



Advies Raad van State inzake het voorstel van wet tot uitvoering van de dataverordening

Nader Rapport

's-Gravenhage, 17 april 2025
Nr. WJZ / 97497049

Aan de Koning

Nader rapport inzake het voorstel van wet tot uitvoering van de dataverordening

Blijkens de mededeling van de Directeur van Uw kabinet van 9 september 2024, nr. 2024002030, machtigde Uwe Majesteit de Afdeling advisering van de Raad van State haar advies inzake het bovenvermelde voorstel van wet rechtstreeks aan mij te doen toekomen. Dit advies, gedateerd 20 november 2024, nr. W15.24.00243/IV, bied ik U hierbij aan.

De tekst van het advies treft u hieronder cursief aan, voorzien van mijn reactie.

Bij Kabinetsmissive van 9 september 2024, no.2024002030, heeft Uwe Majesteit, op voordracht van de Minister van Economische Zaken, bij de Afdeling advisering van de Raad van State ter overweging aanhangig gemaakt het voorstel van wet 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) (Uitvoeringswet dataverordening), met memorie van toelichting.

Het wetsvoorstel Uitvoeringswet dataverordening strekt tot uitvoering van de Dataverordening (verordening) en regelt het nationale toezicht op de verordening.¹ Het wetsvoorstel belegt het toezicht op de verordening bij de Autoriteit Consument & Markt (ACM) en de AP. De Autoriteit Persoonsgegevens (AP) houdt toezicht op een beperkt aantal specifieke bepalingen van de verordening die samenhangen met de Algemene verordening gegevensbescherming (AVG). Ook houdt de AP toezicht op hoofdstuk V van de verordening. De ACM is de toezichthouder op alle andere onderdelen.

De Afdeling advisering van de Raad van State maakt een opmerking over het beleggen van het toezicht op hoofdstuk V van de verordening bij de AP. Zij acht de in de toelichting opgenomen motivering onvolledig. In verband daarmee is aanpassing van de toelichting wenselijk.

1. Inhoud en achtergrond

De verordening maakt deel uit van de Europese datastrategie. De datastrategie heeft als doel om een interne markt voor gegevens te creëren en te reguleren.² De datastrategie bestaat tot nu toe uit twee verordeningen, de Datagovernanceverordening (hierna: DGA) en de verordening. De DGA beoogt het (her)gebruik van overheidsgegevens te vergemakkelijken, en biedt mechanismen voor het vrijwillig delen van andere gegevens zoals databemiddelingsdiensten en data-altruïstische organisaties.³

Binnen de Europese datastrategie biedt de verordening een geharmoniseerd kader voor het delen van gegevens. De doelstellingen zijn onder meer het zorgen voor een eerlijke verdeling van de voordelen die voortvloeien uit gegevens over belanghebbenden, het stimuleren van een concurrerende datamarkt en het toegankelijker maken van gegevens. Uit de datastrategie volgen ook nog domein-specifieke gemeenschappelijke Europese gegevensruimten ('data spaces'). Deze gegevensruimten

¹ 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.

² De verordening hangt ook samen met de Europese digitaliseringsstrategie, met name met de Digitalemarktenverordening. De Digitalemarktenverordening stelt regels voor 'poortwachters', grote platforms met een aanzienlijke impact op de interne markt. Deze 'big-techbedrijven' mogen in het kader van de Dataverordening geen gegevens ter beschikking gesteld krijgen (artikel 5, derde lid, en artikel 6, tweede lid, verordening). De Europese Commissie heeft intussen als poortwachter aangewezen Alphabet, Amazon, Apple, Booking, ByteDance, Meta Platforms en Microsoft.

³ De Uitvoeringswet Datagovernanceverordening is op 22 oktober 2024 door de Eerste Kamer aangenomen.



moeten op specifieke gebieden juridische en technische belemmeringen voor het delen van gegevens tussen organisaties wegnemen.⁴

Het wetsvoorstel belegt het toezicht op de verordening bij de ACM en de AP. De AP houdt toezicht op een beperkt aantal specifieke bepalingen van de verordening die samenhangen met de AVG. Ook houdt de AP toezicht op hoofdstuk V van de verordening.⁵ De ACM is de toezichthouder op alle andere onderdelen.⁶ Daarnaast heeft de AP, op basis van de verordening zelf, een algemene bevoegdheid voor het toezicht op de verordening met betrekking tot de bescherming van persoonsgegevens.⁷

Het voorstel wijst de ACM ook als datacoördinator aan. De datacoördinator is centraal contactpunt, en bevordert de samenwerking met andere (lidstatelijke) bevoegde autoriteiten en het Europees Comité voor gegevensinnovatie (Comité). Daarnaast regelt het voorstel dat de ACM en de AP in een samenwerkingsprotocol nadere afspraken maken.

2. Toezicht op hoofdstuk V van de verordening

Hoofdstuk V van de verordening regelt het op hun verzoek aan overheidsinstanties en EU-organen beschikbaar stellen van gegevens door gegevenshouders, in geval van uitzonderlijke noodzaak. Het wetsvoorstel wijst de AP aan als toezichthouder op hoofdstuk V, met uitzondering van het toezicht op de vergoedingen.⁸ Hiervoor wordt de ACM bevoegd.⁹

Een uitzonderlijke noodzaak kan zich in twee gevallen voordoen. Ten eerste, als de overheidsinstanties of EU-organen gegevens nodig hebben in het kader van een algemene noodsituatie. Hierbij wordt in Nederland kortweg aangesloten bij het staatsnoodrecht. Ten tweede, als geen sprake is van een algemene noodsituatie, maar de overheidsinstantie bepaalde gegevens nodig heeft voor het vervullen van een bij wet opgelegde specifieke taak van algemeen belang.¹⁰

Het verzoek om gegevens is aan voorwaarden gebonden. Uitgangspunt is dat het niet-persoonsgebonden gegevens betreft.¹¹ Alleen als dit ontoereikend is kunnen in geval van een algemene noodsituatie gepseudonimiseerde persoonsgegevens ter beschikking worden gesteld.

De toelichting gaat slechts kort in op het aanwijzen van de AP als toezichthouder voor dit hoofdstuk. De toelichting meldt dat de AP al een rol zou hebben bij het toezicht op dit hoofdstuk omdat overheidsinstanties bij de AP moeten melden wanneer zij om persoonsgegevens verzoeken.¹² Hoofdstuk V heeft verder weinig raakvlak met de rest van de verordening, en het toezicht daarop wordt op deze manier centraal belegd. Doorslaggevend argument lijkt te zijn dat overheidsinstanties al onderworpen zijn aan het (AVG-)toezicht van de AP, en deze nieuwe taak daarom aansluit bij de ervaring van de AP.¹³

De vraag rijst of deze redenering voldoet. Het is waarschijnlijk dat het verzoek om gegevens vooral zal worden gedaan voor het vervullen van een wettelijke overheidstaak (situatie 2).¹⁴ Wanneer daarvan sprake is gaat het in principe niet om persoonsgegevens. In die gevallen noopt de verordening dus niet tot het melden van het verzoek aan de AP. Daarnaast heeft de ACM als datacoördinator tot taak te waarborgen dat verzoeken van overheidsinstanties online openbaar beschikbaar zijn, en bevordert ze vrijwillige gegevensdelingsovereenkomsten tussen overheidsinstanties en gegevenshouders.¹⁵ Toezicht door de ACM zou daarom ook passend kunnen zijn.

De Afdeling merkt op dat de toelichting daar verder niet op ingaat, en daardoor onvolledig is. Dit klem

⁴ Zo worden inmiddels gegevensruimten voorbereid voor gezondheidsgegevens, landbouw, cultureel erfgoed, energie, de financiële sector, de green deal, manufacturing, taal, media, en mobiliteit, de overheid, onderzoek en innovatie, vaardigheden, en toerisme (Europese Commissie, Commission Staff Working Document on Common European Data Spaces, SWD(2024) 21, 24 januari 2024).

⁵ Voorgesteld artikel 3, derde lid; op basis van artikel 37, eerste lid, verordening wijst het voorstel de AP aan als toezichthouder op de artikelen 4, twaalfde lid, 5, zevende en achtste lid, en 6, tweede lid, onderdeel b, en hoofdstuk V, met uitzondering van artikel 20, van de verordening. De AP heeft daarnaast op basis van artikel 37, derde lid, verordening een algemene bevoegdheid voor het toezicht op de verordening met betrekking tot de bescherming van persoonsgegevens.

⁶ Voorgesteld artikel 3, eerste lid.

⁷ Artikel 37, derde lid, verordening.

⁸ Artikel 20 van de Dataverordening.

⁹ Voorgesteld artikel 3, eerste lid.

¹⁰ Artikel 15 van de verordening.

¹¹ Artikel 17, tweede lid, sub e, van de verordening.

¹² Artikel 17, tweede lid, onder i, van de verordening.

¹³ Toelichting, paragraaf 4.1.

¹⁴ De eerste situatie wordt in Nederland aan het staatsnoodrecht gebonden. In de afgelopen jaren is daar bijvoorbeeld sprake van geweest bij het instellen van de avondklok en bij de Wet verplaatsing bevolking. Dit heeft waarschijnlijk niet geleid tot het delen van gegevens.

¹⁵ Artikel 37, zesde lid, sub b, van de verordening.

temeer nu door de cumulatie van Europese regelingen op dit terrein de complexiteit van wetgeving – en toezicht – toeneemt.¹⁶ Zij acht het van belang dat de regering alle relevante overwegingen over een toedeling van bevoegdheden aan toezichthoudende instanties opneemt in de toelichting.

De Afdeling adviseert de toelichting op dit punt aan te vullen.

De Afdeling merkt terecht op dat in de aan de Afdeling voorgelegde memorie van toelichting slechts beperkt is ingegaan op de keuze voor de Autoriteit Persoonsgegevens (AP) als toezichthouder op hoofdstuk V van de verordening, en dat toelichting ontbreekt waarom niet is gekozen om de Autoriteit Consument en Markt (ACM) aan te wijzen. Om die reden is in paragraaf 4.1 van de memorie van toelichting nader toegelicht wat de redenen zijn om de AP aan te wijzen als bevoegde autoriteit voor hoofdstuk V van de verordening en wordt aangegeven waarom de ACM niet wordt aangewezen voor dit hoofdstuk.

Met betrekking tot de twee argumenten die door de Afdeling in haar advies in dit verband worden aangedragen, merkt het kabinet het volgende op. Hoewel het kabinet de opvatting deelt dat de meerderheid van de gegevensverzoeken waarschijnlijk niet zullen zien op algemene noodsituaties – en dus geen persoonsgegevens (mogen) bevatten – is de meer algemene verwachting dat gegevensverzoeken überhaupt weinig zullen voorkomen. Om die reden is het verschil in frequentie tussen de twee typen gegevensverzoeken beperkt van belang bij de keuze voor een toezichthouder. De verwachte lage frequentie is wel een argument om het toezicht voor beide typen gegevensverzoeken te concentreren bij één organisatie, zodat daar zoveel mogelijk expertise kan worden opgebouwd. Daarnaast is ook bij het beoordelen van de vraag of een bepaalde gegevensset géén persoonsgebonden gegevens bevat, expertise nodig op het gebied van persoonsgegevens, waardoor de AP een meer voor de hand liggende keuze is.

De taken die de ACM als datacoördinator krijgt op het gebied van hoofdstuk V van de verordening, geven daarnaast weinig aanleiding om de ACM ook aan te wijzen als bevoegde autoriteit voor dit hoofdstuk. Het publiceren van gegevensverzoeken is administratief van aard en heeft weinig raakvlakken met de taken voor de bevoegde autoriteit voor de uitvoering van hoofdstuk V van de verordening. Het bevorderen van vrijwillige gegevensovereenkomsten heeft wel meer raakvlakken met de inhoud van hoofdstuk V. Deze raakvlakken zijn desalniettemin kleiner dan de raakvlakken tussen het toezicht op hoofdstuk V en de overige taken van de AP. Al met al wegen de argumenten om het toezicht op hoofdstuk V te beleggen bij de AP naar het oordeel van het kabinet dus zwaarder dan de argumenten om dat toezicht bij de ACM te beleggen. Derhalve blijft het kabinet bij de reeds gemaakte keuze. In verband met het voorgaande, is in paragraaf 4.1 van de memorie van toelichting meer toelichting opgenomen over de keuze om de AP aan te wijzen als toezichthouder op hoofdstuk V en wordt aangegeven waarom de ACM niet wordt aangewezen voor dit hoofdstuk.

3. Ambtshalve wijzigingen

De memorie van toelichting is na ommekomst van het advies van de Afdeling geactualiseerd. Voorts zijn het wetsvoorstel en de memorie van toelichting op de volgende punten gewijzigd:

- Artikel 2 van het wetsvoorstel is aangevuld met een tweede en derde lid, op grond waarvan de ACM bevoegd zal zijn om de certificering van geschilbeslechtsingsorganen in te trekken in het geval die organen niet meer voldoen aan de criteria voor certificering of als die organen niet voldoen aan de verplichtingen die krachtens de dataverordening op hen rusten. Dit is nader toegelicht in paragraaf 4.4 van de memorie van toelichting.
- Het vierde lid van artikel 3 van het wetsvoorstel is aangevuld met een tweede volzin, waarin is bepaald dat artikel 14, eerste, vierde en vijfde lid, van de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) van overeenkomstige toepassing is op de uitvoering door de AP van de dataverordening. Daarmee wordt verzekerd dat de AP bevoegd is om de taken uit te voeren en de bevoegdheden uit te oefenen die in de AVG zijn toegekend aan de toezichthoudende autoriteiten, ten aanzien van de onderdelen van de dataverordening die betrekking hebben op de verwerking van persoonsgegevens. Dit is nodig ter uitvoering van artikel 37, derde lid, van de dataverordening. Dit is nader toegelicht in paragraaf 3.8 van de memorie van toelichting.
- In artikel 8, eerste en tweede lid, van het wetsvoorstel is verduidelijkt ten aanzien van welke onderdelen van de dataverordening de ACM en de AP bij overtreding een bestuurlijke boete, bestuursdwang of een last onder dwangsom kunnen opleggen. Dit is in lijn met aanwijzing 5.44 van de Aanwijzingen voor de regelgeving, op grond waarvan door sancties te handhaven bepalingen zo nauwkeurig mogelijk worden geformuleerd. In het verlengde van die aanpassing is de beschrijving van de verschillende onderdelen van de dataverordening in paragraaf 3 van de memorie van toelichting aangevuld. Ook wordt in paragraaf 5.5 van de memorie van toelichting

¹⁶ Advies van de Afdeling advisering van 26 juli 2023 (W18.23.00113), inzake de Uitvoeringswet Datagovernanceverordening, punt 2.



- nader ingegaan op hoe de civielrechtelijke handhaving van verschillende onderdelen van de dataverordening zich verhoudt tot bestuursrechtelijke handhaving en sanctionering door de ACM.
- In artikel 8 van het wetsvoorstel is een derde lid opgenomen waarin is bepaald dat de geldsom, die door AP wordt ontvangen op grond van een opgelegde bestuurlijke boete of last onder dwangsom, toekomt aan de Staat. Dit is in lijn met wat voor de ACM geldt op grond van de Instellingswet ACM en voor de AP op grond van de UAVG.
 - In de artikelen 5, vijfde lid, en 8, vijfde lid, van het wetsvoorstel is verduidelijkt dat de AP niet bevoegd is tot toezicht en handhaving ten aanzien van gedragingen van de Europese Commissie, de Europese Centrale Bank en andere EU-organen in het kader van hoofdstuk V van de verordening inzake het vorderen van gegevens in noodsituaties. Dit is nader toegelicht in paragraaf 3.8 van de memorie van toelichting.
 - In de wijziging van de bijlage bij de Wet handhaving consumentenbescherming (artikel 11 van het wetsvoorstel) is verduidelijkt ten aanzien van welke bepalingen van de dataverordening de ACM bevoegd zal zijn om op grond van die wet toezicht te houden en te handhaven. Artikelen 5 en 8 van het wetsvoorstel zijn voorts aangevuld met een vierde lid waarin is verduidelijkt dat de bevoegdheid van de ACM tot het opleggen van een bestuurlijke boete, bestuursdwang of een last onder dwangsom niet geldt in de gevallen waarin de ACM op grond van de Wet handhaving consumentenbescherming bevoegd zal zijn om bestuurlijke sancties op te leggen ter handhaving van de dataverordening. De paragrafen 4.2 en 5.5 van de memorie van toelichting zijn op dit punt aangevuld.

De Afdeling advisering van de Raad van State heeft een opmerking bij het voorstel en adviseert daarmee rekening te houden voordat het voorstel bij de Tweede Kamer der Staten-Generaal wordt ingediend.

De vice-president van de Raad van State,

Ik verzoek U, mede namens de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties en de Staatssecretaris van Justitie en Veiligheid, het hierbij gevoegde voorstel van wet en de memorie van toelichting aan de Tweede Kamer der Staten-Generaal te zenden.

*De Minister van Economische Zaken,
D.S. Beljaarts.*



Advies Raad van State

No. W15.24.00243/IV

's-Gravenhage, 20 november 2024

Aan de Koning

Bij Kabinetsmissive van 9 september 2024, no.2024002030, heeft Uwe Majesteit, op voordracht van de Minister van Economische Zaken, bij de Afdeling advisering van de Raad van State ter overweging aanhangig gemaakt het voorstel van wet 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) (Uitvoeringswet dataverordening), met memorie van toelichting.

Het wetsvoorstel Uitvoeringswet dataverordening strekt tot uitvoering van de Dataverordening (verordening) en regelt het nationale toezicht op de verordening.¹ Het wetsvoorstel belegt het toezicht op de verordening bij de Autoriteit Consument & Markt (ACM) en de AP. De Autoriteit Persoonsgegevens (AP) houdt toezicht op een beperkt aantal specifieke bepalingen van de verordening die samenhangen met de Algemene verordening gegevensbescherming (AVG). Ook houdt de AP toezicht op hoofdstuk V van de verordening. De ACM is de toezichthouder op alle andere onderdelen.

De Afdeling advisering van de Raad van State maakt een opmerking over het beleggen van het toezicht op hoofdstuk V van de verordening bij de AP. Zij acht de in de toelichting opgenomen motivering onvolledig. In verband daarmee is aanpassing van de toelichting wenselijk.

1. Inhoud en achtergrond

De verordening maakt deel uit van de Europese datastrategie. De datastrategie heeft als doel om een interne markt voor gegevens te creëren en te reguleren.² De datastrategie bestaat tot nu toe uit twee verordeningen, de Datagovernanceverordening (hierna: DGA) en de verordening. De DGA beoogt het (her)gebruik van overheidsgegevens te vergemakkelijken, en biedt mechanismen voor het vrijwillig delen van andere gegevens zoals databemiddelingsdiensten en data-altruïstische organisaties.³

Binnen de Europese datastrategie biedt de verordening een geharmoniseerd kader voor het delen van gegevens. De doelstellingen zijn onder meer het zorgen voor een eerlijke verdeling van de voordelen die voortvloeien uit gegevens over belanghebbenden, het stimuleren van een concurrerende datamarkt en het toegankelijker maken van gegevens. Uit de datastrategie volgen ook nog domein-specifieke gemeenschappelijke Europese gegevensruimten ('data spaces'). Deze gegevensruimten moeten op specifieke gebieden juridische en technische belemmeringen voor het delen van gegevens tussen organisaties wegnemen.⁴

Het wetsvoorstel belegt het toezicht op de verordening bij de ACM en de AP. De AP houdt toezicht op een beperkt aantal specifieke bepalingen van de verordening die samenhangen met de AVG. Ook houdt de AP toezicht op hoofdstuk V van de verordening.⁵ De ACM is de toezichthouder op alle andere onderdelen.⁶ Daarnaast heeft de AP, op basis van de verordening zelf, een algemene bevoegdheid voor het toezicht op de verordening met betrekking tot de bescherming van persoonsgegevens.⁷

Het voorstel wijst de ACM ook als datacoördinator aan. De datacoördinator is centraal contactpunt, en

¹ 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.

² De verordening hangt ook samen met de Europese digitaliseringsstrategie, met name met de Digitalemarktenverordening. De Digitalemarktenverordening stelt regels voor 'poortwachters', grote platforms met een aanzienlijke impact op de interne markt. Deze 'big-techbedrijven' mogen in het kader van de Dataverordening geen gegevens ter beschikking gesteld krijgen (artikel 5, derde lid, en artikel 6, tweede lid, verordening). De Europese Commissie heeft intussen als poortwachter aangewezen Alphabet, Amazon, Apple, Booking, ByteDance, Meta Platforms en Microsoft.

³ De Uitvoeringswet Datagovernanceverordening is op 22 oktober 2024 door de Eerste Kamer aangenomen.

⁴ Zo worden inmiddels gegevensruimten voorbereid voor gezondheidsgegevens, landbouw, cultureel erfgoed, energie, de financiële sector, de green deal, manufacturing, taal, media, en mobiliteit, de overheid, onderzoek en innovatie, vaardigheden, en toerisme (Europese Commissie, Commission Staff Working Document on Common European Data Spaces, SWD(2024) 21, 24 januari 2024).

⁵ Voorgesteld artikel 3, derde lid; op basis van artikel 37, eerste lid, verordening wijst het voorstel de AP aan als toezichthouder op de artikelen 4, twaalfde lid, 5, zevende en achtste lid, en 6, tweede lid, onderdeel b, en hoofdstuk V, met uitzondering van artikel 20, van de verordening. De AP heeft daarnaast op basis van artikel 37, derde lid, verordening een algemene bevoegdheid voor het toezicht op de verordening met betrekking tot de bescherming van persoonsgegevens.

⁶ Voorgesteld artikel 3, eerste lid.

⁷ Artikel 37, derde lid, verordening.



bevordert de samenwerking met andere (lidstatelijke) bevoegde autoriteiten en het Europees Comité voor gegevensinnovatie (Comité). Daarnaast regelt het voorstel dat de ACM en de AP in een samenwerkingsprotocol nadere afspraken maken.

2. Toezicht op hoofdstuk V van de verordening

Hoofdstuk V van de verordening regelt het op hun verzoek aan overheidsinstanties en EU-organen beschikbaar stellen van gegevens door gegevenshouders, in geval van uitzonderlijke noodzaak. Het wetsvoorstel wijst de AP aan als toezichthouder op hoofdstuk V, met uitzondering van het toezicht op de vergoedingen.⁸ Hiervoor wordt de ACM bevoegd.⁹

Een uitzonderlijke noodzaak kan zich in twee gevallen voordoen. Ten eerste, als de overheidsinstanties of EU-organen gegevens nodig hebben in het kader van een algemene noodsituatie. Hierbij wordt in Nederland kortweg aangesloten bij het staatsnoodrecht. Ten tweede, als geen sprake is van een algemene noodsituatie, maar de overheidsinstantie bepaalde gegevens nodig heeft voor het vervullen van een bij wet opgelegde specifieke taak van algemeen belang.¹⁰

Het verzoek om gegevens is aan voorwaarden gebonden. Uitgangspunt is dat het niet-persoonsgebonden gegevens betreft.¹¹ Alleen als dit ontoereikend is kunnen in geval van een algemene noodsituatie gepseudonimiseerde persoonsgegevens ter beschikking worden gesteld.

De toelichting gaat slechts kort in op het aanwijzen van de AP als toezichthouder voor dit hoofdstuk. De toelichting meldt dat de AP al een rol zou hebben bij het toezicht op dit hoofdstuk omdat overheidsinstanties bij de AP moeten melden wanneer zij om persoonsgegevens verzoeken.¹² Hoofdstuk V heeft verder weinig raakvlak met de rest van de verordening, en het toezicht daarop wordt op deze manier centraal belegd. Doorslaggevend argument lijkt te zijn dat overheidsinstanties al onderworpen zijn aan het (AVG-)toezicht van de AP, en deze nieuwe taak daarom aansluit bij de ervaring van de AP.¹³

De vraag rijst of deze redenering voldoet. Het is waarschijnlijk dat het verzoek om gegevens vooral zal worden gedaan voor het vervullen van een wettelijke overheidstaak (situatie 2).¹⁴ Wanneer daarvan sprake is gaat het in principe niet om persoonsgegevens. In die gevallen noopt de verordening dus niet tot het melden van het verzoek aan de AP. Daarnaast heeft de ACM als datacoördinator tot taak te waarborgen dat verzoeken van overheidsinstanties online openbaar beschikbaar zijn, en bevordert ze vrijwillige gegevensdelingsovereenkomsten tussen overheidsinstanties en gegevenshouders.¹⁵ Toezicht door de ACM zou daarom ook passend kunnen zijn.

De Afdeling merkt op dat de toelichting daar verder niet op ingaat, en daardoor onvolledig is. Dit klemmt temeer nu door de cumulatie van Europese regelingen op dit terrein de complexiteit van wetgeving – en toezicht – toeneemt.¹⁶ Zij acht het van belang dat de regering alle relevante overwegingen over een toedeling van bevoegdheden aan toezichthoudende instanties opneemt in de toelichting.

De Afdeling adviseert de toelichting op dit punt aan te vullen.

De Afdeling advisering van de Raad van State heeft een opmerking bij het voorstel en adviseert daarmee rekening te houden voordat het voorstel bij de Tweede Kamer der Staten-Generaal wordt ingediend.

*De vice-president van de Raad van State,
Th.C. de Graaf.*

⁸ Artikel 20 van de Dataverordening.

⁹ Voorgesteld artikel 3, eerste lid.

¹⁰ Artikel 15 van de verordening.

¹¹ Artikel 17, tweede lid, sub e, van de verordening.

¹² Artikel 17, tweede lid, onder i, van de verordening.

¹³ Toelichting, paragraaf 4.1.

¹⁴ De eerste situatie wordt in Nederland aan het staatsnoodrecht gebonden. In de afgelopen jaren is daar bijvoorbeeld sprake van geweest bij het instellen van de avondklok en bij de Wet verplaatsing bevolking. Dit heeft waarschijnlijk niet geleid tot het delen van gegevens.

¹⁵ Artikel 37, zesde lid, sub b, van de verordening.

¹⁶ Advies van de Afdeling advisering van 26 juli 2023 (W18.23.00113), inzake de Uitvoeringswet Datagovernanceverordening, punt 2.



Tekst zoals toegezonden aan de Raad van State: Wet 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) (Uitvoeringswet dataverordening) (ontwerptekst zoals aangeboden aan de afdeling advisering van de Raad van State)

Wij Willem-Alexander, bij de gratie Gods, Koning der Nederlanden, Prins van Oranje-Nassau, enz. enz. enz.

Allen, die deze zullen zien of horen lezen, saluut! doen te weten:

Alzo Wij in overweging genomen hebben, dat het noodzakelijk is regels te stellen ter 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);

Zo is het, dat Wij, de Afdeling advisering van de Raad van State gehoord, en met gemeen overleg der Staten-Generaal, hebben goedgevonden en verstaan, gelijk Wij goedvinden en verstaan bij deze:

Artikel 1 Begripsbepaling

In deze wet en de daarop berustende bepalingen wordt verstaan onder:

Autoriteit Consument en Markt: Autoriteit Consument en Markt als bedoeld in artikel 2, eerste lid, van de Instellingswet Autoriteit Consument en Markt;

Autoriteit persoonsgegevens: Autoriteit persoonsgegevens als bedoeld in artikel 6, eerste lid, van de Uitvoeringswet Algemene verordening gegevensbescherming;

dataverordening: 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).

Artikel 2 Geschillenbeslechtsorgaan

De Autoriteit Consument en Markt certificeert op een verzoek als bedoeld in artikel 10, vijfde lid, van de dataverordening een orgaan als geschillenbeslechtsorgaan.

Artikel 3 Aanwijzing bevoegde autoriteiten

1. De Autoriteit Consument en Markt is de bevoegde autoriteit, bedoeld in artikel 37, eerste lid, van de dataverordening voor de hoofdstukken II, met uitzondering van de artikelen 4, twaalfde lid, 5, zevende en achtste lid, en 6, tweede lid, onderdeel b, III, IV, artikel 20, hoofdstukken VI tot en met VIII, en artikel 37, elfde en twaalfde lid, van de dataverordening.
2. Als bevoegde autoriteit heeft de Autoriteit Consument en Markt de taken en bevoegdheden, bedoeld in artikel 37, vijfde lid, onderdelen a tot en met i, van de dataverordening.
3. De Autoriteit persoonsgegevens is de bevoegde autoriteit, bedoeld in artikel 37, eerste lid, van de dataverordening voor de artikelen 4, twaalfde lid, 5, zevende en achtste lid, en 6, tweede lid, onderdeel b, en hoofdstuk V, met uitzondering van artikel 20, van de dataverordening.
4. Als bevoegde autoriteit heeft de Autoriteit persoonsgegevens de taken en bevoegdheden, bedoeld in artikel 37, vijfde lid, onderdelen a tot en met g en j, van de dataverordening.
5. In afwijking van het eerste lid is de Autoriteit persoonsgegevens de bevoegde autoriteit, bedoeld in artikel 37, eerste lid, van de dataverordening voor artikel 6, eerste lid, van de dataverordening voor zover het de verwerking van persoonsgegevens betreft.

Artikel 4 Aanwijzing datacoördinator

De Autoriteit Consument en Markt is de datacoördinator, bedoeld in artikel 37, tweede lid, van de dataverordening.



Artikel 5 Aanwijzing toezichthouders

1. Met het toezicht op de naleving van de hoofdstukken II, met uitzondering van de artikelen 4, twaalfde lid, 5, zevende en achtste lid, en 6, tweede lid, onderdeel b, III, IV, artikel 20, en hoofdstukken VI tot en met VIII, en artikel 37, elfde en twaalfde lid, van de dataverordening is belast de Autoriteit Consument en Markt.
2. Met het toezicht op de naleving van de artikelen 4, twaalfde lid, en 5, zevende en achtste lid, 6, tweede lid, onderdeel b, en hoofdstuk V, met uitzondering van artikel 20, van de dataverordening zijn belast de leden en buitengewone leden van de Autoriteit persoonsgegevens, de ambtenaren van het secretariaat van de Autoriteit persoonsgegevens, alsmede de bij besluit van de Autoriteit persoonsgegevens aangewezen personen.
3. In afwijking van het eerste lid zijn met het toezicht op de naleving van artikel 6, eerste lid, van de dataverordening voor zover het de verwerking van persoonsgegevens betreft belast de leden en buitengewone leden van de Autoriteit persoonsgegevens, de ambtenaren van het secretariaat van de Autoriteit persoonsgegevens, alsmede de bij besluit van de Autoriteit persoonsgegevens aangewezen personen.

Artikel 6 Samenwerking ACM en AP

1. De Autoriteit Consument en Markt en de Autoriteit persoonsgegevens zijn bevoegd om in het belang van een efficiënt en effectief toezicht op de dataverordening afspraken te maken en daartoe samenwerkingsprotocollen vast te stellen. Een samenwerkingsprotocol wordt bekendgemaakt in de Staatscourant.
2. Onverminderd artikel 19, tweede lid, van de Uitvoeringswet Algemene verordening gegevensbescherming en artikel 7, derde lid, onderdeel a, van de Instellingswet Autoriteit Consument en Markt zijn de Autoriteit Consument en Markt en de Autoriteit persoonsgegevens bevoegd uit eigen beweging en desgevraagd verplicht aan elkaar de gegevens te verstrekken die noodzakelijk zijn voor de uitvoering van deze wet.

Artikel 7 Samenwerking ACM en andere bevoegde autoriteiten

1. De Autoriteit Consument en Markt is bevoegd om in het belang van een efficiënt en effectief toezicht op de dataverordening afspraken te maken met andere bevoegde autoriteiten als bedoeld in artikel 37, vijfde lid, onderdelen g en h, van de dataverordening en daartoe gezamenlijk met deze bevoegde autoriteiten samenwerkingsprotocollen vast te stellen. Een samenwerkingsprotocol wordt bekendgemaakt in de Staatscourant.
2. Bij ministeriële regeling kunnen regels worden gesteld over het verstrekken van gegevens tussen de Autoriteit Consument en Markt en de bevoegde autoriteiten, bedoeld in het eerste lid, die noodzakelijk zijn voor de uitvoering van deze wet.

Artikel 8 Sanctionering

1. De Autoriteit Consument en Markt is ter handhaving van de bepalingen genoemd in artikel 5, eerste lid, bevoegd tot oplegging van:
 - a. een last onder bestuursdwang; of
 - b. een bestuurlijke boete van ten hoogste het bedrag dat is vastgesteld voor de zesde categorie, bedoeld in artikel 23, vierde lid, van het Wetboek van Strafrecht of, indien dat meer is, 10% van de jaaromzet van de overtreder in het voorgaande boekjaar in de Europese Unie.
2. De Autoriteit Persoonsgegevens is ter handhaving van de bepalingen genoemd in artikel 5, tweede lid, bevoegd tot oplegging van:
 - a. een last onder bestuursdwang; of
 - b. een bestuurlijke boete van ten hoogste het bedrag, genoemd in artikel 40, vierde lid, van de dataverordening.

Artikel 9 Wijziging Algemene wet bestuursrecht

Bijlage 2 bij de Algemene wet bestuursrecht wordt als volgt gewijzigd:

1. In artikel 7 wordt in de alfabetische volgorde ingevoegd:

Uitvoeringswet dataverordening: artikelen 2, 5, eerste lid, en 8, eerste lid



2. In artikel 11 wordt in de alfabetische volgorde ingevoegd:

Uitvoeringswet dataverordening: artikelen 2, 5, eerste lid, en 8, eerste lid

Artikel 10 Wijziging Databankenwet

Na artikel 8 van de Databankenwet wordt een artikel toegevoegd, luidende:

Artikel 8a.

Het recht, bedoeld in artikel 2, eerste lid, is niet van toepassing wanneer gegevens worden verkregen uit of gegenereerd door een verbonden product of gerelateerde dienst als bedoeld in artikel 43 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).

Artikel 11 Wijziging Wet handhaving consumentenbescherming

In de bijlage, onderdeel a, wordt aan de tabel de volgende rij toegevoegd:

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)	
--	--

Artikel 12 Wijziging Wet hergebruik overheidsinformatie

Aan artikel 2, eerste lid, van de Wet hergebruik van overheidsinformatie wordt, onder vervanging van de punt aan het slot van dat lid door een puntkomma, een onderdeel toegevoegd, luidende:

- k. informatie die oorspronkelijk is verkregen op grond van hoofdstuk V van de 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).

Artikel 13 Inwerkingtreding

Deze wet treedt in werking met ingang van 12 september 2025. Indien het Staatsblad waarin deze wet wordt geplaatst, wordt uitgegeven na 11 september 2025, treedt zij in werking met ingang van de dag na de datum van uitgifte van het Staatsblad waarin zij wordt geplaatst.

Artikel 14 Citeertitel

Deze wet wordt aangehaald als: Uitvoeringswet dataverordening.

Lasten en bevelen dat deze in het Staatsblad zal worden geplaatst en dat alle ministeries, autoriteiten, colleges en ambtenaren die zulks aangaat, aan de nauwkeurige uitvoering de hand zullen houden.

De Minister van Economische Zaken,

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,

De Staatssecretaris van Justitie en Veiligheid,



MEMORIE VAN TOELICHTING

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 of de Dataverordening).

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, de Staatssecretaris 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.

Reeds in de Verordening voor het vrije verkeer van niet-persoonsgebonden gegevens (Verordening (EU) 2018/1807, in het Engels ook wel bekend als de Free Flow of Data Regulation)³ werd verwezen naar een kader voor zelfregulering van gegevensportabiliteit tussen gegevensverwerkingsdiensten (art. 6), naast een verbod op ongerechtvaardigde gegevenslokalisatievereisten. De Europese Commissie (hierna: Commissie) werd hierin verplicht gedragscodes met de sector op te stellen waarin contractuele modelbepalingen staan. Dit heeft geleid tot de Switching and Porting (SWIPO) gedragscodes. Dit heeft de ongelijke marktmacht in de cloudmarkt echter niet afdoende verholpen.

De 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

¹ Kamerstukken II 2018/19, 26 643, nr. 594.

² Kamerstukken II 2022/23, 26 643, nr. 941.

³ Verordening (EU) 2018/1807 van het Europees Parlement en de Raad van 14 november 2018 inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie (PbEU 2018, L 303).

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 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.

Om deze visie te verwezenlijken worden gemeenschappelijke Europese dataruimten opgezet om het betrouwbaar en veilig delen van data in economisch strategische sectoren te vergemakkelijken. De EU biedt financiële ondersteuning voor deze sector- en domeinspecifieke datadeelinitiatieven en de werkzaamheden op het gebied van standaarden en interoperabiliteit.

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 Gegevensbescherming⁴ (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-paper⁵ 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 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.

⁴ 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).

⁵ Kamerstukken II 2021/22, 21501-33, nr. 875.

In het effectbeoordelingsverslag zijn door de Europese Commissie alternatieve maatregelen onderzocht.⁶ 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 algemeen 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 de gebruiker van een landbouwwapparaat 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.

⁶ Effectbeoordelingsverslag en ondersteunende studies bij het voorstel voor een dataverordening | Shaping Europe's digital future (europa.eu).

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 bedrijven⁷ worden gemaakt of geleverd. Middelgrote ondernemingen⁸ 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 Digitale marktenverordening (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 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

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

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

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 mkb⁹ 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. De verordening regelt dat in een aantal situaties de gebruiker of derde met de gegevenshouder overeen kan komen de zaak voor te leggen aan een voor de verordening gecertificeerd geschillenbeslechtsorgaan. Het gaat om de situatie dat een gebruiker of derde, met betrekking tot elk geschil met de gegevenshouder over de in het tweede lid van dat artikel bedoelde contractuele beperkingen of verboden (artikel 4, derde lid, verordening), het besluit van een gegevenshouder om het delen van gegevens te weigeren kan aanvechten (artikelen 4, negende lid, en 5, twaalfde lid, verordening). Naast geschillenbeslechting heeft de gebruiker of derde ook de mogelijkheid om een klacht in te dienen bij de bevoegde autoriteit of om naar de rechter te gaan. Een geschillenbeslechtsorgaan weigert een verzoek om beslechting van een geschil dat al voor een ander geschillenbeslechtsorgaan of een rechterlijke instantie is gebracht (artikel 10, zevende lid, van de verordening). Ook na geschillenbeslechting is het mogelijk om naar de rechter te gaan (artikel 10, dertiende lid, verordening).

De verordening legt vast dat lidstaten organisaties kunnen certificeren om geschillen onder hoofdstukken II, III, IV en VI van de verordening te beslechten. Ook legt de verordening de voorwaarden vast waar geschillenbeslechtsorganen aan moeten voldoen om te worden gecertificeerd. Geschillenbeslechtsorganen moeten onder andere onafhankelijk en deskundig zijn, partijen redelijkerwijs de mogelijkheid geven hun standpunten aan te dragen en jaarlijkse activiteitenverslagen openbaar maken. Uitspraken van geschillenbeslechtsorganen zijn alleen bindend als alle partijen vooraf hebben ingestemd met het bindende karakter van de uitspraken. Zoals in overweging 55 van de verordening aangegeven moeten geschillenbeslechtsorganen om uniforme toepassing van de verordening te waarborgen rekening houden met (door de Commissie te ontwikkelen en aan te bevelen) niet-bindende modelcontractvoorwaarden en met Unie- of nationaal recht waarin de gegevensdelingsverplichtingen worden gespecificeerd of richtsnoeren van sectorale autoriteiten voor de toepassing van dat recht.

⁹ Zoals aangemerkt in artikel 3 van de bijlage bij Aanbeveling 2003/361/EG.

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

Aanvullend op hoofdstuk III specificeert **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 de toegang en het 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, en in gelijkwaardige omstandigheden, tijdig en doeltreffend kan verkrijgen. De overheidsinstantie moet aantonen dat er geen andere manier was de gegevens tijdig te verkrijgen, bijvoorbeeld via vrijwillige datadeling of een specifiek datadelingsmechanisme zoals de aankomende Europese ruimte voor gezondheidsgegevens. 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. In deze situaties van uitzonderlijke noodzaak mogen de verzoeken alleen betrekking hebben op niet-persoonsgebonden gegevens, tenzij de overheidsinstantie aantoont dat dit ontoereikend is om te voldoen aan de uitzonderlijke noodzaak. In zulke gevallen moeten de gegevens worden gepseudonimiseerd en moet de overheidsinstantie maatregelen vaststellen om de gegevens te beschermen. De gegevensverwerking moet zowel in lijn met de eisen uit de Dataverordening als in lijn met de AVG en ander Unierecht en nationaal recht ter bescherming van persoonsgegevens en de persoonlijke levenssfeer plaatsvinden. Voor de verwerking van gezondheidsgegevens geldt dat dit bijzondere persoonsgegevens zijn in de zin van de AVG en dat zij daarmee extra bescherming genieten..

De tweede situatie waarin sprake is van een uitzonderlijke noodzaak is wanneer het ontbreken van de specifieke gegevens een overheidsinstantie ervan weerhoudt een wettelijke 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 datacoördinator¹⁰ in de lidstaat waar de verzoekende overheidsinstantie is gevestigd. De datacoördinator maakt alle verzoeken online openbaar, tenzij dit een risico voor de openbare veiligheid oplevert. De bevoegde autoriteit, in Nederland de Autoriteit Persoonsgegevens, kan de rechtmatigheid van het verzoek beoordelen en indien nodig handhavend optreden. 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 mkb¹¹, 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 wettelijke 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 statistiekbureaus 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 statistiekbureaus 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 of wanneer een EU-instelling voornemens is gegevens op te vragen bij een gegevenshouder, informeert zij eerst de bevoegde autoriteit van die lidstaat. De bevoegde autoriteit onderzoekt het verzoek en kan het vervolgens doorsturen naar de gegevenshouder of afwijzen.

¹⁰ De datacoördinator is de autoriteit die onder de verordening verantwoordelijk is voor de samenwerking tussen de verschillende bevoegde toezichthouders (zie paragraaf 3.9).

¹¹ Zoals aangemerkt in artikel 3 van de bijlage bij Aanbeveling 2003/361/EG.

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 paragraaf van de 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 edgetechnologie¹² worden aangeboden, zowel cloudinfrastructuurdiensten als 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 overstappen¹³ 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

¹² 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 clouddiensten worden gegevens op een centrale locatie verwerkt.

¹³ Artikelen 23(d) 30(1) en 30(3) uit de verordening

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

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 worden 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 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, waarbij het derde land en de EU en/of de lidstaat partij is. 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 het 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. Het Europees Comité voor gegevensinnovatie (zie paragraaf 3.8 van de memorie van toelichting) adviseert en assisteert de Commissie bij het opstellen van richtsnoeren voor de beoordeling van de vraag of aan deze voorwaarden wordt voldaan.

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 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 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 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 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 datageletterdheid¹⁴ 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 (tenzij de datacoördinator van oordeel is dat een dergelijke publicatie een risico voor de openbare veiligheid zou opleveren), en bevordert de datacoördinator vrijwillige overeenkomsten voor het delen van gegevens tussen overheidsinstanties en datahouders. Met betrekking tot bedrijfsgeheimen stelt de datacoördinator de 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. De datacoördinator moet natuurlijke en rechtspersonen op verzoek alle benodigde informatie verstrekken om hun klachten bij de juiste bevoegde autoriteit in te dienen. Die autoriteiten moeten worden verplicht samen te werken om ervoor te zorgen dat een klacht naar behoren wordt behandeld en doeltreffend en tijdig wordt opgelost. De bevoegde autoriteiten kunnen gebruik maken van het samenwerkingsnetwerkmechanisme voor consumentenbescherming uit Verordening (EU) 2017/2394¹⁵ (artikel 47 verordening). Ook is een representatieve vordering mogelijk overeenkomstig Richtlijn (EU) 2020/1828¹⁶ (artikel 48 verordening).

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. Bovendien is in sommige situaties ook geschillenbeslechting mogelijk (zie paragraaf 3.2 van de memorie van toelichting).

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.

¹⁴ 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.

¹⁵ Verordening (EU) 2017/2394 van het Europees Parlement en de Raad van 12 december 2017 betreffende samenwerking tussen de nationale autoriteiten die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming en tot intrekking van Verordening (EG) nr. 2006/2004 (PbEU 2017, L 345).

¹⁶ Richtlijn (EU) 2020/1828 van het Europees Parlement en de Raad van 25 november 2020 betreffende representatieve vorderingen ter bescherming van de collectieve belangen van consumenten en tot intrekking van Richtlijn 2009/22/EG (PbEU 2020, L 409).

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 handhavingsmaatregelen 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.

Toezicht persoonsgegevens

De toezichthoudende autoriteiten die verantwoordelijk zijn voor het toezicht op de AVG, zijn verantwoordelijk voor de 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 en V 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 (onderdeel III) 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 is verantwoordelijk voor de algemene uitvoering van de verordening, met uitzondering van de bepalingen waarvoor de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties of de Staatssecretaris voor Rechtsbescherming verantwoordelijk zijn. 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 staatssecretaris is tevens coördinerend verantwoordelijk voor het verzelfstandigingsbeleid van de Rijksoverheid en daarom ook om die reden betrokken bij het toebedelen van nieuwe taken aan de ACM en de AP. De Staatssecretaris voor Rechtsbescherming is verantwoordelijk voor databankregelgeving (hoofdstuk X). De Uitvoeringswet wordt daarom medeondertekend door de Staatssecretaris voor Rechtsbescherming en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties. Deze memorie van toelichting is namens alle drie deze bewindspersonen opgesteld.

4.1 Aanwijzen bevoegde autoriteiten

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

Het uitgangspunt bij de uitvoering van wettelijke taken in Nederland, is 'publiek, tenzij'. Dat wil zeggen dat taken worden belegd bij een organisatie die onder de ministeriële verantwoordelijkheid valt, zodat democratische controle kan plaatsvinden, tenzij er overtuigende redenen zijn om dit niet te doen. Artikel 37, achtste lid, van de verordening stelt echter eisen aan de 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.

Organisaties die vallen onder de volledige ministeriële verantwoordelijkheid, voldoen niet aan deze onafhankelijkheidseisen. Om die reden, kunnen deze taken alleen worden belegd bij een of meerdere zelfstandige bestuursorganen (zbo's) die zijn uitgezonderd van de mogelijkheid om instructies te ontvangen voor individuele gevallen.

Autoriteit Consument en Markt

De Autoriteit Consument en Markt (hierna: ACM) wordt in de Uitvoeringswet (artikel 3, eerste lid) aangewezen als de bevoegde autoriteit voor hoofdstukken II (met uitzondering van artikelen 4, twaalfde lid, en 5, zevende en achtste lid, 6, eerste lid (voor zover het de verwerking van persoonsgegevens betreft) en tweede lid, onderdeel b, van de verordening), III, IV, artikel 20, VI, VII en VIII, en artikel 37, elfde en twaalfde lid, van de verordening. De ACM voldoet als zbo aan de onafhankelijkheidseisen uit de verordening. De ACM heeft 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 ACM heeft immers al een toezichtsfunctie op het gebied van telecom en wordt in diverse andere wetsvoorstellen aangewezen als bevoegd orgaan en toezichthouder op digitaliseringsgebied. Zie daartoe onder andere de Uitvoeringswet datagovernanceverordening, de Uitvoeringswet digitale dienstenverordening en de Uitvoeringswet digitale marktenverordening. De ACM heeft daarmee de vereiste ervaring op het gebied van gegevens en elektronische communicatiediensten (artikel 37, vierde lid, onderdeel b, van de verordening). 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.

De keuze voor ACM als bevoegde autoriteit op een groot deel van de verordening sluit aan bij de rol van de ACM als coördinerend toezichthouder op de Datagovernanceverordening. De verordening heeft ook raakvlakken met de AVG, maar de AVG en de verordening hebben uiteenlopende doelen waardoor het beleggen van beide verordeningen bij één toezichthouder niet meteen voor de hand ligt. De AVG ziet op de bescherming van persoonsgegevens, de verordening beoogt juist een breder gebruik van bepaalde gegevens te stimuleren. Bovendien heeft de verordening naast gegevensbescherming ook raakvlakken met onderwerpen als consumentenbescherming en eerlijke concurrentie, waar ACM ervaring en expertise in heeft.

Het thema 'digitale economie' is bovendien één van de drie thema's die de ACM tot prioriteit heeft bestempeld in haar meest recente uitvoeringsagenda¹⁷. De ACM treedt in dat kader op tegen

¹⁷ Focus Werkzaamheden ACM 2023 | ACM.nl

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 digitale dienstenverordening 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 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 de economische ontwikkeling die gepaard gaat met de groei van de productcategorie verbonden apparaten. In combinatie met bovenstaande redenen maakt dit het aanwijzen van de ACM als toezichthouder op Hoofdstuk II een logische stap. De ACM zal bij dit toezicht ook rekening moeten houden met de uitzondering op het databankrecht (artikel 43 van de verordening).

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 hoofdstukken III en IV van de verordening toezicht van de ACM gewenst is.

Het toezicht op artikel 20 van de verordening betreft vergoeding voor het beschikbaar stellen van gegevens in geval van uitzonderlijke noodzaak en is vergelijkbaar met artikel 9 ten aanzien van vergoedingen voor het beschikbaar stellen van gegevens, en past daarom het beste bij de ACM. De normadressaten van dit artikel betreft gegevenshouders en overheidsinstanties, de Commissie, de Europese Centrale Bank of het orgaan van de Unie die gegevens hebben ontvangen in geval van uitzonderlijke noodzaak.

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.

Artikel 37, elfde en twaalfde lid, van de verordening heeft betrekking op de wettelijke vertegenwoordigers van entiteiten die binnen het toepassingsgebied van de verordening vallen. Gezien de ACM de bevoegde autoriteit voor een groot deel van de verordening is en als datacoördinator wordt aangewezen (zie paragraaf 4.3 van het algemene deel van de toelichting) is het wenselijk de ACM bevoegd te maken voor deze bepalingen.

Autoriteit Persoonsgegevens

De Autoriteit Persoonsgegevens (hierna: AP) is, als toezichthoudende autoriteit die verantwoordelijk is voor het toezicht op de AVG, verantwoordelijk voor de toepassing van de verordening wat betreft de bescherming van persoonsgegevens (artikel 37, derde lid, van de verordening). De AP wordt in de Uitvoeringswet (artikel 3, derde en vijfde lid) aangewezen als de bevoegde autoriteit voor artikelen 4, twaalfde lid, en 5, zevende en achtste lid, 6, eerste lid (voor zover het de verwerking van persoonsgegevens betreft) en tweede lid, onderdeel b, en hoofdstuk V (met uitzondering van artikel 20) van de Dataverordening. De AP voldoet als zbo aan de onafhankelijkheidseisen uit de verordening.

Het toezicht op artikelen 4, twaalfde lid, van de Dataverordening ziet op de grondslag voor de verwerking van persoonsgegevens. In artikel 4, twaalfde lid, van de Dataverordening staat 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. Artikel 5, achtste lid, van de Dataverordening betreft de rechten van betrokkenen op grond van de AVG. Artikel 6, eerste lid, van de Dataverordening bepaalt dat de derde de ontvangen gegevens niet voor andere doeleinden of onder andere voorwaarden mag verwerken dan met de gebruiker zijn overeengekomen, dat het Unierecht en nationale recht inzake de bescherming van persoonsgegevens in acht moet worden genomen, met inbegrip van de rechten van betrokkenen op grond van de AVG. Artikel 6, tweede lid, onderdeel b, van de Dataverordening bepaalt dat de derde de ontvangen gegevens niet gebruikt voor profilering als bedoeld in artikel 4, vierde lid, van de AVG, niettegenstaande artikel 22, tweede lid, onderdelen a en c, AVG, tenzij dit noodzakelijk is om de door de gebruiker gevraagde dienst te verlenen. De bepalingen zien op het beschermen van persoonsgegevens en uitleg van AVG-begrippen en vallen daarom onder het toezicht van de AP.

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.¹⁸

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).

¹⁸ AP jaarplan 2024 | Autoriteit Persoonsgegevens

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, en veertiende lid, 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 daarom 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 verordening. 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.

Artikel 8 van de Uitvoeringswet bepaalt dat bij overtreding van de verordening de ACM en de AP een bestuurlijke boete en een last onder bestuursdwang, en daarmee ook een last onder dwangsom, kunnen opleggen.

De hoogte van de boete sluit deels aan bij de bestaande praktijk rondom bestuurlijke boetes. Voor de hoogte van de maximale boete voor de ACM wordt aangesloten bij de boetebepalingen in de Uitvoeringswet datagovernanceverordening. Deze wet kan worden gezien als aangrenzend rechtsgebied gelet op de taken voor de ACM op het terrein van digitalisering. 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 in de Europese Unie. 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.

Gelet op artikel 40, derde lid, onderdeel f, van de verordening moet worden uitgegaan van de jaaromzet van de inbreukmakende partij in het voorgaande boekjaar in de Europese Unie. Dit sluit grotendeels aan op artikel 12o, eerste lid, van de Instellingswet ACM dat onder omzet van de overtreder wordt verstaan de netto-omzet, bedoeld in artikel 377, zesde lid, van Boek 2 van het Burgerlijk Wetboek die de overtreder heeft behaald in het meest recente boekjaar ten aanzien waarvan de overtreder een jaarrekening beschikbaar heeft of zou moeten hebben. Het betreft de opbrengst uit levering van goederen en diensten uit het bedrijf van de rechtspersoon, onder aftrek van kortingen en dergelijke en van over de omzet geheven belastingen.

De in de Uitvoeringswet gekozen systematiek wijkt af van de Boetebeleidsregel ACM 2014. Daarin staat dat het in principe gaat om de in Nederland behaalde omzet (artikel 2.6, eerste lid), tenzij dit naar het oordeel van de ACM geen passende beboeting toelaat, dan gaat het om de wereldwijde omzet (artikel 2.6, tweede lid). Daar het echter een bepaling uit de verordening is die vastlegt dat sanctionering op basis van de omzet in de Europese Unie geschied achten we deze afwijking opportuun.

Gelet op artikel 40, vierde lid, van de verordening betreft de hoogte van de bestuurlijke boete die de AP kan opleggen, een maximum van 20 miljoen euro of voor een onderneming 4% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit een hoger bedrag vertegenwoordigt. Hiermee wordt aangesloten op de sanctionering van AVG overtredingen en de boetebeleidsregels van de AP.

Voor entiteiten die in Nederland zijn gevestigd geldt dat in het geval van overtredingen de bevoegde autoriteit bevoegd is uit de lidstaat waar de entiteit is gevestigd. Als een entiteit in Nederland is gevestigd gaat het dus om de ACM of AP. Zowel voor sanctionering door de ACM als door de AP geldt dat een bedrijf dat in meerdere lidstaten omzet behaalt slechts in één lidstaat sancties kan worden

opgelegd. Hierbij wordt, zoals hierboven beschreven staat, dus wel uitgegaan van de jaaromzet in de gehele Europese Unie.

De ACM en de AP moeten bij het opleggen van boetes rekening houden met het *ne bis in idem*-beginsel. Dit beginsel is in artikel 50 van het Handvest van de grondrechten van de Europese Unie verankerd en houdt in dat een (rechts)persoon niet nogmaals mag worden vervolgd of bestraft wanneer dezelfde (rechts)persoon voor dezelfde gedraging (*idem*) reeds op basis van een eerdere definitieve beslissing is veroordeeld of vrijgesproken (*bis*). Daarnaast kan strijd met het *ne bis in idem*-beginsel achteraf door de rechter worden gecorrigeerd. Indien achteraf toch sprake blijkt te zijn van een inbreuk op het *ne bis in idem*-beginsel, kan artikel 52 van het Handvest van de grondrechten van de Europese Unie hiervoor nog een rechtvaardiging bieden. Via dit artikel kan een inbreuk worden gerechtvaardigd, indien: (i) het optreden van de autoriteiten bij wet is voorzien (ii) het gaat om een cumulatie op grond van verschillende regelingen, welke verschillende en aanvullende doelstellingen nastreven, en (iii) het evenredigheidsbeginsel wordt gerespecteerd. Met de Uitvoeringswet wordt aan het eerste vereiste in ieder geval voldaan. Artikel 5 van de Uitvoeringswet bepaalt de bevoegdheid van de ACM en de AP om te verordening te kunnen handhaven. Daarnaast heeft de AP handhavende bevoegdheden met betrekking tot de AVG. Voor de andere twee vereisten zijn de omstandigheden van het geval bepalend. Het is aan de rechter om te bepalen of een eventuele inbreuk op het *ne bis in idem*-beginsel kan worden gerechtvaardigd.

Samenwerking met andere autoriteiten

De bevoegde autoriteiten moeten samenwerken met andere autoriteiten. Het gaat hier om samenwerking tussen (1) de bevoegde autoriteiten in Nederland (ACM en AP), en (2) de bevoegde autoriteiten die verantwoordelijk zijn voor de uitvoering van andere Unie- of nationale rechtshandelingen (zoals de Autoriteit Persoonsgegevens voor de AVG en sectorale toezichthouders) en (3) de bevoegde autoriteiten van andere lidstaten, de Commissie en het Europees Comité voor gegevensinnovatie. Dit laatste wordt geregeld in de verordening, zie verder paragraaf 3.8 van het algemeen deel van de toelichting. Om deze samenwerking tussen de bevoegde autoriteiten (ACM, AP en sectorale toezichthouders) te vergemakkelijken regelt de Uitvoeringswet dat afspraken in een samenwerkingsprotocol gemaakt kunnen worden.

(1) Samenwerking tussen de ACM en de AP: Samenwerking tussen de ACM en de AP is nodig, aangezien 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. De Dataverordening doet geen afbreuk aan de AVG en de bevoegdheden van de AVG-toezichthouder (artikel 1, vijfde lid, van de verordening). Alle verwerkingen van persoonsgegevens die op basis van de verordening plaatsvinden moeten onverminderd voldoen aan de AVG. Samenwerking kan nodig zijn gelet op de taken en bevoegdheden van de ACM en de AP uit de Dataverordening en de AVG¹⁹. Het kan bijvoorbeeld gaan om afstemming ten aanzien van een uniforme uitleg van de Dataverordening, de vraag of in de praktijk in overeenstemming met de AVG wordt gehandeld of afstemming als de toezichthouders gelijktijdig dezelfde overtreding onderzoeken. Om de samenwerking tussen de ACM en de AP goed te laten verlopen regelt de Uitvoeringswet (artikel 6, eerste lid) dat de ACM en de AP bevoegd zijn om in het belang van een efficiënt en effectief toezicht op de Dataverordening afspraken te maken en daartoe gezamenlijk samenwerkingsprotocollen vast te stellen. Hierin dienen de toezichthouders ook afspraken te maken met betrekking tot het *ne bis in idem*-beginsel. In het geval van hetzelfde feitencomplex is het van belang dat dubbele beboeting door de ACM en AP wordt voorkomen. Een verdere inkadering en formalisering van de samenwerking dan de bevoegdheid om samenwerkingsprotocollen vast te stellen is overwogen maar acht het kabinet niet wenselijk. Het is belangrijk om de ACM en de AP de ruimte te geven om zelf invulling te geven aan de samenwerking. De samenwerking wordt geëvalueerd (zie paragraaf 7 van het algemeen deel van de toelichting).

(2) Samenwerking met sectorale toezichthouders: Bij de uitoefening van het toezicht is in sommige gevallen echter ook de expertise van een andere toezichthouder of instantie noodzakelijk. Zo heeft de Rijksinspectie Digitale Infrastructuur (hierna: RDI) relevante expertise op het terrein van cybersecurity voor het toezicht op de 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

¹⁹ 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.

expertise bezit die de bevoegde autoriteit niet in huis heeft, bijvoorbeeld op het gebied van bepaalde typen verbonden apparaten zoals medische apparatuur. Met welke toezichthouders en instanties de bevoegde autoriteiten zullen moeten samenwerken kan in de loop van de tijd veranderen naar mate er in aanvulling op hoofdstukken 2, 3 en 4 van de verordening meer sectorale wetgeving over gegevensdeling komt. Zo zal de verordening betreffende de Europese ruimte voor gezondheidsgegevens²⁰ binnenkort in Nederland moeten worden geïmplementeerd en bereidt de Commissie wetgeving met betrekking tot toegang tot voertuiggegevens²¹ voor. Wanneer deze en andere sectorale wetgeving van toepassing zal zijn, zal dit voor de bevoegde autoriteiten voor de verordening samenwerking met nieuwe instanties vergen of de samenwerking met bepaalde instanties veranderen.

Gegevensuitwisseling tussen toezichthouders

Voor de samenwerking is gegevensuitwisseling tussen ACM en AP en andere toezichthouders noodzakelijk.

(1) Gegevensuitwisseling tussen de ACM en de AP: ACM en AP zullen gezien hun samenwerking als bevoegde autoriteiten en datacoördinator onderling meer structureel gegevens moeten uitwisselen. Zo zal de ACM wanneer zij wil afstemmen met de AP over toepassing van de AVG mogelijk informatie over een casus met de AP moeten delen. Het gaat bijvoorbeeld om gegevensuitwisseling voor de afhandeling van een klacht of onderzoek naar de toepassing van de verordening. De gegevensuitwisseling ziet op gewone persoonsgegevens namelijk naam en contactgegevens voor communicatie met de betrokkene, leeftijd en geboortedatum om de identiteit van betrokkene te kunnen verifiëren en apparaat- en internetgegevens (zoals IP-adres en metadata) om te duiden waar de klacht of het onderzoek op ziet. Om die gegevensuitwisseling te faciliteren creëert de Uitvoeringswet (artikel 6, tweede lid) een grondslag voor de bevoegde autoriteiten om de informatie uit te wisselen die relevant is voor het toezicht op de verordening.

(2) Samenwerking met sectorale toezichthouders: Toezichthouders kunnen al incidenteel informatie uitwisselen met andere toezichthouders (artikel 5:16 Awb). Daarnaast kan het voorkomen dat de ACM als datacoördinator en toezichthouder op hoofdstukken II, III en IV van de verordening voor de samenwerking met andere bevoegde autoriteiten en instanties meer structureel gegevens moet kunnen uitwisselen. Het gaat om toezichthouders en instanties die specifieke kennis hebben (zoals de RDI met cybersecurity kennis) die de ACM nodig heeft voor het toezicht op de verordening en om toezichthouders die toezicht houden op (toekomstige) gegevenswetgeving die raakvlakken heeft met de verordening. Gezien de aankomende wetgeving met betrekking tot gegevensdeling is te voorzien dat in de loop van de tijd zal veranderen met welke toezichthouders en instanties de ACM gegevens moet kunnen uitwisselen om toezicht te houden op de verordening. Het is daarom noodzakelijk dat de grondslag voor gegevensuitwisseling tussen ACM en andere instanties kan worden aangepast. De Uitvoeringswet (artikel 7, tweede lid) legt om die reden vast dat per ministeriële regeling een grondslag voor het delen van gegevens voor andere bevoegde autoriteiten kan worden gecreëerd in het kader van toezicht op de verordening.

(3) Samenwerking met de bevoegde autoriteiten van andere lidstaten, de Commissie, het Europees Comité voor gegevensinnovatie: De grondslag voor informatie-uitwisseling met bevoegde autoriteiten uit andere lidstaten, de Commissie en het Europees Comité voor gegevensinnovatie volgt rechtsreeks uit de verordening (artikel 37, vijfde lid, onderdeel f).

De verordening bepaalt expliciet dat de bevoegde autoriteiten het vertrouwelijkheidsbeginsel, het beroeps- en handelsgeheim, en persoonsgegevens beschermen overeenkomstig het Unie-of nationale recht (artikel 37, zestiende lid, van de verordening). En dat alle informatie die wordt uitgewisseld en wordt verstrekt uitsluitend gebruikt wordt in verband met de aangelegenheid waarvoor zij is gevraagd.

4.3 Aanwijzen datacoördinator

De ACM wordt in de Uitvoeringswet (artikel 4) aangewezen als datacoördinator. De ACM wordt de bevoegde autoriteit op het overgrote deel van de verordening, waardoor de ACM een voor de hand liggende optie is om de samenwerking tussen autoriteiten te faciliteren en ondertoezichtgestelden bij te staan. Bovendien heeft ACM in het kader van de Wet handhaving consumentenbescherming, de Uitvoeringswet datagovernanceverordening en de Uitvoeringswet digitale dienstenverordening al de nodige relevante ervaring met de uitvoering van een coördinerende rol in het kader van toezicht en handhaving. Om deze redenen acht het kabinet de ACM het meest geschikt om de rol van datacoördinator uit te voeren onder de verordening.

²⁰ COM(2022) 197 final, zie eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:52022PC0197&from=NL

²¹ Toegang tot voertuiggegevens, -functies en -hulpmiddelen (europa.eu)

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

4.4 Certificering geschillenbeslechtsorgaan

Gebruikers, gegevenshouders, gegevensontvangers, klanten en aanbieders van dataverwerkingsdiensten hebben toegang tot een gecertificeerd geschillenbeslechtsorgaan om geschillen uit hoofdstukken II, III, IV en VI 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 voornamelijk geen gebruik van gemaakt.

4.5 Advisering bij internationale overheidstoegang en overdracht van niet-persoonsgebonden gegevens

Zoals beschreven in paragraaf 3.6 van het algemeen deel van de toelichting moeten aanbieders van dataverwerkingsdiensten de nationale bevoegde autoriteit voor internationale juridische samenwerking en de bevoegde autoriteiten voor nationale veiligheid en defensie om advies kunnen vragen over het voldoen aan bepaalde besluiten van rechterlijke instanties of administratieve autoriteiten. Aangezien de bevoegdheden omtrent internationale juridische samenwerking als nationale veiligheid en defensie in Nederland verspreid zijn over verschillende organisaties, zal er bij de RVO een loket worden ingericht waar partijen terecht kunnen met hun adviesvragen. De RVO zal waar nodig in samenwerking met de relevante bevoegde autoriteiten adviezen opstellen.

4.6 Rechtsbescherming

De verordening biedt verscheidene soorten van rechtsbescherming. Bij een mogelijke schending van de verordening kan een partij een klacht indienen bij de bevoegde autoriteit, in sommige gevallen ook naar een geschillenbeslechtsorgaan, en kan een partij in beroep tegen het besluiten die de bevoegde autoriteiten nemen (zie paragraaf 3.8 van het algemeen deel van de toelichting).

De Uitvoeringswet (artikel 9) regelt de beroepsmogelijkheden tegen besluiten van de ACM op grond van dit wetsvoorstel. Tegen besluiten van de ACM kan beroep in eerste aanleg bij de Rechtbank Rotterdam worden ingesteld en hoger beroep bij het College van Beroep voor het bedrijfsleven (hierna: CBB). 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.

Tegen besluiten van de AP kan beroep in eerste aanleg bij de rechtbanken en hoger beroep bij de Afdeling bestuursrechtspraak van de Raad van State. Hiermee wordt aangesloten op de bestaande rechtsmachtverdeling als voor AP besluiten onder de AVG. De bepalingen uit de verordening buiten Hoofdstuk V waar de AP als toezichthouder voor is aangewezen hebben ook inhoudelijk raakvlakken met bepalingen uit de AVG. Daarmee wordt beroep tegen AP besluiten neergelegd bij de rechter die daar de meeste expertise voor heeft. Bovendien vergemakkelijkt de mogelijkheid om bij lokale rechtbanken beroep in te stellen de toegankelijkheid van beroepsmogelijkheden voor betrokkenen als burgers en mkb'ers.

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, de regelgeving genoemd in artikel 1, vijfde tot en met tiende lid, van de verordening en in diverse overwegingen van de verordening. In deze paragraaf van de memorie van toelichting wordt hier nader op ingegaan. Daarnaast wordt ingegaan op andere voor deze verordening relevante regelgeving. Het gaat om: AVG en ePrivacy-richtlijn (par. 5.1), EU-verordeningen op het terrein van digitalisering (par. 5.2), Richtlijn bedrijfsgeheimen (par. 5.3), intellectueel eigendomsrecht (par. 5.4), contractenrecht en consumentenrecht (par. 5.5), diverse strafrechtelijke, financiële, defensie en openbare orde regelgeving (par. 5.6), staatsnoodrecht (par. 5.7), regelgeving over hergebruik overheidsinformatie (par. 5.8), statistiek regelgeving (par. 5.9), regeling over interoperabiliteit en normalisatie (par. 5.10) en verbod op misbruik van economische machtspositie (par. 5.11).

De verordening voorziet in horizontale regels. Deze verordening doet geen afbreuk aan het Unierecht, waarin, gebaseerd op specifieke behoeften van een sector, verdere vereisten kunnen worden vastgesteld. Deze vereisten dienen wel rekening te houden met de Dataverordening. Een voorbeeld is de beoogde verordening betreffende de Europese ruimte voor gezondheidsgegevens (EHDS), die specifieke regels bevat waarbij rekening gehouden wordt met de gevoeligheid van gezondheidsgegevens.²² 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.²³ Hier kan worden gedacht aan betaalgegevens in de PSD2-richtlijn²⁴, gegevens over motoren in de Motor verordening²⁵ en elektriciteitsverbruik in de Elektriciteitsrichtlijn²⁶.

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 en ePrivacy-richtlijn

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.

AVG : 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 gegenereerd met een verbonden product of gerelateerde dienst en op verzoek van de gebruikers

²² Voorstel voor een verordening betreffende de Europese ruimte voor gezondheidsgegevens, zie: eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:52022PC0197.

²³ 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.

²⁴ 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).

²⁵ 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).

²⁶ 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).

worden gedeeld met een derde partij (artikelen 4, 5 en 6 van de verordening).

Rechtmatig: elke verwerking van persoonsgegevens op grond van deze verordening moet een geldige rechtsgrond hebben in de zin van artikel 6 van de AVG (en in voorkomend geval de voorwaarden van artikel 9 AVG en artikel 5, derde lid, ePrivacy-richtlijn). De verordening vormt geen rechtsgrond voor het verzamelen of genereren van persoonsgegevens door de gegevenshouder (overweging 7 van de verordening). In plaats daarvan legt deze verordening gegevenshouders de verplichting op om persoonsgegevens beschikbaar te stellen aan gebruikers of derden naar keuze van de gebruiker, op verzoek van die gebruiker. Dergelijke toegang moet worden verleend tot persoonsgegevens die door de gegevenshouder worden verwerkt op basis van een AVG-rechtsgrondslag. Tenzij de AVG anders bepaalt mag de derde de gegevens die door het gebruik van een verbonden product of een gerelateerde dienst zijn gegenereerd alleen met een andere derde delen indien dat gebeurt op grond van een overeenkomst met de gebruiker (artikel 6, tweede lid, sub a van de verordening). 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 (overweging 38 verordening). Indien de gebruiker geen datasubject is, schept deze verordening echter geen rechtsgrond om toegang te verlenen tot persoonsgegevens of persoonsgegevens ter beschikking te stellen van een derde, en mag zij niet worden opgevat als een verlening van een nieuw recht aan de gegevenshouder om persoonsgegevens te gebruiken die door het gebruik van een verbonden product of een gerelateerde dienst zijn gegenereerd. Ook dan moet er een geldige rechtsgrond uit artikel 6 AVG bestaan (artikelen 4, twaalfde lid, en 5, zevende lid, van de verordening).

Doelbinding: vergelijkbaar met de AVG bepaalt de verordening dat de gegevenshouder niet-persoonsgebonden productgegevens niet beschikbaar stelt aan derden voor andere doeleinden dan de uitvoering van zijn overeenkomst met de gebruiker (artikel 4, veertiende lid, van de verordening). De derde mag gegevens die op verzoek van een gebruiker aan hem ter beschikking zijn gesteld alleen verwerken voor de met de gebruiker overeengekomen doeleinden (artikel 6, eerste lid, van de verordening).

Beginsel van minimale gegevensverwerking: de gegevenshouder mag alleen informatie opvragen en bewaren over een persoon voor zover dat nodig is voor de goede uitvoering van het toegangsverzoek van een gebruiker of derde en voor de beveiliging en het onderhoud van de data-infrastructuur (artikelen 4, vijfde lid, en 5, vierde lid, van de verordening). In lijn met het beginsel van minimale gegevensverwerking mogen derden alleen toegang hebben tot de informatie die nodig is voor de levering van de aan de gebruiker gevraagde dienst (overweging 38).

Opslagbeperking: de derde moet de gegevens verwijderen indien ze niet langer nodig zijn voor het overeengekomen doel, tenzij anders is overeengekomen met de gebruiker (artikel 6, eerste lid, van de verordening).

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 (Hoofdstuk V van de verordening). 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).

AVG: Rechten van betrokkene, waaronder recht op inzage en dataportabiliteit

De verordening doet geen afbreuk aan de AVG-rechten van datasubjecten (artikel 1, vijfde lid, van de verordening en zie ook artikelen 5, dertiende lid, en 6, eerste lid, van de verordening). Ook het verzuim van de gegevenshouder en de derde om regelingen voor het doorgeven van de gegevens overeen te komen, mag de uitoefening van AVG-rechten niet belemmeren, beletten of verstoren (artikel 5, achtste lid, van de verordening).

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.

Profilering: in artikel 22, eerste lid, AVG staat het recht voor betrokkenen om niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft. Ook gaat de verordening in op profilering (artikel 6, tweede lid, onderdeel b, van de verordening). 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.

ePrivacy-richtlijn

Richtlijn 2002/58/EG²⁷ (hierna: ePrivacy-richtlijn) beschermt het privéleven en de vertrouwelijkheid van communicatie. Deze verordening vormt een aanvulling op en doet geen afbreuk aan de ePrivacy-richtlijn. Geen enkele bepaling van deze verordening mag zodanig worden toegepast of uitgelegd dat het recht op privacy en vertrouwelijkheid van communicatie wordt beperkt. Elke verwerking van persoonsgegevens op grond van deze verordening moet voldoen aan de gegevensbeschermingswetgeving van de Unie, met inbegrip van de voorwaarden artikel 5, derde lid, van de ePrivacy-richtlijn. Dit artikel is in Nederland geïmplementeerd in artikel 11.7a, eerste lid, van de Telecommunicatiewet: 'Onverminderd de AVG is het via een elektronisch communicatienetwerk opslaan van of toegang verkrijgen tot informatie in de randapparatuur van een gebruiker, alleen toegestaan op voorwaarde dat de betrokken gebruiker: (a) is voorzien van duidelijke en volledige informatie overeenkomstig de AVG, in ieder geval over de doeleinden waarvoor deze informatie wordt gebruikt, en (b) daarvoor toestemming heeft verleend.'

De ePrivacy-richtlijn beschermt ook de integriteit van de eindapparatuur van de gebruiker wat betreft het gebruik van verwerkings- en opslagmogelijkheden en het verzamelen van informatie. Apparaat voor verbonden producten wordt als eindapparatuur beschouwd indien deze direct of indirect verbonden is met een openbaar communicatienetwerk. Deze richtlijn stelt voorwaarden aan de opslag van en de toegang tot persoonsgegevens en niet-persoonsgebonden gegevens in eindapparatuur. Het vereist de toestemming van de abonnee of gebruiker in de zin van die richtlijn, tenzij toegang strikt noodzakelijk is voor de levering van een uitdrukkelijk door de gebruiker of de abonnee gevraagde dienst van de informatiemaatschappij of uitsluitend de doorgifte van een communicatie tot doel heeft.

²⁷ Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (PbEG 2002, L 201).

5.2 Datagovernanceverordening, Digitale marktenverordening, Digitaal dienstenverordening, Artificial intelligence verordening en 'Platform-to-Business' verordening

Datagovernanceverordening

De Datagovernanceverordening²⁸ (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.

Free Flow of Data-verordening

De verordening voor het vrije verkeer van niet-persoonsgebonden gegevens (hierna: *Free Flow of Data*-verordening)²⁹ beoogt het vrije verkeer van niet-persoonsgebonden gegevens binnen de Europese Unie te waarborgen door regels vast te leggen met betrekking tot gegevenslokalisatievereisten, de beschikbaarheid van gegevens voor bevoegde autoriteiten en de portabiliteit van gegevens voor professionele gebruikers. Die verordening moedigt aanbieders van dataverwerkingsdiensten aan om zelfregulerende gedragscodes te ontwikkelen die beste praktijken bevatten voor onder meer een gemakkelijkere overstap naar een andere aanbieder van dataverwerkingsdiensten en het overdragen van gegevens.

Aangezien er slechts beperkt gebruik wordt gemaakt van de zelfregulerende kaders die er naar aanleiding daarvan zijn ontwikkeld, en er een algemene gebrek is aan open normen en interfaces, is het noodzakelijk om in de Dataverordening een reeks minimale wettelijke verplichtingen voor aanbieders van dataverwerkingsdiensten vast te stellen ter uitbanning van precommerciële, commerciële, technische, contractuele en organisatorische belemmeringen – zoals, maar niet uitsluitend, vertraagde dataoverdracht bij het vertrek van een klant – die een doeltreffende overstap tussen dataverwerkingsdiensten bemoeilijken.

²⁸ 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).

²⁹ Verordening (EU) 2018/1807 van het Europees Parlement en de Raad van 14 november 2018 inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie (PbEU 2018, L 303).

Digitalemarktenverordening

De digitalemarktenverordening³⁰ (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, 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 digitaledienstenverordening³¹ (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 Artificiële intelligentieverordening (hierna: AI-verordening)³² 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

³⁰ Verordening (EU) 2022/1925 over betwistbare en eerlijke markten in de digitale sector (de digitalemarktenverordening) (PbEU 2022, L 265).

³¹ 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).

³² 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).

van toepassing op de ontwikkeling en het gebruik van AI-systemen.

'Platform-to-business verordening

De Verordening Platform-to-Business³³ (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 bedrijfsgeheimen³⁴ 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 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 geschillenbeslechtscommissie. 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 Databankrichtlijn³⁵, 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 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

³³ 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).

³⁴ 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).

³⁵ Richtlijn 96/9/EG van het Europees Parlement en de Raad van 11 maart 1996 betreffende de rechtsbescherming van databanken (PbEG 1996, L 77).

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, met name Richtlijn 93/13/EEG³⁶ (hierna: Richtlijn oneerlijke bedingen in consumentenovereenkomsten), Richtlijn 2005/29/EG³⁷ (hierna: Richtlijn oneerlijke handelspraktijken) en Richtlijn 2011/83/EU³⁸ (hierna: Richtlijn consumentenrechten).

Contractvoorwaarden gegevensdeling

Op basis van het beginsel van contractvrijheid blijft het partijen vrijstaan om, binnen het kader van algemene regels voor het beschikbaar stellen van gegevens, bij hun overeenkomsten te onderhandelen over de precieze voorwaarden 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. Volgens het Nederlandse recht is daaraan ook voldaan als de gegevenshouder in zijn voorwaarden, waarmee de gebruiker bij het aangaan van de overeenkomst heeft ingestemd, een wijzigingsbeding heeft opgenomen. Daarbij geldt wel de eis dat de wijziging redelijk moet zijn. Ook moeten de nieuwe voorwaarden kenbaar zijn gemaakt aan de gebruiker en moeten zij na de vaste looptijd ingaan. Indien de gegevenshouder zich niet aan deze eisen houdt, kan de gebruiker de aanpassing in de overeenkomst laten vernietigen, waarmee zij ongeldig wordt.

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.

In overeenkomsten tussen een gegevenshouder en een consument als gebruiker van een verbonden product of gerelateerde dienst die gegevens genereert, is het consumentenrecht van de Unie, met name de Richtlijn oneerlijke bedingen in consumentenovereenkomsten en de Richtlijn oneerlijke handelspraktijken, van toepassing om ervoor te zorgen dat een consument niet onderworpen is aan oneerlijke contractvoorwaarden.

³⁶ Richtlijn 93/13/EEG van de Raad van 5 april 1993 betreffende oneerlijke bedingen in consumentenovereenkomsten (PbEG 1993, L 95).

³⁷ Richtlijn 2005/29/EG van het Europees Parlement en de Raad van 11 mei 2005 betreffende oneerlijke handelspraktijken van ondernemingen jegens consumenten op de interne markt en tot wijziging van Richtlijn 84/450/EEG van de Raad, Richtlijnen 97/7/EG, 98/27/EG en 2002/65/EG van het Europees Parlement en de Raad en van Verordening (EG) nr. 2006/2004 van het Europees Parlement en de Raad ('Richtlijn oneerlijke handelspraktijken') (PbEU 2005, L149).

³⁸ Richtlijn 2011/83/EU van het Europees Parlement en de Raad van 25 oktober 2011 betreffende consumentenrechten, tot wijziging van Richtlijn 93/13/EEG van de Raad en van Richtlijn 1999/44/EG van het Europees Parlement en de Raad en tot intrekking van Richtlijn 85/577/EEG en van Richtlijn 97/7/EG van het Europees Parlement en de Raad (PbEU L 304/64).

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 van een verbonden product of gerelateerde dienst die gegevens genereert, het Europese consumentenrecht (met name Richtlijn oneerlijke bedingen in consumentenovereenkomsten en Richtlijn oneerlijke handelspraktijken) van toepassing is om ervoor te zorgen dat een consument niet onderworpen is aan oneerlijke contractvoorwaarden. Uit de Richtlijn oneerlijke bedingen in consumentenovereenkomsten jo. artikel 6.233 BW volgt dat consumenten zich kunnen beschermen tegen oneerlijke bedingen door de mogelijkheid tot vernietiging van het oneerlijke beding. Daarnaast toetst de rechter ambtshalve op de vernietigbaarheid van oneerlijke bedingen. Ook kan de ACM gelet op de Wet handhaving consumentenrechten handhaven (zie artikel 11 van de Uitvoeringswet).

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. Daarnaast kunnen natuurlijke personen en rechtspersonen op grond van de verordening ook een klacht indienen bij de bevoegde autoriteit als hun rechten uit de verordening worden geschonden (paragraaf 3.8 van het algemeen deel van de toelichting).

Verdere (consumenten)bescherming gebruikers

Derden noch gegevenshouders mogen de uitoefening van keuzes of rechten door de gebruiker onnodig moeilijk maken, door de gebruiker op niet-neutrale wijze keuzemogelijkheden aan te bieden, of door de gebruiker op enigerlei wijze te dwingen, te misleiden of te manipuleren, of door de autonomie, besluitvorming of keuzes van de gebruiker te ondermijnen of te beperken, onder meer door middel van een digitale gebruikersinterface of een deel daarvan (artikelen 4, vierde lid, en 6, tweede lid, onderdeel a, van de verordening). In dat verband mogen derden of gegevenshouders zich bij het ontwerpen van hun digitale interfaces niet baseren op donkere patronen, ontwerptechnieken die consumenten aanzetten tot beslissingen die negatieve gevolgen voor hen hebben. Gangbare en legitieme handelspraktijken die in overeenstemming zijn met het Unierecht, mogen op zichzelf niet als donkere patronen worden beschouwd. Derden en gegevenshouders moeten voldoen aan hun verplichtingen uit hoofde van het toepasselijke Unierecht, met name de vereisten die zijn vastgesteld in Richtlijn 98/6/EG³⁹, Richtlijn 2000/31/EG⁴⁰, Richtlijn oneerlijke handelspraktijken en Richtlijn consumentenrechten.

³⁹ Richtlijn 98/6/EG van het Europees Parlement en de Raad van 16 februari 1998 betreffende de bescherming van de consument inzake de prijsaanduiding van aan de consument aangeboden producten (PbEG 1998, L 80).

Contractvoorwaarden betreffende overstappen en interoperabiliteit

In hoofdstuk VI van de verordening worden eisen gesteld aan contractvoorwaarden betreffende een overstap naar een andere aanbieder van dataverwerkingsdiensten of naar een on-premises-ICT-infrastructuur (artikel 25). De rechten van de klant en de verplichtingen van de aanbieder van dataverwerkingsdiensten moeten in een schriftelijk contract duidelijk zijn vastgesteld. Dit contract moet voldoen aan Richtlijn (EU) 2019/770⁴¹ (hierna: Richtlijn levering digitale inhoud), geïmplementeerd in Boek 7 Titel 1aa van het Burgerlijk Wetboek, en de in artikel 25 van de verordening gestelde voorwaarden. Bestaande rechten in verband met de beëindiging van overeenkomsten, waaronder de rechten die zijn ingevoerd bij de AVG en de Richtlijn levering digitale inhoud, moeten onverlet worden gelaten. De verordening mag niet worden opgevat als een beletsel voor een aanbieder van dataverwerkingsdiensten om klanten nieuwe en verbeterde diensten, kenmerken en functionaliteiten aan te bieden of om daarop met andere aanbieders van dataverwerkingsdiensten te concurreren.

Daarnaast bevat de verordening voor aanbieders van dataverwerkingsdiensten informatieverplichtingen (artikelen 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 uit de verordening die rechtstreeks werken en in lijn zijn met Nederlands recht.

Slimme contracten

In paragraaf 3.7 van het algemeen deel van de toelichting is toegelicht wat slimme contracten zijn en welke essentiële eisen de verordening (artikel 36) daaraan stelt. De essentiële eisen zijn van toepassing op de verkopers van slimme contracten, behalve als zij binnen hun bedrijf slimme contracten voor uitsluitend intern gebruik ontwikkelen. De essentiële eis dat slimme contracten moeten kunnen worden onderbroken en beëindigd, impliceert wederzijdse instemming van de partijen bij de overeenkomst inzake het delen van gegevens. Het gebruik van slimme contracten voor de geautomatiseerde uitvoering van gegevensdelingsovereenkomsten laat de toepasselijkheid van de relevante regels van burgerlijk, contractueel en consumentenbeschermingsrecht op dergelijke overeenkomsten onverlet.

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.

⁴⁰ Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt ('Richtlijn inzake elektronische handel') (PbEG 2000, L 178).

⁴¹ Richtlijn (EU) 2019/770 van het Europees Parlement en de Raad van 20 mei 2019 betreffende bepaalde aspecten van overeenkomsten voor de levering van digitale inhoud en digitale diensten (PbEU 2019, L 136).

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 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 algemene noodtoestand waarop artikel 15, eerste lid, onderdeel a, van de Dataverordening van toepassing kan zijn, is dus alleen sprake als aan twee cumulatieve voorwaarden wordt voldaan:

1. er moet sprake zijn van een uitzonderlijke (nood)situatie die in de tijd beperkt is; en
2. deze situatie wordt vastgesteld of afgekondigd overeenkomstig de relevante Unie- of nationaalrechtelijke procedures.

Binnen Nederland, is daarom de verhouding met het Nederlandse (staats)nood- en crisisrecht van belang.

Het Nederlandse staatsnoodrecht heeft een grondwettelijke basis in artikel 103 van de Grondwet voor uitzonderingstoestanden die is uitgewerkt in de Coördinatiewet uitzonderingstoestanden. Uitzonderingstoestanden zijn de beperkte of algemene noodtoestand die bij koninklijk besluit kunnen worden afgekondigd.⁴² Beide noodtoestanden zijn te beschouwen als een algemene noodsituatie onder de Dataverordening. Als een noodtoestand wordt afgekondigd kunnen bij koninklijk besluit bevoegdheden uit staatsnoodwetten die zijn genoemd in de bijlages bij de Coördinatiewet uitzonderingstoestanden in werking gesteld worden.

Naast de beperkte of algemene noodtoestand kunnen de bevoegdheden uit sectorale staatsnoodwetten in buitengewone omstandigheden separaat in werking worden gesteld. Dit is niet geregeld in de Coördinatiewet uitzonderingstoestanden, maar in sectorale wetgeving en verloopt volgens een standaardprocedure die in alle relevante noodwetten is opgenomen. Ook deze procedure voldoet aan de hiervoor vermelde twee voorwaarden en is daarom een 'algemene noodsituatie' als bedoeld in de verordening.

Naast het wettelijke stelsel inzake het klassieke staatsnoodrecht, bestaan er ook andere wettelijke kaders om rampen en crises mee te bestrijden. Bij wijze van voorbeeld wordt gewezen op de openbare orde-bevoegdheden van de burgemeester uit de Gemeentewet, zoals het noodbevel en de noodverordening, of specifieke crisisbepalingen uit de Wet veiligheidsregio's. Voor het gebruik van deze bepalingen is geen formele vaststelling of afkondiging vereist. Zij vallen dus buiten de reikwijdte van hoofdstuk V van de verordening.

Zodra een noodtoestand is afgekondigd of een noodbevoegdheid separaat in werking is gesteld, is dus sprake van een algemene noodsituatie als bedoeld in de Dataverordening. Indien de overheidsinstantie die beschikt over deze noodbevoegdheid vervolgens aan de overige voorwaarden van hoofdstuk V van de Dataverordening voldoet, kan deze een verzoek doen aan gegevenshouders om bepaalde gegevens beschikbaar te stellen. De verordening stelt daaraan verschillende eisen: het verzoek moet zijn gericht aan een rechtspersoon, niet zijnde een overheidsinstantie, het moet gaan om gegevens die noodzakelijk zijn om te reageren op de algemene noodsituatie en de overheidsinstantie in kwestie moet geen andere middelen tot diens beschikking hebben om dergelijke gegevens tijdig, doeltreffend en in gelijkwaardige omstandigheden te verkrijgen. Verder bevat hoofdstuk V van de verordening diverse andere voorwaarden waaraan zo'n gegevensverzoek moet voldoen en worden er regels gesteld over bijvoorbeeld de wijze waarop met de verkregen gegevens moet worden omgegaan.

⁴² In een brief van 6 december 2022 (Kamerstukken II 2022/23, 29 668, nr. D) is aangekondigd dat het staatsnoodrecht wordt gemoderniseerd. In die brief zijn ook enkele wijzigingen van de Coördinatiewet uitzonderingstoestanden aangekondigd. Eén van die wijzigingen is dat de beperkte noodtoestand komt te vervallen.

Artikel 16 van de verordening geeft daarnaast nog aan dat hoofdstuk V niet van toepassing op overheidsinstanties, de Commissie, de Europese Centrale Bank of organen van de Unie die activiteiten uitvoeren met het oog op het voorkomen, onderzoeken, opsporen en vervolgen van strafrechtelijke of administratieve inbreuken of de tenuitvoerlegging van straffen, noch op de douane- of belastingadministratie. Uit de Engelse tekst wordt echter duidelijk dat dit hoofdstuk slechts niet van toepassing is op de genoemde organisaties voor zover zij dergelijke activiteiten uitvoeren (*'when carrying out activities'*). Hiermee wordt dus niet bedoeld dat organisaties die in algemene zin beschikken over bevoegdheden op die terreinen, geen gebruik kunnen maken van de bevoegdheden van hoofdstuk V.

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 richtlijn⁴³ 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 11 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

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 Statistiekverordening⁴⁴ en laat deze onverlet (overweging 67 van de verordening).⁴⁵

Zoals reeds beschreven in paragraaf 3.4 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

⁴³ 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).

⁴⁴ 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).

⁴⁵ 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).

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 artikel 33, eerste tot en met derde lid, van de Wet op het CBS en/of 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

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 Verordening (EU) 1025/2012⁴⁶ (hierna: Normalisatieverordening) Europese normalisatieorganisaties verzoeken geharmoniseerde normen voor de interoperabiliteit van dataverwerkingsdiensten op te stellen.

Ook voor de interoperabiliteit van dataruimtes en de geautomatiseerde uitvoering van gegevensdelingsovereenkomsten 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 volgens uit de verordening moeten voldoen aan de vereisten uit de Normalisatieverordening (Bijlage II).

5.11 Verbod op misbruik economische machtspositie

Artikel 102 van het Verdrag inzake de Werking van de Europese Unie (hierna: VWEU) verbiedt één of meer ondernemingen misbruik te maken van een economische machtspositie op de interne markt of op een wezenlijk deel daarvan, voor zover de handel tussen lidstaten daardoor ongunstig kan worden beïnvloed. Artikel 24 van de Mededingingswet bevat een soortgelijk verbod. Het toezicht op deze verbodsbepalingen vindt achteraf plaats (ex post).

Een van de knelpunten zoals benoemd in paragraaf 3.3 van het algemeen deel van de toelichting is het feit dat mede als gevolg van ongelijke marktmacht middelgrote en kleine bedrijven (MKB) vaak geen

⁴⁶ 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).

evenwichtige data-uitwisselingscontracten met sterkere marktspelers kunnen sluiten. Dit staat niet per definitie gelijk aan misbruik van een economische machtspositie, maar in specifieke gevallen kan sprake zijn van overlap tussen bepalingen uit de verordening die het opleggen van oneerlijke contractvoorwaarden tegengaan en het verbod op misbruik van een economische machtspositie. Oneerlijke contractvoorwaarden kunnen namelijk in het kader van een onderzoek naar misbruik van een economische machtspositie ook dienen als bewijs voor het vaststellen van misbruik. In het kader van artikel 102 VWEU wordt echter wel een ruimere norm gehanteerd voor onbillijke contractvoorwaarden dan de voorwaarden die in de verordening worden benoemd. Dat laat onverlet dat een onderneming in sommige gevallen zowel een bepaling uit de verordening, als het verbod op misbruik van een economische machtspositie kan hebben overtreden. In deze situaties is het aan de toezichthoudende autoriteit om te beoordelen welke instrument het meest effectief is om in te zetten. Daarvoor geldt evenwel dat de inzet van de Dataverordening geen afbreuk mag doen aan het mededingingsrecht.⁴⁷ De toezichthouder kan initieel ook onderzoek verrichten op basis van meerdere wettelijke grondslagen, maar dit mag in de boetefase niet afdoen aan het *ne bis in idem* beginsel. Bewijs verkregen bij de inzet van bevoegdheden wordt daarom getoetst aan het toepasselijke regime waaronder de boete wordt opgelegd. Zo mag bewijs uit een huisdoorzoeking onder de Mededingingswet (artikel 50) niet gebruikt worden voor een onderzoek onder deze verordening, omdat de toezichthouder onder de verordening geen bevoegdheid heeft voor huisdoorzoeking (artikel 5:15, eerste lid, van de Awb). Het is aan de toezichthouder om per geval te bepalen op basis van welke wet wordt gehandhaafd.

5.12 Kaderwet zelfstandige bestuursorganen

De Kaderwet zelfstandige bestuursorganen (hierna: 'Kaderwet zbo's') stelt basisregels die in beginsel op alle zbo's van toepassing zijn. Zowel de ACM als de AP zijn zbo's, waardoor de Kaderwet zbo's in beginsel ook op hen van toepassing is. Artikel 3 van de Kaderwet zbo's schrijft voor dat een bestaande zbo slechts met een nieuwe taak, inhoudende de uitoefening van openbaar gezag, wordt belast, indien een van de situaties als bedoeld in het eerste lid zich voordoet. Daarbij is het kabinetsbeleid om geen gebruik meer te maken van de instellingsgronden van onderdelen b en c van dat lid. In zowel het geval van de ACM als dat van de AP is echter sprake van de situatie als bedoeld onderdeel a van dat lid, namelijk dat er behoefte is aan onafhankelijke oordeelsvorming op grond van specifieke deskundigheid. In het geval van de ACM ziet die deskundigheid op marktordening. In het geval van de AP op persoonsgegevens. Zoals is toegelicht in paragraaf 4.1, vereist de verordening dat de bevoegde autoriteiten onpartijdig zijn en vrij zijn van enige, directe of indirecte, invloed van buitenaf en mogen zij voor individuele gevallen geen instructies van andere overheidsinstanties of particuliere partijen vragen of aanvaarden. Daarmee ligt ook het toebedelen van deze taken aan een of meerdere zbo's in de rede.

De mate van onafhankelijkheid moet echter wel voldoende zijn om binnen de regels van te verordening te passen. Op grond van artikel 22 van de Kaderwet zbo's heeft de minister die het aangaat de bevoegdheid om besluiten van zbo's te vernietigen. Deze bepaling zou in strijd zijn met het verbod om instructies van andere overheidsinstanties te aanvaarden, ware het niet dat deze bevoegdheid op grond van artikel 13 van de UAVG ten aanzien van de AP helemaal uitgesloten en ten aanzien van de ACM op grond van artikel 10, eerste lid, van de Instellingswet Autoriteit Consument en Markt beperkt is tot besluiten van algemene strekking. De verordening verzet zich niet tegen instructies die niet zien op individuele gevallen. Beide zbo's voldoen daarom op dit vlak aan de vereisten uit de verordening. Hetzelfde geldt ten aanzien van de bevoegdheid van de minister om op grond van artikel 21 van de Kaderwet zbo's beleidsregels vast te stellen. Ook die is op de AP in het geheel niet van toepassing en voor de ACM niet in strijd met de verordening omdat het gaat om generieke instructies. Ook de bevoegdheid van artikel 23 van de Kaderwet zbo's om in te grijpen bij taakverwaarlozing, ziet niet op individuele gevallen en kan niet worden gekwalificeerd als een aantasting van de onpartijdigheid of als een vorm van directe of indirecte beïnvloeding van de uitvoering van de bevoegdheden van de ACM overeenkomstig de verordening. De regels van de Kaderwet zbo's, in samenhang met de betreffende instellingswetten van de AP en de ACM, voldoen dus tevens aan de voorwaarden van de verordening.

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.

⁴⁷ Zie hiervoor overweging 116 van de verordening.



De verordening zorgt wel voor een toegenomen regeldruk. De Commissie heeft in haar impact assessment een analyse gegeven over de gevolgen voor regeldruk van de verordening op de gehele Europese Unie.⁴⁸ 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 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.

Het Adviescollege Toetsing Regeldruk (ATR) heeft het dossier niet geselecteerd voor een formeel advies, omdat de uitvoeringswet zelf geen gevolgen op het gebied van regeldruk heeft.

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 krijgen. Het voornemen is om ACM aan te wijzen voor hoofdstukken II, met uitzondering van artikelen 4, twaalfde lid, en 5, zevende en achtste lid, 6, eerste en tweede lid, onderdeel b, III, IV, artikel 20, VI, VII en VIII, en om AP aan te wijzen voor artikelen 4, twaalfde lid, en 5, zevende en achtste lid, 6, eerste en tweede lid, onderdeel b, en hoofdstuk V, met uitzondering van artikel 20. Op het moment van aanbidding aan de Raad van State zijn er nog geen extra structurele middelen vrijgemaakt voor deze uitvoeringstaken. Vanuit de Ministeries van Economische Zaken en Binnenlandse Zaken en Koninkrijksrelaties zijn wel incidentele middelen vrijgemaakt voor 2024 en 2025 voor (de voorbereiding op) de uitvoering. Op basis van de uitvoerbaarheids- en handhaafbaarheidstoetsen van de AP en de ACM zullen de Ministeries van Economische Zaken en Binnenlandse Zaken en Koninkrijksrelaties bij de voorjaarsbesluitvorming van 2025 zorg dragen voor de dekking van de structurele middelen voor de uitvoering en handhaving van de verordening.

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

Artikel 49 van de verordening stelt dat uiterlijk op 12 september 2028 de Commissie een evaluatie van

⁴⁸ Impact Assessment report and support studies accompanying the Proposal for a Data Act | Shaping Europe's digital future (europa.eu).

deze verordening uitvoert. In de evaluatie wordt o.a. het effect van de verordening beoordeeld op: het (her)gebruik van gegevens, de praktische toepassing van hoofdstuk V, intellectueel-eigendomsrechten en bedrijfsgeheimen, de verlaging van de overstapkosten van dataverwerkingsdiensten, doeltreffendheid van de handhaving en de innovatiecapaciteit van het midden- en kleinbedrijf. Lidstaten verstrekken de Europese Commissie de nodige informatie voor het opstellen van de evaluatie.

Voorafgaand aan de evaluatie door de Commissie zal het kabinet de verordening en de uitvoeringswet evalueren om de nodige informatie op te halen. Hier zal onder meer stilgestaan worden bij de samenwerking tussen de betrokken toezichthouders. Daarnaast is in de uitvoerings- en handhavingstoetsen door ACM en AP naar voren gebracht dat ze graag de werking van de uitvoeringswet en specifiek effectiviteit van de hoeveelheid ter beschikking gestelde financiële middelen evalueren. Hier zal ook aandacht aan worden besteed in de nationale evaluatie.

8. Advies en consultatie

8.1 Internetconsultatie

Het wetsvoorstel is in internetconsultatie gegeven van 4 maart 2024 tot en met 1 april 2024. In totaal zijn acht reacties ontvangen, waarvan vijf openbaar. De openbare reacties zijn afkomstig van advocaten, de Vereniging voor Informaticarecht Advocaten en Arthur's Legal, en een aantal natuurlijke personen.

Over het algemeen kan het onderhavige wetsvoorstel ter uitvoering van de verordening rekenen op steun. Dat is verheugend. Wel zijn er vragen over de uitwerking van het toezicht in de praktijk, met name waar het gaat om de samenhang met het toezicht op andere wetgeving, waaronder de AVG. Naar aanleiding van de consultatie is het wetsvoorstel op een aantal onderdelen aangepast. Daarnaast is de memorie van toelichting op een aantal onderdelen verhelderd. Op de reacties wordt, voor zover nodig, hieronder thematisch nader ingegaan.

Geschillenbeslechting, publiek toezicht en rechtsbescherming

Samenwerking ACM en AP en normuitleg DA/AVG

In de reacties worden zorgen geuit over de raakvlakken tussen de AVG en de verordening. De Dataverordening bepaalt dat geen afbreuk wordt gedaan aan de AVG. De zorgen zien op 'grensconflicten', waarbij de ACM en de AP een andere normuitleg zouden kunnen hanteren op gelijke of vergelijkbare normen. Afstemmingsproblemen zouden kunnen leiden tot een gebrek aan daadkracht bij de toezichthouder, rechtsonzekerheid voor burgers en verschil in handhaving. De VIRA adviseert om samenwerking tussen de ACM en de AP nadere duiding te geven in de Uitvoeringswet.

Het kabinet vindt een effectieve samenwerking tussen de ACM en de AP belangrijk. Ten eerste is hiervoor een goede afbakening van de toezichtstaken van de ACM en de AP relevant. De AP was in de versie van het wetsvoorstel dat ter consultatie is gegeven reeds de beoogde toezichthouder op onderdelen van de verordening die vergelijkbaar zijn met AVG-begrippen en zien op de verwerking van persoonsgegevens (artikelen 4, twaalfde lid, en 5, zevende en achtste lid, van de verordening). Gelet op de uitvoerings- en handhavingstoets van de AP (paragraaf 8.3 van het algemeen deel van de toelichting) is de afbakening tussen de toezichtstaken van de ACM en de AP aangescherpt. Aan het AP toezicht zijn bepalingen toegevoegd die vergelijkbaar zijn met het bestaande AVG-toezicht (artikel 6, eerste lid en tweede lid, onderdeel b, van de verordening).

Begrippen in de AVG hebben een eigen autonome uitleg. Die begrippen zien op de bescherming van persoonsgegevens, worden uitgelegd door de AVG-toezichthouders en zijn voorzien van eigen rechtspraak. Het ligt daarom voor de hand om voor begrippen in de Dataverordening die vergelijkbaar zijn met begrippen uit de AVG afstemming te zoeken, met daarbij acht voor de context (bescherming niet-persoonsgebonden gegevens, uit IoT-producten, etc.).

In aanvulling op de hierboven benoemde verduidelijking regelt de Uitvoeringswet dat in het kader van efficiënt en effectief toezicht op de Dataverordening de ACM en de AP afspraken kunnen maken in een samenwerkingsprotocol en bevoegd zijn gegevens uit te wisselen (artikel 6 van de Uitvoeringswet). Een nadere invulling van de samenwerking acht het kabinet niet wenselijk, omdat dit juist de als risico benoemde afstemmingsproblemen kan veroorzaken. Daarom is ten opzichte van de consultatieversie de bevoegdheid voor de ACM geschrapt om, indien zij dit noodzakelijk acht, advies te vragen aan de AP over of er afbreuk wordt gedaan aan de AVG door een voorgenomen ACM besluit. Het is juist gezien het feit dat ACM en AP onder de verordening anders zullen moeten samenwerken dan voorheen belangrijk om ruimte te geven aan de ACM en de AP om hier zelf invulling aan te geven. In paragraaf 4.2 van het algemeen deel van de toelichting is nu expliciet gemaakt dat de toezichthouders

afspraken moeten maken over de handhaving van het *ne bis in idem* beginsel bij sanctionering van ondertoezichtgestelden. Daarnaast is paragraaf 4.1 van het algemeen deel van de toelichting over de keuze voor ACM als toezichthouder verder uitgebreid.

Naar aanleiding van een suggestie om de samenwerking tussen AP en ACM te evalueren zal gelijktijdig met de evaluatie van de verordening door de Europese Commissie, zoals omschreven in artikel 49 van de verordening, op nationaal niveau de samenwerking tussen AP en ACM worden geëvalueerd (zie paragraaf 7 van het algemeen deel van de toelichting).

Ook is gevraagd waarom er niet is gekozen voor één toezichthouder voor data, die toezicht houdt op zowel de AVG als de Dataverordening. Naar aanleiding van deze opmerking wordt dit nader toegelicht in paragraaf 4.1 van het algemeen deel van de toelichting.

Boetes en boetebeleidsregels

Een aantal reacties vraagt verduidelijking over de boetes die bevoegde autoriteiten op basis van de Uitvoeringswet kunnen opleggen. Zo wordt in een aantal reacties opgemerkt dat het behulpzaam zou zijn de boetebeleidsregels inzichtelijk te maken. Op grond van artikel 4:81, eerste lid, van de Awb kan een bestuursorgaan beleidsregels vaststellen met betrekking tot een aan hem toekomende bevoegdheid. De ACM en de AP zijn bevoegd om bestuurlijke boetes op te leggen in het kader van de Dataverordening en zijn daarmee ook bevoegd om boetebeleidsregels op te stellen. Hierbij kan worden aangesloten bij de reeds bestaande boetebeleidsregels die de ACM en de AP hanteren.

Daarnaast wordt gevraagd om verduidelijking over de maximumhoogte van de boetes die de ACM en de AP mogen opleggen en hoe dit zich verhoudt tot de maximumhoogte van de boetes uit de AVG. Het kabinet deelt de lezing dat uit de Dataverordening volgt dat voor AVG-toezichthouders (de AP) aansluiting moet worden gezocht bij de AVG-boetes. Desalniettemin hoeft voor de boetes die de ACM kan opleggen niet per definitie te worden aangesloten bij de AVG. Naar aanleiding van deze opmerking is in artikel 8, tweede lid, van de Uitvoeringswet expliciet gemaakt dat de hoogte van de boetes die de AP kan opleggen aansluit bij de AVG. Verder is in artikel 8, eerste lid, van de Uitvoeringswet verhelderd dat de bestuurlijke boete die de ACM kan opleggen ziet op de jaaromzet van de overtreder in het voorgaande boekjaar in de Europese Unie (zie artikel 40, derde lid, onderdeel f, van de verordening). In paragraaf 4.2 van het algemeen deel en in de artikelsgewijze toelichting is meer toelichting opgenomen over de maximumhoogte van de boetes die de ACM en de AP kunnen opleggen.

Samenloop privaat en publiek toezicht

De VIRA vraagt hoe, gelet op de verordening, het private fundament van geschillenbeslechting en beroep bij de burgerlijke rechter (art. 6:233 BW) en daarnaast publiekrechtelijk toezicht en handhaving door de ACM en de AP zich tot elkaar verhouden. Hoe is de burger beschermd en waar kan die zijn klacht indienen?

Indien een partij denkt dat zijn rechten uit de verordening zijn geschonden kan hij een klacht indienen bij de bevoegde autoriteit (artikel 38 verordening) of naar de rechter (artikel 39 verordening). Daarnaast regelt de verordening voor een aantal situaties omtrent het beschikbaar stellen van gegevens onder hoofdstukken II, III, IV en VI van de verordening dat de gebruiker of de derde met de gegevenshouder, en klanten met een aanbieder van dataverwerkingsdiensten, kan overeenkomen de zaak voor te leggen aan een geschillenbeslechtsorgaan. Na geschillenbeslechting of een klacht is het nog steeds mogelijk om naar de rechter te gaan. Dit is uitgebreider toegelicht in paragrafen 3.2 en 3.8 van het algemeen deel van toelichting. Hiermee staat zowel de privaatrechtelijke route (burgerlijke rechter) als publiekrechtelijke handhaving (klacht of geschillencommissie) ter beschikking. Dit is anders dan bij consumentenbescherming waar niet de klacht zelf direct wordt opgelost maar het bedrijf wordt aangesproken op zijn handelspraktijken.

Geschillenbeslechting

De VIRA heeft diverse opmerkingen over geschillencommissies. Ten eerste geeft de VIRA in overweging om bestaande geschillencommissies, zoals een door de AP geaccrediteerd toezichthoudend orgaan op AVG gedragscodes (artikel 41 AVG), een rol te geven bij geschillenbeslechting onder de verordening. Het staat bestaande geschillencommissies vrij om zich te laten certificeren, mits zij voldoen aan de eisen uit artikel 10, vijfde lid, van de verordening.

Ten tweede wordt er op gewezen dat de interpretatie van de certificeringscriteria wel nationale implementatie vergt, bijvoorbeeld via een beleidsregel van de ACM. Het kabinet ziet deze ruimte er alleen voor zover de verordening daar ruimte voor geeft. Uit artikel 10, vijfde lid, en overweging 52 van de verordening blijkt dat de verordening bepaalt wat de certificeringsvoorwaarden zijn en dat

lidstaten alleen extra regels kunnen stellen over de certificeringsprocedure.

Ten derde, stelt de VIRA de vraag of het wenselijk is dat de certificering van geschillenbeslechtsorganen en handhaving in één hand bij de ACM liggen. De VIRA geeft aan dat het zuiverder is om certificering te laten doen door een instantie die zelf aan alternatieve geschilbeslechting doet (beeldvorming: goedkeuring op procesmatige gronden en geen inhoudelijke gronden). Omdat bij certificering uitgebreide kennis van de verordening gewenst is (art. 10 lid 5 sub b), is de ACM hier echter de meest geschikte optie.

Ten vierde, vaagt de VIRA wat er gebeurt als het orgaan en de ACM een andere interpretatie over regelgeving hebben, bijvoorbeeld doordat de ACM beleidsregel kan opstellen en geschilbeslechtsorganen aanbevelingen kunnen publiceren over de wijze waarop problemen kunnen worden voorkomen of opgelost (artikel 10, elfde lid, verordening). Het kabinet ziet weinig risico voor verschillende interpretatie. Geschillenbeslechtsorganen moeten zich houden aan door de Commissie te ontwikkelen en aan te bevelen niet-bindende modelcontractvoorwaarden en met Unie- of nationaal recht waarin de gegevensdelingsverplichtingen worden gespecificeerd of richtsnoeren van sectorale autoriteiten voor de toepassing van dat recht (overweging 55 verordening). Ook de aanbevelingen van een geschillenbeslechtsorgaan moeten hieraan voldoen. Dit wordt nu ook toegelicht in paragraaf 3.2 van het algemeen deel van de toelichting.

Rechtbank Rotterdam exclusief bevoegd

De VIRA vraagt wat de exclusieve bevoegdheid van de Rechtbank Rotterdam betekent voor geschillen waarbij naast de Dataverordening ook de AVG een rol speelt. Mede gelet op het feit dat de consument op grond van de AVG in zijn eigen woonplaats procedures kan starten (artikel 79 lid 2 AVG).

Naar aanleiding van deze opmerking is de bevoegdheidsverdeling aangepast. Het voorstel is om aan te sluiten bij de bestaande rechtsmachtverdeling zoals voorzien in andere wetten op grond waarvan de ACM en de AP besluiten nemen. Voor de AP wordt aangesloten bij de bestaande rechtsmachtverdeling zoals geldt voor AVG-besluiten (beroep over AP-besluiten bij de rechtbanken en hoger beroep bij de Afdeling Bestuursrechtspraak van de Raad van State). Voor beroepen tegen besluiten van ACM blijft de voorgestelde concentratie van rechtspraak bij de Rechtbank Rotterdam en hoger beroep bij het College van Beroep voor het bedrijfsleven. Dit heeft geleid tot aanpassing van artikel 9 de Uitvoeringswet en wordt nader toegelicht in paragraaf 4.6 van het algemeen deel van de toelichting.

Overige punten

Toestemming als grondslag voor gegevensverwerking

Een reactie zag specifiek op een passage in paragraaf 5.1 van de memorie van toelichting over rechtmatige gegevensverwerking: *'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.'* Volgens de reactie klopt deze passage niet en zou deze moeten worden geschrapt.

Deze passage komt uit overwegingen 37 en 38 van de verordening. De passage was beperkt tot gegevensuitwisseling tussen de derde en een andere derde. Naar aanleiding van de opmerkingen is deze passage in paragraaf 5.1 van het algemeen deel van de toelichting aangevuld met informatie over de vereiste grondslag en zijn verwijzingen naar de relevante artikelen en overwegingen uit de verordening toegevoegd.

Toestemming voor wijziging overeenkomst

Een reactie wees er ook op dat in paragraaf 5.5 van het algemeen deel van de toelichting staat dat iedere wijziging van de overeenkomst voor een verbonden product of gerelateerde dienst de geïnformeerde toestemming van de gebruiker vereist. Deze tekst komt uit overweging 25 van de verordening. In paragraaf 5.5 van het algemeen deel van de toelichting is verhelderd wat dit volgens het Nederlandse recht betekent.

Wet open overheid en Verdrag van Aarhus

In een van de reacties werden zorgen geuit over het risico dat als gegevens vanuit de agrarische sector op grond van hoofdstuk V van de verordening met overheden worden gedeeld, deze via de Woo openbaar zullen worden. Ingevolge het Verdrag van Aarhus, dat is geïmplementeerd in de Woo, is de drempel voor openbaarmaking van milieu-informatie namelijk lager dan voor andere informatie.

De indiener uit diens zorgen over het risico dat de betreffende informatie in handen komt van activisten.

Het gevreesde risico doet zich naar het inzicht van het kabinet echter niet voor. Op grond van artikel 17, tweede lid, onderdelen d en e, van de verordening moet de opvragende instantie de gegevens vertrouwelijk behandelen. En op grond van artikel 19, eerste lid, van de verordening moeten zij daarbij doelbinding betrachten, moeten zij technische en organisatorische maatregelen nemen om die vertrouwelijkheid te waarborgen en moeten zij de gegevens wissen zodra de gegevens niet meer nodig zijn voor het doel waarvoor zij zijn opgevraagd. Omdat de verordening EU-recht betreft, kan de Woo, die Nederlands recht betreft, deze vertrouwelijkheidsverplichting niet doorbreken. De gegevens in kwestie zullen dus niet openbaar worden gemaakt.

Harmonisatie regulering data-economie

Daarnaast is door belanghebbende gereageerd dat harmonisatie van Europese regelgeving ten aanzien van de data-economie belangrijk is, hierbij werd met name gerefereerd naar de EHDS. Op basis van dit commentaar zijn geen wijzigingen in de Uitvoeringswet en memorie van toelichting opgenomen.

8.2 Uitvoerbaarheid- en handhaafbaarheidstoets ACM

De Uitvoeringswet wijst de ACM aan als datacoördinator en als toezichthouder op een groot deel van de verplichtingen uit de verordening. De Uitvoeringswet is voorgelegd aan de ACM voor een uitvoerbaarheid- en handhaafbaarheidstoets. De ACM acht het wetsvoorstel uitvoerbaar en handhaafbaar, mits de volgende wetstechnische opmerkingen in acht worden genomen.

Inhoudelijke opmerkingen

Ten eerste verzoekt de ACM om in de Uitvoeringswet te verduidelijken dat zij op alle partijen uit artikel 1, derde lid, van de verordening toezicht kan houden. De ACM kan inderdaad op deze partijen toezicht houden voor zover het gaat om bepalingen waarop de ACM als toezichthouder is aangewezen. Omdat het niet noodzakelijk is in de Uitvoeringswet te benoemen op welke partijen het ACM toezicht ziet, is deze opsomming geschrapt.

Ten tweede verzoekt de ACM om een bevoegde autoriteit aan te wijzen in de zin van artikel 3, aanhef en onder 6, van de Verordening (EU) 2017/2394 (hierna: CPC-verordening). Doordat artikel 47 van de verordening de Dataverordening toevoegt aan de bijlage bij de CPC-verordening wordt de Dataverordening gebracht onder het 'Unierecht ter bescherming van de consumentenbelangen' in de zin van artikel 3, eerste lid, van de CPC-verordening en is er een bevoegde autoriteit nodig in de zin van artikel 3, aanhef en onder 6, van de CPC-verordening. De ACM geeft in overweging dat het toezicht op de CPC-verordening nauw aansluit bij de bestaande rol van de ACM ten aanzien van consumentenbescherming en dat de ACM ook bereid is om deze toezichtstaken op zich te nemen. Dit kan door een wijziging van onderdeel a van de bijlage van de Wet handhaving consumentenbescherming. Het voorstel van de ACM is overgenomen in artikel 11 van de Uitvoeringswet.

Ten derde verzoekt de ACM om in de memorie van toelichting meer uitleg te geven over de verhouding tussen de verordening en consumentenregelgeving. De ACM geeft aan dat slechts summier wordt ingegaan op een deel van de relevante consumentenregelgeving. Naar aanleiding van de opmerking van de ACM zijn paragrafen 3.8 en 5.5 van het algemeen deel van de toelichting aangevuld.

Tot slot wijst de ACM erop dat in de Nederlandse taalversie van de verordening een aantal (ver)taalfouten en onvolledigheden staan. De ACM vraagt om de Europese regelgever te verzoeken deze onvolkomenheden te wijzigen. Het kabinet zal dit punt onder de aandacht brengen bij de Europese Commissie.

Toezicht en handhavingskosten

De ACM geeft in de uitvoerings- en handhavingstoets een kosteninschatting voor de uitvoering en handhaving. Op het moment van aanbidding aan de Raad van State zijn er nog geen extra structurele middelen vrijgemaakt voor deze uitvoeringstaken. Vanuit het Ministerie van Economische Zaken zijn wel incidentele middelen vrijgemaakt voor 2024 en 2025 voor (de voorbereiding op) de uitvoering. Op basis van de uitvoerbaarheids- en handhaafbaarheidstoetsen van de AP en de ACM zal het Ministerie van Economische Zaken bij de voorjaarsbesluitvorming van 2025 zorg dragen voor de dekking van de structurele middelen voor de uitvoering en handhaving van de verordening. De ACM stelt voor om in 2027 gezamenlijk te evalueren of de benodigde fte passend is. In paragraaf 7 van de toelichting is

beschreven op welke wijze we met de ACM en AP de passende inzet van middelen beogen te evalueren.

8.3 Uitvoerbaarheid- en handhaafbaarheidstoets AP

De Uitvoeringswet wijst de AP aan als toezichthouder op een deel van de verplichtingen uit de verordening. Daarnaast veroorzaakt de verordening een uitbreiding van de AVG-toezichthouder taken. De Uitvoeringswet is voorgelegd aan de AP voor een uitvoerbaarheid- en handhaafbaarheidstoets. De AP acht het wetsvoorstel uitvoerbaar en handhaafbaar, mits de Uitvoeringswet op twee punten wordt aangepast en mits er voldoende structurele middelen beschikbaar worden gesteld aan de AP om haar taken uit te kunnen voeren.

Inhoudelijke opmerkingen

Ten eerste, stelt de AP voor om in de Uitvoeringswet een meldplicht op te nemen ten aanzien van besluiten van de ACM die tot gegevensdeling strekken. De voorgestelde formulering betreft: 'De ACM stelt de AP in kennis van een voornemen tot het nemen van een besluit op grond van de Dataverordening dat een verplichting tot gegevensdeling inhoudt. De ACM neemt een dergelijk besluit niet eerder dan twee maanden nadat de AP in kennis is gesteld, tenzij bijzondere omstandigheden daartoe dwingen.' De AP geeft aan dat deze bepaling zorgt voor rechtszekerheid, effectiviteit en transparantie voor derden doordat zichtbaar is geborgd dat de AP betrokken is bij de voorbereiding van het besluit.

Het kabinet erkent het belang van samenwerking tussen ACM en AP voor effectieve handhaving van de verordening. Daarbij merkt het op dat toezichthouders gezamenlijk afspraken kunnen maken over de manier van samenwerken. Om de samenwerking tussen de ACM en de AP goed te laten verlopen regelt de Uitvoeringswet dat de ACM en de AP bevoegd zijn om in het belang van een efficiënt en effectief toezicht op de Dataverordening afspraken te maken en daartoe gezamenlijk samenwerkingsprotocollen vast te stellen. Het kabinet wil – in lijn met het advies van de Afdeling advisering van de Raad van State bij de Uitvoeringswet datagovernanceverordening⁴⁹ – de toezichthouders graag de ruimte geven om deze samenwerking zo goed mogelijk in te vullen. Daarvoor is het belangrijk om deze samenwerking niet onnodig te formaliseren en flexibiliteit te behouden. Het is onvoldoende duidelijk waarom de door AP beoogde manier van samenwerken voor deze specifieke gevallen niet middels een samenwerkingsprotocol met ACM tot stand kan komen. Het opnemen van een dergelijke bepaling zou onnodig gedetailleerd voorschrijven hoe de toezichthouders uitvoering aan de wet geven. Juist omdat de samenwerking tussen AP en ACM mogelijk nieuwe vormen zal aannemen is het niet wenselijk wettelijk voor te schrijven hoe de samenwerking er uit zal zien. Een samenwerkingsprotocol laat zich bovendien gemakkelijker wijzigen wanneer blijkt dat dat voor de uitvoeringspraktijk van belang is. Omdat het om een nieuwe taak gaat waar beide toezichthouders nog ervaring mee moeten opdoen, wordt deze flexibiliteit nuttig geacht. Wel zal de samenwerking tussen betrokken toezichthouders worden geëvalueerd, zoals beschreven in paragraaf 7 van het algemene deel van de toelichting. Dan zal opnieuw worden gekeken naar de noodzaak om de voorgestelde meldplicht in de wet op te nemen.

Ten tweede, acht de AP het noodzakelijk om aangewezen te worden als bevoegd toezichthouder op artikel 6, eerste lid, van de verordening, voor zover er sprake is van verwerking van persoonsgegevens, en op artikel 6, tweede lid, onderdeel b, van de verordening. Hierin wordt onder meer verwezen naar doelbinding, regelgeving inzake bescherming van persoonsgegevens, AVG-rechten van betrokkene en profilering in de zin van de AVG. Het is door de AP voldoende helder gemaakt hoe deze artikelen aansluiten op het bestaande AP toezicht, en daarom wordt dit voorstel overgenomen in artikel 5 van de Uitvoeringswet en toegelicht in paragraaf 4.1 van het algemeen deel van de toelichting.

Tot slot geeft de AP aan moeite te hebben met de uitvoerbaarheid van artikel 22 van de verordening ten aanzien van grensoverschrijdende samenwerking. Het gaat om de situatie waarin een verzoek van een andere overheidsinstelling van een andere lidstaat is gericht aan een Nederlandse gegevenshouder en de AP in dat geval moet beoordelen of er in een andere lidstaat sprake is van uitzonderlijke noodzaak. De AP mist in de verordening een verplichting tot samenwerking met bevoegde autoriteiten in de lidstaten om assistentie te beiden bij nationale interpretaties en beoordeling. De AP verwacht dat EZK en BZK zullen optreden richting de EU en andere lidstaten en op dit onderwerp assisteren bij het bevorderen van de samenwerking.

De verordening schrijft in artikel 37, vijfde lid, onderdeel f, voor dat bevoegde autoriteiten samenwerken met de bevoegde autoriteiten van andere lidstaten om de consistente en efficiënte toepassing van

⁴⁹ Kamerstukken II 2023/24, 36 451, nr. 4, onderdeel 3, onder a.

de verordening te waarborgen. Daarnaast krijgt ook het Europees Comité voor gegevensinnovatie in artikel 42 van de verordening de taak om de Commissie te adviseren en bij te staan bij de ontwikkeling van een consistente praktijk van de bevoegde autoriteiten bij de handhaving van onder andere hoofdstuk V van de verordening. Desalniettemin zal het kabinet het belang van samenwerking en consistente toepassing van de verordening blijven uitdragen in Europees verband.

Toezicht en handhavingskosten

De AP geeft in de uitvoerings- en handhavingstoets een kosteninschatting voor de uitvoering en handhaving. Op het moment van aanbieding aan de Raad van State zijn er nog geen extra structurele middelen vrijgemaakt voor deze uitvoeringstaken. Vanuit de Ministeries van Economische Zaken en Binnenlandse Zaken en Koninkrijksrelaties zijn wel incidentele middelen vrijgemaakt voor 2024 en 2025 voor (de voorbereiding op) de uitvoering. Op basis van de uitvoerbaarheids- en handhaafbaarheidstoetsen van de AP en de ACM zullen de Ministeries van Economische Zaken en Binnenlandse Zaken en Koninkrijksrelaties bij de voorjaarsbesluitvorming van 2025 zorg dragen voor de dekking van de structurele middelen voor de uitvoering en handhaving van de verordening.

8.4 Wetgevingstoets AP

De AP geeft in haar wetgevingstoets aan bezwaar te hebben tegen het voorgestelde artikel uit de Uitvoeringswet over de samenwerking tussen de ACM en de AP daar waar er sprake is van verwerking van persoonsgegevens en adviseert de procedure niet voort te zetten tenzij het bezwaar is aangenomen. Daarnaast heeft de AP nog twee aanmerkingen bij de voorgestelde uitvoeringswet. Twee van de drie punten betreffen dezelfde punten als de AP al in de uitvoerings- en handhavingstoets naar voren heeft gebracht (paragraaf 8.3 van het algemeen deel van de toelichting).

Het bezwaar van de AP is dat het voorgestelde artikel uit de Uitvoeringswet over de samenwerking tussen de ACM en de AP onvoldoende waarborgt dat de ACM bij besluiten die strekken tot een verplichte gegevensdeling tijdig met de AP zal afstemmen of de gegevensdeling ook conform de AVG kan plaatsvinden. De AP stelt als waarborg voor tijdige afstemming voor om de ACM te verplichten om een voornemen tot een dergelijk besluit telkens te melden aan de AP. Dit voorstel wordt niet overgenomen. Zie paragraaf 8.3 van het algemeen deel van de toelichting voor de reactie op dit voorstel, dat door de AP ook werd gedaan in de uitvoerings- en handhavingstoets.

Daarnaast acht de AP het noodzakelijk om aangewezen te worden als bevoegd toezichthouder op zowel artikel 6, eerste lid, voor zover er sprake is van de verwerking van persoonsgegevens, als op artikel 6, tweede lid, onder b, van de verordening. Ook deze opmerking is in lijn met opmerkingen uit de uitvoerings- en handhavingstoets van AP. Dit voorstel wordt overgenomen in artikelen 3 en 5 van de Uitvoeringswet en toegelicht in paragraaf 4.1 van het algemeen deel van de toelichting.

Tot slot merkt de AP op dat de verordening voorziet in (enige) vergoeding van kosten die gepaard gaan met de terbeschikkingstelling van gegevens door een gegevenshouder aan bepaalde overheden bij uitzonderlijke noodzaak, maar dat de verordening géén bepalingen bevat met betrekking tot de vergoeding van de waarde van de data. Naar het oordeel van de AP kan niet worden uitgesloten dat een vordering van data als hier aan de orde een inmenging in het recht op eigendom is die verlies van waarde meebrengt en dat in voorkomend geval mogelijk aanspraak bestaat op vergoeding van waardeverlies. De AP kan als toezichthouder met dergelijke klachten van gegevenshouders worden geconfronteerd. De AP merkt op dat er procedurele waarborgen, zoals voorafgaande onafhankelijke waardebeoordeling, in het voorstel zouden kunnen worden opgenomen om dit risico te mitigeren. Het kabinet neemt dit voorstel niet over. De verordening voorziet niet in een dergelijke vergoeding. De verordening bepaalt wel in artikel 20, tweede lid, van de verordening dat een gegevenshouder recht heeft op een eerlijke vergoeding voor het beschikbaar stellen van gegevens in naleving van een verzoek overeenkomstig artikel 15, eerste lid, onderdeel b, van de verordening. Die vergoeding dekt de technische en organisatorische kosten die zijn gemaakt om aan het verzoek te voldoen, met inbegrip van, in voorkomend geval, de kosten van anonimisering, pseudonimisering, aggregatie en technische aanpassing, en met een redelijke marge. De verordening biedt geen ruimte voor een andere vergoeding zoals voorgesteld door de AP. Het gaat hier immers om geharmoniseerde regels.⁵⁰

Bovendien ziet het kabinet de noodzaak van een bepaling zoals door AP voorgesteld niet. De waarde van data wordt al beschermd door bedrijfsgeheimen- en intellectueel eigendomsrecht. De verordening doet geen afbreuk aan het intellectueel eigendomsrecht en de bescherming van bedrijfsgeheimen blijft onder de verordening gewaarborgd (zie paragraaf 5.3 en 5.4 van het algemeen deel van de toelichting). De verordening bevat verschillende bepalingen om het risico op openbaring van

⁵⁰ Artikel 1, eerste lid, onderdeel c, van de verordening.

bedrijfsgeheimen te minimaliseren. Zo moeten overheidsinstanties in hun verzoeken specifiek aangeven welke gegevens noodzakelijk zijn en de mate van detail en het volume van de benodigde gegevens moet proportioneel zijn ten opzichte van de uitzonderlijke noodzaak. Daarnaast zijn overheidsinstanties verplicht de legitieme doelstellingen van gegevenshouders te eerbiedigen en bedrijfsgeheimen te beschermen. Bedrijfsgeheimen hoeven bovendien alleen wanneer dat strikt noodzakelijk is voor het doel van het verzoek en onder de voorwaarde dat de overheidsinstantie alle nodige maatregelen neemt om de bedrijfsgeheimen te beschermen met een overheidsinstantie te worden gedeeld. Zolang de overheidsorganisaties in kwestie zich houden aan hun verplichtingen, treedt daarbij dus geen waardeverlies op voor de gegevenshouder. Indien de overheidsorganisaties in kwestie de regels overtreden en daardoor schade ontstaat voor de gegevenshouder, kunnen zij uiteraard aansprakelijk worden gesteld onder het normale schadevergoedingsrecht.

8.5 Advies Raad voor de rechtspraak

De Raad voor de rechtspraak (hierna: de Raad) onderkent het belang van de Uitvoeringswet, maar geeft in overweging om de Uitvoeringswet op de volgende onderdelen te verduidelijken of aan te passen.

Inhoudelijke opmerkingen

Ten eerste, merkt de Raad op dat in de Uitvoeringswet de ACM en de AP de bevoegdheid wordt toegekend om een bij overtreding van de verordening een bestuurlijke boete of een last onder dwangsom op te leggen en dat in de memorie van toelichting staat dat ook een last onder bestuursdwang kan worden opgelegd. De Raad adviseert om de bevoegdheid voor een last onder bestuursdwang ook in de Uitvoeringswet op te nemen. Dit advies is overgenomen en verwerkt in artikel 8 van de Uitvoeringswet, bijbehorende artikelsgewijze toelichting en in paragraaf 4.2 van het algemene deel van de toelichting.

Ten tweede, gaat de Raad in op de rechtsbescherming. De Raad kan zich vinden in concentratie van rechtspraak bij Rechtbank Rotterdam ten aanzien van beroepen tegen besluiten van de ACM. Aan de eis van specifieke deskundigheid en de verwachting dat het aantal beroepszaken beperkt zal zijn uit het Toetsingskader wettelijke concentratie is voldaan. De Raad adviseert voor besluiten van de AP om geen bijzondere bestuursrechter aan te wijzen. Voor besluiten van de AP geldt doorgaans de reguliere rechtsbescherming van beroep bij de rechtbank en hoger beroep bij de Afdeling bestuursrechtspraak van de Raad van State. Met het aanwijzen van een bijzondere bestuursrechter wordt in dit geval niet voldaan aan de eis van specifieke deskundigheid zoals opgenomen in het concentratiebeleid van de Raad. Daarbij leidt deze keuze tot twee verschillende beroepsgangen voor besluiten van de AP, hetgeen de Raad niet wenselijk acht. In dit verband wijst de Raad nog op het wetsvoorstel Uitvoeringswet digitaaldienstenverordening waarin ook is gekozen voor de reguliere rechtsbescherming voor de besluiten van de AP naast de aanwijzing van een bijzondere bestuursrechter voor de besluiten van de ACM. De Raad adviseert om de Uitvoeringswet op dit punt aan te passen. Dit advies is overgenomen en verwerkt in artikel 9 van de Uitvoeringswet, bijbehorende artikelsgewijze toelichting en in paragraaf 4.6 van het algemeen deel van de toelichting.

Ten derde merkte de Raad op dat wanneer er op één en dezelfde partij zowel een transparantieverplichting inzake gegevens rust als de bevoegdheid tot het wel of niet verlenen van toegang tot deze gegevens, dan de vraag is hoe 'uitzonderlijke omstandigheden' en 'ernstige economische schade' (zoals omschreven in artikel 4, achtste lid en artikel 5, elfde lid van de verordening) worden vastgesteld. De Raad is adviseert de toelichting ten aanzien van dit punt aan te passen. De toelichting in paragraaf 3.1 van het algemeen deel van de toelichting legt echter slechts de verordening uit en beschrijft de rollen zoals die in de verordening omschreven staan. Het kan inderdaad zo zijn dat de aanbieder van een verbonden product en de gegevenshouder één en dezelfde partij zijn, maar dit is in de verordening zo georganiseerd. Hoofdstuk III van de toelichting verduidelijkt de verordening reeds, en daarnaast is verdere normuitleg door de bevoegde autoriteiten mogelijk. Het advies tot aanpassing van de Raad is daarom niet overgenomen.

Ten vierde, merkt de Raad op dat in de memorie van toelichting een aparte paragraaf ontbreekt waarin helder en overzichtelijk uiteen gezet wordt op welke wijze de rechtsbescherming in de Uitvoeringswet is vormgegeven. Geadviseerd wordt om zo'n paragraaf op te nemen. Dit advies is overgenomen in paragraaf 4.6 van het algemeen deel van de toelichting.

Werklast

De Raad verwacht als gevolg van de Uitvoeringswet geen significante werklast-gevolgen voor de Rechtspraak. Daarbij merkt de Raad op dat deze conclusie inmiddels ook getrokken is bij een aantal adviezen over uitvoeringswetten bij verordeningen in 2023, namelijk de Uitvoeringswet datagovernan-

ceverordening, de Uitvoeringswet digitaledienstenverordening en Uitvoeringswet digitale marktenverordening. De effecten op de werklust van deze verordeningen kunnen bij elkaar opgeteld wel degelijk leiden tot een substantiële werklustverzwaring voor de rechtspraak, in het bijzonder bij het CBb. Daarom is de Raad voornemens om de balans hiervan op te maken en daarop nog terug te komen, zo mogelijk bij de besprekingen over de ontwerpbegroting voor de Rechtspraak 2026.

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 13 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 Geschillenbeslechtsorgaan

Gebruikers, gegevenshouders en gegevensontvangers, klanten en aanbieders van dataverwerkingsdiensten hebben toegang tot een gecertificeerd geschillenbeslechtsorgaan om geschillen bedoeld in artikel 10, eerste en vierde lid, van de verordening te beslechten. De lidstaat waar het geschillenbeslechtsorgaan 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 geschillenbeslechtsorganen 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 geschillenbeslechtsorgaan 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.

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, tweede alinea, en zesde lid, en 38, eerste lid, tweede volzin, van de verordening. Zie voor wat betreft de

publicatie van verzoeken onder hoofdstuk V ook artikel 17, tweede lid, onderdeel g, van de verordening. Zie voor een toelichting op de taken paragraaf 3.8 van het algemeen deel van de toelichting.

Artikel 5 Aanwijzing toezichthouders

Artikel 5 van de Uitvoeringswet bepaalt 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. Het toezicht ziet op normerende bepalingen uit de verordening.

In artikel 5, eerste lid, van de Uitvoeringswet wordt de ACM belast met het toezicht op de naleving van het grootste deel van de verplichtingen in de verordening. Artikel 12a van de Instellingswet ACM bevat de grondslag voor de ACM om bij besluit de ambtenaren aan te wijzen die belast zijn met de uitvoering van het toezicht van op de naleving van wettelijke voorschriften dat is opgedragen aan de ACM. Om die reden wordt in onderhavig artikel de ACM aangewezen als toezichthouder, terwijl in artikel 5, tweede lid, van de Uitvoeringswet bepaalde ambtenaren van de AP worden aangewezen als toezichthoudende ambtenaren.

In artikel 5, tweede en derde lid, van de Uitvoeringswet worden de daar genoemde ambtenaren van de AP belast met het toezicht op de naleving van een aantal artikelen uit hoofdstuk II van de verordening die zien op het beschermen van persoonsgegevens en uitleg van AVG-begrippen en op hoofdstuk V van de verordening. Zie voor een toelichting hierop nader paragraaf 4.1 van het algemeen deel van de toelichting. De genoemde ambtenaren zijn dezelfde als die op grond van artikel 15 van de UAVG zijn belast met het toezicht op de naleving van de AVG en die wet.

Artikel 6 Samenwerking ACM en AP

Voor effectief toezicht op de verordening moeten ACM en AP samenwerken. Het gaat om samenwerking vanuit hun rol als bevoegde autoriteiten, de ACM als datacoördinator (artikel 37, tweede en vijfde lid, onderdeel c, van de verordening) en de AP als AVG-toezichthouder (artikel 37, vijfde lid, onderdeel g, van de verordening). 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.

Het voorgestelde artikel 6, eerste lid, van de Uitvoeringswet bepaalt dat de ACM en de AP bevoegd zijn afspraken te maken over toezicht op de verordening en dat ze daarvoor een samenwerkingsprotocol kunnen opstellen, waarvan in de Staatscourant mededeling wordt gedaan. 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.

Het voorgestelde artikel 6, tweede lid, van de Uitvoeringswet voorziet in een grondslag voor het delen van 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 7 Samenwerking ACM en andere bevoegde autoriteiten

Voor effectief toezicht op de verordening moeten de bevoegde autoriteiten samenwerken met andere bevoegde autoriteiten als bedoeld in artikel 37, vijfde lid, onderdelen g en h, van de verordening. Het betreft onder meer sectorale toezichthouders die verantwoordelijk zijn voor de uitvoering van andere Unie of nationale regelgeving, waaronder de Rijksdienst Digitale Infrastructuur. 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.

Het voorgestelde artikel 7, eerste lid, van de Uitvoeringswet bepaalt dat de ACM en de AP (als bevoegde autoriteiten en de datacoördinator) bevoegd zijn om met deze andere bevoegde autoriteiten afspraken te maken over toezicht op de verordening en dat ze daarvoor een samenwerkingsprotocol kunnen opstellen, waarvan in de Staatscourant mededeling wordt gedaan. Er kan ook worden gekozen om een bestaand samenwerkingsprotocol aan te passen.

Verder biedt artikel 7, tweede lid, van de Uitvoeringswet een grondslag om bij ministeriële regeling regels te kunnen stellen over het verstrekken van gegevens tussen de ACM en de andere bevoegde autoriteiten voor zover dat noodzakelijk is voor de uitvoering van deze wet. Het gaat om situaties waarin sprake is van structurele samenwerking en gegevensuitwisseling. Vooralsnog wordt geen

gebruik gemaakt van deze grondslag. Voor het incidenteel uitwisselen van informatie tussen toezicht-houders biedt artikel 5:16 Awb al een grondslag. De verwachting is dat in de toekomst de vorm en frequentie samenwerking tussen de ACM en andere toezichthouders zal veranderen, bijvoorbeeld naar aanleiding van nieuwe sectorale wetgeving of het toenemende gebruik van verbonden producten en dataverwerkingsdiensten.

Artikel 8 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 bestuursdwang, en daarmee ook een last onder dwangsom, kan opleggen. Voor de maximale hoogte van de bestuurlijke boete wordt voor de ACM aangesloten bij vergelijkbare wetgeving en de jaaromzet van de inbreukmakende partij in het voorgaande boekjaar in de Europese Unie (artikel 40, derde lid, onderdeel f, van de verordening). Voor de maximale hoogte van de bestuurlijke boete wordt voor de AP aangesloten bij de AVG-boete hoogte (artikel 40, vierde lid, van de verordening jo. artikel 83, vijfde lid, van de AVG). Zie verder paragraaf 4.2 van het algemeen deel van de toelichting.

Artikel 9 Wijziging Algemene wet bestuursrecht

Dit artikel van de Uitvoeringswet regelt de beroepsmogelijkheden tegen besluiten van de ACM 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). Zie verder paragraaf 4.6 van het algemeen deel van de toelichting.

Artikel 10 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 11 Wijziging Wet handhaving consumentenbescherming

Artikel 47 van de verordening wijzigt de bijlage van Verordening (EU) 2017/2394⁵¹ (hierna: CPC-verordening) waardoor de Dataverordening valt onder het 'Unierecht ter bescherming van de consumentenbelangen' in de zin van artikel 3, eerste lid, van de CPC-verordening. In de bijlage bij de Wet handhaving consumentenbescherming is geregeld welke toezichthouder in Nederland toezicht houdt op de naleving van de verschillende Europese consumenten richtlijnen en verordeningen. Dit artikel van de Uitvoeringswet voegt de Dataverordening toe aan onderdeel a van de bijlage bij de Wet handhaving consumentenbescherming. Dit betekent gelet op artikel 2.2 van de Wet handhaving consumentenbescherming dat de ACM is belast met het toezicht op de naleving van de Dataverordening.

Artikel 12 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 Datagovernance-verordening (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.

⁵¹ Verordening (EU) 2017/2394 van het Europees Parlement en de Raad van 12 december 2017 betreffende samenwerking tussen de nationale autoriteiten die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming en tot intrekking van Verordening (EG) nr. 2006/2004 (PbEU 2017, L 345).



Artikel 13 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	

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
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 transparantieverplichtingen 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 Europees Comité voor gegevensinnovatie (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	

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
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 en samenwerken bevoegde autoriteiten)	Artikelen 4 en 6 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 bevoegde autoriteit)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Lid 5 (taken en bevoegdheden bevoegde autoriteiten)	Artikelen 3, tweede en vierde lid, en artikelen 5, 6 en 7 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 4 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 9 Uitvoeringswet Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks	Geen	
Artikel 40 (Sancties)			
Lid 1 (sancties vaststellen)	Artikel 8 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 Tweede zin : Behoeft naar de aard van deze bepaling geen implementatie; gericht tot EC	Geen	



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
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 en Artikel 8, tweede lid, Uitvoeringswet	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 10 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 bevoegdheids-delegatie)	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)	Artikel 11 Uitvoeringswet	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,