Europees wetsvoorstel Dataverordening

Standpunten VNO-NCW/MKB-Nederland over het Europese voorstel voor een Dataverordening nader toegelicht

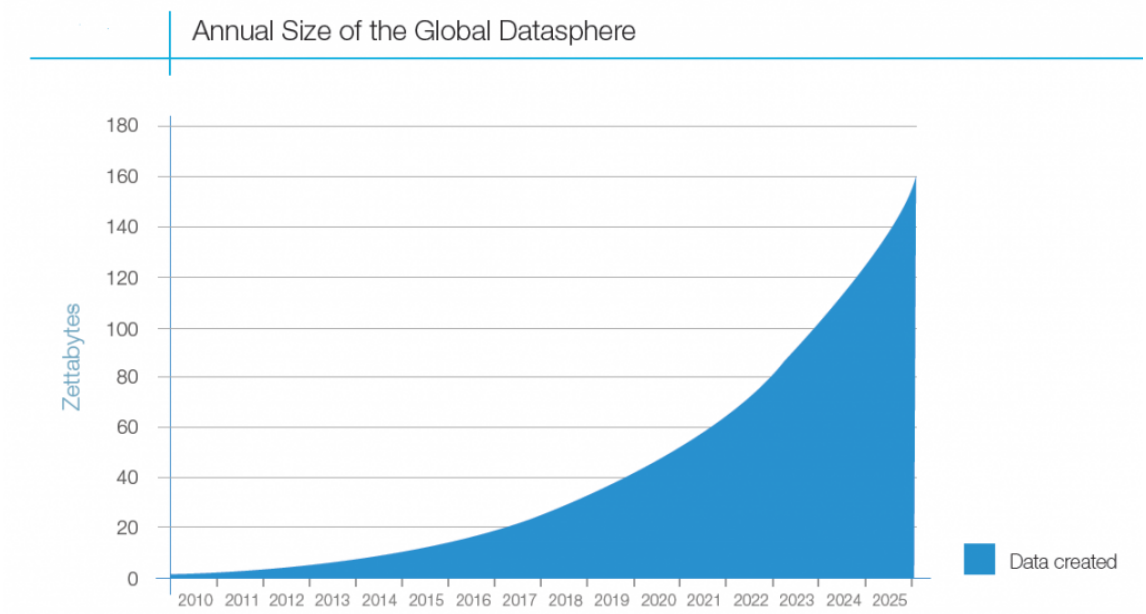
Data zijn de motor van onze digitale economie. Het delen en breder gebruik van data bieden veel kansen voor het bedrijfsleven. Denk bijvoorbeeld aan het verbeteren van de gezondheidszorg, veiliger transport, bijdragen aan klimaatdoelstellingen en het vergroten van productiviteit. Het volume aan data neemt snel toe. Naar verwachting zal in 2025 175 Zettabyte aan data geproduceerd worden.[1] Om een beeld te geven, in 2018 werd 33 Zettabyte aan data geproduceerd. De waarde die uit data kan worden behaald in 2025 wordt geschat op EUR 829 biljoen (5,8% EU GDP). In 2018 was dit EUR 301 biljoen (2.4% EU GDP). Het delen en breder gebruik van data biedt veel kansen voor het bedrijfsleven. Om het volle potentieel uit data te benutten en Europa als wereldleider in de digitale data-economie neer te zetten, is samenwerking op Europees niveau nodig. De Europese datastrategie is erop gericht om dit te bewerkstelligen. Onderdeel van deze brede Europese datastrategie zijn de onlangs gepubliceerde Europese regels voor het breder gebruik van IoT-data. De focus op IoT-data is in lijn met de verwachting van Gartner[2] dat in 2025 80% van de dataverwerking en –analyse plaats zal vinden in: a. slimme verbonden producten (IoT); en b. decentraal, door het product zelf of een apparaat in de nabije omgeving (edge computing).

We steunen de doelstelling van de Europese regels om optimaal data te benutten en te kiezen voor een EU brede aanpak. Maar de huidige tekst kan leiden tot onbedoelde gevolgen. We komen hierop terug onder het kopje 'Beoordeling Europees wetsvoorstel'.[3]

[1] Factsheet Europese Datastrategie: https://ec.europa.eu/commission/presscorner/api/files/attachment/862109/European_data_strategy_en.pdf; IDC, 2018

2 Gartner, 2017; zie ook de Factsheet Europese Datastrategie: https://ec.europa.eu/commission/presscorner/api/files/attachment/862109/European_data_strategy_en.pdf

[3] *Pagina 8 onderaan*



Grafische weergave van cijfers Gartner rapport uit 2017

1. *Het Europese voorstel voor een Dataverordening*

De Europese Commissie wil met de nieuwe regels voor een breder gebruik van data toegang tot én verder gebruik van data bevorderen om te zorgen voor een redelijke verdeling van (de waarde van) data zodat:

- *Alle bedrijven (in alle sectoren) in de Unie in staat zijn om te innoveren en te concurreren op basis van IoT gebruiks- en omgevingsdata;*
- *Individuen effectief in staat zijn om hun rechten op hun IoT gebruiks- en omgevingsdata uit te oefenen; en*
- *Overheidsorganen beter in staat zijn om grote beleidsuitdagingen van publiek belang het hoofd te bieden met behulp van private data.*

<u>Het Europese voorstel voor een Dataverordening bevat regels voor het:</u>

i) **Faciliteren van toegang tot en verder gebruik van IoT gebruiks- en omgevingsdata door bedrijven en consumenten**

De Dataverordening verplicht hiertoe producenten van verbonden producten om de producten en daaraan gerelateerde diensten zo te ontwerpen dat gebruikers makkelijk en veilig toegang hebben tot hun gebruiks- en omgevingsdata (toegang-by-design). Waar directe toegang voor de gebruiker niet mogelijk is, verplicht de Dataverordening grote en middelgrote bedrijven gebruiks- en omgevingsdata aan gebruikers beschikbaar te stellen zonder onredelijke vertraging, gratis en waar mogelijk, op continue basis en in 'real-time'. De gebruiker kan er ook voor kiezen om een andere partij aan te wijzen aan wie toegang tot zijn gebruiks- en omgevingsdata wordt verleend. Aan zogenaamde Poortwachters (zoals gedefinieerd onder de Data Market Act) mag echter geen toegang worden verleend, ook niet als de gebruiker dat zou willen. De verplichting om data te

delen geldt overigens niet voor het micro en kleinbedrijf.[4]

ii) **Beschermen van mkb tegen oneerlijke handelspraktijken (aanpakken misbruik machtsongelijkheid)**

Het wetsvoorstel houdt op meerdere manieren rekening met de specifieke behoeften van het mkb.[5] Micro-, kleine en middelgrote bedrijven maken 99% uit van alle bedrijven in de EU.[6] Het wetsvoorstel bevat een 'zwarte lijst' van onredelijke bepalingen die niet bindend zijn als deze eenzijdig aan een micro, klein of middelgroot bedrijf zijn opgelegd; en een 'grijze lijst' van bepalingen die vermoed worden onredelijk te zijn. Deze aanpak is vergelijkbaar met de zwarte en grijze lijsten voor bedingen in algemene voorwaarden in het burgerlijk wetboek. Ook bevat het wetsvoorstel de verplichting voor de Europese Commissie om een datadeel-modelcontract op te stellen om het mkb te ondersteunen. Het gebruik van dit modelcontract is vrijwillig maar kan wel een behulpzaam middel zijn voor het mkb.

iii) **Faciliteren dat overheidsorganen en Europese publieke instellingen in bepaalde uitzonderlijke situaties private data kunnen krijgen voor een specifiek publiek belang; alsook voor de uitoefening van hun publieke taak**

Daartoe bevat het wetsvoorstel de verplichting voor grote en middelgrote bedrijven om data (in de meest brede zin) op verzoek te delen met publieke instellingen als er sprake is van een publieke noodsituatie (nationale en regionale noodtoestanden); of als de publieke instelling de data nodig heeft voor de vervulling van haar taken en ze niet op een andere manier aan de data kan komen.

iv) **Vergemakkelijken van overstappen tussen cloud- en edgediensten (hierna: dataverwerkingsdiensten)**[7]

Daartoe bevat het wetsvoorstel de verplichting voor cloud- en edge dienstaanbieders om kosteloos, zonder verstoring van de dienstverlening en binnen een periode van een maand de overstap naar een andere aanbieder te faciliteren. Deze verplichting omvat de verplichting om alle data (inclusief meta data, configuratie parameters, security settings, toegangsrechten en toegangslogs), applicaties en digitale assets kosteloos en geruisloos te migreren naar de nieuwe aanbieder. Er mogen geen technische, organisatorische, commerciële of contractuele hindernissen worden opgeworpen.

[4] Ondernemingen waar minder dan 50 personen werkzaam zijn en waarvan de jaaromzet of het jaarlijkse balanstotaal €10 miljoen niet overschrijdt.
[5] Mkb heeft minder dan 250 werknemers in dienst en hun omzet moet minder zijn dan 50 miljoen euro of een jaarlijks balanstotaal van maximaal 43 miljoen euro.
[6] Factsheet Europees Parlement: europarl.europa.eu/factsheets/nl/sheet/63/kleine-en-middelgrote-ondermemingen
[7] Dit zijn digitale diensten, zoals clouddiensten, die op aanvraag toegang bieden tot schaalbare computermiddelen.

v) Creëren van waarborgen tegen onrechtmatige toegang en inzage in data door overheidsorganen van landen buiten de EU

Daartoe bevat het wetsvoorstel de verplichting voor cloud- en edge dienstaanbieders om alle mogelijke maatregelen te nemen om internationale overdracht van, of toegang door overheidsinstanties tot, niet-persoonsgebonden gegevens te voorkomen wanneer de overdracht of toegang een conflict met nationale of Europese regelgeving oplevert.

vi) Ontwikkelen van interoperabiliteitsstandaarden voor het hergebruik van data tussen sectoren

Hiertoe bevat het wetsvoorstel eisen waaraan Europese interoperabiliteitstandaarden moeten voldoen: resultaatgericht zijn; verbeteren migratie van digitale assets tussen cloud- en edge aanbieders[8] die eenzelfde type dienst aanbieden; en garanderen van functionele gelijkwaardigheid (waar technisch mogelijk) tussen cloud- en edge aanbieders van schaalbare infrastructuur. Als je voldoet aan Europese interoperabiliteitsstandaarden, gaat men ervan uit dat je voldoet aan de interoperabiliteitseisen die gesteld worden in het wetsvoorstel. De Europese Commissie behoudt zich het recht voor (wat we steeds vaker tegenkomen in Europese verordeningen) om zogenaamde algemene specificaties ('common specifications') op te stellen als Europese standaarden uitblijven of naar het (subjectieve) oordeel van de Europese Commissie niet voldoen.

<u>Het Europese voorstel voor een Dataverordening is relevant voor:</u>

i) Producenten[9] van fysieke IoT-producten;
ii) Leveranciers[10] van gerelateerde diensten. Dit zijn diensten die nodig zijn om van de functionaliteit van het fysieke IoT-product gebruik te maken (incl. leveren van software; bij twijfel is de Dataverordening van toepassing);
iii) Zakelijke datahouders (partijen die de data feitelijk kunnen delen: omdat ze de rechten hebben om persoonsgegevens te delen of omdat ze de technische controle over niet-persoonsgebonden gegevens hebben);
iv) Aanbieders van dataverwerkingsdiensten (cloud- en edge serviceproviders);
v) Zakelijke dataontvangers in alle sectoren van de markt;
vi) Zakelijke en particuliere gebruikers van IoT-producten;
vii) Nationale en Europese publieke instellingen.

[8] In het wetsvoorstel aangeduid als 'dataprocessingsdiensten'.

[9] Grote en middelgrote bedrijven (middelgrote bedrijven zijn bedrijven met maximaal 250 werknemers en maximaal 50 miljoen omzet of een jaarlijks balanstotaal van maximaal 43 miljoen euro. Grote bedrijven zijn bedrijven die 250 of meer werknemers in dienst hebben en een omzet hebben van meer dan 50 miljoen euro of een jaarlijks balanstotaal hoger dan 49 miljoen euro).

[10] Grote en middelgrote bedrijven (middelgrote bedrijven zijn bedrijven met maximaal 250 werknemers en maximaal 50 miljoen omzet of een jaarlijks balanstotaal van maximaal 43 miljoen euro. Grote bedrijven zijn bedrijven die 250 of meer werknemers in dienst hebben en een omzet hebben van meer dan 50 miljoen euro of een jaarlijks balanstotaal hoger dan 49 miljoen euro).

Om wat voor data gaat het?

Data zijn breed omschreven in het wetsvoorstel. Onder 'data' wordt elke digitale weergave verstaan van activiteiten, feiten of informatie, inclusief beeld en geluid. Bij de verplichting tot het delen van data gaat het om data die wordt verzameld of gegeneerd door het (actieve en inactieve) gebruik dat wordt gemaakt van (gekochte of gehuurde) verbonden producten. In deze notitie noemen we dit: "IoT gebruiks- en omgevingsdata". Data kan zowel persoonsgegevens omvatten als niet-persoonsgebonden gegevens.[11] Data die worden afgeleid van of berekend op basis van de IoT gebruiks- en omgevingsdata lijkt te zijn uitgesloten van de datadeelverplichting.

Welke IoT Producten en diensten vallen binnen de scope?

Bij verbonden producten gaat het om producten die verbonden kunnen worden met het internet[12] om met andere producten of systemen data uit te wisselen. Het gaat om de producten zelf en om daaraan gerelateerde diensten. Onder gerelateerde diensten worden diensten verstaan die noodzakelijk zijn om gebruik te kunnen maken van de functionaliteit van het product (denk hierbij aan voice assistenten, zoals Siri of Alexa). Via het internet kan de data over het (actieve en inactieve) gebruik van het product (en de gerelateerde dienst) en data over de omgeving van het product worden verzameld en verspreid. Deze producten (en daaraan gerelateerde diensten) worden ook 'slimme producten', 'internet der dingen' of 'Internet-of-Things' (IoT) genoemd. Het gaat om een breed scala aan slimme producten, zoals medische apparatuur, auto's, landbouwmachines, industriële machines, slimme verpakkingen, slimme meters, slimme koelkasten en slimme wasmachines.
Producten die primair bedoeld zijn om inhoud op te slaan, weer te geven, op te nemen, af te spelen of door te geven (zoals smartphones, tablets, laptops, servers, camera's, webcams, geluidsopname systemen en tekst scanners) zijn van de Dataverordening uitgezonderd. Dit lijkt niet zozeer een logische maar meer een politieke keuze te zijn.

Verhouding van de Dataverordening met andere relevante Europese wet- en regelgeving?
Om het volle potentieel uit data te behalen en daarmee economische en duurzaamheidsvoordelen te benutten, werkt de Europese Commissie aan een sterke interne markt voor data. Hiertoe heeft de Europese Commissie begin 2020 haar brede **Europese Data Strategie**[13] gepubliceerd. De Europese Datastrategie is erop gericht om Europa als wereldleider in de digitale data-economie neer te zetten. Het Europese wetsvoorstel voor een Dataverordening[14] vloeit voort uit deze bredere Europese Data Strategie. Om een sterke interne markt te bevorderen, heeft de Europese Commissie gekozen voor maximale harmonisatie in de vorm van een verordening (zoveel mogelijk dezelfde regels laten gelden binnen de hele Europese Unie).

[11] Op persoonsgegevens blijft de Algemene Verordening Gegevensbescherming (AVG) onverkort van toepassing.
[12] Of een ander publieke elektronisch communicatienetwerk
[13] COM/2020/66 final; gepubliceerd februari 2020.
[14] https://digital-strategy.ec.europa.eu/en/library/data-act-proposal-regulation-harmonised-rules-fair-access-and-use-data

Een ander onderdeel van de Europese Datastrategie is de **Gegevensbeheerverordening** (Data Governance Act).[15] De Dataverordening vormt een aanvulling op de in november 2020 voorgestelde Gegevensbeheerverordening, het eerste resultaat van de Europese strategie voor gegevens. Deze verordening is in werking getreden op 23 juni 2022 en zal van toepassing zijn vanaf 23 september 2023. Waar de Gegevensabeheerverordening de processen en structuren creëert om het delen van data te faciliteren en een raamwerk neerzet voor het vrijwillig delen van publieke data (in aanvulling op de minimumregels voor het hergebruik van publieke data zoals gesteld in de **Open Data Richtlijn**[16]), bevat de Dataverordening verplichtingen voor het delen van private data, wie waarde kan creëren uit deze data en onder welke voorwaarden.

De bedoeling is dat de horizontaal werkende Dataverordening wordt aangevuld met **sectorspecifieke wetsvoorstellen** voor zogenaamde **Europese Data Ruimtes**.[17] Er zijn al sectorspecifieke voorstellen in de maak voor de gezondheidssector (European Health Data Space, EHDS)[18] en de voertuigensector[19]. Ook heeft de Europese Commissie aangekondigd met sectorspecifieke voorstellen te komen voor de financiële sector en de agrarische sector. Deze voorstellen zullen naar verwachting gevolgd worden door andere sectorspecifieke wetsvoorstellen. De Dataverordening zal bestaande sectorale wetgeving intact laten maar toekomstige sectorale wetgeving zal in lijn moeten zijn met de principes van de Dataverordening.

Zowel persoonsgegevens als niet-persoonsgebonden IoT-gebruiks- en omgevingsdata vallen binnen de scope van de Dataverordening. De bestaande **Algemene Verordening Gegevensbescherming** (AVG) blijft onverminderd van toepassing op persoonsgegevens. De datahouder kan dan ook alleen aan de datadeelverplichting van de Dataverordening voldoen als hij/zij een verwerkingsverantwoordelijke is in de zin van de AVG en een rechtsgeldige AVG-grondslag heeft om de persoonsgegevens te mogen delen.

Het is de bedoeling dat de Dataverordening de **AI Act** versterkt. Voor het adequaat trainen van AI-systemen (om bijvoorbeeld bias tegen te gaan) zijn doorgaans grote hoeveelheden data nodig[20]. De toegang tot en bredere gebruik van IoT gebruiks- en omgevingsdata kan bijdragen aan deze databehoefte.

De Dataverordening verwijst naar de term Poortwachters (Gatekeepers) zoals gedefinieerd in de recent aangenomen Europese **Digitale Markten Verordening** (DMA)[21]: dit zijn zeer grote online platforms met een poortwachtersfunctie met een omzet van >7,5 miljard (of

---

[15] https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32022R0868&from=EN; [EU 2022/868]. De Data beheers verordening (Data Governance Act) reguleert het verdere gebruik van data (in het bezit) van publieke organen. De Data Act reguleert het gebruik van data (in het bezit) van private partijen. Een gewijzigde versie is door het Europees Parlement aangenomen op 6 april 2022.
[16] OJ L 172, 26 juni 2019, p. 56-83
[17] VESTAGER HINTS AT AGRICULTURAL DATA LEGISLATION**:** The Data Act is a "horizontal framework" — but the EU has its eyes set to add more secondary legislation to that, catering to specific sectors. "This is a horizontal piece of legislation, we expect more sectoral approaches," Vestager said — with health and the car industry as first targets. But: "There may also be a need for agricultural sectoral legislation," she added.
[18] Europese ruimte voor gezondheidsgegevens (europa.eu)
[19] Toegang tot voertuiggegevens, -functies en -hulpmiddelen (europa.eu)
[20] Gartner rapport 'Over 100 Data and Analytics Predictions through 2025 by Alan D. Duncan, Gartner Inc. / G00744238, p. 4: by 2024 60% of the data used for the development of AI and analytics solutions will be synthetically generated.
[21] Zie voorwaarden voor kwalificatie als *Poortwachter (Gatekeeper)* in art. 3 lid 1 en lid 2 DMA jo. art. 2 onder 2.

een marktkapitalisatie >75 miljard), die één of meer core platform services[22] uitvoeren. In het wetsvoorstel voor een Dataverordening is specifiek opgenomen dat gebruikers niet mogen bepalen dat aan Poortwachters toegang wordt verleend tot hun IoT gebruiks- en omgevingsgegevens. In het DMA-wetsvoorstel is voor Poortwachters de datadeelverplichting opgenomen om hun zakelijke gebruikers toegang te geven tot data die wordt gegenereerd door het gebruik dat gemaakt wordt van de diensten van de Poortwachter. Ook is in de DMA opgenomen dat poortwachters die data niet zelf mogen gebruiken om te concurreren met die zakelijke gebruikers. In de DMA zijn de verplichtingen beperkt tot de 'core platform diensten' van een Poortwachter (en strekken niet uit tot overige diensten van een Poortwachter).

De herziening van de Algemene productveiligheidsrichtlijn (GPSR), de te verwachten herziening van de Productaansprakelijkheidsrichtlijn (PLD) en de nieuw te verwachten Europese AI aansprakelijkheidswetgeving zullen relevant zijn voor de producenten en gebruikers van IoT producten. De nieuwe verplichtingen en rechten van de Dataverordening zullen nopen tot een herziening van de huidige verantwoordelijkheden en aansprakelijkheden. Het is hierbij van belang dat een goede balans wordt gezocht qua verantwoordelijkheden en aansprakelijkheden.

2. Nederlandse positie Europese wetsvoorstel

Het kabinet erkent het belang van data voor de economie en maatschappij en staat positief tegenover de doelstelling van het wetsvoorstel, ondersteunt de keuze van de Europese Commissie om Europees leiderschap te tonen door regels te stellen die het veilig en betrouwbaar delen en breder gebruik van data bevorderen en is overwegend positief over het wetsvoorstel. Dit is enigszins verbazend omdat het wetsvoorstel niet aansluit bij de kabinetsvisie op datadeling tussen bedrijven[23] uit 2019 waarin als één van de drie uitgangspunten voor beleidsontwikkeling op datadeling tussen bedrijven is benoemd dat datadeling bij voorkeur vrijwillig is.[24] De Europese Commissie is met de Dataverordening een andere weg ingeslagen door data delen verplicht te stellen. Het kabinet verwelkomt specifiek dat er aandacht is voor de versterking van grip op gegevens voor consumenten en bedrijven, dat naar generieke standaarden en afspraken wordt gekeken om verantwoorde datadeling te bevorderen en dat betrokken partijen meer duidelijkheid krijgen over mogelijkheden, voorwaarden en controle bij datadeling. Het kabinet heeft echter nog vragen bij de reikwijdte van verschillende onderdelen van het voorstel en ook de nieuwe mogelijkheden voor overheden om gegevens op te vragen behoeven nadere duiding. Het kabinet zal hierover nadere uitleg vragen aan de Commissie. Het kabinet is net als ons van mening dat bij meer datadeling de bescherming van persoonsgegevens, rechten van derden en wettelijke doelbinding wel goed moeten zijn geborgd.

[22] 'Core platform diensten' zoals omschreven in de Digitale Markt Verordening (DMA).
[23] Kamerstuk 26643, nr. 594
[24] Op initiatief van het kabinet is in mei 2019 een groep datadeelinitiatieven, branches, bedrijven en kennisinstellingen samengebracht. De deelnemers hebben samen een open samenwerking voor cross-sectoraal datadelen opgezet, de zogenoemde Data Sharing Coalition. Het kabinet heeft de visie ook actief bij Europese lidstaten en de Commissie uitgedragen.

Daarnaast werkt het kabinet ook aan diverse sectorspecifieke data-initiatieven, zoals in de zorg, onderwijs en onderzoek en transport en zorgt hierbij dat aansluiting en interoperabiliteit tussen de verschillende initiatieven geborgd is om de baten voor de (data)economie en maatschappij zo groot mogelijk te laten zijn.

3. Beoordeling Europese wetsvoorstel

Het veilig, betrouwbaar en verantwoord optimaal benutten van data is een krachtig middel om onze internationale concurrentiepositie te behouden en uit te bouwen en Europa als wereldleider in de digitale data-economie neer te zetten. Het breed benutten van data biedt veel kansen voor het bedrijfsleven en is een randvoorwaarde voor groei en innovatie in het kader van de digitale transitie. We verwelkomen dan ook de insteek om EU breed optimaal data te benutten om zo de interne markt te bevorderen. Om optimaal data te kunnen benutten, is het essentieel dat datadelen gestimuleerd wordt en er prikkels zijn voor innovatie. Ook verwelkomen we de insteek om op diverse manieren specifiek rekening te houden met het mkb zodat ze kunnen groeien en nieuwe opkomende bedrijven in staat worden gesteld om de markt te betreden en te concurreren met bestaande marktpartijen om dataconcentraties te voorkomen. In het voorstel zijn daartoe waarborgen opgenomen tegen oneerlijke handelspraktijken met een verbod op onredelijke voorwaarden, wordt het mkb ondersteund met een vrijwillig modelcontract voor data-delen en is het micro- en klein bedrijf uitgezonderd van verplichtingen rond data delen. *We zetten ons in voor het behoud van deze voorstellen; en het opnemen van stimulansen voor het micro en kleinbedrijf om vrijwillig data te delen.*

Omdat het voorstel voor een Dataverordening nog veel onduidelijkheden bevat (o.a. onduidelijke kernbegrippen) is een eindoordeel over het voorstel pas echt te vellen als een en ander nader is uitgewerkt.

Ondanks de goede insteek van het voorstel waarbij data delen en het benutten van data centraal staan, kan de huidige tekst echter leiden tot onbedoelde gevolgen. We zouden het voorstel dan ook graag nader uitgewerkt en aangepast zien:

- ***Bescherming van bedrijfsgeheimen* voor zover die Europees wettelijk zijn beschermd; en duidelijke borging van de rechten van intellectuele eigendom, in de wet zelf (niet alleen in de overwegingen)**. Om optimaal data te kunnen benutten, is het essentieel dat datadelen gestimuleerd wordt en er prikkels zijn voor innovatie. Wettelijke bescherming van IE-rechten en bedrijfsgeheimen is essentieel voor innovatie en groei. Zonder deze bescherming zouden er geen investeringen worden gedaan in de ontwikkeling van nieuwe slimme producten en het genereren van data omdat er geen garantie zou zijn dat dergelijke investeringen zouden kunnen worden terugverdiend. De wet verplicht echter tot het delen van bedrijfsgeheimen. Voor zover deze wettelijk zijn beschermd, zou de verplichting niet moeten gelden. Bovendien maken we uit de overwegingen van het voorstel op dat het wetsvoorstel toeziet op het delen en breed benutten van ruwe gebruiksdata die gegeneerd wordt door het gebruik van gehuurde of gekochte slimme producten. Niet op daarvan afgeleide of berekende data. Dit blijkt echter niet duidelijk uit de wettekst zelf. Voor

een horizontale goede bescherming is nodig dat de wettekst zelf duidelijk is hierover. *We zetten ons in voor een goede bescherming van bedrijfsgeheimen en intellectuele eigendom.*[25] *Dit houdt onder meer concreet in dat het niet verplicht moet zijn om Europees wettelijk beschermde bedrijfsgeheimen te delen; en dat de bescherming van rechten van intellectuele eigendom duidelijk uit de wettekst zelf moet blijken (en niet alleen in de overwegingen is terug te vinden).*

- ***Goede balans***. Het benutten van data over het functioneren en de prestaties van verbonden slimme producten is relevant voor zowel de zakelijke gebruikers als voor de producenten en andere datahouders. Opdat alle partijen in staat zijn optimaal data te benutten en met elkaar te concurreren binnen het kader van Europese normen en waarden. Dit vereist niet alleen oog hebben voor toegang tot en bredere gebruiksmogelijkheden voor de gebruiker van verbonden producten en diensten en het corrigeren waar nodig van misbruik van ongelijke verhoudingen maar ook oog hebben voor de gebruiksmogelijkheden van data voor de producenten en andere datahouders. We missen in het voorstel ook stimulansen om vrijwillig data delen te bevorderen. Met name het bieden van stimulansen aan het mkb om vrijwillig data te delen. *We zetten ons in dat binnen het kader van de Europese waarden en normen optimaal waarde uit data kan worden benut waarbij het delen van data wordt bevorderd en er prikkels zijn om te investeren in nieuwe IoT-producten en diensten & manieren om waarde te genereren uit IoT-data*.

- **Delen van data met de overheid onder voorwaarden.** We begrijpen dat voor specifieke publieke belangen de overheid baat heeft bij private data. Bedrijven delen met diverse publieke instellingen al jaren data (denk aan data voor het CBS). Het voorstel bevat echter een veel te brede en onduidelijke verplichting voor bedrijven om allerhande data te moeten delen met de overheid. Aan een verplichting tot het delen van data met de overheid moeten scherpe voorwaarden worden verbonden. De uitvraag moet noodzakelijk, proportioneel en doel gebonden zijn en in overeenstemming zijn met onze democratische waarden. Het primaire doel moet vooraf helder zijn maar ook welke nevendoelen toegestaan zijn (en dus ook welke niet). Ook moet er duidelijk zijn welke data gevraagd mogen worden, wat een "publieke noodsituatie" is en hoe lang de data gebruikt of bewaard mogen worden. Er moet helder zijn wanneer de overheid voor de uitoefening van haar taken private data mag opvragen (wanneer is het voor de overheid onmogelijk om op reguliere wijze aan de data te komen). Ook moet helder zijn dat de data niet gebruikt worden in concurrentie met bedrijven. Bovendien kunnen bedrijven baat hebben bij het kunnen benutten van publieke data. Dit is nu op vrijwillige basis geregeld in de onlangs in werking getreden **Gegevensbeheerverordening** (DGA)[26] en de eerdere **Open Data Richtlijn**[27]. Waar private partijen een verplichting wordt opgelegd, wordt

[25] We ondersteunen de verduidelijking in het voorstel dat artikel 7 Databankrecht niet van toepassing is op machine gegenereerde IoT-data maar in het huidige voorstel is in de wet zelf niet duidelijk verwoord dat het hier om machine gegeneerde IoT data gaat (dit is nu alleen terug te vinden in de overwegingen); ook is het nodig dat in de wettekst zelf wordt opgenomen dat de verplichting voor een cloud service aanbieder om data en data assets over te zetten naar een nieuwe aanbieder toeziet op digital assets waarbij de gebruiker over de benodigde gebruiksrechten of andere intellectuele eigendomsrechten beschikt.

[26] https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32022R0868&from=EN; [EU 2022/868].

[27] OJ L 172, 26 juni 2019, p. 56-83

voor publieke instellingen volstaan met een regeling op vrijwillige basis om hun publieke data te delen met bedrijven om deze optimaal te kunnen benutten. We missen hier een balans in benadering.

- **Rechtszekerheid en gelijke toepassing in de EU vereist verduidelijking van kernbegrippen, rechten en verplichtingen.** Er komen steeds meer regels bij in Nederland en Europa en de complexiteit neemt toe. Het is dan ook van wezenlijk belang dat de regels voldoende duidelijk zijn. Duidelijkheid is ook van belang voor een sterke interne markt. De regels moeten in de Unie zoveel mogelijk gelijk en voldoende duidelijk zijn zodat ze in de lidstaten hetzelfde worden toegepast. Het gaat om kerndefinities zoals gebruiks- en omgevingsdata en slimme producten: wat valt daar nu wel en niet onder? Uit de overwegingen valt op te maken dat het om ruwe gebruiksdata gaat die gegeneerd wordt door het gebruik van gehuurde of gekochte slimme producten. Het gaat niet om daarvan afgeleide en berekende data. In de wettekst is echter niet opgenomen wat onder slimme product data moet worden verstaan terwijl dit wel de scope bepaalt van de verplichting. Als dit niet duidelijk wordt gemaakt in de wettekst zelf, blijft er onduidelijkheid bestaan en kan de wettekst verschillend worden geïnterpreteerd met alle gevolgen van dien. De wettekst moet heel duidelijk zijn over of en door wie aan welke verplichting moet worden voldaan. Ook moet duidelijk in de wet zelf worden opgenomen dat de gebruiker de benodigde gebruiksrechten moet hebben op de digital assets die hij mee wil meenemen naar een andere aanbieder (hier mag ook niet alleen worden volstaan met tekst in de overwegingen). Er moet eenduidiger worden omschreven wie datahouder is. Alle kernbegrippen moeten heel duidelijk worden opgenomen, er mag niet worden volstaan met het opsommen van voorbeelden in de toelichting; en de verplichtingen moeten redelijk en praktisch uitvoerbaar zijn, waarbij sprake is van een goede balans tussen alle betrokken partijen. *Het huidige voorstel bevat nog te veel onduidelijkheden. We zetten ons ervoor in om de onduidelijkheden om te zetten in duidelijke, begrijpelijke en uitvoerbare wet- en regelgeving.*

- **Internationale doorgifte en overheidstoegang tot niet-persoonsgebonden data** Het voorkomen van disproportionele overheidstoegang tot niet-persoonsgebonden data (als ook tot persoonsgegevens) van buiten de Unie is iets dat alleen kan worden opgelost op politiek niveau. De oplossing voor dit probleem kan niet worden verwacht van bedrijven.

- **Interoperabiliteitsstandaarden** We verwelkomen de ontwikkeling van technologische en juridische standaarden voor interoperabiliteit. Standaarden zijn van groot belang om producten en/of diensten beter op elkaar te laten aansluiten. Deze aansluiting is essentieel om dataportabiliteit te realiseren. Het komen tot standaarden vindt in principe plaats via zelfregulering. In steeds meer verordeningen zien we terugkomen dat de Europese Commissie de ontwikkeling van standaarden kan afdwingen als dit naar hun subjectieve oordeel niet snel genoeg of niet juist genoeg gebeurt. Er moeten duidelijke en objectieve criteria[28] worden opgenomen op

[28] Dergelijke criteria zouden kunnen zijn – waar relevant - het niet voldoen aan de vereisten van artikel 30.1a-d. We maken hierbij echter de aanvullende kanttekening dat de vereisten van artikel 30.1b-d niet passend zijn voor alle soorten smart contracts.

basis waarvan de Europese Commissie als last resort kan ingrijpen in het zelfreguleringsproces en de ontwikkeling of bijsturing van standaarden kan afdwingen.

- **Toezicht en handhaving** Om te kunnen komen tot een sterke interne datamarkt, is uniform afgestemd toezicht in de Unie van belang. Als de regels in de diverse lidstaten anders worden uitgelegd en toegepast door de verschillende bevoegde autoriteiten in de diverse lidstaten, leidt dit tot fragmentatie in de Unie. Dit bemoeilijkt de uitvoering van de regels en heeft een nadelige invloed op innovatie en groei van de datamarkt.

Uitgangspunten nader uitgewerkt

A. ***Bescherming van bedrijfsgeheimen*** **voor zover die Europees wettelijk zijn beschermd; en duidelijke borging van de rechten van intellectuele eigendom, in de wet zelf (niet alleen in de overwegingen)**.

Het bieden van adequate waarborgen om de rechten van de datahouder te beschermen is essentieel voor innovatie en groei, denk in het bijzonder aan rechten van ***intellectuele eigendom*** *en* ***bedrijfsgeheimen****.*

Bedrijfsgeheimen
We zijn het niet eens met de verplichting in de Dataverordening om bedrijfsgeheimen te moeten verstrekken. Dit doet af aan de Europese wettelijke bescherming die geboden wordt aan bedrijfsgeheimen.[29]

Het bieden van stimulansen om het vrijwillig delen van data te bevorderen,[30] *zou onzes inziens een te prefereren insteek zijn geweest om de doelstellingen van het voorstel te behalen. De Europese Commissie heeft er echter voor gekozen om datadelen van IoT gebruiks- en omgevingsdata verplicht te stellen. Deze horizontale verplichting grijpt in het marktmechanisme. Voor een goede balans tussen datadelen en prikkels voor innovatie is het in ieder geval van essentieel belang dat de Europees wettelijke bescherming die bedrijfsgeheimen genieten, niet wordt ontnomen.*

Bescherming van IE-rechten en bedrijfsgeheimen is essentieel voor innovatie en groei. Zonder deze bescherming zouden er geen investeringen worden gedaan omdat er geen garantie zou zijn dat dergelijke investeringen zouden kunnen worden terugverdiend. Op grond van het huidige voorstel word je als datahouder verplicht om bedrijfsgeheimen ter beschikking te stellen. Deze kunnen vervolgens door een andere aanbieder worden gebruikt om een concurrerende dienst of een andere productcategorie te ontwikkelen. Het is belangrijk een onderscheid te maken tussen gebruiks- en omgevingsgegevens en bedrijfsgeheimen. In overweging 17 is opgenomen dat data zoals gegenereerd door een product binnen de scope van de datadeelverplichtingen valt maar dat daarvan met behulp van software (berekeningen) afgeleide en berekende data buiten de scope valt (omdat er intellectuele

[29] EU's Trade Secrets Directive (2016/943/EU).
[30] In aanvulling op de faciliteiten die zijn opgenomen in de onlangs op Europees niveau aangenomen Data Governance Act

eigendomsrechten op die software kunnen rusten). Afgeleide en gededuceerde gegevens bevatten eerder bedrijfsgeheimen dan 'ruwe' sensorgegevens. Overweging 17 van het voorstel stelt dan ook terecht dat afgeleide en berekende gegevens van de verplichting tot delen zijn uitgesloten. Deze afbakening komt echter niet tot uiting in de ontwerpartikelen zelf. Dit zal leiden tot onduidelijkheid bij de interpretatie van de artikelen. Onduidelijkheid werkt problemen bij de implementatie van de wet in de hand en kan leiden tot fragmentatie in de EU. Ook de term 'digital assets' wordt enkel in overweging 72 toegelicht. In overweging 72 is opgenomen dat de term 'digital assets' verwijst naar digitale elementen waarvoor de klant het recht heeft om deze te gebruiken. Met andere woorden, er bestaat enkel de verplichting om digital assets over te dragen (te switchen) naar een nieuwe aanbieder als de klantgebruiker over de benodigde gebruiksrechten (licenties) beschikt. Deze voor de rechthebbende van de digital assets essentiële afbakening is echter niet terug te vinden in de artikelen zelf. ***We opteren dan ook voor het opnemen van alle kernbegrippen in artikel 2 alsook voor het duidelijk en helder verwoorden van de scope van de verplichtingen in de artikelen zelf. Alleen de artikelen zijn immers bindend.***

Het wetsvoorstel voor een Dataverordening staat derde partijen toe om op basis van de beschikbaar gestelde IoT gebruiks- en omgevingsdata concurrente diensten te ontwikkelen. Voor het creëren van de noodzakelijke ***balans*** *tussen de datahouders en de gebruikers (en door hen aangewezen derde partijen), is het nodig dat er geen verplichting wordt opgenomen om bedrijfsgeheimen te verstrekken. Inbreuken op bedrijfsgeheimen kunnen verstrekkende gevolgen hebben voor de datahouder. Het beschermen van bedrijfsgeheimen, is mede van belang om te voorkomen dat de concurrentiepositie van Europese bedrijven in de internationale handelsmarkt wordt benadeeld. Het kabinet heeft aangegeven nader te willen bestuderen of de geboden waarborgen voldoende zijn, met name om de belangen van gebruikers en datahouders te borgen en de bescherming van gedeelde data te verzekeren.*

De doelstellingen van het wetsvoorstel moeten behaald worden zonder afbreuk te doen aan de bestaande wettelijke bescherming van bedrijfsgeheimen; en met respect voor de rechten van intellectuele eigendom.[31] ***We opteren primair voor het schrappen van de verplichting om bedrijfsgeheimen te moeten verstrekken; dan wel subsidiair voor het duidelijk omschrijven welke beperkte categorie bedrijfsgeheimen onder de datadeel verplichting vallen.***

Zo kan er meer gekeken worden naar opkomende mogelijkheden om data te analyseren zonder dat de data ter beschikking gesteld moet worden aan de analyserende partij.

Sui generis recht (Databankenrichtlijn)

In het huidige voorstel wordt voorgesteld om artikel 7 van het sui generis databankrecht niet van toepassing te laten zijn op IoT-data (gegevens die zijn verkregen uit of gegenereerd door het gebruik van een product of een gerelateerde dienst). Hoewel uit overweging 84 blijkt dat

[31] We ondersteunen de verduidelijking in het voorstel dat artikel 7 Databankrecht niet van toepassing is op machine gegenereerde IoT-data maar in het huidige voorstel is in de wet zelf niet duidelijk verwoord dat het hier om machine gegeneerde IoT data gaat (dit is nu alleen terug te vinden in de overwegingen); ook is het nodig dat in de wettekst zelf wordt opgenomen dat de verplichting voor een cloud service aanbieder om data en data assets over te zetten naar een nieuwe aanbieder toeziet op digital assets waarbij de gebruiker over de benodigde gebruiksrechten of andere intellectuele eigendomsrechten beschikt.

het de bedoeling is dat alleen machinaal gegenereerde IoT data (denk aan data verzameld met behulp van sensoren) buiten de scope van het databankenrecht valt. Dit blijkt echter onvoldoende uit artikel 35. In artikel 35 wordt gesproken over data verzameld door het gebruik dat van IoT producten wordt gemaakt. Dit is veel breder dan is beoogd. Door deze onduidelijkheid kan het idee ontstaan dat artikel 35 niet beperkt is tot machinaal gegenereerde data (zoals beoogd) maar dat het databankenrecht niet van toepassing zou zijn op alle soorten IoT data. Denk hierbij aan databases waar substantiële investeringen zijn gedaan in de verificatie en/of ordening van de data. Volgens de huidige verwoording van artikel 35 zouden deze investeringen niet meer beschermd zijn. Hierdoor neemt onbedoeld de bescherming voor een zeer groot aantal databases af of valt geheel weg. ***We opteren ervoor dat duidelijk in artikel 35 wordt opgenomen dat het om machinaal gegenereerde data gaat (zoals ook bedoeld is en blijkt uit overweging 84): "*****containing data obtained or generated by means of physical components, such as sensors, of a product and a related service."**

Delen van data met de overheid onder voorwaarden.
Het voorstel bevat een te brede en onduidelijke verplichting voor bedrijven om allerhande data te moeten delen met de overheid. Aan deze verplichting moeten scherpe voorwaarden worden verbonden. De uitvraag moet noodzakelijk, proportioneel en doel gebonden zijn en in overeenstemming zijn met onze democratische waarden.

Een belangrijke waarborg is doelbinding. Doelbinding betekent dat data gebruikt wordt voor het doel waarvoor het is verkregen.[32] In het voorstel is het voor een publieke instelling toegestaan om de opgevraagde data ook te gebruiken voor doeleinden die verenigbaar zijn met het doel waarvoor de opgevraagde data ter beschikking is gesteld. Niet alleen de primaire doelstelling moet vooraf helder zijn maar ook de toegestane verenigbare nevendoelen. Ook moet er duidelijk zijn welke data gevraagd mogen worden, wat een "publieke noodsituatie" is en hoe lang de data gebruikt of bewaard mogen worden. Er moet helder zijn wanneer de overheid voor de uitoefening van haar taken private data mag opvragen (wanneer is het voor de overheid onmogelijk om op reguliere wijze aan de data te komen). Ook moet helder zijn dat de data niet gebruikt mogen worden in concurrentie met bedrijven. Bovendien kunnen bedrijven ook baat hebben bij het kunnen benutten van publieke data. De recent aangenomen Europese Databeheersverordening (Data Governance komt hier ten dele aan tegemoet door een kader te scheppen voor het betrouwbaar vrijwillig data delen van publieke data. We missen echter een verplichting voor publieke instellingen om hun publieke data te delen met bedrijven om deze optimaal te kunnen benutten.

Om concurrentievervalsing door publieke instellingen te voorkomen, is het essentieel dat publieke instellingen duidelijk onderbouwen voor welke doelen ze de opgevraagde data gaan gebruiken. ***We opteren ervoor dat de uitgangspunten van de AVG voor doelbinding ook een-op-een gelden voor het delen van niet-persoonlijke data en niet alleen het primaire doel bij de beschikbaarstelling van de data duidelijk moet zijn aangegeven maar ook de beoogde verenigbare verwante secundaire doelen.***

[32] *We kennen het concept van doelbinding uit de AVG.*

Daarnaast lijkt de bevoegdheid van de publieke instellingen om aanspraak te maken op private data te verstrekkend. Onder 'exceptional need' wordt niet alleen verstaan de omstandigheid dat er sprake is, gereageerd moet worden op een publieke noodsituatie of dat ter voorkoming van een publieke noodsituatie maar ook de situaties dat een publieke instelling data nodig heeft voor de reguliere uitoefening van haar publieke taken maar niet aan de data heeft kunnen komen. Bovendien lijkt de bevoegdheid die aan publieke instellingen wordt gegeven, niet beperkt tot te zijn tot IoT gebruiks- en omgevingsdata maar alle data in bezit van private zakelijke partijen te omvatten. Data omvat zowel persoonsgebonden data (data over natuurlijke personen) als niet-persoonsgebonden data, zoals data over rechtspersonen en data over alle mogelijke objecten (data over goederen, documenten, financiële middelen en overige middelen), data over vermogensrechten en overige type data. De definitie van data is dus erg ruim. Het is dan ook niet proportioneel om data in deze brede zin van het woord te gebruiken in relatie tot een verplichting om data aan publieke instellingen te moeten verstrekken. We vragen ons af hoe dit brede recht van de overheid zich verhoudt tot andere rechten zoals het recht op privacy (inclusief bescherming persoonsgegevens), het intellectueel eigendomsrecht en het recht op bescherming van bedrijfsgeheimen. Het kabinet deelt dit en heeft aangekondigd hierover opheldering te vragen bij de Europese Commissie. Bovendien is onduidelijk wat onder een 'publieke noodtoestand' moet worden verstaan. Dit is van wezenlijk belang omdat deze term het doel bepaald waarvoor publieke instellingen data kunnen opvragen. Het kabinet deelt deze mening en zal ook hierover de Europese Commissie om opheldering vragen. Ook vragen we ons af hoe de B2G datadeelverplichting van de Dataverordening zich verhoudt tot andere wetgeving zoals de Telecommunicatiewet. Kan bijvoorbeeld een telecomprovider verplicht worden de telecomdata over zijn klanten die hij tot zijn beschikking heeft en mag verwerken in overeenstemming met de Telecommunicatiewet, te delen met een publieke instelling?

We opteren voor:

- *Het opnemen in een artikel dat zowel de primaire als secundaire doelen vooraf duidelijk kenbaar moeten zijn ten tijde van de beschikbaarstelling van de data.*
- *We opteren voor een duidelijke afbakening van de data die opgevraagd en gedeeld kan worden.*
- *We opteren voor een duidelijke omschrijving van het begrip 'publieke noodsituatie'.*
- *We opteren voor een heldere inkadering van wanneer sprake is van een situatie dat de publieke instelling onmogelijk op andere manieren aan de data heeft kunnen komen.*
- *We opteren voor het verwijderen van de verplichting om bedrijfsgeheimen te moeten overdragen/prijsgeven. Zeker gezien het recht dat een publieke instelling heeft (artikel 17.4) om de data ter beschikking te stellen aan opdrachtnemers (die concurrenten kunnen zijn).*
- *We opteren ook voor verplichte transparante rapportage door de publieke instelling over het daadwerkelijke gebruik van de gegevens.*
- *We opteren ook voor een informatieplicht voor publieke instellingen om voordat de data wordt gedeeld met andere partijen, het bedrijf van wie de verkregen data afkomstig zijn hierover te informeren (zodat het bedrijf in de gelegenheid wordt gesteld om zo nodig zich hiertegen gemotiveerd te kunnen verzetten).*

- *We opteren voor het stellen van concrete heldere* beperkingen met betrekking tot hoe lang publieke instellingen specifieke datasets mogen gebruiken of opslaan voordat ze moeten worden vernietigd.
- *We opteren voor een expliciete bepaling (in artikel 16.2) dat publieke instellingen de data niet mogen gebruiken op een wijze waardoor concurrentievervalsing kan optreden.*
- *We opteren voor een verplichting voor de publieke instellingen om zorg te dragen dat hun aanvragen aan de voorwaarden van de Dataverordening voldoen (op straffe van een boete) en de controle hierop niet bij de datahouder te leggen; maar wel de mogelijkheid voor de datahouder laten bestaan om gemotiveerd te weigeren aan een verzoek te voldoen.*
- *We opteren voor een redelijke vergoeding voor bedrijven als ze verplicht zijn data aan te leveren aan de overheid.*

We verwelkomen de bepaling dat de datahouder een verzoek kan weigeren als het verzoek van de publieke instelling niet aan de voorwaarden van de Dataverordening voldoet.

B. ***Goede balans***

Gegevens over het functioneren en de prestaties van verbonden slimme producten zijn relevant voor zowel de zakelijke gebruikers als voor de producenten en andere datahouders. Dit vereist niet alleen oog voor toegang tot en bredere gebruiksmogelijkheden voor de gebruiker van verbonden producten en diensten en het corrigeren waar nodig van oneerlijke verhoudingen maar ook oog hebben voor de gebruiksmogelijkheden van data voor de producenten en andere datahouders en oog voor behoud van prikkels om te investeren in slimme producten en manieren om waarde te genereren uit data. We zetten ons in voor een goede balans in het voorstel waarbij alle partijen optimaal, op een beheersbare en te controleren manier binnen het kader van onze Europese normen en waarden, de waarde uit data kunnen benutten en op basis hiervan met elkaar kunnen concurreren.

De verplichting om data te delen geldt voor alle bedrijven met uitzondering van het micro en kleinbedrijf. We vragen ons af of de verplichting om investeringen tegen een redelijke vergoeding (=marktconform min), kostprijs of (aan de gebruiker) gratis beschikbaar te moeten stellen, het marktmechanisme van Return on Investment (**ROI**) - voor de bedrijven die als datahouder worden aangemerkt - niet disproportioneel verstoort.

We opteren voor:

- *Een vroeg evaluatie moment van de uitvoering van de verordening op te nemen om – onder andere - de economische effecten in kaart te brengen van het moeten uitvoeren van activiteiten en het moeten doen van extra investeringen (bijvoorbeeld om producten 'toegankelijk-by-design' te maken) zonder dat deze doorberekend mogen worden aan de gebruiker.*
- *Het aanvullend bieden van stimulansen om vrijwillig data delen te bevorderen, met name voor het micro en klein bedrijf. Hierbij zou gedacht kunnen worden aan:*
    - *Fiscale prikkels (belastingvrijstellingen)*

- *Reputatie/publieke erkenningsprogramma's (e.g. maatschappelijk verantwoord ondernemen)*
- *Investering van publieke middelen ter ondersteuning van de ontwikkeling van betrouwbare technische hulpmiddelen voor het delen van B2B en B2G-gegevens.*

- *We opteren voor het behoudt in het wetsvoorstel van de mogelijkheid voor de datahouder om gebruik van de data te maken.*

C. Rechtszekerheid en gelijke toepassing in de EU vereist verduidelijking van kernbegrippen, rechten en verplichtingen.

Er komen steeds meer regels bij in Nederland en Europa en de complexiteit neemt toe. Het is dan ook van wezenlijk belang dat de **regels voldoende duidelijk** zijn. Dat voldoende duidelijk is wat onder kernbegrippen wordt verstaan, wat de verplichtingen en rechten concreet inhouden en op wie de verplichtingen rusten dan wel wie aanspraak op een recht heeft. Als dit niet voldoende duidelijk is, levert dit implementatieproblemen op. Ook is de duidelijkheid van belang om te zorgen dat de regels in de hele EU hetzelfde begrepen worden zodat er een echte **interne markt** tot stand kan komen. Het huidige voorstel bevat nog te veel onduidelijkheden. We zetten ons ervoor in om de onduidelijkheden om te zetten in duidelijke en begrijpelijke wet- en regelgeving. Zo moet er meer handen en voeten worden gegeven aan wat onder kerntermen wordt verstaan als datahouder, 'concurrent product', gebruiks- en omgevingsdata versus afgeleide en berekende data.

De definitie van 'data' is erg ruim. Onder data wordt elke digitale weergave verstaan van activiteiten, feiten of informatie en compilaties daarvan, inclusief beeld en geluid. Met name 'informatie' is een ruim begrip. Informatie veronderstelt een zekere bewerking van waargenomen feiten. Terwijl uit overweging 17 valt op te maken dat bewerkingen van met IoT-producten gegenereerde data buiten de scope vallen. Er bestaat dus onduidelijkheid over wat concreet onder 'gebruiks- en omgevingsdata' moet worden verstaan. In overweging 17 is opgenomen dat data zoals gegenereerd door een product binnen de scope van de datadeelverplichtingen valt maar dat daarvan met behulp van software (berekeningen) afgeleide en berekende data buiten de scope valt (omdat er intellectuele eigendomsrechten op die software kunnen rusten). Uit de wetsartikelen en de definitie van data is dit echter geenszins af te leiden. **We opteren voor een duidelijke definitie in artikel 2 van IoT gebruiks- en omgevingsdata (Gebruikersdata).** Ook is kabinet is van mening dat het onduidelijk is welke data precies worden gezien als gegenereerd door het gebruik van de gebruiker en dus voor welke data de toegangsrechten zullen gelden. Het kabinet heeft aangegeven hier opheldering over te vragen bij de Commissie.

Ook is er onduidelijkheid over welke IoT-producten binnen de scope van de datadeelverplichtingen vallen. In overweging 14 is opgenomen dat fysieke producten die data over hun functionaliteit, gebruik of omgeving kunnen vergaren, genereren of verzamelen met behulp van componenten (zoals sensoren, microfoons of lenzen) en dit via publieke elektronische communicatiemiddelen kunnen doorgeven ('IoT-producten'),

binnen de scope van de Dataverordening vallen. In overweging 15 is opgenomen dat producten die echter primair bedoeld zijn om beeld, geluid en tekst vast te leggen, af te spelen of te tonen of door te geven, zoals servers, webcams, text scanners, camera's, smartphones, tablets, laptops, pc's en sound recording systems, niet binnen de scope van de verplichtingen tot het B2B en B2C delen van data vallen. Zo vermoeden we dat 'niet smartphone-mobiele telefoons' buiten de scope van de Dataverordening vallen omdat telefoons primair bedoeld zijn om geluid door te geven. Maar dit valt niet met zekerheid te zeggen. **We opteren voor een duidelijke definitie van IoT-producten waarop de B2B en B2C datadeelverplichting van toepassing is, door een definitie in artikel 2 op te nemen waarin bepaalde elementen van overwegingen 14 en 15 zijn overgenomen.**

Het begrip data waarop de B2G datadeelverplichting van toepassing is, lijkt breder te zijn dan IoT-data. Ook blijkt niet duidelijk uit artikel 24 dat de klant over de rechten moet beschikken op de over te zetten data, applicaties en digital assets (denk hierbij aan het hebben van de benodigde rechten van intellectuele eigendom, zoals licenties). We kunnen nu alleen afgaan op de toelichting en voorbeelden zoals opgenomen in de overwegingen van het wetsvoorstel. **We opteren voor een duidelijke definitie in artikel 2 van data waarop de B2G datadeelverplichting van toepassing is. Ook opteren we voor het opnemen in artikel 24 (switch-verplichting) dat het om data, applicaties en data assets gaat waarvan de gebruiker over de benodigde rechten beschikt (licenties), zoals nu alleen is opgenomen in overweging 72 van de overwegingen.**

In het voorstel worden afhankelijk of het om persoonsgegevens gaat of om niet-persoonsgebonden gegevens gaat, verschillende criteria gebruikt om een datahouder te definiëren. Ter zake persoonsgegevens moet het gaan om de verwerkingsverantwoordelijke en bij niet-persoonsgebonden is eenieder die technisch in staat is om toegang te verlenen te beschouwen als datahouder. Deze laatste categorie biedt onvoldoende duidelijkheid. Datahouder is echter een kernbegrip en bepaalt op wie datadeelverplichtingen liggen. Het is dan ook van groot belang voor de uitvoerbaarheid en het vertrouwen in data delen dat voldoende duidelijk is afgebakend wie als datahouder is aan te merken.

Ook is niet duidelijk wat onder 'gerelateerde diensten' moet worden verstaan. *Van belang is dat de verhouding met de gebruikte begrippen in de richtlijnen verkoop goederen en richtlijn digitale inhoud nader wordt omschreven aangezien sprake is van een overlap met 'producten' en 'gerelateerde diensten' in het wetsvoorstel voor een Dataverordening.* Daarnaast is er onduidelijkheid over het begrip 'concurrent product' (volledig product of ook separate onderdelen; en hoe om te gaan met doorontwikkelingen van een product) en is er ook onduidelijkheid over wie onder 'Operators of Data spaces' moeten worden verstaan. We zien de term 'Operators of Data spaces' plotseling opduiken in artikel 28 zonder dat het begrip in artikel 2 wordt omschreven. Wel worden er verplichtingen opgelegd aan deze operators of data spaces. De werkbaarheid en redelijkheid van de verplichtingen die op deze operators of data spaces worden gelegd, zijn niet te beoordelen zonder dat duidelijk is wie deze operators zijn.

We **opteren we ervoor dat in de wetsartikelen zelf duidelijke definities en (heldere) afbakeningen worden opgenomen (zoals een duidelijke definitie van 'Operators of data spaces' in artikel 2).**

Ook is het onduidelijk of de bepaling in het Dataverordeningswetsvoorstel dat Poortwachters uitsluit van het ontvangen van IoT-gebruiks- en omgevingsdata van andere gebruikers net als de verplichtingen van de Digitale Markt Verordening (DMA) geldt voor de zogenaamde 'core platform diensten'[33] van een Poortwachter of dat deze bepaling geldt voor alle marktsegmenten waarop een Poortwachter opereert.

Duidelijke definities van kernbegrippen zijn te meer belangrijk omdat ervaring leert dat nationale toezichthouders de wet anders verschillend kunnen gaan interpreteren.[34] Dit lijdt tot onduidelijkheid bij de toepassing van de wet en tot fragmentatie op de interne markt. Deze onbedoelde gevolgen ondermijnen de door de Europese Commissie gestelde doelen voor een Europees sterke datastrategie. **We opteren voor een duidelijke definitie in artikel 2 van 'publieke noodsituaties' ter afbakening van B2G datadeelverplichtingen.** Overigens zou iedere noodsituatie eindig moeten zijn en is het daarom raadzaam om voor dit soort situaties te werken met zogenaamde 'sunset-clausules'.[35]

Uitvoerbare regels
*Om te zorgen dat de doelstelling daadwerkelijk haalbaar is, is het essentieel dat de **regels uitvoerbaar** zijn in de praktijk. Het huidige voorstel heeft hier op punten onvoldoende rekening mee gehouden.*

Continue dienstverlening tijdens transitieperiode
We ondersteunen het doel van de Europese Commissie om vendor lock-in te vermijden en tegemoet te komen aan de behoefte van de klant om bij het switchen tussen aanbieders te worden ondersteund. De vereisten moeten echter uitvoerbaar en evenwichtig zijn. Het juiste evenwicht tussen de operationele verantwoordelijkheden van klanten en providers moet bewaard blijven.
De verplichting voor een dataverwerkingsaanbieder (aanbieder van infrastructuur) om de continuïteit van de dienstverlening te garanderen tijdens de transitie naar een nieuwe aanbieder (artikel 24) kan onredelijk en niet-realistische zijn. In traditionele outsourcingcontracten, waarover intensief wordt onderhandeld, voorzien de daarin overeengekomen serviceniveaus nooit in 100% servicecontinuïteit, aangezien partijen begrijpen en overeenkomen dat de service tijdens een beëindigingsfase niet hetzelfde zal zijn als tijdens het verlenen van de dienst zonder transitieperikelen. Er wordt in het voorstel onvoldoende rekening gehouden met de mogelijke complexiteit en arbeidsintensiviteit van dataoverdracht en de gevolgen daarvan op de servicecontinuïteit. We zetten ons in voor redelijke en uitvoerbare regels, die alle partijen ten goede komen. Bovendien is voor een goede transitie de samenwerking

[33] De 'core platform diensten' zoals omschreven in de Digitale Markt Verordening (DMA).
[34] Dit zien we bijvoorbeeld bij interpretatie door nationale toezichthouders van de Algemene Verordening Gegevensbescherming (AVG).
[35] https://en.wikipedia.org/wiki/Sunset_provision

tussen de dienstaanbieder en de klant essentieel. In de Dataverordening wordt de volledige verantwoordelijkheid voor de transitie bij de dienstaanbieder gelegd. We begrijpen de behoefte maatregelen te treffen om oneerlijke verhoudingen te corrigeren. De verplichtingen moeten echter praktisch uitvoerbaar zijn. De verplichtingen gelden immers ook in gevallen waarbij geen sprake is van oneerlijke verhoudingen. **We opteren dan ook voor redelijke transitieverplichtingen die enerzijds waar nodig misbruik van oneerlijke verhoudingen aanpakken en anderzijds praktisch uitvoerbaar zijn.**

We zien dat ook het kabinet van mening is dat de verplichtingen van de Dataverordening niet tot onevenredige zware lasten voor aanbieders van diensten mogen leiden. Ook zien we dat de erkenning dat sectorale regelgeving geschikter kan zijn om specifieke problemen gericht te adresseren.

Functionele gelijkwaardigheid
Het is onduidelijk hoe aan de verplichting om te zorgen voor functionele gelijkwaardigheid (artikelen 23 en 26) voor aanbieders van 'Infrastructure as a Service' (IaaS) moet worden voldaan. Hoe kan een IaaS-aanbieder hetzelfde kwaliteits- en beveiligingsniveau van dienstverlening garanderen in de omgeving van één van zijn concurrenten? Moet de zittende provider servicelevel agreements (SLAs) vergelijken en de klant hierover adviseren? Moet de klant het advies van de latende aanbieder opvolgen? Wat gebeurt er als de klant niet hetzelfde serviceniveau contracteert omdat hij vindt dat hij niet hetzelfde serviceniveau nodig heeft? In het huidige wetsvoorstel is niets opgenomen om de zittende aanbieder in staat te stellen om te voldoen aan deze verplichting. Het lijkt erop dat de zittende aanbieder medeverantwoordelijk is voor de dienstverlening die geleverd wordt door één van zijn concurrenten zonder dat de zittende aanbieder enige zeggenschap of controle over de dienstverlening van zijn concurrent heeft. In overweging 72 is gespecifieerd dat onder functionele gelijkwaardigheid wordt verstaan: het continueren van een minimumlevel van functionaliteit van een dienst waar de originele en nieuwe dienst (geheel of gedeeltelijk) van hetzelfde type zijn. **We opteren voor redelijke verplichtingen, verplichtingen waarbij in redelijkheid rekening wordt gehouden met de praktische uitvoering ervan, waaronder wie waar controle en invloed over kan uitoefenen; en voor verduidelijking in de wetsartikelen wat onder functionele gelijkwaardigheid wordt verstaan (en niet te volstaan met uitleg in overweging 72).**

Ook roept de afbouw van de financiële vergoedingen voor het switchen (art. 25) vragen op. Is het redelijk om extra verplichtingen en verantwoordelijkheden op te leggen aan dataverwerkingsaanbieders (cloud serviceproviders) waarvoor de eerste 3 jaar na inwerkingtreding van de Dataverordening alleen de kostprijs in rekening mag worden gebracht en na die 3 jaar volledig gratis verleend moeten worden? Met name voor bestaande lopende contracten waarbij partijen geen rekening hebben kunnen houden met deze nieuwe verplichtingen, lijkt dit niet redelijk. Te meer als het contract wordt beëindigd vanwege een schending van het contract door de klant (bijvoorbeeld omdat de klant de diensten deels of volledig niet heeft betaald). **We opteren voor redelijke verplichtingen waarbij sprake is van een goede balans tussen alle betrokken partijen.** De Europese Commissie stelt als doelstelling dat *alle* bedrijven optimaal waarde uit data

kunnen halen en in staat zijn om te innoveren en te concurreren. Dit veronderstelt dat ook datahouders hiertoe in staat gesteld moeten worden.

Het overbrengen van grote hoeveelheden gegevens van het ene systeem naar het andere is vaak kostbaar, omslachtig en tijdrovend. *We opteren dan ook om de verplichting redelijker in te richten, met name voor het mkb. Waaronder de mogelijkheid voor een langere transitieperiode. De transitieperiode is nu vastgesteld op 30 dagen met een mogelijkheid om deze onder bepaalde voorwaarden te verlengen tot maximaal 6 maanden. De mogelijkheid om deze te verlengen is nu beperkt tot de technische onmogelijkheid om de transitie binnen 30 dagen af te ronden.* ***Gezien de krapte op de IT-arbeidsmarkt opteren we voor de mogelijkheid van verlenging als, ondanks inspanningen om personeel aan te trekken, door personeelskrapte de transitie niet binnen 30 dagen afgerond kan worden. Ook opteren we voor meer duidelijkheid wat verstaan wordt onder 'technische onmogelijkheid'.***

D. **Internationale doorgifte en overheidstoegang tot niet-persoonsgebonden data**

Het voorkomen van disproportionele overheidstoegang tot niet-persoonsgebonden data (als ook tot persoonsgegevens) is iets dat alleen kan worden opgelost op politiek niveau. De oplossing voor dit probleem kan niet worden verwacht van bedrijven. Bedrijven maken de surveillance wetten van hun overheid niet noch kunnen zij deze wetten wijzigen. Ook is het van belang om rekening te houden met het verschil in gevoeligheid tussen niet-persoonsgebonden gegevens en persoonsgegevens. Het verbaast ons dat het kabinet positief is over de keuze om de verantwoordelijkheid om onrechtmatige datatoegang te voorkomen bij de aanbieders van dataverwerkingsdiensten te beleggen. Het kabinet stelt ter verantwoording hiervan dat aanbieders van dataverwerkingsdiensten een centrale rol in de dataeconomie hebben en een verantwoordelijkheid hebben voor het veilig en beschermd opslaan en verwerken van de data en diensten die zij voor gebruikers in beheer hebben. Het kabinet gaat hierbij voorbij aan het feit dat dataverwerkingsdiensten tussenpersonen zijn in de zin van de Digital Services Act en geen specifieke kennis hebben of hoeven te hebben over de data die zij opslaan. In de Algemene Verordening Gegevensbescherming (AVG) is de verantwoordelijkheid dan ook belegd bij de verwerkingsverantwoordelijke, degene die de dataverwerkingsaanbieder opdracht geeft om data op te slaan en weet welke data worden opgeslagen en aangeeft welke beveiligingsniveau nodig is ter bescherming van de data. Het is onduidelijk waarom ten aanzien van niet-persoonsgebonden gegevens een andere insteek wordt gekozen dan bij de bescherming van persoonsgegevens (zoals bepaald in de AVG).

E. **Interoperabiliteitsstandaarden**

We verwelkomen dat de ontwikkeling van technologische en juridische standaarden voor interoperabiliteit (inclusief rekening houdend met de beperkte middelen van micro-, kleine en middelgrote ondernemingen) wordt bevorderd. Standaarden zijn van groot belang. Zo maakt de afspraak over de vorm van een batterij het mogelijk dat producten kunnen worden ontwikkeld waar die batterij in past. Ook zijn er afspraken gemaakt over

de kwaliteit van data.[36] Afspraken over interoperabiliteit maken het mogelijk dat verschillende systemen met elkaar 'kunnen communiceren' en dat het toetsen op het voldoen aan wet en regelgeving, bijvoorbeeld door middel van audits, geen overmatige inspanning vereist.[37] We zijn echter niet blij met de toenemende rol die de Europese Commissie naar zich toetrekt als het om de ontwikkeling van standaarden gaat. De ontwikkeling van standaarden is van oudsher een zelfreguleringsproces. Bedrijven komen bij elkaar om af te spreken op welke wijze praktische uitvoering gegeven kan worden aan wettelijke verplichtingen. Op deze wijze wordt bevorderd dat standaarden in de praktijk uitvoerbaar zijn. In steeds meer verordeningen zien we terugkomen dat de Europese Commissie de ontwikkeling van standaarden kan afdwingen als dit naar hun subjectieve oordeel niet snel genoeg of niet juist genoeg gebeurt. Er worden echter geen objectieve criteria opgenomen op basis waarvan de Europese Commissie tot dit oordeel kan komen. Dit doet af aan het zelfreguleringsproces. ***We opteren dan ook voor duidelijke en objectieve criteria[38] op basis waarvan de Europese Commissie als last resort de ontwikkeling of bijsturing van standaarden kan afdwingen.***

NB. Het begrip interoperabiliteit heeft in de Dataverordening een andere inhoud dan in de richtlijn verkoop goederen en de richtlijn digitale inhoud ('het vermogen van de goederen om te functioneren met hardware of software die verschilt van die welke waarmee goederen van hetzelfde type gewoonlijk worden gebruikt'). Het verdient aanbeveling dat de inhoud van de definities nader wordt afgestemd.

F. **Toezicht en handhaving**

Om te kunnen komen tot een sterke interne datamarkt, is het van groot belang dat het toezicht op en de handhaving van de nieuwe regels eenduidig is in de Unie. Als de regels in de diverse lidstaten anders worden uitgelegd en anders worden toegepast door de verschillende bevoegde autoriteiten in de diverse lidstaten, leidt dit tot fragmentatie tussen de verschillende lidstaten dat de uitvoering van de regels bemoeilijkt en de innovatie en groei van de datamarkt nadelig zal beïnvloeden. Dit vereist ook onderling afgestemde eenduidige uitleg (waarbij de uitleg van de Europese hoge rechter leidend is), handhaving en toepassing van de nieuwe regels door de verschillende bevoegde toezichthouders binnen elke lidstaat.

G. ***Mkb***

De regeldruk in Nederland en de rest van Europa is hoog. Als we een gunstig klimaat willen scheppen voor innovatie en groei, om het mogelijk te maken dat nieuwe partijen de markt kunnen betreden en kleine partijen kunnen groeien om te concurreren met andere (machtige) marktpartijen, is het van belang dat rekening wordt gehouden met de specifieke behoeften van het mkb.

[36] ISO/TS 8000:2011

[37] Er wordt momenteel op internationaal niveau een standaard ontwikkeld om datasubjecten en dataobjecten te identificeren. Deze standaarden helpen bij de communicatie tussen systemen (interoperabiliteit).

[38] Dergelijke criteria zouden kunnen zijn – waar relevant - het niet voldoen aan de vereisten van artikel 30.1a-d. We maken hierbij echter de aanvullende kanttekening dat de vereisten van artikel 30.1b-d niet passend zijn voor alle soorten smart contracts.

We verwelkomen dan ook[39]:

- *Dat het micro en kleinbedrijf is uitgezonderd van de verplichtingen tot het verplicht data delen (zowel B2B als B2G);*
- *Misbruik van machtsongelijkheid wordt aangepakt;*
- *Europese Commissie verplicht wordt om vrijwillig te gebruiken gebalanceerde B2B modelcontract clausules op te stellen.*

We opteren voor de mogelijkheid om – waar relevant – in sectorspecifieke wetgeving voor een ruimere categorie van bedrijven[40] (dan de Europees gedefinieerde mkb) eventuele sectorspecifieke machtsongelijkheidsvraagstukken kunnen worden geadresseerd.

Inlichtingen:
mw. mr. I.M. Tempelman
tel: 06 12462344
e-mail: tempelman@vnoncw-mkb.nl

[39] *Ook het kabinet verwelkomt de aandacht voor de specifieke behoeften van het mkb.*
[40] Bijvoorbeeld bedrijven met minder dan 250 werknemers maar met een hogere omzet dan de omzetgrens die voor het mkb wordt gehanteerd.