Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

22 112 Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie

Nr. 3411

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 18 mei 2022

De vaste commissie voor Digitale Zaken heeft een aantal vragen en opmerkingen voorgelegd aan de Minister van Economische Zaken en Klimaat over het EU-voorstel: Geharmoniseerde regels inzake eerlijke toegang tot en eerlijk gebruik van data (Dataverordening) COM (2022) 68 en over de brief van 1 april 2022 over het BNC-Fiche: Dataverordening (Kamerstuk 22 112, nr. 3395).

De vragen en opmerkingen zijn op 15 april 2022 aan de Minister van Economische Zaken en Klimaat voorgelegd. Bij brief van 17 mei 2022 zijn de vragen beantwoord.

De voorzitter van de commissie,
Kamminga

Adjunct-griffier van de commissie,
Van Tilburg

kst-22112-3411
ISSN 0921 - 7371
's-Gravenhage 2022

Vragen en opmerkingen vanuit de fracties en reactie van de Minister

Vragen en opmerkingen van de leden van de VVD-fractie

De leden van de VVD-fractie hebben met belangstelling kennisgenomen van het fiche van het kabinet ten aanzien van de Dataverordening. In algemene zin onderschrijven deze leden de inzet van het kabinet. Deze leden zijn verheugd dat de Europese Commissie beoogt een gelijkwaardiger speelveld te creëren en beoogt de innovatie en concurrentie van Europese bedrijven te vergroten. Ook lezen de leden met grote belangstelling dat de Dataverordening vastlegt dat producten en gerelateerde diensten zo ontworpen moeten worden dat gebruikers makkelijk en veilig toegang hebben tot de data die door hun gebruik worden gegenereerd. Graag willen deze leden nog enkele vragen stellen aan het kabinet.
De leden van de VVD-fractie lezen dat micro-en kleinbedrijven worden uitgezonderd van de regels waarbij gebruikers makkelijk en veilig toegang hebben tot de data die door hun gebruik wordt gegenereerd. Mogen deze bedrijven deze data wel verkopen? Wat gebeurt er met de data wanneer deze micro- en kleinbedrijven zijn uitgegroeid tot grotere bedrijven en ze wel binnen de scope van de regels vallen? Mag deze data nog wel gebruikt worden, gezien deze data is verkregen voordat het een middengroot bedrijf is geworden? Hoeveel bedrijven in Nederland vallen onder de definitie micro- en kleinbedrijf zoals gehanteerd wordt door de Europese Commissie?

De Dataverordening verplicht aanbieders van «Internet-of-Things»(IoT)-producten deze zo te ontwerpen dat de door het gebruik ervan gegenereerde data gemakkelijk en veilig toegankelijk zijn voor de gebruiker. Micro- en kleinbedrijven zijn van deze verplichting uitgezonderd. Wel mogen deze bedrijven op eigen initiatief gebruikers toegang tot data geven of toegang aan derden laten geven. Bestaande regels over het gebruik en delen van data, zoals de Algemene Verordening Gegevensbescherming (AVG), zullen blijven gelden voor de data die gegenereerd wordt door IoT-producten van micro- en kleinbedrijven. Afhankelijk van het type data dat de producten verzamelen zullen er beperkingen op de verkoop van data kunnen liggen. Vanzelfsprekend zijn regels over privacygevoelige of bedrijfsgevoelige data onverminderd van toepassing. Wanneer een micro- of kleinbedrijf uitgroeit tot een midden- of groter bedrijf, dan gelden de voor deze categorie bedrijven geldende regels. Micro-ondernemingen zijn ondernemingen met minder dan 10 personeelsleden en een jaaromzet of jaarlijks balanstotaal van niet meer dan 2 miljoen EUR. Kleine ondernemingen zijn ondernemingen met minder dan 50 personeelsleden en een jaaromzet of jaarlijks balanstotaal van niet meer dan 10 miljoen EUR. Volgens het Centraal Bureau voor de Statistiek waren er in het tweede kwartaal van 2022 in totaal 2.071.330 bedrijven met minder dan 50 personeelsleden in Nederland.[1] Welk deel hiervan IoT-producten aanbiedt, is onbekend.

De leden van de VVD-fractie lezen dat de data-ontvanger de verkregen data wel mag gebruiken voor profilering als het noodzakelijk is voor de verleende dienst. Welke criteria worden gesteld aan de data-ontvanger in het geval dat profilering als noodzakelijk wordt gezien voor de verleende dienst? Verwacht het kabinet dat dit een mogelijkheid kan zijn voor organisaties om de regels te omzeilen?

De dataontvanger ontvangt de gegevens op basis van het in artikel 5 vastgelegde recht van gebruikers om hun gegevens naar een derde partij

[1] https://opendata.cbs.nl/statline/#/CBS/nl/dataset/81589NED/table?dl=673A7

over te dragen; het vindt dus plaats op verzoek van de betrokkene in het geval er persoonsgegevens worden verwerkt. In artikel 5 lid 9 is ook vastgelegd dat er daarbij geen negatieve impact mag ontstaan op de gegevensbeschermingsrechten van derden. Wanneer de dataontvanger conform genoemde procedure gegevens ontvangt is de hoofdregel dat deze partij daar alleen mee doet wat expliciet is verzocht: de dataontvanger kan niet zomaar op eigen initiatief met die gegevens aan de slag. Dit is vastgelegd in artikel 6 lid 1. Als extra waarborg zijn in artikel 6 lid 2 nog een aantal expliciete verboden opgenomen, waaronder dat er in principe geen profilering mag worden toegepast tenzij dit het doel van de verstrekking is om een dienst te leveren. In het geval dat profilering noodzakelijk is voor de verleende dienst gelden daar bovenop onverminderd de regels omtrent de verwerking van persoonsgegevens uit de AVG. Middels de dataverordening worden alleen aanvullende regels gesteld, er mag geen afbreuk aan het beschermingsniveau worden gedaan.

De leden van de VVD-fractie hebben met interesse gelezen dat de Dataverordening ook de onderbenutting van data tegen gaat. Hoe draagt de verordening hier precies aan bij en wat is hierin de rol van de lidstaten?

Momenteel is het in veel gevallen zo dat data uit IoT-producten alleen door de fabrikant van die producten wordt gebruikt terwijl die data ook nuttig kunnen zijn voor andere partijen dan de fabrikant. Hierdoor is inderdaad sprake van onderbenutting, met name omdat data veelal niet van de fabrikant, ofwel data houder, met andere partijen gedeeld wordt. Door gebruikers het recht te geven deze data zelf te gebruiken of door derde partijen toegang te geven zal de data uit IoT-producten door meer partijen benut kunnen worden, terwijl tegelijk de grip op deze data voor de gebruiker van een IoT-product wordt versterkt. Daardoor kunnen deze data voor meer verschillende maatschappelijke en economische doelen gebruikt worden dan nu het geval is. Door de regels over het gebruik van data en het wisselen tussen dataverwerkingsdiensten vast te leggen op EU-niveau worden bovendien belemmeringen op de interne markt voor het hergebruik van data weggenomen. Om die reden is optreden op het niveau van de EU gerechtvaardigd.

De leden van de VVD-fractie delen de vragen die het kabinet heeft bij het datadelen aan publieke instanties wanneer sprake is van uitzonderlijke noodzaak. Deze leden willen graag weten wanneer iets een uitzonderlijke noodzaak betreft. Wat betekent de Dataverordening voor de bevoegdheden van de politie? Graag zouden de leden ook zien dat het niet aan de datahouder is om te beoordelen of aan de verstrekkende eisen is voldaan. Welke mogelijkheden ziet het kabinet om het beoordelen aan een andere partij over te laten?

Zoals aangegeven in het BNC-fiche heeft het kabinet vragen bij het voorgestelde kader om publieke instanties in gevallen van uitzonderlijke noodzaak gegevens bij datahouders op te laten vragen. Deze vragen zijn nog niet door de Europese Commissie beantwoord. Daarmee is voor het kabinet ook nog onvoldoende duidelijk in welke situatie er sprake is van uitzonderlijke noodzaak. Het kabinet heeft zorgen dat de gecreëerde bevoegdheid om in gevallen van uitzonderlijke noodzaak data op te vragen bij datahouders te verstrekkend is en dat het voorgestelde kader te weinig waarborgen omvat.
De in de Data Act gecreëerde bevoegdheid voor overheidsinstanties om data op te vragen mag niet gebruikt worden voor rechtshandhavingsdoel-

einden. De Dataverordening heeft geen implicaties voor de bevoegdheden van de politie. De bestaande wetgeving daarover blijft onverminderd van kracht.

De leden van de VVD-fractie lezen dat de lasten voor midden- en kleinbedrijven (mkb) op kunnen lopen tot 300.000 euro per jaar; voor grotere aanbieders is dit bedrag structureel één miljoen euro per jaar. Kunnen deze bedragen meer worden toegespitst? Vindt het kabinet deze lasten proportioneel?

De aanbieders van IoT-producten kunnen te maken krijgen met kosten verbonden aan het voldoen aan de vereisten uit de dataverordening. In het Impact Assessment geeft de Europese Commissie aan dat het hierbij onder andere gaat om kosten voor bijvoorbeeld de ontwikkeling van datamanagementovereenkomsten en datamanagementsystemen, en bijvoorbeeld om technische infrastructuur op orde te brengen. De dataverordening benoemt echter niet de specifieke manieren waarop de toegangs- en gebruiksrechten toegepast moeten kunnen worden, dit biedt zowel grote als kleine aanbieders flexibiliteit in de uitvoering van deze maatregelen. De Europese Commissie geeft in het Impact Assessment aan dat de inschatting dat deze kosten één miljoen euro bedragen voor grote aanbieders een overschatting lijkt te zijn. Deze inschatting gaat er namelijk vanuit dat de betreffende bedrijven nog niet gebruik maken van data management systemen en daarom dergelijke technische infrastructuur compleet moeten opzetten om te voldoen aan de dataverordening. Dit is echter ook een onjuiste inschatting aangezien de meeste grote aanbieders, waar deze inschatting betrekking op heeft, hier al gebruik van zullen maken en dus reeds klaar zijn om op grote schaal data te delen. Het oordeel over de proportionaliteit is positief, tegenover de kosten staan voordelen voor het bredere bedrijfsleven en consumenten die de kosten overstijgen. Dit is ook de uitkomst van het impact assessment van de Europese Commissie.

De leden van de VVD-fractie willen graag weten welke implementatietermijn het kabinet wenselijk acht voor deze verordening. Deze leden lezen dat hiertoe ook een verzoek zal worden gedaan om de termijn voor het intreden van de verordening te verruimen. Hoe groot acht het kabinet de kans dat deze termijn inderdaad verruimd zal worden?

Het kabinet zal zich inzetten om de implementatietermijn te verruimen om een gedegen wetgevingsproces te kunnen doorlopen. In deze fase van de onderhandelingen is het nog niet mogelijk om een inschatting van de slagingskansen hiertoe te geven.

De leden van de VVD-fractie lezen dat de toezichthouder mogelijk boetes op kan leggen bij het overtreden van de toekomstige wet (na implementatie). Kan het kabinet ingaan op de hoogte van deze boetes en wanneer deze boetes exact opgelegd worden? Welke bestaande onafhankelijke autoriteiten worden verantwoordelijk voor het toezicht op de Dataverordening?

In deze fase van het proces kan het kabinet nog geen uitspraken doen over de inrichting van het toezicht op de verordening. Het kabinet zal nog gaan onderzoeken hoe het toezicht op de dataverordening in Nederland effectief kan worden ingericht, waarbij in eerste instantie wordt gekeken naar bestaande toezichthouders, waaronder de Autoriteit Consument en Markt (ACM), de Autoriteit Persoonsgegevens (AP) en Agentschap Telecom (AT). Op basis van het huidige voorstel is nog geen inschatting te geven over de hoogte van de boetes en wanneer deze opgelegd worden. Daarnaast stelt het voorstel dat voor specifieke sectorale problemen

omtrent datadeling de competentie van sectorale toezichthouders, zoals rijksinspecties, moet worden gerespecteerd.

Vragen en opmerkingen van de leden van de D66-fractie

De leden van de D66-fractie hebben kennisgenomen van het BNC-fiche EU Dataverordening en hebben hier nog enkele vragen over. Voor deze leden staat voorop dat mensen baas over eigen data zijn. Daarnaast is het voor gezonde innovatie belangrijk dat datamonopolie van techbedrijven zo veel mogelijk worden voorkomen of doorbroken.
De leden van de D66-fractie begrijpen de noodzaak als overheid om in uitzonderlijke gevallen data te verzoeken. Echter zijn de hiervoor inperkende definities nog te onduidelijk. Kan de Minister toelichten hoe «uitzonderlijke behoefte» kan worden geïnterpreteerd? Kan de Minister een voorbeeld schetsen van een noodsituatie waar zo'n uitzonderlijke behoefte uit voort zal komen? Acht de Minister het uitvoeren van een publieke taak in het algemeen belang niet een te brede definitie die te makkelijk toepasbaar is? Welke rol spelen universiteiten en kennisinstellingen bij het toegankelijk maken van data?

Het kabinet heeft vragen bij het voorgestelde kader om publieke instanties in gevallen van uitzonderlijke noodzaak gegevens bij datahouders op te laten vragen. Deze vragen zijn nog niet door de Europese Commissie beantwoord. Daarmee is voor het kabinet ook nog onvoldoende duidelijk in welke situatie er sprake is van uitzonderlijke noodzaak. De Europese Commissie geeft in de overwegingen als voorbeelden: een noodsituatie op het gebied van volksgezondheid, grote natuurrampen of door de mens veroorzaakte rampen.

In het huidige voorstel is er geen specifieke rol voor universiteiten en kennisinstellingen bij het toegankelijk maken van data. Wel kunnen deze instellingen onder bepaalde voorwaarden data die is opgevraagd in gevallen van uitzonderlijke noodzaak gebruiken voor wetenschappelijk onderzoek of analyses in lijn met het doel waarvoor de data zijn opgevraagd.

De leden van de D66-fractie lezen dat er nog sectorspecifieke wetgeving zal volgen. Kan de Minister aangeven aan welke sectoren hierbij gedacht wordt en welk tijdspad hierbij komt kijken?

Voor verdere sectorale initiatieven heeft de Commissie aangegeven te luisteren naar de behoeftes vanuit lidstaten en de sectoren zelf. Er zijn al voorbeelden van dergelijke sectorale initiatieven. Zo start de Europese Commissie naar verwachting nog dit jaar een publieke consultatie (*call for evidence*) op het onderwerp «toegang tot voertuigdata, functies en systemen». Dit initiatief is erop geënt om complementair te zijn op de Dataverordening en deze vanuit sectorspecifieke regelgeving aan te vullen. Op 3 mei jl. heeft de Commissie een voorstel voor een «European Health Data Space» gepresenteerd. Dit voorstel bevat regels om veiliger gezondheidsdata te kunnen uitwisselen.

Voor de leden van de D66-fractie is het van groot belang dat consumenten enkel hun data delen met derden na expliciete toestemming. In welke mate bestaat de verplichting dat zulke toestemming enkel actief en niet passief is? Is het toegestaan onder de huidige verordening om diensten of producten te ontzeggen als er niet wordt voldaan aan de toestemming om data te delen met derden? Zo ja, acht de Minister dit onwenselijk? Welke lessen uit het delen van data door consumenten kunnen we vooralsnog leren uit de sinds kort in werking getreden Payment Service Directive 2 (PSD2)? Was er bij PSD2 enige sprake van onvoorziene gevolgen van

geautoriseerd data delen met derden die de gegevensbescherming van mensen in het geding heeft gebracht? Zo ja, welke voorbeelden heeft de Minister hierbij? Is het mogelijk voor een gebruiker om na het toegang geven tot hun data deze toegang weer te ontzeggen? Zo ja, komt hierbij ook een verwijderplicht kijken? Hoe verhoudt dit zich tot de thans geldende regels in de Algemene verordening gegevensbescherming (AVG)? Hoe gaat voorkomen worden dat mixed data, persoonlijke data en niet persoonlijke data, niet gescheiden kunnen worden? Welke risico's ziet de Minister bij mixed data?

De AVG blijft onverminderd van kracht met betrekking tot de bescherming van persoonsgegevens. De AVG schrijft niet voor dat er altijd moet worden gewerkt met expliciete toestemming voor consumenten. Dat zou in de praktijk ook niet wenselijk of werkbaar zijn. Denk bijvoorbeeld aan verwerkingen van persoonsgegevens om apparaten en netwerken goed te beveiligen, of om in iemands belang te handelen als diegene niet in staat is om daar toestemming voor te geven. Daar komt bij dat wanneer wordt gewerkt met de rechtsgrondslag »toestemming» deze alleen »uitdrukkelijk» hoeft te zijn als het gaat om de verwerking van bijzondere persoonsgegevens.[2] De rechten die de AVG burgers geeft ten aanzien van hun persoonsgegevens – waaronder onder meer het recht om gegevens in te zien en in bepaalde gevallen te rectificeren of te laten verwijderen[3] – gelden onverkort voor zover er persoonsgegevens worden verwerkt, hier doet de Dataverordening niets aan af.

De Dataverordening creëert aanvullend in hoofdstuk 2 een systematiek waarbij gebruikers van IoT-producten data kunnen delen met een derde partij. Datahouders mogen alleen op verzoek van de gebruiker data delen onder de Dataverordening. De Dataverordening schrijft aanvullend voor dat voor alle gebruikers van IoT-producten het ontzeggen van datatoegang aan een derde partij even makkelijk moet zijn als het geven van toestemming. Daarnaast mogen data-ontvangers gebruikers op geen enkele manier dwingen, misleiden of manipuleren door de autonomie, besluitvorming of keuzes van de gebruiker te ondermijnen of te beperken. Wat betreft »mixed data» gelden de regels uit de AVG voor zover er persoonsgegevens worden verwerkt.[4]

Binnenkort wordt het rapport betreffende de nationale evaluatie van PSD2 naar de Tweede Kamer gestuurd door de Minister van Financiën, waarin onder meer wordt ingegaan op de toegang van derde partijen tot gegevens van rekeninghouders. Ook op Europees niveau vindt momenteel een evaluatie plaats van PSD2, waarbij dit onderwerp wordt betrokken, de uitkomsten hiervan worden later dit jaar verwacht. Ten aanzien van de mogelijkheid om toegang tot betaalgegevens te ontzeggen geldt dat een betaaldienstgebruiker, na het verlenen van toegang tot zijn rekeninggegevens, daarop kan terugkomen door de overeenkomst met de betreffende betaaldienstverlener te beëindigen of de toegang voor individuele partijen in hun bank-app te blokkeren.

De leden van de D66-fractie begrijpen dat marginale compensatie mogelijk kan zijn bij het delen van data tussen partijen. Wie is straks binnen Nederland verantwoordelijk voor een goed verloop tussen partijen met betrekking tot eerlijke marginale compensatie? Kan de Minister uiteenzetten welke toezichthouder voor welk onderdeel van de verordening verantwoordelijk is? Als het de Autoriteit Persoonsgegevens

---

[2] Zie artikels 6 en 9 AVG
[3] Zie artikels 15 tot en met 20 AVG
[4] Zie hiervoor ook de definitie van »persoonsgegevens» in artikel 4 lid 1 AVG.

betreft, kan de Minister aangegeven of er extra capaciteit vrijkomt om deze nieuwe taken adequaat uit te voeren?

Voor het bepalen van de redelijkheid en eerlijkheid van de voorwaarden en compensatie voor datatoegang zal in Nederland één of meerdere geschilbeslechtingsorganen moeten worden gecertificeerd. Welke partij of partijen dit zullen zijn is nog niet bekend. Het kabinet zal nog gaan onderzoeken hoe het toezicht in Nederland effectief kan worden ingericht, waarbij in eerste instantie wordt gekeken naar bestaande toezichthouders, waaronder de ACM, de AP en AT. De AP is verantwoordelijk voor het toezicht op de bescherming van persoonsgegevens op grond van de AVG en dat zal ook het geval zijn in zoverre het gebruik of delen van persoonsgegevens binnen de reikwijdte van deze verordening valt. Voor het beleggen van nieuwe toezichtstaken zal het kabinet ook in een vroeg stadium kijken naar de benodigde financiering en capaciteit om dit toezicht effectief uit te voeren.

De leden van de D66-fractie achten het voor de concurrentie tussen Cloudaanbieders een belangrijke stap dat interoperabiliteit straks de standaard zal zijn. Kan de Minister toelichten van welke Cloudaanbieders de rijksoverheid gebruik maakt?

Er bestaan rijksbrede contractvoorwaarden voor clouddienstverlening, maar de verantwoordelijkheid voor het inkopen van dergelijke diensten is niet in alle gevallen centraal belegd. Er is daarom geen totaaloverzicht van alle clouddiensten die door alle verschillende onderdelen van de rijksoverheid worden gebruikt. SSC-ICT (verantwoordelijk voor ICT-voorzieningen van zeven ministeries) heeft in ieder geval contracten met de volgende cloudaanbieders:

- Microsoft (Office365, Teams en Azure);
- Fortes Change Cloud (SAAS-oplossing portfoliomanagement);
- Cisco (Web-ex).

De leden van de D66-fractie vernemen dat de onderhandelingen over het datadelen met de Verenigde Staten weer voortgang maken. Kan de Minister een laatste stand van zaken geven met betrekking tot privacy shield?

In het Schrems-II arrest van het Hof van Justitie van de Europese Unie (HvJEU) heeft het HvJEU het »adequaatheidsbesluit»[5] voor de VS ongeldig verklaard, onder meer vanwege zorgen omtrent overheidstoegang tot persoonsgegevens in de VS. Recent is er door de Europese Commissie en de VS een principeakkoord gesloten wat de basis zou kunnen vormen voor een nieuw adequaatheidsbesluit.[6] Onderdeel daarvan is onder meer dat de VS stappen zal zetten om de privacy van Europese burgers te beschermen.[7] In de komende maanden zal duidelijk worden welke precieze maatregelen de VS zal nemen. De Minister voor Rechtsbescherming zal uw Kamer van dit proces op de hoogte houden.

---

[5] Zie artikel 45 AVG Een adequaatheidsbesluit is een besluit van de Europese Commissie dat een derde land een »passend niveau van gegevensbescherming» biedt, wat betekent er rechtmatig persoonsgegevens naar dit land kunnen worden doorgegeven.

[6] «Joint Statement on Trans-Atlantic Data Privacy Framework» te raadplegen via: https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2087

[7] | The White House «FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework», te raadplegen via: https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/

Vragen en opmerkingen van de leden van de PVV-fractie

De leden van de PVV-fractie hebben kennisgenomen van de stukken en hebben daarover nog een aantal vragen. Deze leden hebben onder andere vragen over de uitzondering die gemaakt wordt voor het datadelen met zogenaamde poortwachtersbedrijven. Als gebruikers zelf eigenaar worden van hun data en zelf mogen bepalen met wie ze deze data delen, waarom maakt de verordening het delen met poortwachtersplatforms dan onmogelijk? Wat is de reden dat deze mogelijkheid wordt onttrokken aan de keuzevrijheid van gebruikers? Welk criterium bepaalt of gebruikers, die eigenaar zijn geworden van waardevolle data, deskundig genoeg zijn om te beoordelen wat de gevolgen zijn van het toestemming verlenen voor het gebruik van hun data? Welke voorkennis wordt verondersteld bij hen aanwezig te zijn om deze verantwoordelijkheid te kunnen uitoefenen op een manier waarop ze (later) geen nadeel ondervinden?

Poortwachters zijn grote platforms met een machtige positie waar gebruikers (consumenten en bedrijven) niet omheen kunnen. Deze bedrijven vervullen daadwerkelijk een «poortwachterspositie» op het internet. Om consumenten zoveel mogelijk keuzevrijheid te geven en concurrerende bedrijven te beschermen tegen de macht van de poortwachters, is in Europa speciale wetgeving in de maak: de Digital Markets Act (DMA). In de DMA worden poortwachters verplicht om gebruikers keuze en inzicht in het gebruik te geven van hun eigen data. De Dataverordening bevat, volledig in lijn met de DMA, daarom verschillende waarborgen om te voorkomen dat gebruikers toegang geven aan derde partijen waarop ze nadeel ondervinden. Ten eerste krijgen derde partijen (data-ontvangers) alleen datatoegang met toestemming van de gebruiker. Wanneer de dataontvanger conform genoemde procedure gegevens ontvangt, is de hoofdregel dat deze partij daar alleen mee doet wat expliciet is verzocht: de dataontvanger kan niet zomaar op eigen initiatief met die gegevens aan de slag. Dataontvangers mogen gebruikers bovendien op geen enkele manier dwingen, misleiden of manipuleren door de autonomie, besluitvorming of keuzes van de gebruiker te ondermijnen of te beperken. De Dataverordening schrijft aanvullend voor dat voor alle gebruikers van IoT-producten het ontzeggen van datatoegang aan een derde partij even makkelijk moet zijn als het geven van die toestemming. Tot slot blijven ook de regels over de bescherming van persoonsgegevens uit de AVG onverminderd van kracht.

De leden van de PVV-fractie hebben nog veel vragen en zorgen ten aanzien van de mogelijkheid voor overheden om data te vorderen bij bedrijven in geval van «uitzonderlijke behoefte». Bijvoorbeeld over de definitie; die wordt namelijk omschreven als louter in gevallen van uitzonderlijke behoefte, zoals noodsituaties en rampen, maar er staat ook dat dit mogelijk wordt in geval van het «uitvoeren van een publieke taak in het algemeen belang die expliciet bij wet is beschreven». Dat lijkt op het oog nogal ruim gedefinieerd, want dat laatste is toch immers het geval bij alle reguliere taken van de overheid? Op welke wijze zal deze Dataverordening bijdragen aan de prioriteiten en de doelstellingen van de Green Deal? Op welke wijze zullen burgers daar concreet mee te maken krijgen in hun dagelijks leven? Zou op grond van deze bepaling de overheid bijvoorbeeld toegang kunnen krijgen tot gegevens met betrekking tot stroomverbruik, voertuigdata en water- en gasverbruik van burgers, om te kunnen bepalen hoe «groen» en energiezuinig zij leven?

Het kabinet heeft vragen bij het voorgestelde kader om publieke instanties in gevallen van uitzonderlijke noodzaak gegevens bij datahouders op te laten vragen. Deze vragen zijn nog niet naar tevredenheid door de Europese Commissie beantwoord. Daarmee is voor het kabinet ook nog

onvoldoende duidelijk in welke situatie overheden binnen dit kader data op kunnen vragen. Het door de PVV-fractie geschetste scenario acht het kabinet onwenselijk en het is zeer onwaarschijnlijk dat de Dataverordening dat mogelijk zou maken. Maar het kabinet deelt de zorgen dat de gecreëerde bevoegdheid om in gevallen van uitzonderlijke noodzaak data op te vragen bij datahouders mogelijk te verstrekkend is. In de aankomende gesprekken zal het kabinet daar uitsluitsel over vragen.

Ondanks dat er nadrukkelijk wordt gesteld dat deze publieke bevoegdheid tot het opvragen van data niet kan worden ingezet voor strafrechtelijke- of bestuursrechtelijke rechtshandhavingsdoeleinden, vragen de leden van de PVV-fractie hoe dit uitgangspunt zich verhoudt tot het opvragen en verschaffen van data aan een publieke instantie voor «een specifieke wettelijke taak» en/of publieke taak in het algemeen belang, welke waarborgen deze verordening biedt tegen misbruik en of er, in dat laatste geval, ook rechtsmiddelen met adequate sancties door burgers kunnen worden ingeroepen. Hoe kan bijvoorbeeld worden voorkomen dat een overheid, die eerder data heeft opgevraagd en ontvangen in het kader van het voorkomen van of herstellen van een openbare noodsituatie óf voor het vervullen van een «specifieke wettelijke taak», diezelfde data later gebruikt voor strafrechtelijke- of bestuursrechtelijke handhavingsdoeleinden? Als dat toch gebeurt, welke sancties staan daar dan op en welke rechtsmiddelen kunnen de getroffen burgers of andere private partijen dan aanwenden? Dit klemt te meer nu het in beginsel de datahouder zelf is die dient te beoordelen of een dataverzoek van een publieke instantie aan de eisen voor verstrekking voldoen. Dit kan om uiteenlopende redenen leiden tot mogelijke terughoudend bij de ene partij en grote inschikkelijkheid bij de ander. Staat daarmee de rechtsbescherming niet op de tocht?

In principe sluit het voorstel uit dat data die in geval van uitzonderlijke noodzaak wordt opgevraagd later voor handhavingsdoeleinden kan worden gebruikt. Zoals eerder in deze beantwoording aangegeven heeft het kabinet wel zorgen dat de gecreëerde bevoegdheid om in gevallen van uitzonderlijke noodzaak data op te vragen bij datahouders te verstrekkend is en dat het voorgestelde kader te weinig waarborgen omvat. Het kabinet is het met de leden eens dat de voorgestelde systematiek voor het opvragen van gegevens verbetering behoeft.

De Autoriteit Persoonsgegevens is verantwoordelijk voor het toezicht op de bescherming van persoonsgegevens op grond van de AVG en dat zal ook het geval zijn in zoverre het gebruik of delen van persoonsgegevens binnen de reikwijdte van deze verordening valt. Voor de handhaving van de overige delen van de verordening, kunnen lidstaten zelf bepalen welke autoriteit ze daarvoor aanwijzen. Op grond van artikel 32 kunnen klachten worden ingediend bij de relevante autoriteit en op grond van artikel 33 moeten lidstaten een boetestelsel vastleggen.

Wat is de reden dat de Europese Commissie vindt dat alle data die beschikbaar is, ook «te gelde» gemaakt moet worden? Deelt het Nederlandse kabinet deze visie? Hoe kunnen burgers die hechten aan zoveel mogelijk anonimiteit hun recht op «vergeten te worden» nog uitoefenen als deze verordening van kracht wordt? Wat zijn de opt-out mogelijkheden voor burgers (en bedrijven)? Hoe verhoudt dit zich met de opt-out mogelijkheden die zij in de huidige situatie hebben, dus zonder deze dataverordening?

De AVG en het recht om «vergeten te worden» blijven onverminderd van kracht. De Dataverordening schrijft aanvullend voor dat voor alle gebruikers van IoT-producten het ontzeggen van datatoegang aan een

derde partij even makkelijk moet zijn als het geven van die toestemming. De dataverordening versterkt daarmee tevens de opt-out mogelijkheden van burgers.

De hoofddoelstelling van de Dataverordening is een eerlijkere verdeling van de waarde van de data over de deelnemers aan de data-economie. Daarbij is tevens het doel om consumenten en bedrijven meer controle te geven over hun data. Het kabinet deelt de visie dat gebruikers de door hun gebruik gegenereerde gegevens moeten kunnen (laten) gebruiken voor hun eigen doeleinden, vrijwillig datadelen is daarbij een uitgangspunt. Momenteel is het in veel gevallen echter zo dat data uit IoT-producten alleen door de aanbieder van een IoT-product kan worden gebruikt terwijl die data ook nuttig kunnen zijn voor andere partijen dan de fabrikant. Door gebruikers het recht te geven deze data zelf te gebruiken of door derde partijen te laten gebruiken zal de data uit IoT-producten, op verzoek van de gebruiker, door meer partijen en daarmee voor meer verschillende doelen gebruikt kan worden. Zo wordt de waarde van data eerlijker verdeeld over de deelnemers aan de data-economie.

De leden van de PVV-fractie vragen, tot slot, wat het eventuele effect is van de uitspraak van het Italiaanse Constitutionele Hof in de zaak 14381/2021 op de Dataverordening. In deze uitspraak werd geoordeeld dat eerder verleende toestemming voor het delen van data niet geldig is – lees: in strijd met de General Data Protection Regulation (GDPR) – indien de datahouder/-verzamelaar onvoldoende transparantie heeft betracht rondom eventuele algoritmes. Welke gevolgen zou de hiervoor genoemde uitspraak kunnen hebben op de voorliggende dataverordening?

De AVG en daaraan verbonden bescherming van persoonsgegevens blijft onverkort gelden ook na introductie van de voorliggende dataverordening. De uitspraak heeft zover ik weet geen direct effect op de Dataverordening.

Vragen en opmerkingen van de leden van de CDA-fractie

De leden van de CDA-fractie hebben kennisgenomen van de onderhavige stukken. Deze leden hebben daarover de volgende vragen en opmerkingen. In het fiche Dataverordening staat geschreven dat de data-ontvanger de verkregen data bijvoorbeeld niet mag gebruiken voor profilering van de gebruiker tenzij dit noodzakelijk is voor de verleende dienst. Deze leden vragen wanneer dit noodzakelijk zou zijn. Wat zijn de maatstaven die beoordelen of dit noodzakelijk is?

De dataontvanger ontvangt de gegevens op basis van het in artikel 5 vastgelegde recht van gebruikers om hun gegevens naar een derde partij over te dragen; het vindt dus plaats op verzoek van de betrokkene in het geval er persoonsgegevens worden verwerkt. In artikel 5 lid 9 is ook vastgelegd dat er daarbij geen negatieve impact mag ontstaan op de gegevensbeschermingsrechten van derden. Wanneer de dataontvanger conform genoemde procedure gegevens ontvangt is de hoofdregel dat deze partij daar alleen mee doet wat expliciet is verzocht: de dataontvanger kan niet zomaar op eigen initiatief met die gegevens aan de slag. Dit is vastgelegd in artikel 6 lid 1. Als extra waarborg zijn in artikel 6 lid 2 nog een aantal expliciete verboden opgenomen, waaronder dat er in principe geen profilering mag worden toegepast tenzij dit het doel van de verstrekking is om een dienst te leveren. In het geval dat profilering noodzakelijk is voor de verleende dienst gelden daar bovenop onverminderd de regels omtrent de verwerking van persoonsgegevens uit de AVG. Middels de dataverordening worden alleen aanvullende regels

gesteld, er mag geen afbreuk aan het beschermingsniveau worden gedaan.

De leden van de CDA-fractie zijn blij gesteld dat de positie van het mkb verder versterkt wordt. Wel zijn deze leden van mening dat het onvoldoende duidelijk is hoe in de praktijk getoetst wordt of de contractvoorwaarden oneerlijk en eenzijdig zijn. Graag zouden deze leden hier meer duidelijkheid over ontvangen.

Artikel 13 omschrijft praktijken die ertoe leiden of kunnen leiden dat een contractvoorwaarde als oneerlijk wordt gezien. Over de toetsing van de eenzijdige oplegging van contractvoorwaarden heeft het kabinet de Commissie om opheldering gevraagd. De toetsing van deze bepalingen is aan de toezichthouder en in het geval van een geschil uiteindelijk aan de rechter.

De leden van de CDA-fractie lezen dat gebruikers kosteloos toegang kunnen krijgen tot hun data, maar wel een redelijke compensatie voor datatoegang moeten betalen. Hoe komt de redelijke compensatie tot stand? Hoe wordt er toezicht op gehouden dat dit daadwerkelijk redelijk is? Komen en richtlijnen waar gebruikers zelf kunnen toetsen of dit redelijk is?

Gebruikers zelf krijgen altijd kosteloos toegang. Alleen aan derde partijen die toegang krijgen tot data uit een IoT-product na toestemming van de gebruiker mag een redelijke compensatie gevraagd worden. De hoogte van de compensatie dient onderbouwd te worden door de vragende partij. Voor mkb-bedrijven geldt, wanneer zij als derde partij toegang willen krijgen tot data, dat de gevraagde compensatie niet hoger mag zijn dan de kosten die direct aan het beschikbaar maken van de data verbonden zijn. Onder de Data Act zullen geschilbeslechtingsorganen worden opgericht om te zorgen dat bedrijven bij geschillen hierover niet altijd naar de rechter hoeven te stappen en meer laagdrempelige toegang hebben tot onafhankelijke geschilbeslechting.

De leden van de CDA-fractie lezen in het hoofdstuk over financiële consequenties lezen dat er niet tot nauwelijks indicaties worden gegeven wat dit zou betekenen voor Nederland. Graag zouden deze leden hier uitgebreidere informatie over ontvangen.

De door de Europese Commissie uitgevoerde «impact assessments» die voorstellen begeleiden bevatten inschattingen van regeldruk voor de Europese Unie, zonder specificatie per lidstaat. Het is op basis van de door de Commissie gemaakte inschattingen vooralsnog niet mogelijk de effecten goed te vertalen naar de gevolgen voor specifieke bedrijven en sectoren in Nederland.
De Commissie heeft aangegeven dat de consequenties op lidstaatniveau nu lastig te bepalen zijn, maar dat alle gedane studies aantonen dat in het algemeen de maatschappelijke en economische baten aanzienlijk groter zijn dan de lasten.

Vragen en opmerkingen van de leden van de SP-fractie

De leden van de SP-fractie hebben de Dataverordening en de reactie van het kabinet daarop gelezen en hebben hierover nog enkele opmerkingen en vragen.
De leden van de SP-fractie lezen dat het voorstel bedoeld is om kleine en middelgrote bedrijven aan te zetten om actief te worden in de data-economie. Deze leden zien uiteraard ook dat deze data-economie bestaat en dat daar veel grote belangen spelen. Zij betreuren echter dat de

vraag naar in hoeverre een data-economie wenselijk is amper bediscussieerd is. Vindt het kabinet het wenselijk dat er winst gemaakt wordt op de handel in data van mensen, laat staan dat dit gestimuleerd dient te worden? Wil Nederland een «bloeiende data-economie, waarin data gemakkelijk kunnen worden gedeeld binnen en tussen sectorale ecosystemen» zoals de verordening stelt? Kan het kabinet daarop reflecteren?

Het kabinet verwelkomt, in lijn met het Nederlandse non-paper voor de dataverordening, dat op 14 oktober jl. naar de Tweede Kamer is gestuurd, dat er aandacht is voor de versterking van grip op gegevens voor consumenten en bedrijven. Op deze manier wordt de reeds bestaande data-economie eerlijker gemaakt, en wordt de waarde van data beter verdeeld over de deelnemers van de data-economie. Daar zijn in de dataverordening verschillende waarborgen voor opgenomen, onder andere met betrekking tot de rol van poortwachtersplatforms. Bovendien kan data een belangrijke rol spelen bij onderzoek en innovatie, het oplossen van maatschappelijke vraagstukken en het benutten van de economische kansen van de digitale transitie.

Ook verwelkomt het kabinet dat naar generieke standaarden en afspraken wordt gekeken om verantwoorde datadeling te bevorderen en dat betrokken partijen meer duidelijkheid krijgen over de mogelijkheden, voorwaarden en opties tot controle bij datadeling. Het kabinet deelt de visie dat gebruikers de door hun gebruik gegenereerde gegevens moeten kunnen (laten) gebruiken voor hun eigen doeleinden.

De leden van de SP-fractie vinden het goed als mensen meer zeggenschap krijgen over hun eigen data. Deze leden lezen dat het voorstel wil regelen dat consumenten moeten instemmen als er data gedeeld wordt met een derde partij. Deze leden onderschrijven dat meer zeggenschap voor mensen over wat er met hun data gebeurt toe. Zij vragen echter wel of het voorstel daar daadwerkelijk in voorziet. Zij vrezen het risico dat dit een wassen neus wordt, bijvoorbeeld als consumenten door uitsluiting alsnog gedwongen worden toestemming te verlenen tot datadeling of, zoals gebeurt bij instemmingsverklaringen bij algemene voorwaarden of cookies, wat voor veel mensen begrijpelijkerwijs een automatisme is. Zou bij datadeling door bedrijven niet altijd het principe «nee, tenzij» gehanteerd moeten worden, waarbij altijd expliciete en overduidelijke toestemming vereist is door de consument? Kan het kabinet hier nader op reflecteren? Vindt het kabinet het te verantwoorden dat het voorstel een grote mate van verantwoordelijkheid neerlegt bij consumenten, die hoogstwaarschijnlijk niet allemaal op de hoogte zijn van de betreffende privacyregels, de Dataverordening en/of over de technische kennis beschikken om te kunnen overzien wat er precies met hun data gebeurt?

Onder artikel 5 van de Dataverordening moet het delen van data uit IoT-producten met een derde partij altijd gebeuren op verzoek van de gebruiker. Het kabinet is positief dat het recht op, en daarmee de zeggenschap over, het hergebruik van data bij de gebruiker ligt en dat de aanbieder van een product of dienst en data-ontvanger daarnaast aanvullende regels krijgen opgelegd om de belangen van alle betrokkenen te waarborgen. Zo wordt de rol en verantwoordelijkheid van alle partijen verduidelijkt en worden de belangen van de bij datadeling betrokken partijen beter geborgd. Data-ontvangers mogen onder de Dataverordening data alleen gebruiken voor de doelen die het met de gebruiker is overeengekomen. Data-ontvangers mogen gebruikers bovendien op geen enkele manier dwingen, misleiden of manipuleren door de autonomie, besluitvorming of keuzes van de gebruiker te ondermijnen of te beperken. De regels omtrent de verwerking van persoonsgegevens uit de AVG gelden onverminderd. Middels de dataverordening worden alleen

aanvullende regels gesteld, er mag geen afbreuk aan het beschermingsniveau worden gedaan.

De leden van de SP-fractie vragen naar de uitzondering dat derde partijen wel gebruik mogen maken van dataverwerkingsdiensten die door een aangewezen poortwachter worden aangeboden. Deze uitsluiting van aangewezen poortwachters van het toepassingsgebied van het toegangsrecht uit hoofde van deze verordening belet deze ondernemingen niet om data op andere legale wijze te verkrijgen. Kan het kabinet aangeven dat als deze verordening in werking treedt, de mogelijkheid om voor multinationals als Amazon via in een Nederland gevestigd bedrijf die autosoftware maakt, voet aan de grond te krijgen wordt geblokkeerd of gehinderd? Zo ja, hoe en in welke mate? Zo nee, waarom niet?

Onder de Dataverordening kunnen poortwachterplatforms niet als derde partij toegang tot data uit IoT-producten of verwante diensten krijgen. Ook verbiedt de Dataverordening datahouders om de onder de verordening verkregen data te delen met poortwachterplatforms. Onder poortwachterplatforms worden voor de Dataverordening ook alle juridische entiteiten van een groep ondernemingen waar het poortwachterplatform van uitmaakt verstaan. Daarmee zou de Dataverordening het door de SP-fractie geschetste scenario moeten bemoeilijken.

De leden van de SP-fractie maken zich zorgen over het voorstel dat overheden data van bedrijven kunnen vorderen. Hoewel deze leden dit uiteraard begrijpelijk achten in het geval van crises zoals genoemd, bosbranden en natuurrampen, zien zij ook het gevaar voor oneigenlijk gebruik van data door overheden. Hoewel de data niet gebruikt mag worden voor opsporingsdoeleinden, kan data opgevraagd van fabrikanten van bijvoorbeeld beveiligingscamera's in zeer grote mate privacy schendende gevolgen hebben. Deze leden lezen ook dat overheden data bij bedrijven kunnen opvragen als er hinder is bij het uitvoeren van een publieke taak in het algemeen belang (die expliciet bij wet is beschreven) en die data niet langs andere weg kan worden verkregen. Deze leden vinden deze mogelijkheid expliciet creëren zorgwekkend omdat het begrip algemeen belang voor velerlei uitleg vatbaar is. Kan het kabinet aangeven onder welke omstandigheden zij dit voorstel zouden steunen?

Het is het kabinet ook nog onvoldoende duidelijk hoe verstrekkend de bevoegdheid is om data op te vragen voor het uitvoeren van een publieke taak in het algemeen belang. Als de Europese Commissie meer duidelijk heeft gegeven over het voorgestelde kader zal het kabinet beoordelen hoe de voorziene verplichtingen zich verhouden tot de daarmee in bepaalde gevallen gemoeide inbreuk op grondrechten, waaronder het recht op privacy.

Vragen en opmerkingen van de leden van de Volt-fractie

De leden van de Volt-fractie hebben met interesse kennisgenomen van de Nederlandse positie ten aanzien van het voorstel voor een Dataverordening. Over de Dataverordening en de Nederlandse positie hebben deze leden nog enkele vragen.

Faciliteren van toegang tot, en gebruik van, data door consumenten en bedrijven

De leden van de Volt-fractie merken op dat de Dataverordening ervan uit lijkt te gaan dat fabrikanten van verbonden producten (behorende tot het internet der dingen) feitelijke controle hebben over bepaalde data. Overweging vijf van de Dataverordening maakt duidelijk dat er geen

rechtsgrondslag is voor de toegang tot gegevens voor fabrikanten. In de wettekst is dit minder duidelijk. Deze leden zien graag dat fabrikanten alleen toegang tot data krijgen, waaronder begrepen persoonsgegevens, indien daar een expliciete contractuele basis voor is met de juiste waarborgen in plaats (zoals productveiligheid en updates).

Wat betreft de verwerking van persoonsgegevens blijft de AVG onverminderd van kracht. Overweging vijf van de Dataverordening benoemt expliciet dat de Dataverordening geen nieuwe rechtsgrondslag creëert, noch bestaande rechtsgrondslagen erkent, die de datahouder mogelijkheden geeft om data gegenereerd door het gebruik van een product of gerelateerde dienst te controleren of te gebruiken. De overweging gaat er wel vanuit dat de datahouder, dit kan een fabrikant van een IoT-product zijn, op dit moment effectief wel controle of toegang tot data heeft.

Er zitten diverse beperkingen in het materiële toepassingsgebied van de Dataverordening. Heel specifiek vragen de leden van de Volt-fractie waarom pc's, servers, tablets en smartphones niet onder de verordening vallen. Is dat omdat deze apparaten primair data verwerken of opslaan en niet creëren? Acht het kabinet dit wenselijk en verklaarbaar? Zo ja, waarom? Hoe oordeelt het kabinet over het gegeven dat onlinediensten niet onder de verordening vallen?

Het kabinet beziet nog of het samenstel van maatregelen uit de Dataverordening en de voorgestelde materiële reikwijdtes voldoende bijdraagt aan het versterken van grip op gegevens en of dit voldoende toekomstbestendig is. Het kabinet bevraagt de Europese Commissie hierover. De expliciete uitsluiting van pc's, servers en tablets van de reikwijdte hoofdstuk 2 van de Dataverordening is één van de aspecten die het kabinet daarbij meeweegt. Enkel product gerelateerde online diensten vallen onder hoofdstuk 2, online diensten vallen wel onder de verordening voor zover deze onder de definitie van dataverwerkingsdiensten vallen. In hoofdstuk 6 van de dataverordening worden specifieke maatregelen getroffen voor dataverwerkingsdiensten. Ook dit is één van de aspecten die het kabinet meeneemt in deze beoordeling. Het kabinet beziet hierbij nog de precieze afbakening van de definitie van dataverwerkingsdiensten.

Het kabinet schrijft dat artikel 35 specificeert dat het sui generis recht uit de Databankenrichtlijn niet van toepassing is op de databanken die gegevens bevatten die zijn gegenereerd door het gebruik van een product of gerelateerde dienst. Dit om afbreuk aan gebruiks- en toegangsrechten voor gebruikers te voorkomen. Hoe verhoudt deze bepaling zich tot de Databankenrichtlijn? Is het een specificatie van de Databankenrichtlijn? Of moet het worden gezien als een uitsluitingsgrond ten opzichte van bepaalde data voor het recht uit de Databankenrichtlijn?

De Databankenrichtlijn van 1996 voorziet in een tweeledige structuur van bescherming van intellectueel eigendom: voor originele databanken via het auteursrecht en een specifiek sui generis recht voor databanken (inclusief «niet-originele» databanken) als de kwalitatieve of kwantitatieve investering in het verkrijgen, controle of presenteren van de gegevens substantieel was. Sinds die tijd zijn bedrijven die zich hier mee bezig houden en data(bank)technologieën geëvolueerd en hebben investeringen in gegevens aan belang gewonnen. De interactie van de Databankenrichtlijn met de huidige data-economie, met name gezien de mogelijke toepassing van het sui generis recht op databanken met door machines of in het kader van IoT gegenereerde gegevens, kan ongewenste effecten opleveren. Artikel 35, in samenspraak met overweging 84, van de Dataverordening verduidelijkt daarom dat het sui generis databankenrecht niet van toepassing is op databanken die data bevatten die door de

Dataverordening worden bestreken. De Databankenrichtlijn wordt niet aangepast en artikel 35 Dataverordening is geen aanvulling op de Databankenrichtlijn. Het doel is de afbakening van beide instrumenten te verduidelijken en zo onjuist gebruik van het sui generis recht op databanken te voorkomen en daarmee de juiste toepassing van de Dataverordening te bevorderen.

De begrippen «toegang» en «gebruik» zijn niet in de Dataverordening gedefinieerd. Het blijft dus onduidelijk welke rechten er voor gebruikers en producenten (en eventuele tussenpersonen) ontstaan. Het is goed om de rechten van gebruikers en producenten te verduidelijken. Het kabinet geeft ook aan zorgen te hebben over hoe gebruikers hun rechten in de praktijk kunnen uitoefenen. Kan het kabinet voorbeelden geven?

Deze zorgen hebben er betrekking op dat het voorstel geen gerichte maatregelen bevat om de interoperabiliteit te bevorderen zodat gebruikers hun toegangs- en gebruiksrechten in de praktijk kunnen uitoefenen. Om data daadwerkelijk te kunnen hergebruiken moet de data-ontvanger ook toegang krijgen op een manier die het mogelijk maakt om ook echt met de data aan de slag te gaan. Als een garage voor de reparatie van een slim vervoersmiddel alleen toegang tot ongestructureerde data over dit vervoersmiddel zou krijgen kan de monteur hiermee geen analyses doen of de auto repareren. Hiervoor moeten de systemen van de datahouder en data-ontvanger «interoperabel» zijn, ofwel in staat zijn tot (effectieve) onderlinge communicatie en uitwisseling van data. Hoofdstuk 8 voorziet in het vereisten voor de interoperabiliteit van data. Het kabinet bekijkt nog nader of dit hoofdstuk genoeg waarborgen voor een functionele interoperabiliteit van data bevat om te zorgen dat gebruiks- en toegangsrechten gewaarborgd worden.

De Dataverordening beoogt voor elkaar te krijgen dat gebruikers eigenaar worden van hun eigen data. In hoeverre slaagt de Dataverordening daarin, volgens het kabinet? Hoe ziet dit er concreet uit? Hoe kunnen gebruikers de toegang tot hun data in de praktijk weer ontzeggen als deze eenmaal is gedeeld?

De Dataverordening voorziet expliciet niet in (juridisch) eigenaarschap van data, maar voorziet in gebruiks- en toegangsrechten. Dit geeft gebruikers meer controle over de eigen data en daarmee meer grip op gegevens. Ten slotte draagt dit bij aan een eerlijkere verdeling van de waarde van data over de deelnemers aan de data-economie. De geschetste maatregelen en vooral de ingestelde toegangsrechten voorzien hier goed in als horizontale basis. Sectoraal kunnen aanvullende eisen gesteld worden waar nodig. De AVG, en het daarin onder meer vervatte recht om «vergeten te worden» blijven onverminderd van kracht. De Dataverordening schrijft aanvullend voor dat data-ontvangers gebruikers op geen enkele manier mogen dwingen, misleiden of manipuleren door de autonomie, besluitvorming of keuzes van de gebruiker te ondermijnen of te beperken.
Bovendien moet voor gebruikers van IoT-producten het ontzeggen van datatoegang aan een derde partij even makkelijk zijn als het geven van die toestemming.

Het beschermen van mkb tegen oneerlijke handelspraktijken

Het kabinet geeft aan dat een verbreding van de reikwijdte proportioneel en duidelijk gedefinieerd moet zijn, om onevenredig zware lasten voor aanbieders van diensten te voorkomen. Eventuele sectorale regelgeving kan dan geschikter zijn om specifieke problemen gericht te adresseren. Tegelijkertijd zou het kabinet ook andere maatregelen kunnen nemen om

te voorkomen dat de regeldruk voor het mkb te groot wordt, door bijvoorbeeld bijstand aan te bieden. Hoe ziet het kabinet dit? Is een fundamentele koerswijziging zoals de Dataverordening (generiek) probeert te regelen niet juist hoe we naar de economie van de toekomst moeten kijken? Is het kabinet het met de leden van de Volt-fractie eens dat we juist moeten kijken hoe we het mkb kunnen ondersteunen in de aanpassing aan voorstellen die ten gunste komen van de samenleving?

Het kabinet ziet het belang van een toekomstbestendig horizontaal kader dat bepaalde basisprincipes voor de hele economie vastlegt. De horizontale basisregels laten binnen het door de Dataverordening gestelde kader ruimte voor verschillende sectorale oplossingen om verdere invulling aan de toegangs- en gebruiksrechten te geven. De conceptverordening kent diverse voorstellen die bijdragen aan de data-economie en een eerlijke verdeling van de waarde van data over de deelnemers daarin, in het bijzonder ook aan het mkb. Daarbij worden bijvoorbeeld aanvullende maatregelen genomen om het mkb te beschermen tegen oneerlijke handelspraktijken, zoals eenzijdige contractvoorwaarden. Ook met betrekking tot de mogelijkheid om compensatie te vragen voor het beschikbaar stellen van data zijn er waarborgen specifiek gericht op het mkb ingesteld.

De waarborgen uit de artikelen 5 en 6 van de Dataverordening bevatten waarborgen voor onder meer het beschermen van bedrijfsgeheimen. Het kabinet gaat nader onderzoeken of die waarborgen voldoende zijn. Hoe oordeelt het kabinet over de zorg dat artikel 6 lid 2 sub e multi-interpretabel is en bedrijven mogelijk afschrikt om gebruik te maken van de data, omdat dat kan leiden tot schadeclaims? Is deze bepaling voldoende specifiek volgens het kabinet?

Het kabinet ziet deze bepaling als voldoende specifiek en is niet van mening dat dit artikel multi-interpretabel is.

Het faciliteren van toegang tot private data voor overheidsinstanties in gevallen van uitzonderlijke noodzaak

De leden van de Volt-fractie hebben vaker gevraagd naar de beschikbaarheid van data voor onderzoeksinstellingen en universiteiten, zodat beter onderzoek kan worden gedaan en kennis gecreëerd kan worden voor de samenleving. Het kabinet beziet nog of hergebruik van data door publieke instanties zoals onderwijs- en onderzoeksinstellingen voldoende faciliteert. Indien dit niet het geval is, gaat het kabinet er dan voor pleiten dat deze directe datadeling mogelijk wordt gemaakt?

Dit vraagstuk heeft betrekking op hoofdstuk 2 uit de dataverordening en de mogelijkheid voor deze instellingen om toegang te krijgen tot data uit IoT-producten. Het kabinet beziet nog of in het huidige voorstel voor een verordening voldoende mogelijk is voor publieke instanties om toegang te krijgen tot deze data en of dit tegen een gereduceerd tarief kan. Tevens beziet het kabinet nog op welke manier publieke instanties zoals onderwijs- en onderzoeksinstellingen binnen de definities van de dataverordening vallen en hoe de gebruikersdata van onderwijs IoT-producten binnen de reikwijdte vallen. Op basis van de uitkomsten hiervan zal het kabinet later de positie op dit punt bepalen.

Het vergemakkelijken van overstappen tussen cloud- en edgediensten

De Europese Commissie beoogt de interoperabiliteit tussen verschillende cloud-aanbieders te vergroten. Het moet makkelijker worden voor gebruikers om van de ene dienst op de andere dienst over te stappen. Dit

versterkt het recht op dataportabiliteit uit de AVG. Welke standaarden moeten volgens het kabinet de Europese standaard worden wat betreft dataportabiliteit? Met welke belangenorganisaties en partijen spreekt het kabinet op dit moment over deze normen?

Om overstappen tussen dataverwerkingsdiensten makkelijker te maken is interoperabiliteit een voorwaarde. Hiervoor hanteert de overheid een openstandaardenbeleid, omdat het gebruik van open standaarden bijdraagt aan leveranciersonafhankelijkheid. Als stakeholder neemt de Nederlandse overheid deel aan een veelheid van internationale en Europese fora waarin gebruikers en industrie samenwerken om deze open standaarden te ontwikkelen en vast te stellen, denk hierbij aan het Europees Telecommunicatie en Standaardisatie Instituut (ETSI), de Europese Commissie voor Normalisatie (CEN), de Europese Commissie voor Elektrotechnische Standaardisatie (CENELEC), de Internationale Telecommunicatie-unie (ITU), etc. Het kabinet zal zelf echter geen standaarden voorschrijven. De Dataverordening geeft de Europese Commissie het mandaat om met dergelijke partijen in contact te treden over het opstellen van standaarden.

Om te voorkomen dat interoperabiliteitsinspanningen stranden bij goede intenties is het van belang dat naast een focus op data, ook wordt gekeken naar de interoperabiliteit tussen softwaremodaliteiten van cloud-aanbieders en dataruimtes. Hoe oordeelt het kabinet hierover?

Het kabinet verwelkomt de aandacht voor interoperabiliteit in het voorstel en ziet interoperabiliteit als belangrijke voorwaarde voor een goed functionerende data-economie. Het kabinet deelt de zorg dat interoperabiliteitsinspanningen kunnen stranden bij goede intenties. Behalve de ontwikkeling van interoperabiliteitsstandaarden is ook brede implementatie ervan nodig, waarbij de focus breder dan data alleen moet liggen. Om deze reden zijn ook dataverwerkingsdiensten onderwerp van regulering. Belangrijk is dat wordt voorgebouwd op- en aangesloten bij lopende (sectorale) initiatieven om silovorming te voorkomen. Het kabinet steunt het voornemen om de Commissie mandaat te geven om normalisatieorganisaties te verzoeken standaarden te ontwikkelen. Het kabinet is positief dat er specifiek aandacht is voor de interoperabiliteit van dataverwerkingsdiensten en dat de Commissie de bevoegdheid krijgt om met gedelegeerde handelingen standaarden voor de interoperabiliteit van dataverwerkingsdiensten status te geven. Dat is van groot belang om het overstappen tussen dataverwerkingsdiensten in de praktijk mogelijk te maken. Hier zal tijdens de onderhandelingen over de Dataverordening ook door Nederland over worden doorgevraagd. De interoperabiliteit van softewaremodaliteiten wordt al geadresseerd door de Dataverordening.

Het creëren van waarborgen tegen onrechtmatige dataoverdracht

De leden van de Volt-fractie willen benadrukken dat de Dataverordening geen parallelle structuur moet optuigen met betrekking tot het verwerken van persoonsgegevens. Verwerking van persoonsgegevens zouden alleen verwerkt mogen worden onder (volledige) toepassing van de AVG. Het kabinet steunt dat standpunt, maar kan het kabinet een overzicht geven van de knelpunten die zij ziet en wat zij voornemens is daaraan te doen? Worden daarbij ook belangen van burgers geraakt?

De regels omtrent de verwerking van persoonsgegevens uit de AVG gelden onverminderd. Middels de dataverordening worden alleen aanvullende regels gesteld, er mag geen afbreuk aan het beschermingsniveau worden gedaan. De Dataverordening voorziet in gebruiks- en toegangsrechten van IoT apparaten en aanverwante diensten. Dit geeft

gebruikers meer controle over de eigen data en daarmee meer grip op gegevens. Ten slotte draagt dit bij aan een eerlijkere verdeling van de waarde van data over de deelnemers aan de data-economie. De Dataverordening zet nadrukkelijk geen parallelle structuur op.

Om onrechtmatige datastromen te voorkomen, «verwelkomt» het kabinet dat de Europese Commissie richtsnoeren zal opstellen ten behoeve van de uitvoering van maatregelen om dit te voorkomen. Welke aspecten wil het kabinet terugzien in die richtsnoeren? Hoe gaat het kabinet daarop toezien? Zijn richtsnoeren het juiste middel volgens het kabinet?

Het kabinet verwelkomt de maatregelen in de Dataverordening om onrechtmatige internationale datastromen of toegang te voorkomen bij niet-persoonlijke data in dataverwerkingsdiensten. Deze maatregelen lijken bij te dragen aan een betere bescherming van niet-persoonlijke data wanneer deze bij cloudaanbieders staat opgeslagen. Het kabinet heeft wel aandacht voor het mogelijk ontstaan van rechtsmachtsconflicten doordat aanbieders van dataverwerkingsdiensten door de voorgestelde maatregelen eventueel worden verplicht geen gehoor te geven aan rechterlijke uitspraken of beslissingen van overheidsinstanties uit derde landen. Hier dient bij het opstellen van richtsnoeren ook rekening mee te worden gehouden. Het kabinet wil dit blijven bezien in het licht van het belang van internationale data stromen voor digitale handel, onderzoek en innovatie en heeft nog vragen over de uitwerking van deze maatregel in de praktijk. Richtsnoeren zijn een nuttig middel om te zorgen dat deze maatregelen consistent worden geïnterpreteerd en uitgevoerd door bedrijven. Aanvullend kunnen bedrijven toezichthouders om informatie vragen over de rechtmatigheid van internationale datastromen. Het doel van de voorgestelde richtsnoeren is om ervoor te zorgen dat bedrijven duidelijkheid hebben aan welke verzoeken ze wel en niet dienen te voldoen. Het toezien op de toepassing van deze richtsnoeren en de rechtsbescherming van datahouders en -gebruikers vindt plaats via toezichthouders.

Het kabinet geeft aan het toezicht voor zover het bescherming van persoonsgegevens betreft bij de Autoriteit Persoonsgegevens te laten. Kan het kabinet aangeven hoe zij voornemens is het toezicht op de Dataverordening verder in te richten?

Het kabinet gaat nog onderzoeken hoe het toezicht in Nederland effectief kan worden ingericht, waarbij in eerste instantie wordt gekeken naar bestaande toezichthouders (waaronder de ACM en de AP en AT. De Autoriteit Persoonsgegevens is verantwoordelijk voor het toezicht op de bescherming van persoonsgegevens op grond van de AVG en dat zal ook het geval zijn in zoverre het gebruik of delen van persoonsgegevens binnen de reikwijdte van deze verordening valt. Voor het beleggen van nieuwe toezichtstaken zal het kabinet ook in een vroeg stadium kijken naar de benodigde financiering en capaciteit. Het kabinet verwacht dat de Dataverordening vrij omvangrijke toezichtstaken met zich mee zal brengen, maar hier is op dit moment nog geen precieze inschatting van te maken.

Wat zijn de ervaringen met de Data Sharing Coalition? Hoe brengt het kabinet de visie onder de aandacht bij Europese lidstaten en de Europese Commissie? Om welke lidstaten gaat het? Hoe wordt de visie door deze lidstaten ontvangen?

Het kabinet steunt de inzet van de Data Sharing Coalition om meer economische en maatschappelijke waarde uit data te halen met grip op de data, conform de visie op datadeling. De coalitie is opgericht in 2019 bestaat inmiddels uit 56 partijen, afkomstig uit vele verschillende

sectoren. Zij delen de kennis die nodig is om datadeling tussen sectoren mogelijk te maken, dit omdat er veel technische, juridische en operationele belemmeringen zijn die moeten worden opgelost om data interoperabel te maken. Daarnaast worden momenteel diverse *use-cases* uitgewerkt die van nut zijn voor alle sectoren die data willen delen, om interoperabiliteit te stimuleren.

De kabinetsvisie op datadelen tussen bedrijven is sinds het verschijnen in 2019 vele malen onder de aandacht gebracht in bilaterale gesprekken met EU lidstaten en via diverse evenementen. De visie is zeer goed ontvangen en heeft mede als inspiratie gediend voor diverse andere beleidsinitiatieven op het terrein van data. Voorbeelden hiervan zijn de door de Europese Commissie gepresenteerde datastrategie, de Duitse datastrategie en het GAIA-X initiatief.

Het kabinet oordeelt negatief over beperkingen van de Dataverordening van het stimuleren van eenvoudig data delen binnen sectoren en niet door sectoren heen? Wat gaat zij hier aan doen?

Het kabinet steunt juist de keuze van de Commissie voor horizontale wetgeving die basisregels voor het gebruik van data voor alle sectoren vastlegt, zoals aangegeven in het BNC-fiche. Ook steunt het kabinet de keuze dat de Dataverordening als lex generalis geen afbreuk doet aan bestaande of toekomstige EU-wetgeving die het hergebruik van specifieke data reguleert. Aangezien het niet in de impact analyse is meegenomen, zal het kabinet wel aandacht vragen hoe voorkomen wordt dat belemmeringen ontstaan voor het datadelen tussen sectoren, bij (sectorale) wetgeving.

De Dataverordening lijkt verbinding met de Data Governance Act (DGA) te missen. Kan het kabinet toelichten waarom de definitie van «Europese gegevensruimte» uit de DGA lijkt te ontbreken, zoals die wel in de DGA is opgenomen? Hoe oordeelt het kabinet over het vervangen van het begrip «open normen» door open interoperabiliteitsspecificaties?

Het kabinet heeft de voorkeur om waar mogelijk in de Dataverordening dezelfde definities aan te houden als in de Data Governance Act, aangezien beide wetgevingsvoorstellen onderdeel zijn van de Europese datastrategie. De beide wetsvoorstellen beogen echter andere doelen te bereiken. Dit kan ten grondslag liggen aan verschillen in de opgenomen definities en bepalingen. «Open normen» en «open interoperabiliteitspecificaties» zijn verschillende begrippen, waarbij de term «open normen» op een breder begrippenkader betrekking kan hebben.