeld als de gegevenshouder en de gebruiker, of de door de gebruiker gekozen derde partij, vóór het delen alle noodzakelijke maatregelen nemen om de vertrouwelijkheid ervan te waarborgen, met name ten aanzien van derden. Wanneer hierover geen overeenstemming bestaat dan kan een gegevenshouder de toegang tot de betreffende gegevens weigeren of opschorten. Bovendien kan, maar alleen in uitzonderlijke omstandigheden, wanneer de houder van de gegevens kan aantonen dat het zeer waarschijnlijk is dat hij/zij ernstige economische schade zal lijden door de openbaarmaking van bedrijfsgeheimen ondanks dergelijke technische en organisatorische maatregelen, van geval tot geval een verzoek om toegang tot de specifieke gegevens in kwestie worden geweigerd.

3.2 Verplichtingen voor gegevenshouders die krachtens het Unierecht verplicht zijn gegevens beschikbaar te stellen

Aanvullend op de specifieke regels voor gegevensdeling uit verbonden producten legt **hoofdstuk III** van de verordening een horizontaal kader vast voor situaties waarin ondernemingen door de Europese of nationale regelgeving worden verplicht gegevens te delen met andere ondernemingen. Dit hoofdstuk heeft betrekking op de verplichting aan gegevenshouders om gegevens met derde partijen te delen onder hoofdstuk II en andere, eventueel toekomstige, verplichtingen. Duidelijke en eerlijke voorwaarden zijn belangrijk om te zorgen dat zulke verplichtingen ook in de praktijk tot de gewenste gegevensdeling leiden. Hoofdstuk III legt daarom op hoofdlijnen vast onder welke voorwaarden ondernemingen gegevens beschikbaar moeten stellen. Het basisprincipe dat hoofdstuk III vastlegt is dat ondernemingen gegevens altijd onder eerlijke en redelijke voorwaarden beschikbaar moeten stellen en hierin niet mogen discrimineren tussen verschillende (groepen) ondernemingen waar zij gegevens mee delen. Daarnaast legt het hoofdstuk vast dat gegevenshouders beschermingsmaatregelen zoals encryptie mogen treffen om ongeoorloofde toegang tot gegevens te voorkomen en naleving van de overeengekomen voorwaarden te waarborgen.

Vergoeding voor gegevenshouders

Het beschikbaar stellen van gegevens kan kosten met zich meebrengen voor gegevenshouders. Daarom mogen gegevenshouders een redelijke vergoeding aan de gegevensontvanger vragen voor het beschikbaar stellen van gegevens. De vergoeding mag niet worden opgevat als betaling voor de gegevens zelf. Om te voorkomen dat gegevenshouders onevenredig hoge vergoedingen gaan vragen voor het voldoen aan een wettelijke verplichting specificeert de verordening wat wordt verstaan onder een redelijke vergoeding.

Een redelijke vergoeding kan bestaan uit de kosten die zijn gemaakt voor het beschikbaar stellen van de gegevens, bijvoorbeeld voor het omzetten naar een bruikbaar format of het onderhouden van een applicatie om toegang tot de gegevens te geven. Daarnaast kan de vergoeding eventueel een marge bevatten afhankelijk van de kosten en investeringen die zijn gemaakt voor het verzamelen van de gegevens en de mate waarin andere partijen hebben bijgedragen aan de creatie van de gegevens. Wanneer gegevens bijvoorbeeld zijn gegenereerd door acties van een gebruiker van een verbonden product en de gegevenshouder geen aanzienlijke aanvullende investeringen heeft gedaan om de gegevens te verzamelen kan de marge beperkt of zelfs uitgesloten zijn. Wanneer de gegevensontvanger een mkb⁸ of een onderzoeksorganisatie zonder winstoogmerk is mag de redelijke vergoeding alleen de kosten voor het beschikbaar stellen van de gegevens omvatten.

Geschillenbeslechting

Over de voorwaarden waaronder gegevens beschikbaar worden gesteld door gegevenshouders en de weigering, tegenhouding of opschorting om gegevens te delen op grond van een bedrijfsgeheim kunnen geschillen ontstaan tussen gegevenshouders, gegevensontvangers en gebruikers. Daarom legt de verordening vast dat lidstaten organisaties kunnen certificeren om geschillen onder hoofdstukken II, III en IV van de verordening te beslechten. Ook legt de verordening de voorwaarden vast waar geschillenbeslechtsingsorganen aan moeten voldoen om te worden gecertificeerd. Geschillenbeslechtsingsorganen moeten onder andere onafhankelijk en deskundig zijn, partijen redelijkerwijs de mogelijkheid geven hun standpunten aan te dragen en jaarlijkse activiteitenverslagen openbaar maken. Uitspraken van geschillenbeslechtsingsorganen zijn alleen bindend als alle partijen vooraf hebben ingestemd met het bindende karakter van de uitspraken. Ook doet de mogelijkheid tot geschillenbeslechting geen afbreuk aan het recht van partijen om verhaal te halen bij een rechterlijke instantie.

3.3 Oneerlijke contractuele bedingen met betrekking tot de toegang tot en het gebruik van gegevens tussen ondernemingen

⁸ Zoals aangemerkt in artikel 3 van de bijlage bij Aanbeveling 2003/361/EG.

Aanvullend op hoofdstuk III specificereert **hoofdstuk IV** van de verordening wanneer contractuele voorwaarden in overeenkomsten tussen bedrijven met betrekking tot de toegang tot en het gebruik van gegevens oneerlijk zijn. Net als hoofdstuk III van de verordening is dit een horizontaal kader. Bedrijven, met name kleinere bedrijven, zijn vanwege verschillen in machtsposities niet altijd in staat de inhoud van contracten die ze worden opgelegd te beïnvloeden. Daardoor accepteren bedrijven, wanneer zij diensten afnemen, soms ongunstige contractvoorwaarden met betrekking tot toegang en gebruik van gegevens, bijvoorbeeld dat ze gegevens die ze verstrekken zelf niet mogen gebruiken. Om het opleggen van zulke oneerlijke contractvoorwaarden tegen te gaan stelt de verordening dat alle oneerlijke contractvoorwaarden met betrekking tot de toegang tot en het gebruik van gegevens die eenzijdig zijn opgelegd niet bindend zijn. De verordening geeft hiertoe een lijst met contractuele voorwaarden die in alle omstandigheden oneerlijk zijn en een lijst met voorwaarden die mogelijk oneerlijk zijn. Het hoofdstuk is van toepassing op alle eenzijdig opgelegde contractvoorwaarden. Een contractuele voorwaarde wordt gezien als eenzijdig opgelegd wanneer een partij geen invloed op de inhoud ervan heeft gehad ondanks een poging erover te onderhandelen. De partij die de contractuele voorwaarde heeft laten opnemen moet bewijzen dat deze niet eenzijdig is opgelegd.

3.4 Gegevens beschikbaar stellen aan overheidsinstanties en EU-instellingen op grond van uitzonderlijke behoefte

Hoofdstuk V van de verordening gaat over situaties waarin overheidsinstanties en EU-instellingen (hierna: overheidsinstanties) een 'uitzonderlijke noodzaak' hebben om bepaalde gegevens van rechtspersonen die geen overheidsinstanties zijn, zoals bedrijven of stichtingen, te gebruiken om hun wettelijke taak van algemeen belang uit te voeren. De verordening beoogt te voorkomen dat overheidsinstanties in onvoorziene situaties door een gebrek aan gegevens worden belemmerd in het uitvoeren van hun wettelijke taak van algemeen belang. Daartoe creëert dit hoofdstuk een kader waarbinnen gegevenshouders in die situaties van 'uitzonderlijke noodzaak' bepaalde gegevens aan overheidsinstanties moeten verstrekken. Overheidsinstanties kunnen binnen dit hoofdstuk geen gegevens opvragen voor strafrechtelijke of bestuursrechtelijke rechtshandavingsdoeleinden.

Een uitzonderlijke noodzaak om bepaalde gegevens te gebruiken wordt bepaald door specifieke omstandigheden en is altijd beperkt in tijd en reikwijdte. Er zijn twee omstandigheden waarin een overheidsinstantie een uitzonderlijke noodzaak kan hebben om gegevens te gebruiken om hun wettelijke taak van algemeen belang uit te voeren. De eerste situatie is wanneer een overheidsinstantie bepaalde gegevens nodig heeft voor het reageren op een algemene noodsituatie en de overheidsinstantie deze gegevens niet op een andere manier tijdig en doeltreffend kan verkrijgen op een andere manier en in gelijkwaardige omstandigheden. Of er sprake is van een noodsituatie wordt bepaald of verklaard overeenkomstig het Unie- of nationaal recht en relevante procedures (zie paragraaf 5.7 van het algemeen deel van de toelichting). Denk hierbij aan noodsituaties op het gebied van volksgezondheid, grote natuurrampen, zoals bosbranden, of door de mens veroorzaakte rampen, zoals cyberincidenten.

De tweede situatie waarin sprake is van een uitzonderlijke noodzaak is wanneer het ontbreken van de specifieke gegevens een overheidsinstantie ervan weerhoudt een wettelijk taak van algemeen belang te vervullen. Hierbij valt te denken aan het opstellen van officiële statistieken of beperking van of herstel na een algemene noodsituatie. In deze situaties kan een overheidsinstantie alleen gegevens opvragen als het alle andere manieren om de gegevens tijdig te verkrijgen heeft uitgeput. De gegevens moeten dus niet verkregen kunnen worden door bijvoorbeeld vrijwillige overeenkomsten, het aankopen van de gegevens op de markt, het vaststellen van nieuwe wetgeving die de tijdige beschikbaarheid van gegevens mogelijk maakt of door een beroep te doen op reeds bestaande verplichtingen. In deze situatie van uitzonderlijke noodzaak mogen overheidsinstanties alleen niet-persoonsgebonden gegevens opvragen.

Alleen wanneer aan de hierboven genoemde voorwaarden voor een uitzonderlijke noodzaak is voldaan, kan een publieke instantie een verzoek doen om gegevens op te vragen. Deze verzoeken moeten aan strikte eisen voldoen. Zo moeten overheidsinstanties in hun verzoeken duidelijk onderbouwen welke gegevens ze nodig hebben voor welk doel en hierbij de proportionaliteit van het verzoek, gegevensbeschermingswaarborgen en de belangen van alle betrokkenen in acht nemen. Wanneer een gegevenshouder van mening is dat door de beschikbaarstelling van gegevens zijn rechten zijn geschonden, kan hij een klacht indienen bij de bevoegde autoriteit.

De overheidsinstantie moet het verzoek delen met de datacoördinator⁹ in de lidstaat waar de verzoekende overheidsinstantie is gevestigd. De datacoördinator maakt het verzoek online openbaar, tenzij dit een risico voor de openbare veiligheid oplevert. EU-instellingen zullen hun verzoek zelf online openbaar maken en de Commissie hierover informeren. Indien een verzoek persoonsgegevens omvat moet de overheidsinstantie de gegevensbeschermingsautoriteit in de lidstaat waar de gegevenshouder is gevestigd informeren.

Dataverzoek weigeren of wijzigen

Een gegevenshouder die een verzoek ontvangt, stelt de gegevens zo spoedig mogelijk ter beschikking. De gegevenshouder kan het verzoek weigeren of wijzigen wanneer het verzoek niet voldoet aan de voorwaarden uit de verordening, de gegevenshouder geen zeggenschap heeft over de gevraagde gegevens of een soortgelijk verzoek al eerder is ingediend. Bij openbare noodsituaties dient dit binnen vijf werkdagen te gebeuren en bij andere situaties van uitzonderlijke behoefte binnen 30 werkdagen. Als een overheidsinstantie de weigering wil aanvechten, kan deze worden voorgelegd aan de bevoegde autoriteit in de lidstaat waar de gegevenshouder gevestigd is.

Vergoeding

In situaties waarbij overheidsinstanties gegevens nodig hebben voor het reageren op een openbare noodsituatie stellen gegevenshouders, met uitzondering van het mkb¹⁰, de gevraagde gegevens kosteloos ter beschikking.

In situaties waarbij overheidsinstanties gegevens nodig hebben voor het vervullen van een specifieke taak, in een situatie waarin sprake is van een uitzonderlijke behoefte of wanneer het ontbreken van de specifieke gegevens een overheidsinstantie ervan weerhoudt een wettelijk taak van algemeen belang te vervullen, heeft de gegevenshouder recht op een vergoeding. Deze vergoeding dekt de technische en organisatorische kosten. Ook mag een redelijke marge in rekening gebracht worden. Op verzoek van de overheidsinstantie verstrekt de gegevenshouder informatie over de berekening van de kosten en de redelijke marge. Wanneer overheidsinstanties het niet eens zijn met de hoogte van de gevraagde vergoeding, kunnen zij een klacht indienen bij de bevoegde autoriteit in de lidstaat waar de gegevenshouder gevestigd is.

Wetenschappelijk onderzoek en statistiek

Een overheidsinstantie mag de beschikbaar gestelde gegevens delen met personen en organisaties voor wetenschappelijk onderzoek in lijn met het doel waarvoor de gegevens zijn opgevraagd. Ook mogen door overheidsinstanties gegevens worden gedeeld met nationale statistiebureaus en Eurostat voor de productie van officiële statistieken, wanneer zij daarom verzoeken ter uitvoering van Europese statistiekverordeningen. Zodra een overheidsinstantie het voornemen heeft gegevens te delen met onderzoekers, de nationale statistiebureaus of Eurostat, informeert zij de gegevenshouder van wie het gegevens heeft ontvangen hierover. Indien de gegevenshouder het niet eens is met de beschikbaarstelling van gegevens, kan hij een klacht indienen bij de bevoegde autoriteit in de lidstaat waar hij is gevestigd.

Grensoverschrijdende verzoeken

Wanneer een overheidsinstantie voornemens is om gegevens op te vragen bij een gegevenshouder die in een andere lidstaat is gevestigd, informeert zij eerst de bevoegde autoriteit van die lidstaat. De bevoegde autoriteit kan het verzoek doorsturen naar de gegevenshouder of het verzoek afwijzen.

3.5 Het vergemakkelijken van overstappen tussen dataverwerkingsdiensten

De bepalingen uit de verordening met betrekking op dataverwerkingsdiensten, ook wel clouddiensten genoemd, staan zowel in hoofdstuk VI als hoofdstuk VIII van de verordening. In deze sectie van de memorie van toelichting wordt dan ook op beide hoofdstukken ingegaan.

Hoofdstuk VI van de verordening stelt regels vast voor aanbieders van cloud- en edgediensten (dataverwerkingsdiensten). Hieronder valt een breed spectrum aan diensten die via cloud- of edgetechnologie¹¹ worden aangeboden, zowel cloudinfrastructuurdiensten als

⁹ De datacoördinator is de autoriteit die onder de verordening verantwoordelijk is voor de samenwerking tussen de verschillende bevoegde toezichthouders (zie paragraaf 3.9).

¹⁰ Zoals aangemerkt in artikel 3 van de bijlage bij Aanbeveling 2003/361/EG.

¹¹ Bij edgetechnologie vindt de verwerking van gegevens gedistribueerd plaats, vaak in de buurt van de bron van de gegevens om deze sneller en kostenefficiënter te kunnen verwerken. Bij cloudtechnologie worden gegevens op een centrale locatie verwerkt.

cloudsoftwarediensten. Voorbeelden van dergelijke diensten zijn boekhoudsoftware of voorraadbeheerssoftware. Het doel van dit hoofdstuk is om concurrentie in de markt voor dataverwerkingsdiensten te stimuleren en transparantie en controle voor gebruikers van dataverwerkingsdiensten te vergroten. Dit hoofdstuk beoogt daarvoor het makkelijker te maken over te stappen tussen dataverwerkingsdiensten van verschillende aanbieders. Momenteel worden gebruikers van dataverwerkingsdiensten vaak door aanbieders belemmerd over te stappen naar diensten van andere aanbieders of diensten van verschillende aanbieders met elkaar te combineren (zogenoeten *vendor lock-in*). Dit beperkt de concurrentie en keuzevrijheid en leidt tot bundeling van diensten in de markt voor dataverwerkingsdiensten.

De regels in dit hoofdstuk zijn niet van toepassing op tijdelijke test- en evaluatieversies van dataverwerkingsdiensten. De bepalingen met betrekking tot overstapkosten en enkele technische eisen aan het overstappen¹² zijn niet van toepassing op dataverwerkingsdiensten die specifiek voor een individuele gebruiker zijn ontwikkeld of waar het merendeel van de belangrijke componenten specifiek voor een individuele gebruiker zijn ontwikkeld en de dataverwerkingsdienst niet op grote commerciële schaal wordt aangeboden.

Hoofdstuk VIII vult hoofdstuk VI aan met maatregelen zodat gebruikers van dataverwerkingsdiensten makkelijker diensten van verschillende aanbieders gelijktijdig en verbonden kunnen gebruiken. Veel bedrijven gebruiken meerdere types dataverwerkingsdiensten. Gebruikers hebben er in zulke gevallen baat bij dat die verschillende diensten gelijktijdig en verbonden kunnen worden gebruikt, bijvoorbeeld doordat verkoopsoftware (continu) gegevens kan uitwisselen met een voorraadbeheersysteem en boekhoudsoftware. Dan kunnen gegevens van een verkoop meteen worden verwerkt in de voorraad en de boekhouding. Momenteel is dit soort 'gelijktijdig gebruik' voor veel diensten alleen mogelijk als de diensten bij dezelfde (groep van) aanbieder(s) worden afgenomen. De verordening beoogt te zorgen dat dergelijk gelijktijdig gebruik ook mogelijk wordt tussen dataverwerkingsdiensten van verschillende aanbieders. Bepaalde verplichtingen uit hoofdstuk VI zijn daarom ook van toepassing op aanbieders van dataverwerkingsdiensten (hierna: aanbieders) om interoperabiliteit voor gelijktijdig gebruik te faciliteren.

De verordening verplicht aanbieders om alle belemmeringen weg te nemen die gebruikers ervan weerhouden over te stappen naar andere aanbieders met het behoud van functionele gelijkwaardigheid. Daarbij moet het voor gebruikers mogelijk zijn gegevens en applicaties over te dragen en verschillende diensten los te koppelen. Functionele gelijkwaardigheid betekent dat bij het overstappen naar een nieuwe dataverwerkingsdienst van hetzelfde type, de nieuwe dataverwerkingsdienst op basis van de overgedragen gegevens en applicaties zou moeten kunnen functioneren en bij gedeelde functies een vergelijkbare output geeft op basis van dezelfde input. Als een gebruiker van voorraadbeheerssoftware wisselt en beide diensten geven een overzicht van een prijsontwikkeling over tijd, zou deze functie voor beide systemen vergelijkbare output moeten geven op basis van de overgedragen input. Met het oog op gelijktijdig gebruik, moeten aanbieders ook belemmeringen voor interoperabiliteit wegnemen. In aanvulling op deze algemene verplichtingen om belemmeringen weg te nemen bevat het hoofdstuk ook specifieke verplichtingen met betrekking tot contractvoorwaarden, overstapkosten en de technische vereisten voor het overstappen.

Contractuele aspecten van overstappen

Om te voorkomen dat gebruikers door contractvoorwaarden niet kunnen overstappen moeten aanbieders de rechten en plichten van de gebruiker en de aanbieder met betrekking tot het overstappen uiteenzetten in een contract. De gebruiker heeft het recht zonder onnodige vertraging over te stappen. De aanbieder moet onder andere het overstappen redelijkerwijs faciliteren en gedurende het overstapproces of gelijktijdig gebruik de veiligheid en bedrijfscontinuïteit verzekeren. Eventuele risico's moeten daarbij duidelijk kenbaar worden gemaakt aan de gebruiker. Ook moet het contract afspraken over continuïteit bevatten en moeten aanbieders voordat de overeenkomst wordt gesloten de relevante kosten duidelijk communiceren, waaronder, wanneer relevant, de kosten voor het overstappen of het vroegtijdig beëindigen van het contract. De aanbieder moet de gebruiker daarnaast voorzien van informatie over beschikbare overdrachtsmethoden en -formats voor het overstappen en een online register bijhouden met details over alle datastructuren, dataformaten, relevante normen en interoperabiliteitsspecificaties waarin de exporteerbare gegevens beschikbaar zullen zijn.

Overstapkosten

¹² Artikelen 23(d) 30(1) en 30(3) uit de verordening

Vanaf 12 januari 2027 mogen aanbieders geen overstapkosten meer in rekening brengen. Tot die tijd mogen aanbieders verlaagde overstapkosten in rekening brengen. Deze kosten mogen in ieder geval niet hoger zijn dan de kosten die de aanbieder daadwerkelijk maakt in het betreffende overstapproces. De aanbieder dient uit te leggen op welke aspecten van haar dienstverlening deze kosten van toepassing zijn zodat de gebruiker kan controleren of hier niet te veel in rekening wordt gebracht.

Technische eisen aan het overstappen

Aanbieders van cloudinfrastructuurdiensten (IaaS) moeten alle redelijke en haalbare maatregelen nemen die nodig zijn voor de gebruiker, om na het overstappen naar een vergelijkbare dienst van een andere aanbieder functionele gelijkwaardigheid te bereiken. Specifiek voor aanbieders van IaaS geldt dus een zwaardere verplichting met betrekking tot functionele gelijkwaardigheid dan de eerdergenoemde verplichting om belemmeringen weg te nemen die functionele gelijkwaardigheid na het overstappen beletten.

Aanbieders van andere dataverwerkingsdiensten, zoals cloudplatformdiensten en cloudsoftwareapplicaties zijn verplicht kosteloos interfaces beschikbaar te stellen aan gebruikers en andere aanbieders om het overstappen te faciliteren en gelijktijdig gebruik mogelijk te maken. Aanbieders van deze dataverwerkingsdiensten moeten om interoperabiliteit te bevorderen hun diensten ook verenigbaar maken met de relevante open standaarden voor interoperabiliteit van dataverwerkingsdiensten die de Europese Commissie publiceert in lijn met de bevoegdheden uit hoofdstuk VIII (zie paragraaf 3.7 van het algemeen deel van de toelichting).

Internationale toegang en doorgifte

Aanbieders dienen op hun website informatie te publiceren over het recht waaronder de infrastructuur van hun dataverwerkingsdiensten valt of vallen. Daarnaast dienen ze gebruikers te informeren over de maatregelen die ze in lijn met hoofdstuk VII van de verordening nemen om te voorkomen dat overheden toegang kunnen krijgen tot niet-persoonsgebonden gegevens die in de Europese Unie wordt bewaard, wanneer dergelijke doorgifte strijdig zou zijn met EU of nationaal recht.

Aanvullend stelt dit hoofdstuk eisen aan open specificaties en geharmoniseerde standaarden voor de interoperabiliteit van clouddiensten. Hier wordt in paragraaf 3.7 van het algemeen deel van de toelichting verder op ingegaan.

3.6 Internationale overheidstoegang en overdracht van niet-persoonsgebonden gegevens

Hoofdstuk VII van de verordening gaat over overheidstoegang vanuit landen buiten de Europese Unie tot niet-persoonsgebonden gegevens die door dataverwerkingsdiensten in de Europese Unie worden opgeslagen of verwerkt. Vanuit het Unie- of nationaal recht bestaat ten aanzien van een aantal niet-persoonsgebonden gegevens de verplichting om ze te beschermen. Dit gaat bijvoorbeeld om de bescherming van de fundamentele belangen van een lidstaat in verband met de nationale veiligheid of de bescherming van commercieel gevoelige gegevens, inclusief bedrijfsgeheimen en intellectuele eigendomsrechten. Overheden uit derde landen toegang verlenen tot zulke gegevens is strijdig is met de verplichting tot bescherming ervan. Daarom moeten aanbieders van dataverwerkingsdiensten technische, juridische en organisatorische maatregelen nemen om te voorkomen dat zij niet-persoonsgebonden gegevens overdragen naar een overheid uit een derde land wanneer dit in strijd is met het Europees recht of het recht van een lidstaat. Relevante maatregelen kunnen bijvoorbeeld versleuteling en adequaat organisatorisch toegangsbeleid zijn.

Indien een beslissing, uitspraak of besluit van een rechterlijke instantie of administratieve autoriteit uit een derde land toegang of overdracht van niet-persoonsgebonden gegevens vereist, mogen aanbieders van dataverwerkingsdiensten een dergelijke beslissing, uitspraak of besluit in principe alleen honoreren als deze is gebaseerd op een relevante internationale overeenkomst, zoals een verdrag inzake wederzijdse rechtshulp. Bij afwezigheid van een dergelijke internationale overeenkomst en wanneer de naleving van een dergelijke beslissing, uitspraak of besluit de aanbieder van dataverwerkingsdiensten 'in strijd zou kunnen brengen met Europees of nationaal recht, mogen aanbieders alleen onder specifieke voorwaarden de overdracht van of toegang tot gegevens laten plaatsvinden. Deze voorwaarden zijn dat i) de beslissing, uitspraak of besluit volgens het rechtssysteem uit het derde land specifiek moet zijn en de evenredigheid moet worden onderbouwd, ii) gemotiveerde bezwaren tegen het besluit door een bevoegde rechtelijke instantie worden gehoord en iii) de bevoegde rechterlijke instantie het juridisch belang van de datahouders in Europa mag meewegen. Wanneer aan deze voorwaarden is voldaan kan de aanbieder het besluit honoreren en de minimale toegestane hoeveelheid gegevens beschikbaar stellen. Aanbieders zullen

de datahouder informeren over een ontvangen verzoek voor zij hieraan voldoen, behalve als het verzoek betrekking heeft op rechtshandhaving en dit in de weg staat van effectieve rechtshandhaving.

Advies vragen bij de bevoegde autoriteit

De aanbieder kan de bevoegde autoriteit voor internationale juridische samenwerking om advies vragen om te bepalen of aan de hierboven genoemde vereisten is voldaan. Dit speelt met name bij bedrijfsgeheimen en andere commercieel gevoelige gegevens, intellectuele-eigendomsrechten en als de overdracht van gegevens tot heridentificatie zou kunnen leiden. Wanneer de aanbieder constateert dat het verzoek afbreuk kan doen aan de nationale veiligheid of de defensie van de Europese Unie of lidstaten vraagt het advies van de nationale bevoegde autoriteit met relevante competenties op dit terrein. Als er binnen een maand niet gereageerd wordt op het adviesverzoek, of de conclusie van het advies van de bevoegde autoriteit is dat er niet aan de voorwaarden is voldaan, dan mag de aanbieder het verzoek weigeren.

3.7 Interoperabiliteit

Hoofdstuk VIII stelt regels om interoperabiliteit te bevorderen: voor dataruimtes, dataverwerkingsdiensten en de geautomatiseerde uitvoering van gegevensdelingsovereenkomsten (slimme contracten). Interoperabiliteit is belangrijk om gegevens voor de ontvanger vindbaar, toegankelijk en gebruiksvriendelijk te maken. Om interoperabiliteit te bereiken worden er eisen gesteld aan de machineleesbaarheid van gegevens, datastructuren en -formaten, en de technische mogelijkheden om toegang tot gegevens te krijgen, zodat (automatische) toegang en overdracht van gegevens tussen partijen mogelijk wordt.

De verordening stelt eisen aan open specificaties en geharmoniseerde standaarden voor de interoperabiliteit van dataverwerkingsdiensten. De interoperabiliteitsspecificaties dienen in te gaan op zowel de infrastructuur, data- als applicatielaag. Zij zullen moeten worden ontworpen op een manier die technologische ontwikkeling, nieuwe functies en innovaties mogelijk maken. Het streven naar interoperabiliteit mag echter de veiligheid en integriteit van dataverwerkingsdiensten niet aantasten. De Europese Commissie kan de Europese normalisatie-organisaties verzoeken deze eisen verder uit te werken tot geharmoniseerde normen, en specificaties die voldoen aan de eisen uit de verordening als gemeenschappelijke specificaties vaststellen. Deze gemeenschappelijke specificaties kunnen middels uitvoeringshandelingen door de Europese Commissie worden gepubliceerd in het publicatieblad van de EU. Wanneer lidstaten van mening zijn dat een gemeenschappelijke specificatie niet aan de eisen uit de verordening voldoet kunnen zij de Europese Commissie hiervan op de hoogte stellen. Indien nodig kan de Europese Commissie de gemeenschappelijke specificatie wijzigen.

Om interoperabiliteit binnen en tussen dataruimten te faciliteren legt de verordening een aantal interoperabiliteitseisen op aan deelnemers aan dataruimten, bijvoorbeeld met betrekking tot semantiek of de beschrijving van metadata. Ook voor dit onderdeel kan de Europese Commissie normalisatie-organisaties verzoeken deze eisen verder uit te werken tot geharmoniseerde normen, en specificaties die voldoen aan de eisen uit de verordening als gemeenschappelijke specificaties vaststellen. Deze worden gepubliceerd in het publicatieblad van de EU.

Slimme contracten, contracten die zichzelf automatisch uitvoeren zodra er aan de voorwaarden in het contract is voldaan hebben het potentieel om gegevenshouders en gegevensontvangers garanties te bieden dat de door hen afgesproken voorwaarden voor het delen van gegevens worden gerespecteerd. Gegevensdeling kan door middel van slimme contracten geautomatiseerd worden uitgevoerd op basis van vooraf bepaalde voorwaarden. Zo kunnen ze (her)gebruik van gegevens in dataruimtes faciliteren.

Slimme contracten dienen gebaseerd te zijn op wederzijdse instemming. Daarom dient een verkoper of beheerder van applicaties die gebruik maakt van slimme contracten voor de geautomatiseerde uitvoering van gegevensdelingsovereenkomsten het mogelijk te maken dat slimme contracten kunnen worden onderbroken of beëindigd. Daarnaast dient aan data-archiveringseisen te worden voldaan, ook nadat een slim contract is gedeactiveerd, zodat transactionele gegevens, back logs en code kunnen worden bewaard.

3.8 Uitvoering en handhaving

Hoofdstuk IX stelt regels over toezicht.

Bevoegde autoriteiten en datacoördinator

Elke lidstaat zal één of meerdere bevoegde autoriteiten benoemen die verantwoordelijk worden voor de toepassing en het toezicht van de verordening. Lidstaten mogen nieuwe bevoegde autoriteiten oprichten of taken toebedelen aan bestaande autoriteiten. De bevoegde autoriteiten hebben verschillende taken en bevoegdheden waaronder het behandelen van klachten, het verrichten van onderzoeken naar zaken die betrekking hebben op de toepassing van de verordening, het opleggen van sancties en het samenwerken met andere autoriteiten, de Commissie en het Europees Comité voor gegevensinnovatie. Bevoegde autoriteiten zorgen voor het bevorderen van datageletterdheid¹³ en bewustmaking van de rechten en verplichtingen uit deze verordening. Daarnaast moeten zij toezicht houden op technologische en commerciële ontwikkelingen die relevant zijn voor het beschikbaar stellen en gebruiken van gegevens, de opheffing van de overstapkosten (overeenkomstig artikel 29 van de verordening) en onderzoeken zij gegevensverzoeken van overheidsinstanties uit hoofdstuk V van de verordening.

Indien een lidstaat meer dan één bevoegde autoriteit aanwijst, wijst hij onder deze bevoegde autoriteiten één centraal contactpunt aan, de datacoördinator, om de samenwerking tussen hen te vergemakkelijken en bevoegde autoriteiten bij te staan met de uitvoering, toepassing en handhaving van de verordening. Met betrekking tot hoofdstuk V waarborgt de datacoördinator dat overheidsverzoeken online openbaar beschikbaar zijn, en bevordert de datacoördinator vrijwillige overeenkomsten voor het delen van gegevens tussen overheidsinstanties en datahouders. Met betrekking tot bedrijfsgeheimen stelt de datacoördinator de Europese Commissie in kennis wanneer datadelen wordt geweigerd vanwege risico's op ernstige economische schade. Ook verstrekt de datacoördinator natuurlijke en rechtspersonen op verzoek alle benodigde informatie om hun klachten bij de juiste bevoegde autoriteit in te dienen. Als er slechts één bevoegde autoriteit wordt aangewezen, dan vervult deze, waar nodig, automatisch ook de taken van de datacoördinator.

Klachtrecht en beroep

Indien een partij denkt dat zijn/haar rechten uit deze verordening zijn geschonden is er de mogelijkheid om een klacht in te dienen bij de bevoegde autoriteit in de lidstaat waar deze partij is gevestigd.

Indien een bevoegde autoriteit nalaat een klacht te behandelen, heeft de klager recht op een doeltreffende voorziening in rechte of op toetsing door een onpartijdige instantie met de nodige expertise. Daarnaast is beroep mogelijk tegen juridisch bindende besluiten die door de autoriteiten zijn genomen.

Sancties

Voor inbreuk op de regels uit deze verordening stellen lidstaten doeltreffende sancties op. Hierin moet bijvoorbeeld rekening worden gehouden met de ernst van de inbreuk, verkregen financiële voordelen en/of eerdere inbreuken.

Samenwerking bevoegde autoriteiten

Lidstaten moeten ervoor zorgen dat bevoegde autoriteiten samenwerken met andere autoriteiten. Dit gaat om de andere bevoegde autoriteiten binnen de lidstaat, de bevoegde autoriteiten van andere lidstaten, de Commissie, het Europees Comité voor gegevensinnovatie en bevoegde autoriteiten die verantwoordelijk zijn voor de uitvoering van andere Unie- of nationale rechtshandelingen (zoals de Autoriteit Persoonsgegevens voor de AVG en sectorale autoriteiten). Indien een datacoördinator is aangewezen faciliteert die deze samenwerking.

Door de uitoefening van hun onderzoeksbevoegdheden moeten de bevoegde autoriteiten informatie kunnen opzoeken en verkrijgen met betrekking tot entiteiten die in de lidstaat zijn gevestigd. Een entiteit die in de Unie verbonden producten of diensten aanbiedt en niet in de Unie is gevestigd, wijst een wettelijke vertegenwoordiger aan in een van de lidstaten. In grensoverschrijdende situaties moeten bevoegde autoriteiten uit verschillende lidstaten samenwerken. Zij moeten elkaar tijdig bijstaan, met name wanneer een bevoegde autoriteit in een lidstaat over relevante informatie beschikt voor een onderzoek dat door de bevoegde autoriteiten in andere lidstaten wordt uitgevoerd, of wanneer een bevoegde autoriteit in een lidstaat informatie kan verzamelen waar de bevoegde autoriteiten in de lidstaat waar de entiteit is gevestigd geen toegang toe hebben. Indien een bevoegde autoriteit in een lidstaat om bijstand of handavingsmaatregelen van een bevoegde autoriteit in een andere lidstaat verzoekt, dient zij een gemotiveerd verzoek in. Na ontvangst van een dergelijk verzoek geeft een bevoegde autoriteit onverwijld een antwoord met een gedetailleerde beschrijving van de maatregelen die zijn genomen of gepland.

¹³ Datageletterdheid zijn de vaardigheden, kennis en het inzicht die gebruikers, consumenten en bedrijven in staat stellen zich bewust te worden van de potentiële waarde van de gegevens die zij genereren, produceren en delen.

Toezicht persoonsgegevens

De toezichthoudende autoriteiten die verantwoordelijk zijn voor het toezicht op de AVG, zijn verantwoordelijk voor het toepassing van de verordening wat betreft de bescherming van persoonsgegevens. In Nederland is dit de Autoriteit persoonsgegevens (AP). De AP kan gebruik maken van de toezichtsbevoegdheden uit de Algemene Verordening Gegevensbescherming (AVG) en boetes opleggen voor overtredingen met betrekking tot de verwerking van persoonsgegevens in situaties zoals bedoeld in hoofdstukken II, III, V en VI van de verordening.

De Europese toezichthouder voor gegevensbescherming is verantwoordelijk voor het toezicht op de toepassing van deze verordening voor zover deze betrekking heeft op de Commissie, de Europese Centrale Bank of organen van de Unie. De Europese toezichthouder voor gegevensbescherming kan voor inbreuken op verplichtingen uit hoofdstuk V boetes opleggen aan deze EU-instellingen (overeenkomstig artikel 66 van Verordening 2018/1725).

Europees Comité voor gegevensinnovatie

Het Europees Comité voor gegevensinnovatie is een deskundigengroep met de volgende taken: het adviseren over consistent toezicht, het stimuleren van samenwerking en informatie-uitwisseling tussen de toezichthouders uit de verschillende EU-lidstaten, het adviseren over gemeenschappelijke normen en uitvoering en het adviseren over uitvoering- en/of gedelegeerde handelingen.

3.9 Sui-generis-recht krachtens richtlijn 96/9/EC

Hoofdstuk X verduidelijkt dat het sui-generis-recht uit de Databankrichtlijn niet van toepassing is op gegevens verkregen uit, of gegenereerd door, een verbonden product of gerelateerde dienst (zie paragraaf 5.4 van het algemeen deel van de toelichting). Het sui-generis-recht beschermt databanken waarin substantieel is geïnvesteerd. Door te verduidelijken dat dit recht niet van toepassing is op gegevens uit verbonden producten en gerelateerde diensten wordt voorkomen dat het sui-generis-recht het delen van deze gegevens onevenredig belemmert.

4. Inhoud Uitvoeringswet

De bepalingen uit de verordening zijn onverkort van toepassing in de Nederlandse rechtsorde. De verordening regelt diverse rechten en verplichtingen die rechtstreeks gelden (zie de transponeringstabel aan het einde van de toelichting). Ter uitvoering van de verordening wordt een aantal bevoegde autoriteiten aangewezen en wordt voorzien in het toezicht en de handhaving van de verordening.

De Minister van Economische Zaken en Klimaat is verantwoordelijk voor de algemene uitvoering van de verordening, met uitzondering van de bepalingen waarvoor de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties of de Minister voor Rechtsbescherming verantwoordelijk is. De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties is verantwoordelijk voor de uitvoering van het beschikbaar stellen van gegevens aan overheidsinstanties in gevallen van uitzonderlijke noodzaak (hoofdstuk V en verwante artikelen). De Minister voor Rechtsbescherming is verantwoordelijk voor databankregelgeving (hoofdstuk X). De Uitvoeringswet en bijbehorende memorie van toelichting zijn door de Minister van Economische Zaken en Klimaat mede namens de Minister voor Rechtsbescherming en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties opgesteld.

4.1 Aanwijzen bevoegde autoriteiten

Gelet op artikel 37, eerste lid, van de verordening moet Nederland één of meer bevoegde autoriteiten aanwijzen om toezicht te houden op de bepalingen uit de verordening. In deze paragraaf wordt beschreven welke autoriteiten worden aangewezen en waarom.

In algemene zin stelt de verordening in artikel 37, achtste lid, eisen aan te wijzen bevoegde autoriteiten. Bij de uitvoering van hun taken en bevoegdheden overeenkomstig deze verordening moeten bevoegde autoriteiten onpartijdig zijn en vrij zijn van enige, directe of indirecte, invloed van buitenaf, en vragen noch aanvaarden zij voor individuele gevallen instructies van andere overheidsinstanties of particuliere partijen.

Autoriteit Consument en Markt

De Autoriteit Consument en Markt (hierna: ACM) wordt in de Uitvoeringswet aangewezen als de bevoegde autoriteit voor hoofdstukken II, III, IV, VI, VII en VIII van de verordening. De ACM is een zbo met als doel het bevorderen van goed functionerende markten, van ordelijke en transparante marktprocessen en van een zorgvuldige behandeling van consumenten (artikel 2, vijfde lid, van de Instellingswet Autoriteit Consument en Markt (hierna: Instellingswet ACM)). De doelstellingen van de verordening en de aard van de verplichtingen sluiten aan bij de bestaande taken en specifieke deskundigheid van de ACM. De normadressaten van hoofdstukken II, III, IV, VI, VII en VIII van de verordening, waaronder aanbieders van dataverwerkingsdiensten en aanbieders van verbonden producten en gerelateerde diensten, zijn ondernemingen die al onderworpen zijn aan het toezicht van de ACM op grond van andere wetgeving, bijvoorbeeld op grond van de Mededingingswet en het consumentenrecht.

Het thema "digitale economie" is bovendien één van de drie thema's die de ACM tot prioriteit heeft bestempeld in haar meest recente uitvoeringsagenda¹⁴. De ACM treedt in dat kader op tegen marktmacht (bijvoorbeeld van grote technologische bedrijven) en misleiding en manipulatie van consumenten, zodat alle mensen en bedrijven met vertrouwen gebruik kunnen maken van digitale markten. De ACM heeft als toezichthouder uitgebreide ervaring en expertise op het terrein van economische ordening. Daarnaast is bij de ACM specifieke technische expertise aanwezig om op de digitale sectoren van de economie toezicht te houden. Vanuit de beoogde rol van de ACM als toezichthouder op de digitaaldienstenverordening zal de ACM hier bovendien verder ervaring mee opdoen. Ook is geconstateerd dat de ACM als organisatie in staat is om de werkzaamheden die deze toezichtstaken met zich meebrengen adequaat te borgen. In lijn met artikel 37, negende lid, van de verordening moet de Minister van Economische Zaken en Klimaat zorgen voor voldoende personele en technische middelen aan de ACM.

De ACM heeft in de periode voorafgaand aan de totstandkoming van de verordening expertise opgebouwd over verbonden apparaten. De economische ontwikkeling die gepaard gaat met de groei van deze productcategorie is een thema waar de ACM ervaring en expertise op heeft. In combinatie met bovenstaande redenen maakt dit het aanwijzen van de ACM als toezichthouder op Hoofdstuk II een logische stap.

Gezien de rol van de ACM bij het toezicht op de Nederlandse economie heeft zij ook ervaring met het beoordelen van overeenkomsten tussen bedrijven onderling en tussen bedrijven en consumenten. Dat maakt dat ook op het derde en vierde hoofdstuk van de verordening toezicht van de ACM gewenst is.

Ten aanzien van het bestuderen van de economische en technologische ontwikkelingen op het gebied van dataverwerkingsdiensten heeft de ACM een leidende rol in het Nederlandse en Europese toezichtlandschap opgebouwd. Dit maakt dat de ACM ook voor hoofdstuk VI en in het verlengde daarvan hoofdstukken VII en VIII de gewenste toezichthouder is.

Autoriteit Persoonsgegevens

De Autoriteit Persoonsgegevens (hierna: AP) wordt in de Uitvoeringswet aangewezen als de bevoegde autoriteit voor hoofdstuk V. Conform de verordening zou de AP als AVG-toezichthouder al een rol hebben bij het toezicht op hoofdstuk V, aangezien overheidsinstanties bij de AP moeten melden wanneer zij persoonsgegevens verzoeken. Door deze rol uit te breiden en AP als bevoegde autoriteit voor hoofdstuk V aan te wijzen, wordt het toezicht op dit onderdeel van de verordening, dat inhoudelijk weinig raakvlakken met de andere onderdelen heeft, centraal belegd. Overheidsinstanties, de normadressaten van hoofdstuk V, zijn bovendien al onderworpen aan toezicht van AP op basis van de AVG. De AP heeft vanuit haar taken als AVG-toezichthouder bovendien ervaring met het beoordelen van de rechtmatigheid en proportionaliteit van verwerkingen van persoonsgegevens door overheidsinstanties. In het meest recente jaarplan van AP is digitale overheid bovendien één van de centrale thema's waar de AP extra aandacht aan wil besteden.¹⁵

Nationale autoriteit hoofdstuk VII

De ACM wordt in de Uitvoeringswet aangewezen als de bevoegde autoriteit voor hoofdstuk VII. Daarnaast worden in hoofdstuk VII van de verordening andere autoriteiten genoemd. Er staat dat de geadresseerde van een beslissing, besluit of rechterlijke uitspraak (dus een aanbieder van dataverwerkingsdiensten) advies kan inwinnen van de nationale instantie of autoriteit die bevoegd is voor internationale samenwerking in juridische aangelegenheden en de nationale bevoegde

¹⁴ [Focus Werkzaamheden ACM 2023 | ACM.nl](#)

¹⁵ [AP jaarplan 2024 | Autoriteit Persoonsgegevens](#)

autoriteit met competenties op het terrein van nationale veiligheid of defensie van de EU of de lidstaten (zie ook paragraaf 3.6 van het algemeen deel van de toelichting).

4.2 Taken en bevoegdheden bevoegde autoriteiten

De taken en bevoegdheden van de bevoegde autoriteiten uit artikel 37, vijfde lid, van de verordening zijn in paragraaf 3.8 van het algemeen deel van de toelichting beschreven. In artikel 3, tweede en vierde lid, van de Uitvoeringswet is bepaald dat de bevoegde autoriteiten bevoegd zijn om de taken uit te voeren en de bevoegdheden uit te oefenen die in de verordening aan de bevoegde autoriteiten zijn toegekend. Voor sommige taken is geen aanvullende nationale regelgeving nodig, namelijk het bevorderen van datageletterdheid, het toezicht op relevante ontwikkelingen, het zorgen voor de opheffing van overstapkosten en het onderzoeken van gegevensverzoeken van overheidsinstanties uit hoofdstuk V van de verordening. Voor andere taken zijn aanvullende bepalingen in nationale regelgeving noodzakelijk. In deze paragraaf wordt aangegeven hoe die taken en bevoegdheden van de bevoegde autoriteiten zijn belegd in Nederlandse regelgeving.

Klachtenbehandeling

De bevoegde autoriteiten moeten klachten over vermeende overtredingen op de verordening behandelen (artikel 37, vijfde lid, onderdeel b, van de verordening; zie ook het recht om een klacht in te dienen in artikel 38 van de verordening). De bevoegde autoriteiten moeten de inhoud van klachten onderzoeken in de mate waarin dat gepast is en klagers, indien relevant overeenkomstig het nationale recht, regelmatig en binnen een redelijke termijn in kennis stellen van de voortgang en het resultaat van het onderzoek, met name wanneer verder onderzoek of coördinatie met een andere bevoegde autoriteit noodzakelijk is.

Het begrip "klacht" heeft in de verordening een autonome betekenis, die moet worden onderscheiden van het begrip "klacht" in de Algemene wet bestuursrecht (hierna: Awb). In de verordening heeft een klacht betrekking op een vermeende schending op rechten uit hoofde van de verordening. In de Awb heeft het woord klacht betrekking op de wijze waarop een bestuursorgaan zich in een bepaalde aangelegenheid heeft gedragen.

Het is afhankelijk van de formulering en de inhoud van de klacht of de klacht naar Nederlands recht beschouwd moet worden als een verzoek van een belanghebbende om een handhavingsbesluit te nemen (artikel 1:3, derde lid, van de Awb) en daarmee als een handhavingsverzoek moet worden beschouwd. Hierbij dient de bevoegde autoriteit onder andere te toetsen of het verzoek voldoende concreet is en of de klager (of zijn gemachtigde) de bevoegde autoriteit enig aanknopingspunt biedt voor onderzoek naar de vraag of er sprake is van een schending van rechten uit de verordening.

Daarnaast dient de klager (of zijn gemachtigde) een belanghebbende te zijn (in de zin van artikel 1:2, eerste lid, van de Awb) om de klacht als handhavingsverzoek te kunnen beschouwen. Als er sprake is van een handhavingsverzoek, heeft de bevoegde autoriteit een beginselplicht tot handhaving. Als de klacht beschouwd wordt als handhavingsverzoek, is de schriftelijke reactie van de bevoegde autoriteit op de klacht een besluit in de zin van artikel 1:3, eerste lid, van de Awb. Hiertegen staat bezwaar en beroep open. Deze kwalificatie naar nationaal recht staat los van de vereisten die de verordening aan het klachtrecht stelt, zoals het recht van partijen om te worden gehoord en passende informatie te ontvangen over de stand van zaken in verband met de klacht. Dit zijn autonome vereisten.

Onderzoeksbevoegdheden

Bevoegde autoriteiten moeten onderzoek kunnen verrichten naar zaken die betrekking hebben op de toepassing van deze verordening. Door de uitoefening van hun onderzoeksbevoegdheden moeten de bevoegde autoriteiten informatie kunnen opzoeken en verkrijgen, met name met betrekking tot activiteiten van entiteiten die onder hun bevoegdheid vallen. Hiervoor moeten zij ook informatie kunnen verkrijgen van andere bevoegde autoriteiten of andere overheidsinstanties en bij grensoverschrijdende gevallen ook van bevoegde autoriteiten uit andere lidstaten (zie hierna samenwerking met andere autoriteiten).

De ACM en de AP zijn aangewezen als toezichthouders op de verordening en beschikken daardoor op grond van titel 5.2 van de Awb over een aantal standaardbevoegdheden die zij kunnen inzetten bij het uitoefenen van hun toezichtstaak op grond van de Uitvoeringswet. De bevoegdheid tot het vorderen van informatie (artikel 37, vijfde lid, onderdeel c, van de verordening) komt overeen met de bevoegdheid tot het vorderen van inlichtingen (artikel 5:16 van de Awb).

De Instellingswet ACM kent de ACM een aantal handhavingsbevoegdheden toe in het kader van het toezicht op en de handhaving van de wettelijke voorschriften waarmee de ACM is belast. Het betreft onder meer de bevoegdheid tot het bindend verklaren van een toezegging (artikel 12h van de Instellingswet ACM) en het opleggen van een bindende aanwijzing (artikel 12j van de Instellingswet ACM), waarbij concreet wordt aangegeven wat er van de normadressaat wordt gevraagd ter nakoming van de open norm. Daarnaast kan de ACM uit eigen beweging een marktonderzoek doen in het kader van de verordening (artikel 2, vierde lid, van de Instellingswet ACM). De ACM zal deze bevoegdheden ook kunnen inzetten ten behoeve van de uitvoering van haar taken op grond van de Uitvoeringswet, wanneer die verheven is tot wet. De bevoegdheid daartoe vloeit rechtstreeks voort uit de Instellingswet ACM. Er bestaat derhalve geen noodzaak om daarover iets te regelen in onderhavige Uitvoeringswet.

Sancties

Om handhaving van de verordening effectief te maken verplicht artikel 37, vijfde lid, onderdeel d, van de verordening dat lidstaten sancties vaststellen, waaronder dwangsommen, voor inbreuken op de verordeningen. De sancties moeten doeltreffend, evenredig en afschrikkend zijn en rekening houden met de aanbevelingen van het Europees Comité voor gegevensinnovatie en de criteria uit artikel 40, derde lid, van de verordening (zoals dat de boete gerelateerd is aan de jaaromzet van de inbreukmakende partij).

Artikel 6 van de Uitvoeringswet bepaalt dat bij overtreding van de verordening de ACM en de AP een bestuurlijke boete en een last onder dwangsom, en daarmee ook een last onder bestuursdwang, kunnen opleggen.

De hoogte van de boete sluit aan bij de bestaande praktijk rondom bestuurlijke boetes. Voor de hoogte van de maximale boete wordt aangesloten bij de boetebepalingen in de Telecommunicatiewet. Deze wet kan worden gezien als aangrenzend rechtsgebied gelet op de taken voor de ACM op het terrein van digitalisering, en de beoogde Uitvoeringswet datagovernanceverordening. Voor een overtreding kan door de ACM een bestuurlijke boete worden opgelegd van ten hoogste het bedrag dat is vastgesteld voor de zesde categorie, bedoeld in 23, vierde lid, van het Wetboek van Strafrecht of, indien dat meer is, 10% van de jaaromzet van de overtreder. Dit is in lijn met de beoogde Wet stroomlijning bestuurlijke boetemaxima en termijnen en is vooruitlopend daarop al verwerkt in dit wetsvoorstel. In de Instellingswet ACM staan regels omtrent de bevoegdheid van de ACM bij het opleggen van bestuurlijke boetes.

Samenwerking met andere autoriteiten

De bevoegde autoriteiten moeten samenwerken met andere autoriteiten. Het gaat hier om de andere bevoegde autoriteiten in Nederland, de bevoegde autoriteiten van andere lidstaten, de Commissie, het Europees Comité voor gegevensinnovatie en de bevoegde autoriteiten die verantwoordelijk zijn voor de uitvoering van andere Unie- of nationale rechtshandelingen (zoals de Autoriteit Persoonsgegevens voor de AVG en sectorale autoriteiten). Zie verder paragraaf 3.8 van het algemeen deel van de toelichting.

Voor elk hoofdstuk uit de verordening is één bevoegde autoriteit aangewezen. Bij de uitoefening van het toezicht is in sommige gevallen echter ook de expertise van een andere toezichthouder noodzakelijk. Zo heeft de Rijksinspectie Digitale Infrastructuur (hierna: RDI) relevante expertise op het terrein van cybersecurity voor het toezicht op hoofdstukken II, VI en VII. Als voor hoofdstuk VII van de verordening de expertise van RDI nodig is om te beoordelen of een aanbieder van dataverwerkingsdiensten adequate technische maatregelen heeft genomen, zal RDI informatie over een specifieke casus moeten kunnen ontvangen. Ook kan samenwerking met een sectorale toezichthouder wenselijk zijn omdat deze expertise bezit die de bevoegde autoriteit niet in huis heeft, bijvoorbeeld op het gebied van bepaalde typen verbonden apparaten zoals medische apparatuur. Om deze samenwerking te vergemakkelijken kunnen afspraken worden gemaakt in een samenwerkingsprotocol.

Daarnaast is samenwerking tussen de ACM en de AP nodig, gezien de AP de toezichthouder op de AVG is en expertise heeft over de bescherming van persoonsgegevens. Een belangrijk deel van de handhaving van de verordening zal betrekking hebben op het verwerken van gegevens, bijvoorbeeld het beschikbaar stellen van gegevens uit producten of het overdragen van gegevens uit dataverwerkingsdiensten. Wanneer deze gegevens persoonsgegevens betreffen is ook de AVG van toepassing en is er overlap tussen de Dataverordening en de AVG. Alle verwerkingen van persoonsgegevens die op basis van de verordening plaatsvinden moeten onverminderd voldoen aan de AVG. In artikel 4, twaalfde lid, en artikel 5, zevende lid, van de verordening wordt bovendien expliciet benoemd dat wanneer een gebruiker die niet de betrokkene is van wie persoonsgegevens

worden gedeeld, de gegevens alleen beschikbaar kunnen worden gesteld als hier een geldige verwerkingsgrond conform de AVG voor is. Hierdoor moet in bepaalde gevallen bij handhaving van de verordening worden beoordeeld of het beschikbaar stellen van gegevens door een gegevenshouder voldoet aan de AVG.

Uit een arrest van het Hof van Justitie van de Europese Unie¹⁶ volgt dat gelet op de verplichting van loyale samenwerking de ACM in bepaalde situaties bij het onderzoeken van een mogelijke overtreding van de verordening advies moet vragen aan de AP of er sprake is van strijd met de AVG. Het gaat onder meer om de situatie dat de ACM twijfels heeft of daarvan sprake is en de situatie dat de AP tegelijkertijd dezelfde overtreding onderzoekt. In dat geval moet de ACM de AP raadplegen. Indien de AP niet binnen een redelijke termijn bezwaar maakt of antwoordt, kan de ACM haar eigen onderzoek voortzetten.

De Uitvoeringswet geeft de ACM de bevoegdheid, indien zij dit noodzakelijk acht, advies te vragen aan de AP. Indien blijkt dat het voor de effectieve handhaving van de verordening noodzakelijk is een termijn te stellen waarbinnen de AP het advies moet geven, kan dit per ministeriële regeling worden vastgesteld.

Voor deze samenwerking is gegevensuitwisseling tussen ACM en AP noodzakelijk. Ook zal de ACM incidenteel gegevens moeten kunnen uitwisselen met andere toezichthouders, waaronder de RDI en sectorale toezichthouders. Toezichthouders hebben uit hoofde van de Awb (artikel 5:16) reeds de bevoegdheid om in incidentele gevallen informatie uit te wisselen met andere toezichthouders. ACM en AP onderling zullen gezien hun samenwerking als bevoegde autoriteiten en datacoördinator en de adviesrol van AP over toepassing van de AVG meer structureel gegevens moeten uitwisselen. Zo zal de ACM wanneer zij advies vraagt aan de AP over toepassing van de AVG mogelijk informatie over een casus met de AP moeten delen. Om die gegevensuitwisseling te faciliteren creëert de Uitvoeringswet een grondslag voor de bevoegde autoriteiten om de informatie uit te wisselen die relevant is voor het toezicht op de verordening.

4.3 Aanwijzen datacoördinator

De ACM wordt aangewezen als datacoördinator. De ACM heeft in het kader van de Wet handhaving consumentenbescherming al de nodige ervaring met de uitvoering van een coördinerende rol in het kader van toezicht en handhaving en zal worden aangewezen als datacoördinator. Als beoogde digitaledienstencoördinator zal de ACM hier bovendien verdere ervaring mee opdoen. Om deze redenen acht het kabinet de ACM het meest geschikt om de rol van datacoördinator uit te voeren onder de verordening.

De taken en bevoegdheden van de datacoördinator volgen rechtstreeks uit artikelen 37, vijfde lid, laatste alinea, en zesde lid, en 38, eerste lid, van de verordening en zijn in paragraaf 3.8 beschreven..

4.4 Certificering geschillenbeslechtsorgaan

Gebruikers, gegevenshouders en gegevensontvangers hebben toegang tot een gecertificeerd geschillenbeslechtsorgaan om geschillen uit hoofdstukken II, III en IV van de verordening te beslechten (zie paragraaf 3.2 van het algemeen deel van de toelichting). Lidstaten zijn niet verplicht een geschillenbeslechtsorgaan op te richten.

De lidstaat waar het geschillenbeslechtsorgaan is gevestigd, certificeert dat orgaan op diens verzoek, indien het heeft aangetoond dat het aan de voorwaarden uit artikel 10, vijfde lid, van de verordening voldoet. In Nederland certificeert de ACM de geschillenbeslechtsorganen (zie artikel 2 van de Uitvoeringswet). De ACM heeft ervaring met het certificeren van geschillenbeslechtsorganen vanuit zijn taken op grond van de Uitvoeringswet Digitaledienstenverordening. Bovendien is de ACM de bevoegde autoriteit voor de onderdelen van de Dataverordening waar de geschillenbeslechtsorganen over zullen oordelen en kan het de expertise van geschillenbeslechtsorganen op deze terreinen beoordelen. Het staat de lidstaten vrij om specifieke regels voor de certificeringsprocedure, waaronder voor het verstrijken of intrekken van certificering, vast te stellen. In Nederland wordt hier vooralsnog geen gebruik van gemaakt.

¹⁶ Hof van Justitie EU van 4 juni 2023, *Meta Platforms Inc., anciennement Facebook Inc. e.a. tegen Bundeskartellamt* (C-251/21), met name overwegingen 62-63.

5. Verhouding tot ander recht

De verordening bevat algemene regels en bepaalt expliciet dat de verordening geen afbreuk doet aan, of een aanvulling betreft op, andere specifieke regelgeving (artikel 1, vijfde tot en met tiende lid, van de verordening). In deze paragraaf van de memorie van toelichting wordt hier nader op ingegaan.

De verordening voorziet in horizontale regels. Deze verordening doet geen afbreuk aan het Unierecht, waarin, gebaseerd op specifieke behoeften van een sector, verdere vereisten worden vastgesteld, zoals in de beoogde verordening betreffende de Europese ruimte voor gezondheidsgegevens (EHDS).¹⁷ Specifieke sectorale vereisten betreffen bijvoorbeeld specifieke technische eisen voor de toegang tot gegevens, of beperkingen dan wel uitbreidingen van het recht op toegang of gebruik van bepaalde gegevens.

Er bestaat reeds diverse sectorale regelgeving over de uitwisseling van (niet persoonsgebonden) gegevens die binnen de scope van de verordening vallen.¹⁸ Hier kan worden gedacht aan betaalgegevens in de PSD2-richtlijn¹⁹, gegevens over motoren in de Motor verordening²⁰ en elektriciteitsverbruik in de Elektriciteitsrichtlijn²¹.

Aangezien de verordening een geharmoniseerd kader betreft mogen lidstaten geen aanvullende nationale voorschriften vaststellen of handhaven over aangelegenheden die binnen het toepassingsgebied van de verordening vallen, tenzij dat uitdrukkelijk is bepaald.

5.1 Algemene verordening gegevensbescherming

Deze verordening doet geen afbreuk aan Unierecht en het nationale recht inzake de bescherming van persoonsgegevens, de persoonlijke levenssfeer en de vertrouwelijkheid van communicatie en de integriteit van eindapparatuur, die van toepassing zijn op persoonsgegevens die worden verwerkt in verband met de hierin vastgelegde rechten en verplichtingen met inbegrip van de bevoegdheden van toezichthoudende autoriteiten en de rechten van datasubjecten. De verordening doet in het bijzonder geen afbreuk aan de Algemene Verordening Gegevensverwerking (AVG). Bij verwerking van persoonsgegevens is de regelgeving met betrekking tot persoonsgegevens altijd van toepassing en bij tegenstrijdigheid met de verordening prevaleert de regelgeving met betrekking tot persoonsgegevens. Dit geldt ook voor de situatie waarin persoonsgegevens en andere gegevens in een gegevensverzameling onlosmakelijk met elkaar verbonden zijn. De Autoriteit Persoonsgegevens (AP) is de toezichthouder met betrekking tot persoonsgegevens op basis van de AVG, en blijft dat. Wanneer bijvoorbeeld is beoordeeld dat het delen van gegevens conform hoofdstuk II van de verordening heeft plaatsgevonden, verhindert dat geenszins de AP om de rechtmatigheid van deze dataverwerking conform de AVG te beoordelen.

Beginselen rechtmatige gegevensverwerking

De verordening regelt dat een aantal beginselen voor rechtmatige gegevensverwerking uit artikel 5 van de AVG ook (deels) van toepassing worden op niet-persoonsgebonden gegevens die zijn

¹⁷ Voorstel voor een verordening betreffende de Europese ruimte voor gezondheidsgegevens, zie: eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:52022PC0197.

¹⁸ Voor meer informatie zie de Studie op verzoek van de EC over 'The emergence of non-personal data markets' (oktober 2023) [https://www.europarl.europa.eu/RegData/etudes/STUD/2023/740098/IPOL_STU\(2023\)740098_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2023/740098/IPOL_STU(2023)740098_EN.pdf), p. 18.

¹⁹ Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad van 25 november 2015 betreffende betalingsdiensten in de interne markt, houdende wijziging van de Richtlijnen 2002/65/EG, 2009/110/EG en 2013/36/EU en Verordening (EU) nr. 1093/2010 en houdende intrekking van Richtlijn 2007/64/EG (PbEU 2015, L 337).

²⁰ Verordening (EU) 2018/858 van het Europees Parlement en de Raad van 30 mei 2018 betreffende de goedkeuring van en het markttoezicht op motorvoertuigen en aanhangwagens daarvan en systemen, onderdelen en technische eenheden die voor dergelijke voertuigen zijn bestemd, tot wijziging van Verordeningen (EG) nr. 715/2007 en (EG) nr. 595/2009 en tot intrekking van Richtlijn 2007/46/EG (PbEU 2018, L 151).

²¹ Richtlijn (EU) 2019/944 van het Europees Parlement en de Raad van 5 juni 2019 betreffende gemeenschappelijke regels voor de interne markt voor elektriciteit en tot wijziging van Richtlijn 2012/27/EU (herschikking) (PbEU 2019, L 158).

gegenereerd met een verbonden product of gerelateerde dienst en op verzoek van de gebruikers worden gedeeld met een derde partij (artikel 6 van de verordening).

Rechtmatig: de derde mag die gegevens alleen met een andere derde delen indien de gebruiker daar toestemming voor heeft gegeven. Bovendien moet het voor de gebruiker even gemakkelijk zijn om toegang van de derde tot de gegevens te weigeren of stop te zetten als het voor de gebruiker is om toegang te verlenen.

Doelbinding: de derde mag die gegevens alleen verwerken voor de met de gebruiker overeengekomen doeleinden (artikel 6, eerste lid, van de verordening).

Beginsel van minimale gegevensverwerking: de derde mag alleen toegang hebben tot de informatie die nodig is voor de levering van de aan de gebruiker gevraagde dienst.

Opslagbeperking: de derde moet de gegevens verwijderen indien ze niet langer nodig zijn voor het overeengekomen doel, tenzij anders is overeengekomen met de gebruiker.

Ook gaat (artikel 6, tweede lid, onderdeel b, van de verordening) in op profilering. De derde mag de gegevens niet gebruiken voor de profilering van natuurlijke personen, tenzij het nodig is voor de door de gebruiker aangevraagde dienst, onder meer in de context van geautomatiseerde besluitvorming. De regels uit artikel 22, tweede lid, onderdelen a en c, AVG zijn onverminderd van kracht. Dat betekent dat een betrokkene zich niet kan beroepen op het recht om niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verboden of dat hem in aanmerkelijke mate treft indien a) het besluit noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke of c) berust op de uitdrukkelijke toestemming van de betrokkene.

Deze beginselen voor rechtmatige gegevensverwerking uit artikel 5 AVG zijn ook (deels) van toepassing op niet-persoonsgebonden gegevens die aan overheden beschikbaar worden gesteld op grond van uitzonderlijke noodzaak. Het gaat onder meer om het hebben van een taak van algemeen belang als grondslag (artikel 15 van de verordening), doelbinding, beveiliging van gegevens en opslagbeperking (artikel 19 van de verordening).

Recht op inzage en dataportabiliteit

Hoofdstuk III van de verordening betreft een aanvulling op het recht op inzage en het recht op dataportabiliteit uit artikelen 15 en 20 van de AVG voor wat betreft productgegevens of gegevens van een gerelateerde dienst (artikel 1, vijfde lid, van de verordening). De verordening geeft gegevenshouders de verplichting om gegevens beschikbaar te stellen aan gebruikers (artikel 4 van de verordening) en de gegevens op verzoek van de gebruikers te delen met derden (artikel 5 van de verordening). De rechten uit hoofde van deze verordening vormen op verschillende manieren een aanvulling op het recht om persoonsgegevens te ontvangen en over te dragen uit hoofde van artikel 20 van de AVG (overweging 35 van de verordening). De verordening verleent gebruikers het recht op toegang tot en beschikbaarstelling aan derden van productgegevens of gegevens van een gerelateerde dienst, ongeacht of het persoonsgegevens betreft en of het actief verstrekte of passief waargenomen gegevens betreft en ongeacht de rechtsgrond van de verwerking. Het biedt gegevenshouders ook de mogelijkheid een redelijke vergoeding vast te stellen die door derden moet worden betaald voor kosten die voortvloeien uit het verlenen van rechtstreekse toegang tot de door het verbonden product van de gebruiker gegenereerde gegevens. Indien een gegevenshouder en een derde niet in staat zijn overeenstemming te bereiken over de voorwaarden voor een dergelijke rechtstreekse toegang, mag het datasubject op geen enkele wijze worden belet de in de AVG vastgestelde rechten, waaronder het recht op overdraagbaarheid van gegevens, uit te oefenen door overeenkomstig die verordening remedies in te stellen. In deze context moet worden begrepen dat, overeenkomstig de AVG, verwerking van bijzondere categorieën persoonsgegevens door de gegevenshouder of de derde op grond van een overeenkomst niet is toegestaan.

Hoofdstuk VI van de verordening draagt eraan bij dat gebruikers van dataverwerkingsdiensten hun gegevens makkelijker kunnen overdragen tussen verschillende diensten. Wanneer deze gegevens persoonsgegevens van de gebruikers omvatten is hier overlap met het recht op dataportabiliteit uit

artikel 20 van de AVG. Indien de betrokken dataverwerkingsdiensten niet in staat zijn de tijdige overdracht van gegevens conform de verordening mogelijk te maken, mag dit de betrokkene op geen enkele wijze beletten de in de AVG vastgestelde rechten, waaronder het recht op overdraagbaarheid van gegevens, uit te oefenen door overeenkomstig die verordening remedies in te stellen.

5.2 Datagovernanceverordening (DGA), Digitaalemarktenverordening (DMA), Digitaalendienstenverordening (DSA), Artificiële intelligentie verordening (AI Act) en 'Platform-to-Business' verordening (P2B)

Datagovernanceverordening

De Datagovernanceverordening²² (hierna: DGA) is samen met de Dataverordening onderdeel van de Europese datastrategie. De verordeningen hebben vier belangrijke raakvlakken. De DGA heeft als inzet om de beschikbaarheid van data te vergroten door het vertrouwen in neutrale databemiddelingsdiensten en erkende data-altruïstische organisaties te versterken.

Het recht op gegevensdeling uit de verordening (Hoofdstuk II) kan rechtstreeks door de gebruiker of, op diens verzoek, via databemiddelingsdiensten en data-altruïstische organisaties (artikel 2, elfde onderdeel, DGA) plaatsvinden. Ook derde partijen onder de verordening kunnen in gegevensdeling door databemiddelingsdiensten worden ondersteund. Databemiddelingsdiensten kunnen ondersteunen bij het aangaan van commerciële relaties. Daarnaast kunnen databemiddelingsdiensten een belangrijke rol spelen bij de toegang tot gegevens, zowel technisch als bij het waarborgen van de gebruikerscontrole over het aanbieden van gegevens en de voorwaarden waaronder gegevens mogen worden gebruikt. Ook wanneer een derde zelf een aanbieder van een databemiddelingsdienst is, zijn de waarborgen met betrekking tot deze diensten uit de DGA van toepassing (artikel 12, DGA).

Ten tweede beoogt de DGA het hergebruik van beschermde gegevens in het bezit van overheidsinstanties die niet binnen de reikwijdte van de open datarichtlijn vallen te faciliteren. Gezien het uitzonderlijke karakter van het opvragen van gegevens door overheden in hoofdstuk V van de verordening zijn op grond van dit hoofdstuk verkregen gegevens niet beschikbaar voor hergebruik onder artikel 2, tweede onderdeel, van de DGA. Zie verder paragraaf 5.8 van het algemeen deel van de toelichting.

Daarnaast worden de taken van het in de DGA opgerichte Europees Comité voor gegevensinnovatie (hoofdstuk VI, DGA) in de verordening uitgebreid. Het Europees Comité voor gegevensinnovatie krijgt een adviesrol in de ontwikkeling van geharmoniseerde normen en de ontwikkeling van gemeenschappelijke Europese dataruimtes (artikelen 42 en 46, Dataverordening).

In de DGA worden ook eisen gesteld aan de internationale doorgifte van gegevens door databemiddelingsdiensten en data-altruïstische organisaties (artikel 27, DGA). Deze bepalingen zijn in doelstelling en uitwerking vergelijkbaar met de bepalingen uit Hoofdstuk VII van de verordening. Ook in het kader van de DGA is de ACM hierop de bevoegde autoriteit.

Digitaalemarktenverordening

De digitaalemarktenverordening²³ (hierna: DMA) bevat regelgeving om een eerlijker speelveld in de digitale economie te creëren door de machtspositie van 'poortwachterplatforms' te verminderen. De DMA staat de Commissie toe een onderneming als poortwachter aan te wijzen. Poortwachters zijn grote platforms met een aanzienlijke marktpositie waar gebruikers (consumenten en bedrijven) niet omheen kunnen en die door hun macht de toegang tot markten kunnen controleren. Deze machtspositie is vaak voor een deel gebaseerd op de ongeëvenaarde hoeveelheid gegevens die platforms tot hun beschikking hebben en kunnen verkrijgen. Als poortwachters via de verordening in staat worden gesteld nog meer gegevens te verzamelen zou dit strijdig zijn met het doel van de DMA om de machtspositie van poortwachterplatforms te adresseren en het doel van de verordening,

²² 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) (PbEU 2022, L 152).

²³ Verordening (EU) 2022/1925 over betwistbare en eerlijke markten in de digitale sector (de digitaalemarktenverordening) (PbEU 2022, L 265).

die een eerlijke verdeling van de waarde uit gegevens beoogt. Een onderneming die onder de DMA is aangewezen als poortwachter krijgt daarom via de verordening geen toegang tot gegevens van gebruikers die zijn gegenereerd door verbonden producten of diensten. Poortwachters komen niet in aanmerking om gegevens te ontvangen als derde partij (artikel 5, derde lid, Dataverordening), en derden mogen geen gegevens beschikbaar stellen aan poortwachters (artikel 6, tweede lid, onderdeel d, Dataverordening). De mogelijkheid tot het sluiten van vrijwillige overeenkomsten tussen poortwachters en gegevenshouders wordt niet door de verordening ingeperkt.

Digitaledienstenverordening

De Digitaledienstenverordening²⁴ (hierna: DSA) bevat regels over de aansprakelijkheid en verantwoordelijkheid van online tussenhandeldiensten. Dit zijn online diensten waarbij het doorgeven en/of opslaan van informatie van gebruikers centraal staat. De DSA onderscheidt respectievelijk mere conduitdiensten, cachingdiensten en hostingdiensten.

Dataverwerkingsdiensten kunnen kwalificeren als een tussenhandeldienst onder de DSA, in welk geval zij onder het bestek van deze horizontale verordening vallen. Dit betekent dat zij, onder voorwaarden, in aanmerking kunnen komen voor de aansprakelijkheidsvrijstellingen neergelegd in de DSA en dat zij aan de zorgvuldigheidsverplichtingen uit de DSA moeten voldoen. De zorgvuldigheidsverplichtingen zijn in de DSA geordend naar categorie tussenhandeldienst en vormen een gelaagde structuur. Zo bevat de DSA een aantal verplichtingen die van toepassing zijn op alle tussenhandeldiensten. Daarbovenop bevat de DSA aanvullende verplichtingen die enkel gelden voor respectievelijk hostingdiensten, online platforms, online marktplaatsen en zogenaamde zeer grote online platforms en zeer grote online zoekmachines. Of een specifieke dataverwerkingsdienst kwalificeert als tussenhandeldienst – en, zo ja, welk type – hangt af van diens technische functies en moet geval per geval worden beoordeeld. Aangezien de DSA en de verordening zeer verschillende onderwerpen op digitaal terrein reguleren zijn de raakvlakken tussen beide verordeningen beperkt.

Artificiële intelligentieverordening

De beoogde AI-verordening²⁵ bevat regels voor de ontwikkeling en het gebruik van artificiële intelligentie. De AI-verordening legt verplichtingen op aan aanbieders en gebruikers van AI-systemen. Welke dat zijn, is vooral afhankelijk van het risico van de AI-toepassing. De verordening en de AI-verordening hebben verschillende doelen die elkaar aanvullen. De AI-verordening heeft als doel ervoor te zorgen dat AI-systemen die op de EU-markt worden gebruikt, veilig zijn en de fundamentele rechten en waarden van de EU respecteren. De verordening reguleert met name welke gegevens voor wie toegankelijk zijn en onder welke voorwaarden. Voor het ontwikkelen en trainen van AI-systemen, zijn gegevens nodig. Gegevens die ondernemingen, bijvoorbeeld als derden onder hoofdstuk II, via de verordening verkrijgen kunnen zij gebruiken voor de ontwikkeling of het gebruik van AI-systemen. De verordening legt in zulke gevallen vast onder welke voorwaarden een onderneming toegang tot gegevens kan krijgen. De AI-verordening stelt eisen aan de ontwikkeling en het gebruik van een AI-systeem, bijvoorbeeld dat er niet wordt gediscrimineerd. Dit betekent dat de opzet van het systeem, de manier van trainen en de gegevens waarmee een systeem getraind wordt, evenwichtig moeten zijn en bepaalde groepen niet mogen bevoordelen of benadelen. AI-systemen die onderdeel zijn van een verbonden product, gerelateerde dienst of dataverwerkingsdienst, kunnen ook gegevens genereren. In zulke gevallen legt de verordening vast welke partijen toegang tot deze gegevens kunnen krijgen en onder welke voorwaarden. De AI-verordening is ook dan van toepassing op de ontwikkeling en het gebruik van AI-systemen.

Platform-to-business verordening

²⁴ Verordening 2022/2065 van het Europees Parlement en de Raad van 19 oktober 2022 betreffende een eengemaakte markt voor digitale diensten en tot wijziging van Richtlijn 2000/31/EG (digitaledienstenverordening) (PbEU 2022, L 277).

²⁵ Voorstel van 21 april 2021 voor een verordening van het Europees Parlement en de Raad tot vaststelling van geharmoniseerde regels betreffende Artificiële Intelligentie (wet op de Artificiële Intelligentie) en tot wijziging van bepaalde wetgevingshandelingen van de Unie (COM(2021) 206 final).

De Verordening Platform-to-Business²⁶ (hierna: P2B) legt onder andere regels vast over geschilbeslechting, transparantie met betrekking tot algemene voorwaarden en de volgorde van zoekresultaten. Met deze regels is de kleinere ondernemer beter beschermd en kan deze met vertrouwen online zaken doen. De doelstellingen raken aan die van regelgeving zoals de DMA en de verordening. De juridische raakvlakken met de verordening zijn beperkt.

5.3 Richtlijn bedrijfsgeheimen

De Richtlijn bedrijfsgeheimen²⁷ beoogt de harmonisatie van de regels inzake bescherming van niet-openbaar gemaakte knowhow en bedrijfsinformatie (bedrijfsgeheimen). De Richtlijn geeft aan wat onder een bedrijfsgeheim wordt verstaan, tegen welke vormen van inbreuk daarop (onrechtmatig verkrijgen, gebruiken of openbaar maken) kan worden opgetreden en welke maatregelen, procedures en rechtsmiddelen daarvoor kunnen worden ingezet. In Nederland is de richtlijn geïmplementeerd in de Wet bescherming bedrijfsgeheimen.

Hoewel de verordening gegevenshouders verplicht tot openbaarmaking van gegevens, waaronder gegevens die in aanmerking komen voor bescherming als bedrijfsgeheimen, aan gebruikers of derden op verzoek van gebruikers, blijft de bescherming van bedrijfsgeheimen onder de Richtlijn bedrijfsgeheimen gewaarborgd. Artikel 4, zesde lid, van de verordening bepaalt dat gegevens die bedrijfsgeheimen bevatten, alleen openbaar gemaakt mogen worden als de gegevenshouder en de gebruiker of derde vóór de openbaarmaking alle noodzakelijke maatregelen nemen om de vertrouwelijkheid ervan te waarborgen, met name ten aanzien van derden. De gegevenshouder of de houder van het bedrijfsgeheim identificeert de gegevens die als bedrijfsgeheimen worden beschermd, inclusief de relevante metadata. Zij komen met de gebruiker proportionele technische en organisatorische maatregelen overeen die nodig zijn om de vertrouwelijkheid van de gedeelde gegevens te bewaren. Wanneer hierover geen overeenstemming bestaat dan kan een gegevenshouder de toegang tot de betreffende gegevens weigeren of opschorten, zo bepaalt artikel 4, zevende lid, van de verordening. Daarnaast bepaalt artikel 4, achtste lid, van de verordening, dat in uitzonderlijke omstandigheden de gegevenshouder van geval tot geval een verzoek om toegang tot de specifieke gegevens in kwestie kan weigeren. De gegevenshouder moet daarvoor kunnen aantonen dat het zeer waarschijnlijk is dat hij/zij ondanks technische en organisatorische maatregelen ernstige economische schade zal lijden door de openbaarmaking van bedrijfsgeheimen. Artikel 4, negende lid, van de verordening bepaalt ten slotte dat de gebruiker hiertegen verhaal kan halen bij een rechterlijke instantie, een klacht kan indienen bij een bevoegde autoriteit of (met de gegevenshouder) overeen kan komen de zaak voor te leggen aan een geschillenbeslechtingscommissie. Artikel 5, negende, tiende en elfde lid, van de verordening bevat gelijke bepalingen ten opzichte van een derde, maar alleen in het geval de gebruiker het recht heeft bedrijfsgeheimen bekend te maken aan derden.

5.4 Intellectuele eigendomsrechten, waaronder de Databankrichtlijn

Voor wat betreft de intellectuele eigendomsrechten laat de verordening EU en nationale regelgeving ten aanzien van de bescherming hiervan, inclusief richtlijnen op het terrein van het auteursrecht- en naburige rechten en de handhaving van intellectuele eigendomsrechten, onverlet.

De verordening regelt specifiek de verhouding tot artikel 7 van de de Databankrichtlijn²⁸, dat betreft een zogenaamde 'recht *sui generis*'. Het betreft een recht voor de producent van een databank, waarvan het verkrijgen, de controle of de presentatie van de inhoud in kwalitatief of kwantitatief opzicht getuigt van een substantiële investering, om de opvraging of het hergebruik van het geheel of een in kwalitatief of kwantitatief opzicht substantieel deel van die inhoud te verbieden. Artikel 43 van de verordening bepaalt dat het *sui generis* recht uit artikel 7 van de Databankrichtlijn niet van toepassing is op gegevens uit een product of gerelateerde dienst. Hiermee wordt voorkomen

²⁶ Verordening (EU) 2019/1150 van het Europees Parlement en de Raad van 20 juni 2019 ter bevordering van billijkheid en transparantie voor zakelijke gebruikers van onlinetussenhandeldiensten (PbEU 2019, L 186).

²⁷ Richtlijn (EU) 2016/943 van het Europees Parlement en de Raad van 8 juni 2016 betreffende de bescherming van niet-openbaar gemaakte knowhow en bedrijfsinformatie (bedrijfsgeheimen) tegen het onrechtmatig verkrijgen, gebruiken en openbaar maken daarvan (PbEU 2016, L 157).

²⁸ Richtlijn 96/9/EG van het Europees Parlement en de Raad van 11 maart 1996 betreffende de rechtsbescherming van databanken (PbEG 1996, L 77).

dat de producent van een databank met gegevens die zijn verkregen of gegenereerd door een product of gerelateerde dienst of andere door een machine gegenereerde gegevens, aanspraak kan maken op het *sui generis* recht op grond van artikel 7 van de Databankrichtlijn, en zo met name het recht van gebruikers op toegang en dataportabiliteit op grond van deze verordening kan belemmeren. Deze uitzondering heeft geen effect op databanken met gegevens die buiten het toepassingsgebied van deze verordening vallen.

5.5 Contractenrecht en consumentenrecht

Privaatrechtelijke regels zijn van cruciaal belang in het algemene kader voor gegevensdeling. Daarom worden met deze verordening de regels van het overeenkomstenrecht op punten aangepast, ter voorkoming van misbruik van contractuele onevenwichtigheden die een eerlijke toegang tot en een eerlijk gebruik van gegevens belemmeren. Tenzij deze verordening anders bepaalt, doet zij geen afbreuk aan het nationale overeenkomstenrecht, waaronder de regels betreffende de totstandkoming, de geldigheid of de gevolgen van overeenkomsten, of de gevolgen van de beëindiging van een overeenkomst. De verordening vormt een aanvulling op, en doet geen afbreuk aan, EU- en nationaal recht gericht op consumentenbescherming.

Op basis van het beginsel van contractvrijheid blijft het partijen vrijstaan om te onderhandelen over de precieze voorwaarden voor het beschikbaar stellen van gegevens in hun overeenkomsten, binnen het kader van algemene regels voor het beschikbaar stellen van gegevens. Ongeacht of een gegevenshouder en een derde een overeenkomst sluiten over gegevensdeling, is het recht van gebruikers om gegevens te delen met derden afdwingbaar voor de nationale rechterlijke instanties. De verordening stelt onder meer regels over informatie die voor het sluiten van de overeenkomst moet worden verstrekt en andere rechten en plichten met betrekking tot het beschikbaar stellen van gegevens. De overeenkomst voor de aankoop, huur of leasing van een verbonden product of gerelateerde dienst vormt de basis voor het gebruik van niet-persoonsgebonden gegevens. Elke contractvoorwaarde die bepaalt dat de gegevenshouder de productgegevens of de gegevens van een gerelateerde dienst mag gebruiken, moet transparant zijn voor de gebruiker, ook over de doeleinden waarvoor de gegevenshouder de gegevens zal gebruiken. Elke wijziging van de overeenkomst vereist de geïnformeerde toestemming van de gebruiker.

De verordening belemmert gebruikers die bedrijven zijn niet om met derden voorwaarden overeen te komen over het beschikbaar stellen van gegevens. Het kan bijvoorbeeld gaan om voorwaarden die het verdere delen van gegevens beperken of begrenzen of die gaan over een vergoeding voor het beschikbaar stellen van gegevens, bijvoorbeeld in ruil voor het opgeven van hun recht om deze gegevens te gebruiken of te delen. Ongeacht of een gegevenshouder en een derde een overeenkomst sluiten over gegevensdeling, is het recht van gebruikers om gegevens te delen met derden afdwingbaar voor de nationale rechterlijke instanties.

Niet bindende bepalingen

De verordening bepaalt wanneer contractvoorwaarden niet bindend zijn. Ten eerste: een contractvoorwaarde die de gebruiker benadeelt omdat die de toepassing van zijn rechten uitsluit, daarvan afwijkt of zijn rechten uit hoofdstuk II van de verordening aantast, is niet bindend voor de gebruiker. Ten tweede: een contractvoorwaarde in een gegevensdelingsovereenkomst die, ten nadele van een partij (waaronder de gebruiker), de toepassing van hoofdstuk III van de verordening uitsluit, daarvan afwijkt of de gevolgen ervan wijzigt, is niet bindend voor die partij.

Ten slotte staat in hoofdstuk IV van de verordening dat een contractuele voorwaarde die verband houdt met het beschikbaar stellen van gegevens en eenzijdig door een onderneming is opgelegd aan een andere onderneming, niet bindend is voor laatstgenoemde onderneming indien dit oneerlijk is. Het gaat om contractvoorwaarden betreffende de toegang tot en het gebruik van gegevens of aansprakelijkheid en remedies in geval van schending of beëindiging van gegevensgerelateerde verplichtingen. Gelet op het principe van contractsvrijheid van bedrijven gaat het alleen om oneerlijke contractvoorwaarden die eenzijdig zijn opgelegd. Dat zijn contractvoorwaarden waarbij de andere partij niet in staat is geweest om de inhoud ervan te beïnvloeden, ondanks een poging om erover te onderhandelen. Het moet gaan om buitensporige contractvoorwaarden waarbij misbruik is gemaakt van een sterkere onderhandelingspositie.

De verordening bevat een lijst met bedingen die altijd oneerlijk worden geacht en een lijst met bedingen die als oneerlijk worden verondersteld. De bepalingen sluiten aan op de onredelijk bezwarende voorwaarden zoals bepaald in artikelen 6:236 en 6:237 van het Burgerlijk Wetboek (hierna: BW), ook wel de grijze en zwarte lijst genoemd.

Bescherming tegen niet bindende bepalingen

In overweging 28 van de verordening staat dat in overeenkomsten tussen een gegevenshouder en een consument als gebruiker, het Europese consumentenrecht van toepassing is om ervoor te zorgen dat een consument niet onderworpen is aan oneerlijke contractvoorwaarden. Uit de Richtlijn oneerlijke bedingen in consumentenovereenkomsten²⁹ jo. artikel 6.233 BW volgt het volgende: Consumenten worden beschermd tegen oneerlijke bedingen doordat de rechter ambtshalve op de vernietigbaarheid van oneerlijke bedingen toetst. Daarnaast kan de ACM gelet op de Wet handhaving consumentenrechten ook handhaven. Mkb'ers moeten zelf een beroep doen op de oneerlijkheid van een beding. Indien de rechter oordeelt dat het een oneerlijke beding betreft zal de rechter het beding vernietigen. Indien een contractueel beding oneerlijk wordt verklaard, blijft de betrokken overeenkomst zonder dat beding van toepassing, tenzij het oneerlijke contractuele beding niet kan worden gescheiden van de andere voorwaarden van de overeenkomst.

Contractvoorwaarden betreffende overstappen en interoperabiliteit

Ook in hoofdstuk VI van de verordening worden eisen gesteld aan contractvoorwaarden (artikel 25) en informatieverplichtingen (artikel 26 en 28) en wordt verplicht om onder meer contractuele belemmeringen weg te halen (artikel 23) om een klant van een dataverwerkingsdienst te beschermen. Dergelijke bescherming wordt ook geboden bij interoperabiliteit (artikel 34). Het gaat om specifieke bepalingen die rechtstreeks werken en in lijn zijn met Nederlands recht.

Modelcontractvoorwaarden en standaardcontractbepalingen

Om ondernemingen te helpen bij het opstellen van overeenkomsten en daarover te onderhandelen, moet de Commissie vóór 12 september 2025 niet-bindende modelcontractvoorwaarden voor gegevensdelingsovereenkomsten tussen ondernemingen, waaronder voorwaarden over redelijke vergoeding en de bescherming van bedrijfsgeheimen, ontwikkelen en aanbevelen, alsook niet-bindende standaardcontractbepalingen voor cloudovereenkomsten. Dit moet een evenwichtiger relatie tussen de contractspartijen tot stand brengen en de rechtszekerheid van de voorwaarden verbeteren en leiden tot meer eerlijke, redelijke en niet-discriminerende contractuele rechten en verplichtingen.

5.6 Strafrecht, witwassen en terrorismefinanciering, nationale veiligheid, defensie, openbare orde, douane, belasting

Artikelen 1, zesde lid, en 16, tweede lid, van de verordening kaderen de reikwijdte van de verordening verder in. Deze verordening heeft geen effect op EU of nationale regelgeving die voorzien in het delen van, de toegang tot en het gebruik van gegevens voor het doel van het voorkomen, onderzoeken, opsporen of vervolgen van strafbare feiten of de tenuitvoerlegging van strafrechtelijke sancties en internationale samenwerking op dat gebied. Ook heeft het geen effect op het verzamelen, delen, de toegang en het gebruik van gegevens op grond van Richtlijn (EU) 2015/849 van het Europees Parlement en de Raad over het voorkomen van het gebruik van het financiële stelsel voor het witwassen van geld en terrorismefinanciering en Verordening (EU) 2015/847 van het Europees Parlement en de Raad betreffende informatie bij de overdracht van middelen. Deze verordening doet geen afbreuk aan de bevoegdheden van de lidstaten betreffende openbare veiligheid, defensie of nationale veiligheid en handhaving van de openbare orde. Deze verordening laat de bevoegdheden van de lidstaten onverlet op het gebied van douane en belastingadministratie en de gezondheid en veiligheid van burgers.

5.7 Staatsnoodrecht

Hoofdstuk V geeft aan (nationale- of EU-)overheidsinstanties het recht om in het geval van een uitzonderlijke noodzaak bepaalde gegevens op te vragen bij gegevenshouders. Er is volgens artikel

²⁹ Richtlijn 93/13/EEG van de Raad van 5 april 1993 betreffende oneerlijke bedingen in consumentenovereenkomsten (PbEG 1993, L 95).

15, eerste lid, onderdeel a, van de Dataverordening onder andere sprake van een 'uitzonderlijke noodzaak' wanneer de gegevens noodzakelijk zijn om te reageren op een algemene noodsituatie en de overheidsinstantie niet in staat is dergelijke gegevens tijdig en doeltreffend op een andere manier en in gelijkwaardige omstandigheden te verkrijgen. Een 'algemene noodsituatie' wordt in de verordening gedefinieerd als: *een in de tijd beperkte uitzonderlijke situatie, zoals een noodsituatie op het gebied van de volksgezondheid, een noodsituatie die voortvloeit uit natuurrampen, of een door de mens veroorzaakte grote ramp, met inbegrip van een groot cyberveiligheidsincident, dat negatieve gevolgen heeft voor de bevolking van de Unie, van een lidstaat of van een deel daarvan, met een risico op ernstige en blijvende gevolgen voor de levensomstandigheden of de economische stabiliteit, de financiële stabiliteit of een aanzienlijke en onmiddellijke verslechtering van de economische activa in de Unie of in de betrokken lidstaat, en die wordt vastgesteld of officieel wordt afgekondigd overeenkomstig de relevante Unie- of nationaalrechtelijke procedures.* Van een noodtoestand waarop artikel 15, eerste lid, onderdeel a, van de Dataverordening van toepassing kan zijn, is dus alleen sprake als wordt vastgesteld of afgekondigd overeenkomstig de relevante Unie- of nationaalrechtelijke procedures. Voor de situatie binnen Nederland, is daarom de verhouding met het Nederlandse (staats)nood- en crisisrecht van belang.

Het klassieke Nederlandse staatsnoodrecht heeft een grondwettelijke basis in artikel 103 van de Grondwet en is uitgewerkt in de Coördinatiewet uitzonderingstoestanden. Naast het wettelijke stelsel inzake het klassieke staatsnoodrecht, bestaat er ook ander wettelijk kader om rampen en crises mee te bestrijden. [PM De verhouding tussen de Nederlandse regelgeving en de bepaling van artikel 15, eerste lid, onderdeel a, van de verordening wordt op dit moment onderzocht.]

5.8 Hergebruik overheidsinformatie

Het Unierecht kent op het moment van schrijven twee stukken regelgeving die zien op het hergebruik van overheidsinformatie door derden. Dit zijn de Open data richtlijn³⁰ en hoofdstuk II van de Datagovernanceverordening (DGA). Beide regelingen gaan ervan uit dat overheidsgegevens veel meerwaarde kunnen hebben voor de economie en voor technologische vooruitgang, maar dat die beschikbaarstelling zonder regelgeving onvoldoende op gang komt. De regelingen voorzien daarom in rechten voor derden om (onder omstandigheden) die gegevens te hergebruiken voor andere doeleinden en voor corresponderende verplichtingen voor overheden om die gegevens beschikbaar te stellen. In de context van hoofdstuk V van de verordening zou daarmee echter het risico ontstaan dat gegevenshouders verplicht kunnen worden om gegevens aan overheden beschikbaar te stellen, die vervolgens weer door derden verplicht zouden kunnen worden om die gegevens ook voor hen beschikbaar te stellen. Omdat het om commercieel gevoelige informatie kan gaan, zouden gegevenshouders daardoor huiverig kunnen worden om mee te werken aan een gegevensverzoek als bedoeld onder hoofdstuk V van de verordening. Aangezien in noodsituaties snelle en soepele medewerking van gegevenshouders noodzakelijk is, moeten dit soort risico's worden voorkomen. Om die reden is in artikel 17, derde lid, van de verordening geregeld dat gegevens die onder hoofdstuk V door gegevenshouders aan overheidsorganisaties beschikbaar worden gesteld, niet beschikbaar zijn voor hergebruik onder de Open data richtlijn en de DGA. Voor het hergebruik onder de DGA werkt deze bepaling direct door. Voor de Open data richtlijn, vereist dit nog een nadere bepaling in de Wet hergebruik van overheidsinformatie, waarin de richtlijn is geïmplementeerd (zie artikel 9 van de Uitvoeringswet). Zonder zo'n extra bepaling zou onduidelijk zijn of de Wet hergebruik overheidsinformatie verder gaat dan de EU-recht voorschrijft.

Het vierde lid van artikel 17 van de verordening regelt overigens dat niet wordt uitgesloten dat de betreffende gegevens voor specifieke doeleinden kunnen worden doorgegeven aan andere overheidsinstanties. In dergelijke gevallen geldt echter ook voor die overheidsinstanties dat de verkregen gegevens niet in aanmerking komen voor hergebruik. Uit overweging 70 van de verordening volgt tevens dat het niet verboden is om op basis van de verkregen gegevens officiële statistieken te maken en publiceren, zolang de onderliggende gegevens maar niet worden gepubliceerd.

5.9 Statistiek

³⁰ Richtlijn (EU) 2019/1024 van het Europees Parlement en de Raad van 20 juni 2019 inzake open data en het hergebruik van overheidsinformatie (PbEU 2019, L 172).

Deze verordening vormt een aanvulling op het Unie- en nationale recht inzake de toegang tot en het gebruik van gegevens voor statistische doeleinden, met name de Statistiekverordening³¹ en laat deze onverlet (overweging 67 van de verordening).³²

Zoals reeds beschreven in paragraaf 3.4 van het algemeen deel van de toelichting regelt de verordening in artikel 15 dat overheden voor statistiekdoeleinden in twee situaties gegevens kunnen opvragen bij private instanties op grond van een uitzonderlijke behoefte om hun wettelijke verplichtingen in het algemeen belang, hun wettelijke taak, uit te voeren: (a) alle gegevens die noodzakelijk zijn om te reageren op een algemene noodsituatie indien de overheidsinstantie niet in staat is dergelijke gegevens tijdig en doeltreffend op een andere manier en in gelijkwaardige omstandigheden te verkrijgen en (b) niet-persoonsgebonden gegevens, indien specifiek geïdentificeerd, en nodig voor een specifieke taak van algemeen belang, zoals het opstellen van officiële statistieken of voor de beperking of het herstel van noodsituaties, mits deze gegevens niet via andere middelen waarover de overheidsinstantie beschikt verkregen kunnen worden. Onder 'andere middelen' valt de aankoop van gegevens op de markt, het gebruik van bestaande verplichtingen om gegevens beschikbaar te stellen of de vaststelling van nieuwe wetgevingsmaatregelen die de tijdige beschikbaarheid van de gegevens kunnen waarborgen. De verplichting om aan te tonen dat een overheidsinstantie niet in staat was om niet-persoonsgebonden gegevens op de markt te kopen, is niet van toepassing indien de gegevens voor officiële statistieken zijn bedoeld en het aankopen van de gegevens volgens nationaal recht niet is toegestaan. Dit betekent dat het CBS niet aan hoeft te tonen dat de gegevens niet gekocht konden worden omdat artikel 33, vierde lid, van de Wet op het Centraal bureau voor de statistiek (hierna: wet op het CBS) bepaalt dat gegevens kosteloos worden verstrekt (en dat geen beroep kan worden gedaan op geheimhoudingsverplichtingen, tenzij deze verplichtingen gebaseerd zijn op internationale regelgeving). Alleen wanneer het CBS alle andere middelen heeft uitgeput die de tijdige beschikbaarheid van gegevens kunnen waarborgen kan het CBS eventueel op grond van uitzonderlijke noodzaak gegevens opvragen. Het 'gebruik van bestaande verplichtingen' betekent in dit geval bijvoorbeeld dat CBS gebruik maakt van enquêtes en overheidsregisters op basis van de CBS wet en het Besluit gegevensverwerving CBS om de gegevens te verwerven. De vaststelling van nieuwe wetgevingsmaatregelen betekent in dit geval dat de Wet op het CBS en het Besluit gegevensverwerving CBS zouden worden uitgebreid zodat CBS verplichtende uitvragen kan opleggen aan bedrijven.

Gegevenshouders, met uitzondering van mkb-bedrijven, moeten gelet op artikel 20, eerste lid, van de verordening de gegevens in (a) een uitzonderlijke noodsituatie gratis beschikbaar stellen. In situatie (b) hebben gegevenshouders geen recht op een vergoeding indien de niet-persoonsgebonden gegevens nodig zijn voor het opstellen van officiële statistieken en de aankoop niet is toegestaan op grond van het nationale recht (artikel 20, vierde lid, van de verordening). Gegevenshouders hebben geen recht op een vergoeding van het CBS aangezien artikel 33, vierde lid, van de Wet op het Centraal bureau voor de statistiek bepaalt dat gegevens kosteloos worden verstrekt.

Verder regelt artikel 21 van de verordening dat overheidsinstanties de uit hoofdstuk V verkregen gegevens mogen delen met onderzoeksorganisaties en met nationale bureaus voor de statistiek of Eurostat voor de productie voor het opstellen van officiële statistieken (zie ook paragraaf 3.4 van het algemeen deel van de toelichting).

5.10 Interoperabiliteit en normalisatie

³¹ Verordening (EG) nr. 223/2009 van het Europees Parlement en de Raad van 11 maart 2009 betreffende de Europese statistiek en tot intrekking van Verordening (EG, Euratom) nr. 1101/2008 betreffende de toezending van onder de statistische geheimhoudingsplicht vallende gegevens aan het Bureau voor de Statistiek van de Europese Gemeenschappen, Verordening (EG) nr. 322/97 van de Raad betreffende de communautaire statistiek en Besluit 89/382/EEG, Euratom van de Raad tot oprichting van een Comité statistisch programma van de Europese Gemeenschappen (PbEU 2009, L 87).

³² Er is een Commissievoorstel van 10 juli 2023 voor een wijziging van Statistiekverordening (COM (2023) 402). In dit voorstel staan onder meer regels om in onverwachte situatie in tijdelijke informatiebehoeften en statistieken te kunnen voorzien. Het kabinet signaleert het risico van dubbele regimes en zet zich tijdens de onderhandelingen in om dubbeling te voorkomen (BNC-fiche van 6 oktober 2023).

Deze verordening heeft als doel het overstappen tussen dataverwerkingsdiensten te vergemakkelijken en de interoperabiliteit van gegevens en van mechanismen en diensten voor gegevensdeling in de Unie te verbeteren. In overeenstemming met de minimumvereiste om overstappen tussen aanbieders van dataverwerkingsdiensten toe te staan, heeft deze verordening ook tot doel de interoperabiliteit voor parallel gebruik van meerdere dataverwerkingsdiensten met aanvullende functionaliteiten te verbeteren. Na het overwegen van relevante internationale en Europese standaarden en zelfreguleringsinitiatieven, kan de Commissie op grond van de Normalisatieverordening³³ Europese normalisatieorganisaties verzoeken geharmoniseerde normen voor de interoperabiliteit van dataverwerkingsdiensten op te stellen.

Ook voor de interoperabiliteit van dataruimtes en de automatische executie van datadeelovereenkomsten via slimme contracten moet de Commissie de huidige belemmeringen beoordelen en op basis hiervan Europese normalisatieorganisaties verzoeken geharmoniseerde normen op te stellen. Alle te ontwikkelen normen volgend uit de verordening moeten voldoen aan de vereisten uit de Normalisatieverordening (Annex II).

6. Gevolgen

6.1 Regeldruk

De Uitvoeringswet heeft geen directe financiële gevolgen voor bedrijven, consumenten en niet-gouvernementele organisaties. De verordening laat slechts beperkte beleidsruimte aan lidstaten en deze wordt in de uitvoeringswet restrictief ingevuld.

De verordening zorgt wel voor een toegenomen regeldruk. De Europese Commissie heeft in haar impact assessment een analyse gegeven voor de gevolgen voor regeldruk van de verordening op de gehele Europese Unie.³⁴ Het is niet mogelijk om deze effecten kwantitatief te vertalen naar effecten voor Nederlandse bedrijven en consumenten.

Het ontwikkelen van technische oplossingen om toegang tot data te faciliteren zal voor aanbieders van verbonden producten en gerelateerde diensten naar schatting eenmalig €410 miljoen en jaarlijks €88 miljoen kosten. Voor een mkb-bedrijf kunnen de structurele kosten volgens de Commissie oplopen tot maximaal €300.000 per jaar. Voor een grote aanbieder kunnen de structurele kosten oplopen tot €1 miljoen per jaar. Daar tegenover staan efficiëntie- en productiviteitswinsten van €196,7 miljard per jaar vanaf 2028 door de toegenomen beschikbaarheid van data voor hergebruik en de toegenomen vraag naar producten als gevolg van de ingevoerde gebruiks- en toegangsrechten. Ook verwacht de Commissie dat de mogelijkheid voor gebruikers om hun data makkelijker tussen producten en diensten uit te wisselen nog eens €68,1 miljard per jaar zal besparen.

De operationele en juridische kosten van de maatregelen om oneerlijke contractvoorwaarden voor datadeling tussen bedrijven tegen te gaan zullen naar verwachting €69 miljoen per jaar bedragen. De verwachte baten van deze maatregelen door productiviteitswinst, datagedreven innovatie en toegenomen vraag zijn €7,4 miljard per jaar. Met name het mkb zal profijt hebben van deze maatregelen.

De Commissie verwacht dat de kosten voor het bedrijfsleven om data beschikbaar te maken voor publieke instanties eenmalig €552,5 miljoen zullen bedragen, voor het opzetten van infrastructuur, en daarna jaarlijks €78,1 miljoen. Daarnaast verwacht de Commissie dat het stroomlijnen van de datadeling met publieke instanties tot een lastenverlichting van €155 miljoen per jaar zal leiden.

Voor de maatregelen gericht op aanbieders van clouddiensten maakt de Commissie geen cijfermatige inschatting van de kosten. De verwachting is dat het de concurrentie, innovatie en de toepassing van nieuwe technologieën in de cloudmarkt zal bevorderen. Ook zal het de overstapkosten voor

³³ Verordening (EU) Nr. 1025/2012 van het Europees Parlement en de Raad van 25 oktober 2012 betreffende Europese normalisatie, tot wijziging van de Richtlijnen 89/686/EEG en 93/15/EEG van de Raad alsmede de Richtlijnen 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG en 2009/105/EG van het Europees Parlement en de Raad en tot intrekking van Beschikking 87/95/EEG van de Raad en Besluit nr. 1673/2006/EG van het Europees Parlement en de Raad (PbEU 2012, L 316).

³⁴ [Impact Assessment report and support studies accompanying the Proposal for a Data Act | Shaping Europe's digital future \(europa.eu\)](#).

gebruikers van clouddiensten sterk verlagen. De maatregelen zullen wel nalevingskosten met zich meebrengen voor aanbieders van clouddiensten. De Commissie verwacht dat deze beperkt zullen zijn omdat de maatregelen bouwen op een marktgedreven standaardisatieproces.

6.2 Gevolgen/uitvoeringslasten voor overheidsorganisaties

Ook voor overheidsorganisaties geldt dat de belangrijkste gevolgen direct voortvloeien uit de verordening zelf. De verordening verplicht lidstaten om bevoegde autoriteiten aan te wijzen. Ook biedt de verordening overheidsorganisaties, zowel nationale als lokale instanties, de mogelijkheid om in geval van uitzonderlijke noodzaak gegevens bij gegevenshouders op te vragen.

De Uitvoeringswet heeft gevolgen voor de AP en de ACM omdat zij worden aangewezen als bevoegde autoriteiten die een toezichtstaak of adviesrol krijgen. Het voornemen is om AP aan te wijzen voor hoofdstuk V en ACM aan te wijzen voor hoofdstukken II, III, IV, VI, VII en VIII. Deze overheidsorganisaties voeren een uitvoerbaarheids- en handhaafbaarheidstoets uit om de precieze gevolgen voor hun organisatie in kaart te brengen (zie paragraaf 8 van het algemeen deel van de toelichting).

De verordening laat geen ruimte om geen organisaties aan te wijzen. De gevolgen voor overheidsorganisaties die direct uit de Uitvoeringswet – en dus niet uit de verordening zelf – voortvloeien, zijn daarom zeer beperkt.

7. Evaluatie

Hoofdstuk XI stelt dat uiterlijk 56 maanden na de datum van inwerkingtreding van deze verordening de Commissie een evaluatie van deze verordening uitvoert. In de evaluatie wordt o.a. het effect van de verordening beoordeeld voor: het (her)gebruik van gegevens, de praktische toepassing van hoofdstuk V, intellectueel-eigendomsrecht en bedrijfsgeheimen, de verlaging van de overstapkosten van dataverwerkingsdiensten, de innovatiecapaciteit van het midden- en kleinbedrijf. Lidstaten verstrekken de Europese Commissie de nodige informatie voor het opstellen van de evaluatie.

8. Advies en consultatie

8.1 Internetconsultatie

[PM uitkomsten consultatie]

8.2 Uitvoerbaarheid en handhaafbaarheidstoetsen

[PM uitkomsten UHT's]

9. Overgangsrecht en inwerkingtreding

De verordening is van toepassing met ingang van 12 september 2025. De Uitvoeringswet dient daarom ook op deze datum in werking te treden, hetgeen vastgesteld wordt in artikel 10 van de Uitvoeringswet. De inwerkingtreding van dit wetsvoorstel wijkt af van het kabinetsbeleid inzake vaste verandermomenten (Kamerstukken II 2009/10, 29 515, nr. 309), inhoudende dat wetsvoorstellen op 1 januari of 1 juli in werking treden met een minimuminvoeringstermijn van twee maanden. Volgens dit kabinetsbeleid kan een uitzondering worden gemaakt indien het de uitvoering van een Europese verordening betreft.

Op een aantal onderwerpen voorziet de verordening in overgangsrecht (artikel 50 van de verordening). De uit artikel 3, eerste lid, van de verordening voortvloeiende verplichting om verbonden producten zo te vervaardigen dat productgegevens en gegevens van een gerelateerde dienst gemakkelijk toegankelijk zijn voor de gebruiker is van toepassing op verbonden producten en de daaraan gerelateerde diensten die na 12 september 2026 in de handel zijn gebracht. Hoofdstuk III van de verordening is van toepassing met betrekking tot verplichtingen om gegevens beschikbaar te stellen op grond van het Unierecht of op grond van overeenkomstig het Unierecht vastgestelde nationale wetgeving die na 12 september 2025 in werking treedt. Hoofdstuk IV van de verordening is van toepassing op overeenkomsten die na 12 september 2025 zijn gesloten. Hoofdstuk IV is met ingang van 12 september 2027 van toepassing op overeenkomsten die op of vóór 12 september

2025 zijn gesloten mits zij van onbepaalde duur zijn, of ten minste 10 jaar na 11 januari 2024 aflopen.

II. Artikelsgewijs

Artikel 2 Geschillenbeslechtingsorgaan

Gebruikers, gegevenshouders en gegevensontvangers hebben toegang tot een gecertificeerd geschillenbeslechtingsorgaan om geschillen bedoeld in artikel 10, eerste lid, van de verordening. De lidstaat waar het geschillenbeslechtingsorgaan is gevestigd, certificeert dat orgaan op diens verzoek indien aan de voorwaarden uit artikel 10, vijfde lid, van de verordening is voldaan. Overweging 52 verheldert dat het lidstaten vrij staat om specifieke regels voor de certificeringsprocedure, waaronder voor het verstrijken of intrekken van certificering, vast te stellen. De bepalingen van deze verordening inzake geschillenbeslechting verplichten de lidstaten niet om geschillenbeslechtingsorganen op te richten. Zie ook paragrafen 3.2 en 4.4 van het algemeen deel van de toelichting over geschillenbeslechting.

Dit artikel in de Uitvoeringswet bepaalt dat de ACM de instantie is waar een geschillenbeslechtingsorgaan het verzoek kan indienen tot certificering in Nederland.

Artikel 3 Aanwijzing bevoegde autoriteiten en toezichthouders

Gelet op artikel 37, eerste lid, van de verordening wijst elke lidstaat één of meerdere bevoegde autoriteiten aan die bevoegd zijn voor de uitvoering en handhaving van de verordening. In artikel 3 van de Uitvoeringswet zijn de ACM en de AP aangewezen als bevoegde autoriteit. Zie voor een toelichting op de aanwijzing paragraaf 4.1 van het algemeen deel van de toelichting.

Artikel 37, vijfde lid, van de verordening bepaalt dat lidstaten moeten zorgen dat de taken en bevoegdheden van de bevoegde autoriteiten duidelijk omschreven zijn en de daargenoemde taken en bevoegdheden omvatten (zie ook paragraaf 3.8 van het algemeen deel van de toelichting). Artikel 3, tweede en vierde lid, van de Uitvoeringswet bepaalt dat de ACM en de AP bevoegd zijn om de (voor hun rol als bevoegde autoriteit relevante) taken en de bevoegdheden uit te oefenen die in de verordening aan de bevoegde autoriteiten zijn opgedragen.

Het vijfde en zesde lid van artikel 3 van de Uitvoeringswet bepalen dat de ACM en de AP voor de hoofdstukken van de verordening waar zij de bevoegde autoriteit voor zijn, daar ook de toezichthouder voor zijn. Daardoor beschikken zij ook over de toezichtbevoegdheden uit titel 5.2 van de Algemene wet bestuursrecht.

Artikel 4 Aanwijzing datacoördinator

Omdat in Nederland meerdere bevoegde autoriteiten worden aangewezen, wordt onder de bevoegde autoriteiten overeenkomstig artikel 37, tweede lid, van de verordening een datacoördinator aangewezen. In artikel 4 van de Uitvoeringswet wordt de ACM aangewezen als de datacoördinator (zie voor een toelichting op de aanwijzing paragraaf 4.3 van het algemeen deel van de toelichting). De taken en bevoegdheden van de datacoördinator volgen rechtstreeks uit de artikelen 37, vijfde lid, laatste alinea, en zesde lid, en 38, eerste lid, van de verordening. Zie voor een toelichting op de taken paragraaf 3.8 van het algemeen deel van de toelichting.

Artikel 5 Samenwerking ACM en AP

Voor effectief toezicht op de verordening moeten de bevoegde autoriteiten samenwerken met andere autoriteiten, waaronder de Rijksdienst Digitale Infrastructuur en sectorale autoriteiten. Zie voor uitleg over de eisen die de verordening stelt aan samenwerking paragraaf 3.8 van het algemeen deel van de toelichting en paragraaf 4.2 over de samenwerking in Nederland.

Artikel 5, eerste lid, van de Uitvoeringswet bepaalt dat de ACM advies kan vragen aan de AP of er afbreuk gedaan wordt aan de toepassing van de AVG door een voorgenomen besluit op basis van deze wet. In paragraaf 4.2 van het algemeen deel van de toelichting is uitgewerkt waarom deze advisering in het wetsvoorstel is opgenomen. Gelet op artikel 5, tweede lid, van de Uitvoeringswet kan bij ministeriële regeling een termijn worden bepaald waarbinnen het advies wordt gegeven. Van deze bepaling zal de Minister gebruikmaken indien in de praktijk blijkt dat onderlinge afspraken niet tot de gewenste uitkomsten leiden.

Het voorgestelde artikel 5, derde lid, van de Uitvoeringswet bepaalt dat de ACM en de AP (als bevoegde autoriteiten en de datacoördinator) bevoegd zijn om met andere bevoegde autoriteiten als bedoelde in artikel 37, vijfde lid, onderdelen f tot en met h, van de verordening afspraken te maken over toezicht op de verordening en dat ze daarvoor een samenwerkingsprotocol kunnen opstellen, waarvan in de Staatscourant mededeling wordt gedaan. Het betreft onder meer sectorale

toezichthouders die verantwoordelijk zijn voor de uitvoering van andere Unie of nationale regelgeving. Er kan ook worden gekozen om een bestaand samenwerkingsprotocol aan te passen, bijvoorbeeld het samenwerkingsprotocol tussen de ACM en AP in het kader van artikel 19, eerste lid, van de UAVG of artikel 7, derde lid, van de beoogde Uitvoeringswet datagovernanceverordening.

Artikel 37, vijfde lid, onderdelen c, g en h van de verordening bepaalt dat bevoegde autoriteiten informatie van andere bevoegde autoriteiten en andere overheidsinstanties moeten kunnen ontvangen. Het voorgestelde artikel 5, vierde lid, van de Uitvoeringswet voorziet in een grondslag voor het delen van niet-persoonsgebonden gegevens tussen de ACM en de AP in het kader van toezicht op de verordening. Het betreft een aanvulling op artikel 19, tweede lid, van de UAVG (uitwisseling van persoonsgegevens tussen AP en andere toezichthouders) en artikel 7 van de Instellingswet ACM (verstrekking van gegevens door de ACM).

Artikel 37, vijfde lid, onderdeel f, van de verordening voorziet in een grondslag voor informatie-uitwisseling met bevoegde autoriteiten uit andere lidstaten, de Commissie en het Europees Comité voor gegevensinnovatie.

Artikel 6 Sanctionering

Gelet op artikelen 37, vijfde lid, onderdeel d, en 40, derde lid, van de verordening moeten lidstaten sancties vaststellen, waaronder dwangsommen, voor inbreuken op de verordeningen. Dit artikel van de Uitvoeringswet bepaalt dat bij overtreding van de verordening de ACM en AP een bestuurlijke boete en een last onder dwangsom, en daarmee ook een last onder bestuursdwang, kan opleggen. Zie verder paragraaf 4.2 van het algemeen deel van de toelichting.

Artikel 7 Wijziging Algemene wet bestuursrecht

Dit artikel van de Uitvoeringswet regelt de beroepsmogelijkheden tegen besluiten van de bevoegde autoriteiten op grond van dit wetsvoorstel. Beroep kan in eerste aanleg bij de Rechtbank Rotterdam (bijlage 2, artikel 7, van de Awb) worden ingesteld en hoger beroep bij het College van Beroep voor het bedrijfsleven (hierna: CBb) (bijlage 2, artikel 11, van de Awb). De reden om één bevoegde rechtbank aan te wijzen is dat er specifieke kennis is vereist voor de toepassing van de bepalingen uit de Uitvoeringswet en de verordening. Naar verwachting zal het aantal beroepen op grond van deze wetgeving te beperkt zijn om bij elke rechtbank in Nederland voldoende specialisatie te verkrijgen en te behouden, en eenheid in de gerechtelijke uitspraken te waarborgen. Er is voor de Rechtbank Rotterdam gekozen, omdat deze rechtbank reeds op verschillende terreinen van het economisch publiekrecht als de bevoegde bestuursrechter is aangewezen. Daarbij kan bijvoorbeeld worden gedacht aan de bevoegdheid in het kader van de beoogde Uitvoeringswet Datagovernanceverordening, de Wet handhaving consumentenbescherming, de Telecommunicatiewet, en de Wet beveiliging netwerk- en informatiesystemen. In lijn met deze reeds bestaande bevoegdheid is de Rechtbank Rotterdam een voor de hand liggende keuze. Tegen een uitspraak van de Rechtbank Rotterdam staat om diezelfde reden hoger beroep open bij het College van Beroep voor het bedrijfsleven.

Artikel 8 Wijziging Databankenwet

Artikel 43 van de verordening bepaalt dat het *sui generis* recht uit artikel 7 van Richtlijn 96/9/EC (Databankrichtlijn) niet van toepassing is op gegevens uit een verbonden product of gerelateerde dienst (zie paragrafen 3.9 en 5.4 van het algemeen deel van de toelichting). Dit *sui generis* recht is geïmplementeerd in artikel 2, eerste lid, van de Databankenwet. De Databankenwet wordt gewijzigd zodat deze in lijn is met de uitzondering in de verordening.

Artikel 9 Wijziging Wet hergebruik overheidsinformatie

Op grond van artikel 17, derde lid, van de verordening, zijn gegevens die zijn verkregen op basis van hoofdstuk V van de verordening niet beschikbaar voor hergebruik als bedoeld in de Datagovernanceverordening (Verordening 2022/868/EU) en de Open data richtlijn (Richtlijn 2019/1024/EU). Die bepaling heeft direct effect op de werking van de Datagovernanceverordening, omdat dat een verordening is. Voor de Open data richtlijn moet die bepaling voor een goede werking nog worden omgezet in nationaal recht. Dat gebeurt door middel van dit artikel. Onder omstandigheden staat het vierde lid van artikel 17 van de verordening toe dat dergelijke gegevens wel met andere overheidsinstanties mogen worden gedeeld. Uiteraard is het niet de bedoeling dat die gegevens via een omweg alsnog voor hergebruik beschikbaar worden gesteld. Met het woord 'oorspronkelijk' in de onderhavige bepaling wordt uitdrukking gegeven aan het feit dat ook doorgegeven gegevens niet beschikbaar zijn voor hergebruik.

Artikel 10 Inwerkingtreding

Voor de inwerkingtreding wordt aangesloten op de datum waarop de verordening van toepassing is.
Zie verder paragraaf 9 van het algemeen deel van de toelichting.

III. Transponeringstabel

Bepaling Dataverordening	Bepaling in wetsvoorstel of bestaande regeling; toelichting indien niet geïmplementeerd of naar zijn aard geen implementatie behoeft	Omschrijving beleidsruimte	Toelichting op de keuze(n) bij de invulling van de beleidsruimte
Hoofdstuk I (Algemene bepalingen)			
Artikel 1 (Onderwerp en toepassingsgebied)	Behoeft naar de aard van deze bepaling geen implementatie; onderwerp en toepassingsgebied	Geen	
Artikel 2 (Definities)	Behoeft naar de aard van deze bepaling geen implementatie; definities	Geen	
Hoofdstuk II (Delen van gegevens tussen bedrijven en consumenten en tussen bedrijven onderling)			
Artikel 3 (Verplichting om productgegevens en gegevens van gerelateerde diensten toegankelijk te maken voor de gebruiker)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks	Geen	
Artikel 4 (De rechten en plichten van gebruikers en gegevenshouders wat betreft het raadplegen, gebruiken en beschikbaar stellen van productgegevens en gegevens van een gerelateerde dienst)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks	Geen	
Artikel 5 (Het recht van de gebruiker om gegevens te delen met derden)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks	Geen	
Artikel 6 (Verplichtingen van derden die op verzoek van de gebruiker gegevens ontvangen)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks	Geen	
Artikel 7 (Reikwijdte van de verplichtingen tot het delen van gegevens tussen bedrijven en consumenten en tussen bedrijven onderling)	Behoeft naar de aard van deze bepaling geen implementatie; reikwijdte	Geen	
Hoofdstuk III (Verplichtingen voor gegevenshouders die krachtens het Unierecht verplicht zijn om gegevens beschikbaar te stellen)			
Artikel 8 (Voorwaarden waaronder gegevenshouders gegevens ter beschikking stellen aan gegevensontvangers)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks	Geen	
Artikel 9 (Vergoeding voor het beschikbaar stellen van gegevens)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks	Geen	
Artikel 10 (Geschillenbeslechting)	Lid 1-4, lid 7-13 : Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks Lid 5 : artikel 2 Uitvoeringswet Lid 6 : Implementatie wordt vorm gegeven door feitelijk handelen; EC informeren.	Keuze welke instantie certificeert	Zie par. 4.4 van deze MvT
Artikel 11 (Technische beschermingsmaatregelen inzake het ongeoorloofd gebruik of de ongeoorloofde openbaarmaking van gegevens)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks	Geen	
Artikel 12 (Reikwijdte van de verplichtingen voor gegevenshouders die krachtens het Unierecht verplicht zijn om gegevens beschikbaar te stellen)	Behoeft naar de aard van deze bepaling geen implementatie; reikwijdte	Geen	
Hoofdstuk IV (Oneerlijke contractuele bedingen met betrekking tot de toegang tot en het gebruik van gegevens tussen ondernemingen)			
Artikel 13 (Oneerlijke contractuele bedingen die eenzijdig worden opgelegd aan een andere onderneming)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks	Geen	
Hoofdstuk V (Gegevens beschikbaar stellen aan overheidsinstanties, de Commissie, de Europese Centrale Bank en organen van de Unie op grond van uitzonderlijke noodzaak)			
Artikel 14 (Verplichting om gegevens beschikbaar te stellen op grond van uitzonderlijke noodzaak)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks	Geen	
Artikel 15 (Uitzonderlijke noodzaak om gegevens te gebruiken)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks	Geen	

Artikel 16 (Verband met andere verplichtingen om gegevens beschikbaar te stellen aan overheidsinstanties, en de Commissie, de Europese Centrale Bank en organen van de Unie)	Behoeft naar de aard van deze bepaling geen implementatie; reikwijdte	Geen	
Artikel 17 (Verzoeken om gegevens beschikbaar te stellen)	Behoeft naar de aard van deze bepaling geen implementatie; lid 5 is gericht tot EC en overige leden werken rechtstreeks	Geen	
Artikel 18 (Naleving van verzoeken om gegevens)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks	Geen	
Artikel 19 (Verplichtingen van overheidsinstanties, de Commissie, de Europese Centrale Bank en organen van de Unie)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks	Geen	
Artikel 20 (Vergoeding in geval van uitzonderlijke noodzaak)	Lid 4 : Implementatie wordt vorm gegeven door feitelijk handelen; informeren EC Overige leden : Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks	Geen	
Artikel 21 (Delen van in de context van een uitzonderlijke noodzaak verkregen gegevens met onderzoeksorganisaties of statistische instanties)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks	Geen	
Artikel 22 (Wederzijdse bijstand en grensoverschrijdende samenwerking)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks	Geen	
Hoofdstuk VI (Overstappen naar een andere dataverwerkingsdienst)			
Artikel 23 (Belemmeringen voor een doeltreffende overstap wegnemen)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks	Geen	
Artikel 24 (Reikwijdte van de technische verplichtingen)	Behoeft naar de aard van deze bepaling geen implementatie; reikwijdte	Geen	
Artikel 25 (Contractvoorwaarden betreffende een overstap)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks	Geen	
Artikel 26 (Verplichting voor aanbieders van dataverwerkingsdiensten om informatie te verstrekken)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks	Geen	
Artikel 27 (Goedetrouwverplichting)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks	Geen	
Artikel 28 (Contractuele transparantieplichtingen inzake internationale toegang en doorgifte)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks	Geen	
Artikel 29 (Stapsgewijze opheffing van overstapkosten)	Behoeft naar de aard van deze bepaling geen implementatie; lid 4 is gericht tot EC, overige leden werken rechtstreeks	Geen	
Artikel 30 (Technische aspecten van een overstap)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks	Geen	
Artikel 31 (Specifieke regeling voor bepaalde dataverwerkingsdiensten)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks, reikwijdte	Geen	
Hoofdstuk VII (Internationale overheidstoegang en overdracht van niet-persoonsgebonden gegevens)			
Artikel 32 (Internationale overheidstoegang en overdracht)	Lid 3 : relevante nationale instantie of bevoegde autoriteit aanwijzen Overige leden : Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks en gericht tot EDIB (lid 3, laatste alinea)	Lid 3 : relevante nationale instantie of bevoegde autoriteit voor internationale samenwerking in juridische aangelegenheden	Zie par. 4.1 van deze MvT
Hoofdstuk VIII (Interoperabiliteit)			
Artikel 33 (Essentiële eisen inzake interoperabiliteit van gegevens, van mechanismen en diensten voor het delen van gegevens alsook van gemeenschappelijke Europese dataruimten)	Lid 11, eerste zin, : Implementatie wordt vorm gegeven door feitelijk handelen; informeren EC Verder: Behoeft naar de aard van deze bepaling geen implementatie; Lid 1, 3, 8 : werkt rechtstreeks Lid 2, 4- 7, 9-11 : gericht tot EC	Geen	
Artikel 34 (Interoperabiliteit met het oog op parallel gebruik van dataverwerkingsdiensten)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks	Geen	

Artikel 35 (Interoperabiliteit voor dataverwerkingsdiensten)	Lid 7, eerste zin : Implementatie wordt vorm gegeven door feitelijk handelen; informeren EC Verder: Behoeft naar de aard van deze bepaling geen implementatie; Lid 1-3 : werkt rechtstreeks Lid 4-9 : gericht tot EC	Geen	
Artikel 36 (Essentiële eisen met betrekking tot slimme contracten voor het uitvoeren van gegevensdelingsovereenkomsten)	Lid 11, eerste zin : Implementatie wordt vorm gegeven door feitelijk handelen; informeren EC Verder: Behoeft naar de aard van deze bepaling geen implementatie; Lid 1-4, 9 : werkt rechtstreeks Lid 5-8, 10 en 11 : gericht tot EC	Geen	
Hoofdstuk IX (Uitvoering en handhaving)			
Artikel 37 (Bevoegde autoriteiten en data-coördinatoren)			
Lid 1 (aanwijzen bevoegde autoriteiten)	Artikel 3, eerste en derde lid, Uitvoeringswet; aanwijzen een of meerdere bevoegde autoriteiten.	Keuze aanwijzen bevoegde autoriteiten	Zie par. 4.1 van deze MvT
Lid 2 (aanwijzen datacoördinator)	Artikel 4 Uitvoeringswet; aanwijzen datacoördinator (indien meerdere bevoegde autoriteiten worden aangewezen).	Keuze aanwijzen data coördinator	Zie par. 4.3 van deze MvT
Lid 3 (rol AVG-toezichthouder)	Eerste zin: Reeds geïmplementeerd via artikel 6 Uitvoeringswet AVG. Tweede zin : Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Lid 4 (rol sectorale autoriteiten en ervaring ervaring bevoegde autoriteit)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Lid 5 (taken en bevoegdheden bevoegde autoriteiten)	Artikel 3, tweede en vierde, vijfde en zesde lid, en artikel 5 Uitvoeringswet; taken en bevoegdheden voor bevoegde autoriteiten aanwijzen; zie ook titel 5.2 Awb; samenwerkingsprotocol nodig , informatie uitwisseling tussen autoriteiten regelen	Geen	
Lid 6 (taken en bevoegdheden datacoördinator)	Artikel 5 Uitvoeringswet; taken en bevoegdheden voor datacoördinator aanwijzen	Geen	
Lid 7 (informeren Commissie)	Implementatie wordt vorm gegeven door feitelijk handelen; informeren EC	Geen	
Lid 8 (onpartijdig)	Implementatie wordt vorm gegeven door feitelijk handelen	Geen	
Lid 9 (middelen en expertise)	Implementatie wordt vorm gegeven door feitelijk handelen; zorgen voor middelen en expertise	Geen	
Lid 10 – 13 (autoriteit bevoegd van lidstaat waar entiteit is gevestigd; wettelijke vertegenwoordiger)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks	Geen	
Lid 14 (bevoegdheid informatie opvragen)	Reeds geïmplementeerd via titel 5.2 Awb	Geen	
Lid 15 (verzoek om bijstand of handhaving aan bevoegde autoriteit in een andere lidstaat)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks	Geen	
Lid 16 (vertrouwelijkheid)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks	Geen	
Artikel 38 (Recht om een klacht in te dienen)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks	Geen	
Artikel 39 (Recht op een doeltreffende voorziening in rechte)	Artikel 7 Uitvoeringswet Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks	Geen	
Artikel 40 (Sancties)			
Lid 1 (sancties vaststellen)	Artikel 6 Uitvoeringswet	Ruimte om boete hoogte te bepalen	Zie par. 4.2 (sancties) van deze MvT
Lid 2 (informeren Commissie en register)	Eerste zin: Implementatie wordt vormgegeven door feitelijk handelen; informeren EC	Geen	

	Tweede zin : Behoeft naar de aard van deze bepaling geen implementatie; gericht tot EC		
Lid 3 (aanbevelingen ECvG en criteria voor sancties)	Implementatie wordt vormgegeven door feitelijk handelen; rekening houden met aanbevelingen en criteria bij opstellen sancties	Ruimte om boete hoogte te bepalen	Zie par. 4.2 (sancties) van deze MvT
Lid 4 (AVG-boetes)	Reeds geïmplementeerd via artikel 6 jo. 14, derde lid, Uitvoeringswet AVG	Geen	
Lid 5 (geldboetes EDPS)	Behoeft naar de aard van deze bepaling geen implementatie; gericht tot EDPS	Geen	
Artikel 41 (Modelcontractvoorwaarden en standaardcontractbepalingen)	Behoeft naar de aard van deze bepaling geen implementatie; gericht tot EC	Geen	
Artikel 42 (Rol van het Europees Comité voor gegevensinnovatie)	Behoeft naar de aard van deze bepaling geen implementatie; gericht tot EDIB	Geen	
Hoofdstuk X (Sui-generis-recht krachtens Richtlijn 96/9/EC)			
Artikel 43 (Databanken die bepaalde gegevens bevatten)	Artikel 8 Uitvoeringswet	Geen	
Hoofdstuk XI (Slotbepalingen)			
Artikel 44 (Andere Unierechtshandelingen betreffende rechten en verplichtingen inzake de toegang tot en het gebruik van gegevens)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks	Geen	
Artikel 45 (Uitoefening van de bevoegdheidsdelegatie)	Behoeft naar de aard van deze bepaling geen implementatie; gericht tot EC, EP en de Raad	Geen	
Artikel 46 (Comitéprocedure)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks	Geen	
Artikel 47 (Wijziging van Verordening (EU) 2017/2394)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks	Geen	
Artikel 48 (Wijziging van Richtlijn (EU) 2020/1828)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks	Geen	
Artikel 49 (Evaluatie en herziening)	Lid 3 : Implementatie wordt vorm gegeven door feitelijk handelen; EC informatie geven t.b.v. evaluaties Overig: Behoeft naar de aard van deze bepaling geen implementatie; gericht tot EC	Geen	
Artikel 50 (Inwerkingtreding en toepassing)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks	Geen	

De Minister van Economische Zaken en Klimaat,