EUROPESE
COMMISSIE

Brussel, 23.2.2022
COM(2022) 68 final

2022/0047 (COD)

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

betreffende geharmoniseerde regels inzake eerlijke toegang tot en eerlijk gebruik van data
(Dataverordening)

(Voor de EER relevante tekst)

{SEC(2022) 81 final} - {SWD(2022) 34 final} - {SWD(2022) 35 final}

TOELICHTING

1. ACHTERGROND VAN HET VOORSTEL

• Motivering en doel van het voorstel

Deze toelichting is gevoegd bij het voorstel voor een verordening betreffende geharmoniseerde regels inzake eerlijke toegang tot en eerlijk gebruik van data (dataverordening).

Data zijn een centraal onderdeel van de digitale economie en een essentiële hulpbron voor de groene en digitale transitie. De hoeveelheid data die door mensen en machines wordt gegenereerd, is de afgelopen jaren exponentieel toegenomen. De meeste data blijven echter ongebruikt of de waarde ervan is in handen van slechts een paar grote ondernemingen. Het potentieel van datagestuurde innovatie wordt belemmerd door een laag vertrouwen, tegenstrijdige economische prikkels en technologische belemmeringen. Het is daarom van cruciaal belang om dit potentieel te ontsluiten door hergebruik van data mogelijk te maken en door belemmeringen voor de ontwikkeling van de Europese data-economie weg te nemen. Dit moet gebeuren overeenkomstig de Europese regels en met volledige eerbiediging van de Europese waarden, en in overeenstemming met de doelstelling om de digitale kloof te verkleinen zodat iedereen van deze kansen kan profiteren. Door te zorgen voor een beter evenwicht in de verdeling van de waarde van data, in combinatie met de nieuwe golf van niet-persoonsgebonden industriële data en de verspreiding van verbonden producten die behoren tot het internet der dingen, is er een enorm potentieel voor het stimuleren van een duurzame data-economie in Europa.

Het reguleren van de toegang tot en het gebruik van data is een fundamentele voorwaarde om de kansen van dit digitale tijdperk te grijpen. De voorzitter van de Commissie, Ursula von der Leyen, verklaarde in haar politieke beleidslijnen voor de Commissie voor 2019-2024 dat Europa „*dataverkeer en -gebruik in evenwicht moet brengen met inachtneming van hoge normen op het gebied van privacy, beveiliging, veiligheid en ethiek*”[1]. Het werkprogramma van de Commissie voor 2020[2] bevat verschillende strategische doelstellingen, waaronder de Europese datastrategie[3], die in februari 2020 is aangenomen. Deze strategie is erop gericht een echte interne datamarkt tot stand te brengen en van Europa een wereldleider in de data-agile economie te maken. Daarom is de dataverordening een belangrijke pijler en het tweede belangrijke initiatief dat in de datastrategie is aangekondigd. Zij draagt met name bij tot de totstandbrenging van een sectoroverschrijdend governancekader voor de toegang tot en het gebruik van data door middel van wetgeving inzake aangelegenheden die van invloed zijn op de betrekkingen tussen actoren in de data-economie, om horizontale uitwisseling van data tussen sectoren te stimuleren.

In de conclusies van de Europese Raad van 21-22 oktober 2021 werd benadrukt „*dat er snel vooruitgang moet worden geboekt met bestaande en toekomstige initiatieven, met name door het benutten van de waarde van gegevens in Europa, meer bepaald door middel van een alomvattend regelgevingskader dat innovatie bevordert, een betere overdraagbaarheid van en*

[1] Ursula von der Leyen, Een Unie die de lat hoger legt — Mijn agenda voor Europa, Politieke beleidslijnen voor de volgende Europese Commissie 2019-2024, 16 juli 2019.

[2] Europese Commissie, bijlagen bij het werkprogramma van de Commissie voor 2020 — Een Unie die de lat hoger legt, COM (2020) 37 van 29 januari 2020.

[3] COM/2020/66 final.

eerlijke toegang tot gegevens faciliteert en interoperabiliteit verzekert"[4]. Op 25 maart 2021 heeft de Europese Raad aangedrongen op „*betere benutting van het potentieel van data en digitale technologieën ten behoeve van de samenleving en de economie*"[5]. Op 1-2 oktober 2020 benadrukte de Raad „*de noodzaak om data van hoge kwaliteit eenvoudiger beschikbaar te maken en om een betere uitwisseling en bundeling van gegevens alsook interoperabiliteit te bevorderen en mogelijk te maken*"[6]. Wat clouddiensten betreft, hebben de EU-lidstaten op 15 oktober 2020 unaniem een gezamenlijke verklaring aangenomen over de opbouw van clouddiensten van de volgende generatie voor ondernemingen en de overheidssector in de EU. Deze clouddiensten moeten bijvoorbeeld voldoen aan de hoogste normen op het gebied van overdraagbaarheid en interoperabiliteit[7].

In de resolutie van het Europees Parlement van 25 maart 2021 over een Europese datastrategie werd er bij de Commissie op aangedrongen een gegevenswet voor te stellen om in alle sectoren een grotere en eerlijkere gegevensstroom, tussen bedrijven onderling (B2B), tussen bedrijven en de overheid (B2G), tussen de overheid en bedrijven (G2B) en tussen overheden (G2G) aan te moedigen en mogelijk te maken[8]. In zijn resolutie van 25 maart 2021 benadrukte het Europees Parlement ook de noodzaak om gemeenschappelijke Europese dataruimten tot stand te brengen met het oog op het vrije verkeer van niet-persoonsgebonden data over grenzen heen en tussen sectoren en tussen bedrijven, de academische wereld, relevante belanghebbenden en de publieke sector. Vanuit dit oogpunt moedigt het de Commissie aan de gebruiksrechten te verduidelijken, met name in B2B- en B2G-marktomgevingen. Het benadrukte ook dat onevenwichtigheden op de markt als gevolg van de concentratie van data de concurrentie beperken, de drempels voor markttoegang verhogen en de toegang tot en het gebruik van gegevens op ruimere schaal verminderen.

In zijn resolutie heeft het Europees Parlement er ook op gewezen dat contractuele overeenkomsten tussen bedrijven niet noodzakelijkerwijs een adequate toegang tot data voor kleine en middelgrote bedrijven garanderen. De reden hiervoor is dat er verschillen zijn in onderhandelingsmacht en deskundigheid. Het Europees Parlement heeft daarom benadrukt dat in contracten duidelijke verplichtingen en aansprakelijkheidsbepalingen moeten worden opgenomen voor de toegang tot data en de verwerking, het delen en de opslag ervan, om misbruik ervan te beperken.

Daarom werd de Commissie en de EU-lidstaten verzocht na te gaan welke rechten en plichten de actoren hebben wat betreft toegang tot data die zij hebben helpen genereren en hen daar beter bewust van te maken, met name het recht om toegang te krijgen tot data, om data over te dragen, om er bij een andere partij op aan te dringen data niet langer te gebruiken, of om data te corrigeren of te verwijderen, en tevens de houders van die rechten te identificeren en de aard van die rechten af te bakenen.

Op het gebied van business-to-government heeft het Europees Parlement de Commissie verzocht nader te bepalen onder welke omstandigheden en voorwaarden en met welke

---

4 Europese Raad, Bijeenkomst van de Europese Raad (21-22 oktober 2021) — Conclusies EUCO 17/21, 2021, blz. 2.

5 Europese Raad, Verklaring van de leden van de Europese Raad (25 maart 2021) — Verklaring SN 18/21, blz. 4.

6 Europese Raad, Bijeenkomst van de Europese Raad (1-2 oktober 2020) — Conclusies EUCO 13/21, 2020, blz. 5.

7 Europese Commissie (2020). *Commission welcomes Member States' declaration on EU cloud federation*, persbericht.

8 Resolutie van het Europees Parlement van 25 maart 2021 over een nieuwe datastrategie voor Europa (2020/2217(INI)).

stimulansen de particuliere sector moet worden verplicht om data te delen met de openbare sector, bijvoorbeeld omdat dit noodzakelijk is voor de organisatie van datagestuurde overheidsdiensten en ook te kijken naar regelingen voor verplichte B2G-data-uitwisseling, bijvoorbeeld in geval van overmacht.

Tegen deze achtergrond stelt de Commissie de voorgestelde **dataverordening** voor, om te **zorgen voor eerlijke waardeverdeling uit data aan actoren in de data-economie en om de toegang tot en het gebruik van data te bevorderen**.

Het voorstel zal bijdragen tot de verwezenlijking van de bredere beleidsdoelstellingen, namelijk ervoor zorgen dat EU-bedrijven in alle sectoren in staat zijn te innoveren en te concurreren, dat personen daadwerkelijk mondiger worden met betrekking tot hun data en bedrijven en overheidsinstanties beter worden toegerust met een evenredig en voorspelbaar mechanisme om grote beleids- en maatschappelijke uitdagingen aan te pakken, waaronder noodsituaties en andere uitzonderlijke situaties. Bedrijven zullen met hun data en andere digitale activa gemakkelijk kunnen overstappen tussen concurrerende aanbieders van clouddiensten en andere dataverwerkingsdiensten. Het delen van data binnen en tussen economische sectoren vereist een interoperabiliteitskader dat bestaat uit procedurele en wetgevende maatregelen om het vertrouwen te vergroten en de efficiëntie te verbeteren. Het creëren van gemeenschappelijke Europese dataruimten voor strategische economische sectoren en domeinen van algemeen belang zal bijdragen tot een echte interne datamarkt waarbinnen data tussen sectoren gedeeld en gebruikt kunnen worden. Deze verordening draagt derhalve bij tot deze governancekaders en -infrastructuur en tot het delen van data buiten de dataruimten.

De specifieke doelstellingen van het voorstel worden hieronder uiteengezet.

– **De toegang tot en het gebruik van data door consumenten en bedrijven vergemakkelijken, met behoud van stimulansen om te investeren in manieren om door middel van data waarde te genereren.** Dit omvat het vergroten van de rechtszekerheid rond het delen van data die zijn verkregen uit of gegenereerd door het gebruik van producten of gerelateerde diensten, en het operationeel maken van regels die moeten leiden tot eerlijke data-uitwisselingsovereenkomsten. Het voorstel **verduidelijkt** de toepassing van de relevante rechten uit hoofde van Richtlijn 96/9/EG betreffende de rechtsbescherming van databanken (de **databankrichtlijn**)[9] op de bepalingen ervan.

– **Voorzien in het gebruik door overheidsinstanties en EU-instellingen, -agentschappen of -organen van data die in het handen zijn van ondernemingen in bepaalde situaties waarin er sprake is van een uitzonderlijke noodzaak om de data te gebruiken.** Dit heeft voornamelijk betrekking op openbare noodsituaties, maar ook op andere uitzonderlijke situaties waarin het verplicht delen van data tussen bedrijven en overheden gerechtvaardigd is, ter ondersteuning van empirisch onderbouwd, doeltreffend, efficiënt en prestatiegericht overheidsbeleid en -diensten.

– **Het overstappen tussen cloud- en edgediensten vergemakkelijken.** Toegang tot concurrerende en interoperabele dataverwerkingsdiensten is een voorwaarde voor een bloeiende data-economie, waarin data gemakkelijk kunnen worden gedeeld binnen en tussen sectorale ecosystemen. De mate van vertrouwen in dataverwerkingsdiensten is bepalend voor het gebruik van dergelijke diensten door gebruikers in alle sectoren van de economie.

9 PB L 77 van 27.3.1996, blz. 20.

– **Voorzien in waarborgen tegen onrechtmatige data-overdracht zonder kennisgeving door aanbieders van clouddiensten.** De reden hiervoor is dat er bezorgdheid is over de onrechtmatige toegang tot data door overheden van buiten de EU/de Europese Economische Ruimte (EER). Dergelijke waarborgen moeten leiden tot meer vertrouwen in de dataverwerkingsdiensten die de Europese data-economie in toenemende mate ondersteunen.

– **Interoperabiliteitsnormen ontwikkelen voor data die tussen sectoren kunnen worden hergebruikt**, om belemmeringen voor het delen van data tussen domeinspecifieke gemeenschappelijke Europese dataruimten overeenkomstig de sectorale interoperabiliteitsvereisten uit de weg te ruimen, evenals belemmeringen voor het delen van data die niet binnen het toepassingsgebied van een specifieke gemeenschappelijke Europese dataruimte vallen. Volgens het voorstel zal ook de vaststelling van normen voor „slimme contracten" worden ondersteund. Dit zijn computerprogramma's die werken met elektronische registers, die transacties uitvoeren en afwikkelen op basis van vooraf bepaalde voorwaarden. Zij kunnen houders en ontvangers van data garanderen dat de voorwaarden voor het delen van data worden nageleefd.

• **Verenigbaarheid met bestaande bepalingen op het beleidsterrein**

Dit voorstel is in overeenstemming met de bestaande regels inzake de **verwerking van persoonsgegevens** (waaronder de algemene verordening gegevensbescherming[10], hierna „AVG" genoemd) en de bescherming van het privéleven en de **vertrouwelijkheid van communicatie**, alsook met alle (persoonlijke en niet-persoonsgebonden) gegevens die zijn opgeslagen in en waartoe toegang wordt verkregen via eindapparatuur (de e-privacyrichtlijn[11], die moet worden vervangen door de e-privacyverordening waarover momenteel wordt onderhandeld). Dit voorstel vormt een aanvulling op bestaande rechten, met name rechten met betrekking tot data die worden gegenereerd door een product van een gebruiker dat verbonden is met een openbaar elektronisch communicatienetwerk.

De **verordening inzake het vrije verkeer van niet-persoonsgebonden gegevens**[12] heeft een belangrijke bouwsteen van de Europese data-economie tot stand gebracht door ervoor te zorgen dat niet-persoonsgebonden data overal in de EU kunnen worden opgeslagen, verwerkt en overgedragen. Daarin stond ook een nieuwe, zelfregulerende aanpak van het probleem van „vendor lock-in" op het niveau van aanbieders van dataverwerkingsdiensten, namelijk de invoering van gedragscodes om de overdracht van data tussen clouddiensten te vergemakkelijken (de door de sector ontwikkelde gedragscodes voor „Switching Cloud Providers and Porting Data (SWIPO)"). Dit voorstel bouwt hierop voort en helpt bedrijven en burgers optimaal gebruik te maken van het recht om over te stappen naar een andere cloudprovider en data over te dragen. Het is ook volledig in overeenstemming met de richtlijn oneerlijke bedingen in overeenkomsten, wat het verbintenissenrecht betreft[13]. Aangezien de zelfregulerende aanpak de marktdynamiek niet aanzienlijk lijkt te hebben beïnvloed, wordt voor clouddiensten nu voorgesteld om regels op te stellen voor het bovengenoemde probleem, dat in de verordening inzake het vrije verkeer van niet-persoonsgebonden data aan de orde is gesteld.

---

10 PB L 119 van 4.5.2016, blz. 1.
11 PB L 201 van 31.7.2002, blz. 37.
12 PB L 303 van 28.11.2018, blz. 59; SWIPO (2021), zie *website*.
13 PB L 95 van 21.4.1993, blz. 29.

De internationale verwerking en opslag van data en de overdracht van data vallen onder de algemene verordening gegevensbescherming, de handelsverbintenissen van de Wereldhandelsorganisatie (WTO), de Algemene Overeenkomst inzake de handel in diensten (GATS) en bilaterale handelsovereenkomsten.

Het **mededingingsrecht**[14] is van toepassing in het kader van onder meer concentratiecontrole, het delen van data door ondernemingen of misbruik van een machtspositie van een onderneming.

De **databankrichtlijn**[15] voorziet in een bescherming sui generis van databanken die zijn gecreëerd als gevolg van een substantiële investering, ook al is de databank zelf geen originele intellectuele schepping die door het auteursrecht wordt beschermd. Voortbouwend op de grote hoeveelheid jurisprudentie waarin de bepalingen van de databankrichtlijn worden geïnterpreteerd, pakt dit voorstel de bestaande rechtsonzekerheid aan over de vraag of databanken die data bevatten die zijn gegenereerd of verkregen door het gebruik van producten of gerelateerde diensten, zoals sensoren, of andere soorten machinaal gegenereerde data, recht zouden hebben op een dergelijke bescherming.

De **verordening onlinetussenhandelsdiensten**[16] legt transparantieverplichtingen op, waarbij platforms worden verplicht om voor zakelijke gebruikers de data te beschrijven die bij de dienstverlening zijn gegenereerd.

De **richtlijn open data**[17] bevat minimumvoorschriften voor het hergebruik van data die in handen zijn van de overheidssector en van door de overheid gefinancierde onderzoeksdata die via databanken openbaar worden gemaakt.

Het **initiatief Interoperabel Europa** beoogt de invoering van een samenwerkingsbeleid inzake interoperabiliteit voor een gemoderniseerde overheidssector. Het initiatief kwam voort uit ISA^2, een EU-financieringsprogramma dat liep van 2016 tot 2021 en dat steun verleende voor de ontwikkeling van digitale oplossingen om interoperabele grens- en sectoroverschrijdende overheidsdiensten mogelijk te maken[18].

Dit voorstel vormt een aanvulling op de onlangs aangenomen **datagovernanceverordening**, die tot doel heeft de vrijwillige uitwisseling van data door personen en bedrijven te vergemakkelijken en de voorwaarden voor het gebruik van bepaalde overheidsdata te harmoniseren, zonder dat de materiële rechten met betrekking tot de data of de vastgestelde toegangs- en gebruiksrechten voor data worden gewijzigd[19]. Het vormt ook een aanvulling op het voorstel voor een **verordening inzake digitale markten**, op grond waarvan bepaalde aanbieders van kernplatformdiensten die als „poortwachters” zijn aangemerkt, onder meer moeten zorgen voor een effectievere overdraagbaarheid van data die zijn gegenereerd door de activiteiten van zakelijke en eindgebruikers[20].

Dit voorstel doet geen afbreuk aan de bestaande regels op het gebied van intellectuele eigendom (met uitzondering van de toepassing van het recht sui generis van de databankrichtlijn), mededinging, justitie en binnenlandse zaken en daarmee verband houdende (internationale) samenwerking, handelsgerelateerde verplichtingen of de rechtsbescherming

14 PB L 335 van 18.12.2010, blz. 36.
15 PB L 77 van 27.3.1996, blz. 20.
16 PB L 186 van 11.7.2019, blz. 57.
17 PB L 172 van 26.6.2019, blz. 56.
18 PB L 318 van 4.12.2015, blz. 1.
19 COM/2020/767 final.
20 PB L 186 van 11.7.2019, blz. 57.

van bedrijfsgeheimen.

Op verschillende gebieden zijn aanpassingen van de wetgeving nodig om de digitale transitie te bevorderen. In het kader van het Europees digitaal productpaspoort (als onderdeel van het initiatief voor duurzame producten) zullen duidelijke regels worden vastgesteld voor de toegang tot specifieke data die nodig zijn voor circulariteit en duurzaamheid van bepaalde producten gedurende hun hele levenscyclus en in niet-uitzonderlijke situaties[21]. Privaatrechtelijke regels vormen een essentieel onderdeel van het algemene kader. Deze verordening past derhalve het verbintenissenrecht en andere regels aan, om de voorwaarden voor hergebruik van data op de interne markt te verbeteren en te voorkomen dat contractpartijen misbruik maken van onevenwichtigheden in de onderhandelingsmacht ten nadele van zwakkere partijen.

Als horizontaal voorstel voorziet de **dataverordening** in **basisregels voor alle sectoren** met betrekking tot het recht om data te gebruiken, bijvoorbeeld op het gebied van slimme machines of consumptiegoederen. De rechten en plichten inzake de toegang tot en het gebruik van data zijn echter ook op sectoraal niveau in verschillende mate gereguleerd. De dataverordening zal dergelijke bestaande wetgeving niet wijzigen, maar toekomstige wetgeving op deze gebieden moet in beginsel worden afgestemd op de horizontale beginselen van de dataverordening. De convergentie met de horizontale regels van de dataverordening moet worden beoordeeld bij de herziening van sectorale instrumenten. Dit voorstel laat ruimte voor verticale wetgeving om meer gedetailleerde regels vast te stellen voor de verwezenlijking van sectorspecifieke regelgevingsdoelstellingen.

Gezien de bestaande sectorale wetgeving zal de herziening[22] van de **Inspire-richtlijn**[23], met betrekking tot de totstandbrenging van de dataruimte voor de Green Deal, verdere vrije beschikbaarheid en hergebruik van ruimtelijke en milieudata mogelijk maken. Dit initiatief moet het voor overheden, bedrijven en burgers in de EU gemakkelijker maken om de overgang naar een groenere en koolstofneutrale economie te ondersteunen en de administratieve lasten te verminderen. Het initiatief zal naar verwachting op grote schaal diensten voor herbruikbare data ondersteunen om bij te dragen tot het verzamelen, delen, verwerken en analyseren van grote hoeveelheden data die relevant zijn om de naleving van de milieuwetgeving en de prioritaire acties van de Europese Green Deal te waarborgen. Het zal de verslaglegging stroomlijnen en de lasten verminderen door middel van een beter hergebruik van bestaande data, en door via datamining en bedrijfsinformatie automatisch verslagen te genereren.

Op grond van de **EU-elektriciteitsverordening**[24] moeten transmissiesysteembeheerders data verstrekken aan regelgevende instanties en voor de planning van de toereikendheid van hulpbronnen, terwijl de **EU-elektriciteitsrichtlijn**[25] voorziet in transparante en niet-discriminerende toegang tot data en de Commissie machtigt om daarmee verband houdende interoperabiliteitsvereisten en -procedures te ontwikkelen om dit te vergemakkelijken. De **richtlijn betalingsdiensten 2**[26] opent onder bepaalde voorwaarden een aantal soorten betalingstransactie- en rekeninginformatie, waardoor het delen van data tussen bedrijven op

21 COM/2020/98 final.

22 Initiatief GreenData4All (REFIT) | Dienstregeling wetgevingstrein (Engels) | Europees Parlement (europa.eu).

23 PB L 108 van 25.4.2007, blz. 1.

24 PB L 158 van 14.6.2019, blz. 54.

25 PB L 158 van 14.6.2019, blz. 125.

26 PB L 337 van 23.12.2015, blz. 35.

het gebied van Fintech mogelijk is. In de mobiliteits- en vervoerssector bestaan er tal van uiteenlopende regels voor de toegang tot en het delen van data. Voor reparatie- en onderhoudsinformatie van motorvoertuigen en landbouwmachines gelden specifieke verplichtingen inzake toegang tot/uitwisseling van data uit hoofde van de **typegoedkeuringswetgeving**[27]. Er zijn echter nieuwe regels nodig om ervoor te zorgen dat de bestaande wetgeving inzake typegoedkeuring van voertuigen geschikt is voor het digitale tijdperk en de ontwikkeling van schone, geconnecteerde en geautomatiseerde voertuigen bevordert. Voortbouwend op de dataverordening als kader voor de toegang tot en het gebruik van data, zullen deze regels gericht zijn op sectorspecifieke uitdagingen, waaronder de toegang tot voertuigfuncties en -middelen.

In het kader van de **richtlijn intelligente vervoerssystemen**[28] zijn verschillende gedelegeerde verordeningen opgesteld die verder zullen worden ontwikkeld, met name om de toegankelijkheid van data voor weg- en multimodaal personenvervoer te specificeren, met name via nationale toegangspunten. Op het gebied van luchtverkeersbeheer zijn niet-operationele data belangrijk om de intermodaliteit en connectiviteit te verbeteren. Operationele data met betrekking tot luchtverkeersbeheer vallen onder de specifieke regeling die is vastgesteld in het kader van het **gemeenschappelijk Europees luchtruim**[29]. Bij scheepvaartmonitoring zijn vaartuiggerelateerde data (tracking en tracing) belangrijk voor betere intermodaliteit en connectiviteit: deze data vallen onder de specifieke regeling van de richtlijn monitoring- en informatiesystemen voor de zeescheepvaart[30]. Het valt ook onder de bevoegdheid van het digitale maritieme systeem en de digitale maritieme diensten[31]. In het voorstel voor een verordening inzake de uitrol van **infrastructuur voor alternatieve brandstoffen**[32] wordt gespecificeerd welke relevante soorten data beschikbaar moeten worden gesteld, in synergie met het algemene kader dat is vastgesteld in de richtlijn intelligente vervoerssystemen.

- **Verenigbaarheid met andere EU-beleidsterreinen**

Dit voorstel is in overeenstemming met de prioriteiten van de Commissie om **Europa klaar te maken voor het digitale tijdperk** en een toekomstgerichte economie op te bouwen die werkt voor de mensen[33], waarbij de digitalisering van de interne markt wordt gekenmerkt door een hoge mate van vertrouwen, zekerheid, veiligheid en keuze voor consumenten. De digitalisering van de interne markt is zeer concurrerend dankzij een kader dat transparantie, concurrentie en innovatie bevordert en technologieneutraal is. Het ondersteunt de **faciliteit voor herstel en veerkracht**[34] door waar nodig lering te trekken uit de COVID-19-pandemie en de voordelen van gemakkelijker toegankelijke data.

Dit voorstel ondersteunt de cruciale rol die data op verschillende manieren spelen bij het bereiken van de **doelstellingen van de Europese Green Deal**. Ten eerste door overheden, bedrijven en individuen beter inzicht te geven in de gevolgen van producten, diensten en materialen in de hele toeleveringsketen voor de samenleving en de economie. Ten tweede, door de bestaande schat aan relevante data van de particuliere sector te mobiliseren om

27 PB L 151 van 14.6.2018, blz. 1; PB L 60 van 2.3.2013, blz. 1.
28 PB L 207 van 06.08.2010, blz. 1.
29 PB L 96 van 31.3.2004, blz. 1; PB L 96 van 31.3.2004, blz. 10; PB L 96 van 31.3.2004, blz. 20.
30 PB L 308 van 29.10.2014, blz. 82.
31 PB L 96 van 12.4.2016, blz. 46.
32 COM/2021/559 final.
33 COM/2020/67 final.
34 PB L 57 van 18.2.2021, blz. 17.

kwesties in verband met klimaat, biodiversiteit, vervuiling[35] en natuurlijke hulpbronnen aan te pakken, in lijn met de doelstellingen van de Europese Green Deal[36], de desbetreffende conclusies van de Raad[37] en standpunten van het Europees Parlement[38]. Ten derde, door kennishiaten te dichten en daarmee samenhangende crises te beheersen door middel van betere maatregelen op het vlak van risicobeperking, paraatheid, respons en herstel.

Overeenkomstig de **industriestrategie**[39] heeft het voorstel betrekking op uiterst strategische technologieën zoals cloudcomputing en artificiële-intelligentiesystemen: gebieden waarvan het potentieel van de EU nog beter moet worden benut, nu de volgende industriële datagolf zich aandient. Hiermee wordt uitvoering gegeven aan de **datastrategie**[40] om bedrijven beter in staat te stellen te innoveren en te concurreren op basis van de EU-waarden en het beginsel van **vrij verkeer van data binnen de interne markt**. Het voorstel heeft ook betrekking op het **actieplan inzake intellectuele eigendom**[41], waarin de Commissie zich ertoe heeft verbonden de databankrichtlijn te herzien.

Dit voorstel moet ook overeenstemmen met de beginselen van het actieplan voor de Europese pijler van sociale rechten[42] (EPSR) en de toegankelijkheidseisen van Richtlijn (EU) 2019/882 betreffende de toegankelijkheidseisen voor producten en diensten[43].

2. RECHTSGRONDSLAG, SUBSIDIARITEIT EN EVENREDIGHEID

• Rechtsgrondslag

De rechtsgrondslag van dit voorstel is artikel 114 van het Verdrag betreffende de werking van de Europese Unie, dat tot doel heeft de interne markt tot stand te brengen en te laten functioneren door de maatregelen voor de onderlinge aanpassing van de nationale regels te versterken.

Dit voorstel beoogt de voltooiing van de interne datamarkt te bevorderen, waarbinnen data van de overheidssector, bedrijven en particulieren optimaal worden gebruikt, met inachtneming van de rechten met betrekking tot dergelijke data en de investeringen die worden gedaan om ze te verzamelen. De bepalingen inzake het overstappen tussen dataverwerkingsdiensten hebben tot doel eerlijke en concurrerende marktvoorwaarden tot stand te brengen voor de interne markt voor cloud-, edge- en gerelateerde diensten.

De bescherming van vertrouwelijke bedrijfsgegevens en bedrijfsgeheimen is een belangrijk aspect van de goede werking van de interne markt, zoals het geval is in andere contexten waarin diensten worden uitgewisseld en goederen worden verhandeld. Dit voorstel waarborgt de eerbiediging van bedrijfsgeheimen in de context van datagebruik tussen bedrijven of door consumenten. Het initiatief zal de EU in staat stellen te profiteren van de omvang van de interne markt, aangezien producten of gerelateerde diensten vaak worden ontwikkeld met

---

35 COM(2021) 400 final.
36 COM/2019/640 final.
37 Digitalisering ten bate van het milieu, 11 december 2020 , Conclusies van de Raad over het nieuwe actieplan voor de circulaire economie, 11 december 2020 , Conclusies van de Raad over de biodiversiteitsstrategie voor 2030, 16 oktober 2020 , Conclusies over de verbetering van de luchtkwaliteit, 5 maart 2020
38 Noodsituatie op het gebied van klimaat en milieu, 28 november 2019 (europa.eu).
39 COM/2021/350 final.
40 COM/2020/66 final.
41 COM/2020/760 final.
42 COM/2021/102 final.
43 PB L 151 van 7.6.2019.

behulp van data uit verschillende lidstaten en later in de hele EU worden gecommercialiseerd.

Sommige lidstaten hebben wetgevende maatregelen genomen om de hierboven beschreven problemen aan te pakken, in B2B- en B2G-scenario's, terwijl andere dat niet hebben gedaan. Dit kan leiden tot versnippering van de wetgeving op de interne markt en tot uiteenlopende regels en praktijken in de EU en tot daarmee verband houdende kosten voor bedrijven die aan verschillende regelingen zouden moeten voldoen. Daarom is het belangrijk ervoor te zorgen dat de voorgestelde maatregelen in alle lidstaten consequent worden toegepast.

- **Subsidiariteit (bij niet-exclusieve bevoegdheid)**

Gezien het grensoverschrijdende karakter van datagebruik en de vele gebieden waarop de dataverordening van invloed is, kunnen de kwesties die in dit voorstel aan bod komen niet doeltreffend op het niveau van de lidstaten worden aangepakt. Versnippering als gevolg van verschillende nationale regels moet worden vermeden, aangezien dit zou leiden tot hogere transactiekosten, gebrek aan transparantie, rechtsonzekerheid en ongewenste forumshopping. Dit vermijden is met name van belang in alle situaties met betrekking tot de data-aspecten van B2B-betrekkingen, waaronder eerlijke contractvoorwaarden en de verplichtingen die gelden voor fabrikanten van producten of gerelateerde diensten van het internet der dingen, aspecten waarvoor een homogeen kader voor de hele EU nodig is.

Een beoordeling van de grensoverschrijdende aspecten van datastromen op het gebied van het delen van data tussen bedrijven en overheden (B2G) toont ook aan dat op EU-niveau moet worden opgetreden. Veel particuliere actoren die over relevante data beschikken, zijn multinationals. Deze mogen niet worden geconfronteerd met een versnipperd rechtsstelsel.

Cloudcomputingdiensten worden zelden in slechts één lidstaat aangeboden. In overeenstemming met de AVG en de verordening inzake het vrije verkeer van niet-persoonsgebonden data, die consumenten en bedrijven in staat stellen persoonsgebonden en niet-persoonsgebonden gegevens overal in de EU te verwerken, is de grensoverschrijdende verwerking van data binnen de EU van essentieel belang om zaken te kunnen doen op de interne markt. Het is daarom van cruciaal belang dat de bepalingen inzake het overstappen naar een andere dataverwerkingsdienst op EU-niveau worden toegepast om schadelijke versnippering op een anders eengemaakte markt voor dataverwerkingsdiensten te voorkomen.

Alleen middels een gemeenschappelijk optreden op EU-niveau kunnen de doelstellingen van dit voorstel worden verwezenlijkt, waaronder de totstandbrenging van een innovatief en concurrerend gelijk speelveld voor datagestuurde bedrijven en burgers zeggenschap te geven. Deze gemeenschappelijke actie is een zelfverzekerde stap voorwaarts om de visie van een echte interne datamarkt te realiseren.

- **Evenredigheid**

In dit voorstel worden de rechten en belangen van de betrokken belanghebbenden in evenwicht gebracht met de algemene doelstelling om een ruimer gebruik van data voor een breed scala aan actoren te vergemakkelijken. Het creëert een faciliterend kader dat niet verder gaat dan nodig is om de doelstellingen te bereiken. Hiermee worden bestaande belemmeringen aangepakt die ertoe leiden dat de potentiële waarde van data bij bedrijven, consumenten en de overheid niet optimaal benut kunnen worden. Het bevat ook een kader voor toekomstige sectorale regels om versnippering en rechtsonzekerheid te voorkomen. Het verduidelijkt de bestaande rechten en voorziet, waar nodig, in toegangsrechten tot data, en draagt zo bij tot de ontwikkeling van een interne markt voor het delen van data. Het initiatief laat een aanzienlijke mate van flexibiliteit voor de toepassing op sectorspecifiek niveau.

Dit voorstel zal financiële en administratieve kosten met zich meebrengen. Deze moeten voornamelijk worden gedragen door nationale autoriteiten, fabrikanten en dienstverleners, zodat zij voldoen aan de in deze verordening vastgestelde verplichtingen. Op basis van de verkenning van verschillende opties en de verwachte kosten en baten is een uitgebalanceerd instrument ontwikkeld. Evenzo zullen de kosten voor datagebruikers en -houders worden gecompenseerd door de waarde die voortvloeit uit de bredere toegang tot en het gebruik van data, alsmede door de marktintroductie van nieuwe diensten.

- **Keuze van het instrument**

De keuze voor een verordening is gemaakt omdat dit het beste mechanisme is om de bredere beleidsdoelstellingen te verwezenlijken, namelijk ervoor zorgen dat alle bedrijven in de EU in staat worden gesteld te innoveren en te concurreren, consumenten beter in staat zijn controle te houden over hun data en de EU-instellingen, -agentschappen en -organen beter zijn toegerust om grote beleidsuitdagingen, waaronder openbare noodsituaties, aan te pakken. Een verordening is nodig om te komen tot de nagestreefde brede harmonisatie, die moet leiden tot rechtszekerheid en transparantie voor marktdeelnemers, waaronder micro-, kleine en middelgrote bedrijven, en tot hetzelfde niveau van wettelijk afdwingbare rechten en verplichtingen voor alle rechtspersonen en natuurlijke personen in alle lidstaten, waardoor de regels in alle lidstaten consistent gehandhaafd kunnen worden en de bevoegde autoriteiten van de verschillende lidstaten doeltreffend kunnen samenwerken.

Het voorstel zal de interne markt voor data versterken door meer de rechtszekerheid te bieden en een uniform, horizontaal en samenhangend rechtskader te waarborgen.

3. EVALUATIE, RAADPLEGING VAN BELANGHEBBENDEN EN EFFECTBEOORDELING

- **Evaluatie van bestaande wetgeving en controle van de resultaatgerichtheid ervan**

Dit voorstel bouwt gedeeltelijk voort op de meest recente evaluatie van de databankrichtlijn en de studie van de Commissie ter ondersteuning van de herziening van die richtlijn[44]. Bij de databankrichtlijn is onder meer een specifiek recht sui generis ingevoerd om databanken te beschermen wanneer de producent van een databank aanzienlijk heeft geïnvesteerd in het verkrijgen, verifiëren en presenteren van de data. Sinds de eerste vaststelling ervan is de richtlijn tweemaal geëvalueerd. Beide evaluaties zijn aangevuld met mededelingen van de Commissie over het beleid voor de data-economie[45].

Het Hof van Justitie van de Europese Unie heeft het begrip substantiële investeringen in een databank aangescherpt en verduidelijkt dat het recht sui generis gericht is op de bescherming van investeringen in het verzamelen, en niet het creëren van data[46] als bijproduct van een andere economische activiteit. Er blijft echter onzekerheid bestaan over de onvoorziene of onbedoelde toepassing van het recht sui generis op databanken die machinaal gegenereerde data bevatten, d.w.z. data die zijn verkregen uit of gegenereerd door het gebruik van producten of gerelateerde diensten. Er is behoefte aan evenwichtige beleidsdoelstellingen inzake de bescherming van intellectuele eigendom van dergelijke databanken in de context

[44] COM/2017/09 final; SWD(2018) 146 final, punt 5.4.2; Studie ter ondersteuning van een effectbeoordeling voor de evaluatie van de databankrichtlijn.

[45] COM/2017/09 final; COM/2020/66 final; COM/2020/760 final.

[46] Fixtures Marketing Ltd/Veikkaus Ab (C-46/02, 9/11/2004), Fixtures Marketing Ltd/Svenska Spel Ab (C-338/02, 9/11/2004) British Horseracing Board Ltd/William Hill (C-203/02, 9/11/2004) Fixtures Marketing Ltd/OPAP (C-444/02, 9/11/2004).

van de data-economie, waar de exclusiviteit van data als een niet-concurrerend goed over het algemeen als een belemmering voor innovatie wordt beschouwd. Om de samenhang met de regelgevende maatregelen in dit voorstel te waarborgen, wordt de vastgestelde problematische toepassing van het recht sui generis in de context van het internet der dingen specifiek aangepakt. De Commissie bereidt momenteel ook de evaluatie van Verordening (EU) 2018/1807 voor, die in november 2022 wordt verwacht. Uit eerste verslagen van externe contractanten is gebleken dat de SWIPO-gedragscodes slechts een beperkt effect hebben op de overstap naar andere aanbieders van clouddiensten.

- **Raadpleging van belanghebbenden**

Tijdens het mandaat van de vorige Commissie is een begin gemaakt met uitgebreide werkzaamheden om de problemen in kaart te brengen die de EU beletten het potentieel van datagestuurde innovatie in de economie ten volle te benutten. Het voorstel bouwt voort op eerdere raadplegingsacties, zoals de openbare raadpleging van 2017 ter ondersteuning van de mededeling van de Commissie „*Bouwen aan een Europese data-economie*”[47], de openbare raadpleging van 2017 over de evaluatie van de databankrichtlijn, de openbare raadpleging van 2018 over de herziening van de richtlijn inzake het hergebruik van overheidsinformatie, de raadpleging van het panel van kleine en middelgrote ondernemingen van 2018 over de beginselen en richtsnoeren voor het delen van data tussen ondernemingen, en de online openbare raadpleging van de Commissie over de datastrategie[48] van februari tot mei 2020.

Op 28 mei 2021 is op het portaal voor betere regelgeving een aanvangseffectbeoordeling gepubliceerd, waarop gedurende 4 weken feedback kon worden gegeven. De Commissie heeft 91 bijdragen ontvangen[49], voornamelijk van bedrijven.

Vervolgens is op 3 juni 2021 een online openbare raadpleging over de dataverordening gepubliceerd. Deze liep tot 3 september 2021. De raadpleging had betrekking op de onderwerpen die in het initiatief aan de orde kwamen, met relevante onderdelen en vragen. Zij was gericht op alle soorten belanghebbenden, waarbij input werd verzameld over het delen van data, de toegang tot en het gebruik in B2B- en B2G-context, over empowerment van consumenten en de overdraagbaarheid van data, de mogelijke rol van technische maatregelen zoals slimme contracten, de mogelijkheid dat gebruikers overstappen naar andere aanbieders van clouddiensten, intellectuele-eigendomsrechten (d.w.z. de bescherming van databanken) en de bescherming van niet-persoonsgebonden data in internationale context. Na een grondige analyse van de antwoorden heeft de Commissie een samenvattend verslag op haar website gepubliceerd[50].

In totaal werden 449 bijdragen ontvangen uit 32 landen. Zakelijke entiteiten leverden het grootste aantal bijdragen, waaronder 122 bedrijfsverenigingen en 105 bedrijven/bedrijfsorganisaties. Daarnaast reageerden 100 overheidsinstanties en 58 burgers. In het algemeen bevestigden de antwoorden dat er tal van belemmeringen zijn voor een doeltreffende en efficiënte uitwisseling van data in alle soorten datarelaties.

Hoewel het delen van data tussen bedrijven een gangbare praktijk is, meldden respondenten in de B2B-context onder andere technische belemmeringen (formaten, gebrek aan normen - 69 %); weigering van toegang tot data zonder dat er mededingingsbezwaren waren (55 %) en misbruik van contractuele onevenwichtigheid (44 %). Wat contractuele kwesties betreft, was

47 COM/2017/09 final.

48 Europese Commissie (2020). *Resultaat van de onlineraadpleging over de Europese datastrategie*.

49 *Webpagina* van de Europese Commissie: *Geef uw mening - Dataverordening en gewijzigde regels voor de rechtsbescherming van databanken.*

50 Europese Commissie (2021). *Openbare raadpleging over de dataverordening: Samenvattend verslag*.

bijna de helft van de respondenten voorstander van de invoering van een oneerlijkheidstoets (46 %), terwijl 21 % daar geen voorstander was. Kleine en middelgrote bedrijven toonden zich sterk voorstander van een oneerlijkheidstoets (50 %) en een aanzienlijk aantal grote bedrijven was er ook voorstander van (41 %). Evenzo was 46 % van de belanghebbenden uit de verschillende sectoren voorstander van algemene toegangsregels op basis van eerlijke, redelijke en niet-discriminerende voorwaarden. 60 % van de respondenten was het ermee eens dat modelcontractvoorwaarden kunnen bijdragen tot meer uitwisseling van data, bij micro-, kleine en middelgrote bedrijven was dat zelfs 78 %. Van de belanghebbenden was 70 % van mening dat er sprake is van een eerlijkheidsprobleem in verband met data die worden gegenereerd in het kader van het internet der dingen, en dat fabrikanten van verbonden producten of gerelateerde diensten niet eenzijdig mogen beslissen wat er gebeurt met de data die door dergelijke producten worden gegenereerd. 79 % van de respondenten was van mening dat slimme contracten een doeltreffend instrument kunnen zijn om de toegang tot en het gebruik van data technisch uit te voeren in de context van gezamenlijk gegenereerde data over het internet der dingen.

Rechtsonzekerheid en juridische belemmeringen, negatieve commerciële prikkels en een gebrek aan passende infrastructuur behoorden tot de belangrijkste factoren die de uitwisseling van data tussen bedrijven en overheden in de weg stonden. Bijna alle overheidsinstanties zijn van mening dat actie (van de EU of een lidstaat) op het gebied van het delen van data tussen bedrijven en overheden nodig is, tegenover 80 % van de academische/onderzoeksinstellingen en 38 % van de bedrijven/bedrijfsorganisaties/verenigingen. Een duidelijke meerderheid van de belanghebbenden (met name burgers en overheidsdiensten) was ook van mening dat het delen van data tussen bedrijven en overheden verplicht moet zijn, met duidelijke waarborgen voor specifieke gebruiksgevallen met een duidelijk algemeen belang in noodsituaties en voor crisisbeheersingsdoeleinden, voor officiële statistieken, voor milieubescherming en voor een gezondere samenleving in het algemeen.

De respondenten bevestigden ook het nut van een recht op overstappen voor zakelijke gebruikers van cloudcomputingdiensten. Wat betreft de waarborgen voor niet-persoonsgebonden data in internationale context, beschouwt 76 % van de respondenten de potentiële toegang tot data door buitenlandse autoriteiten op basis van buitenlandse wetgeving als een risico voor hun organisatie, waarbij 19 % aangeeft dat dit een groot risico is.

- **Bijeenbrengen en gebruik van expertise**

Het voorstel werd ondersteund door verschillende studies, workshops en andere input van deskundigen:

– **Studie ter ondersteuning van deze effectbeoordeling over het verbeteren van het gebruik van gegevens in Europa**, waaronder interviews met specifieke belanghebbenden. Dit omvatte twee sectoroverschrijdende workshops over het delen van data tussen bedrijven onderling en tussen bedrijven en overheden, en een afsluitende valideringsworkshop die in het voorjaar van 2021 werd georganiseerd.

– **Studie over modelcontractvoorwaarden, eerlijkheidscontrole bij het delen van gegevens en in cloudcontracten en over de rechten inzake gegevenstoegang**. Deze beoordeelde met name de eerlijkheidsaspecten in de relaties tussen bedrijven onderling, en omvatte interviews met specifieke belanghebbenden en een validatieworkshop.

– **Studie over de economische nadelen van oneerlijke en onevenwichtige contractvoorwaarden op het gebied van clouddiensten.** Deze omvatte een online-

enquête onder een steekproef van kleine en middelgrote bedrijven en start-ups die cloudcomputing gebruiken om hun activiteiten uit te voeren.

– **Studie over het overstappen naar een andere aanbieder van clouddiensten**, met een sectoroverschrijdende workshop in het tweede kwartaal van 2017.

– **Studie ter ondersteuning van de herziening van de databankrichtlijn**, met interviews met specifieke belanghebbenden. Deze studie heeft de Commissie input gegeven bij de voorbereiding van de effectbeoordeling bij de herziening van de databankrichtlijn, in het kader van de dataverordening en bij de verwezenlijking van de onderling verweven doelstellingen ervan.

– **Methodologische ondersteuning van de effectbeoordeling van het gebruik van data die in particuliere handen zijn voor officiële statistieken.** Deze exercitie levert input voor de effectbeoordeling van het B2G-hergebruik van data voor officiële statistieken, door een methodologische aanpak te ontwikkelen en door de kosten en baten van hergebruik van data en van specifieke gebruiksgevallen voor verschillende statistische gebieden en verschillende soorten data uit de particuliere sector te beschrijven. Daarnaast zij het bij tot lopend onderzoek en beraadslagingen die beter inzicht moeten bieden in het delen van data tussen bedrijven en overheden.

– **Webinars op platforms voor persoonsgegevens en industriële dataplatforms.** Op 6, 7 en 8 mei 2020 werden drie webinars georganiseerd. Zij hebben de relevante projecten samengebracht in de portefeuille van het dataplatform van publiek-private partnerschap „Big Data Value".

– **Verslag van de deskundigengroep op hoog niveau inzake het delen van gegevens tussen ondernemingen en de overheid** Het verslag bevat een analyse van de problemen in verband met het delen van data tussen bedrijven en overheden in de EU en bevat een reeks aanbevelingen om te zorgen voor schaalbare, verantwoorde en duurzame data-uitwisseling tussen bedrijven en overheden in het algemeen belang. Naast de aanbeveling aan de Commissie om de optie van een juridisch kader op dit gebied te onderzoeken, presenteert de deskundigengroep verschillende manieren om particuliere ondernemingen aan te moedigen hun data uit te wisselen. De mogelijkheden omvatten zowel financiële als niet-financiële prikkels, zoals fiscale prikkels, overheidsinvesteringen ter ondersteuning van de ontwikkeling van betrouwbare technische instrumenten en erkenningsregelingen voor het uitwisselen van data.

– **Workshop over labels voor/certificering van aanbieders van technische oplossingen voor gegevensuitwisseling**. Dit webinar werd op 12 mei 2020 bijgewoond door ongeveer honderd deelnemers uit grote en kleine bedrijven, Europese instellingen en de academische wereld. Het doel was na te gaan of een etiketterings- of certificeringsregeling de acceptatie van databemiddelaars door bedrijven zou kunnen stimuleren door het vertrouwen in het data-ecosysteem te vergroten.

– **Tussen juli en november 2019 werden tien workshops georganiseerd waaraan meer dan 300 belanghebbenden deelnamen en die betrekking hadden op verschillende sectoren**. Tijdens de workshops werd besproken hoe het **delen van data op bepaalde gebieden**, zoals milieu, landbouw, energie en gezondheidszorg, de samenleving als geheel ten goede kan komen, publieke actoren kan helpen beter beleid uit te stippelen en overheidsdiensten te verbeteren, en particuliere actoren kan

helpen diensten te produceren die helpen maatschappelijke uitdagingen aan te pakken.

– **Raadpleging van het MKB-panel.** In het kader van deze raadpleging, die van oktober 2018 tot januari 2019 werd gehouden, werd gevraagd naar de standpunten van kleine en middelgrote bedrijven over de beginselen en richtsnoeren van de Commissie voor het delen van data tussen bedrijven onderling en over de mededeling „*Naar een gemeenschappelijke Europese gegevensruimte*" bij het werkdocument van de diensten van de Commissie van 25 april 2018[51].

– **De meest recente Eurobarometer over de impact van digitalisering.** Deze algemene enquête over het dagelijks leven van Europeanen bevat vragen over de controle over en de uitwisseling van persoonlijke informatie. Het op 5 maart 2020 gepubliceerde document bevat informatie over de bereidheid van Europese burgers om hun persoonlijke informatie te delen, en onder welke voorwaarden.

– **Het advies van de Europese Toezichthouder voor gegevensbescherming** (EDPS) over de Europese datastrategie[52]. Op 16 juni 2020 heeft de EDPS advies 3/2020 over de Europese datastrategie aangenomen. De EDPS was ingenomen met de strategie en beschouwt de uitvoering ervan als een kans om een voorbeeld te stellen voor een alternatief model voor de data-economie.

• **Effectbeoordeling**

Dit voorstel gaat vergezeld van een effectbeoordeling[53], die op 29 september 2021 en 13 december 2021 aan de Raad voor regelgevingstoetsing (RSB) is voorgelegd. Op 21 januari 2022 heeft de Raad onder voorbehoud een positief advies uitgebracht.

• **Resultaatgerichtheid en vereenvoudiging**

Door te verduidelijken dat het recht sui generis uit hoofde van de databankrichtlijn (Richtlijn 96/9/EG) niet van toepassing is op databanken die data bevatten die zijn gegenereerd of verkregen door het gebruik van producten of gerelateerde diensten, zorgt het voorstel ervoor dat het recht sui generis geen afbreuk doet aan het recht van bedrijven en consumenten op toegang tot en gebruik van data en op het delen van data waarin deze verordening voorziet. De verduidelijking zal de toepassing van het recht sui generis afstemmen op het doel van het wetgevingsvoorstel en een positief effect hebben op de uniforme toepassing van de regels binnen de interne markt en voor de data-economie.

Door de toegang tot en het gebruik van data te vergemakkelijken, moet de dataverordening de lasten verminderen, zowel in de overheidssector als in het bedrijfsleven, voornamelijk als gevolg van lagere transactiekosten en efficiëntiewinsten. In het kader van de „one in, one out"-benadering[54], die erop gericht is de gevolgen en kosten voor burgers en bedrijven in verband met de toepassing van de wetgeving tot een minimum te beperken, wordt in de op basis van de effectbeoordeling geraamde netto administratieve last van de dataverordening rekening gehouden met voordelen die waarschijnlijk niet alleen zullen worden gecompenseerd, maar ook ruimschoots opwegen tegen de daaraan verbonden administratieve kosten.

---

51 COM/2018/232 final; SWD(2018) 125 final van 25.4.2018.

52 Advies 3/2020 van de EDPS over de Europese datastrategie.

53 **[Links to final document and to the summary sheet to be added.]**.

54 SWD(2021) 305 final.

- **Grondrechten**

Het voorstel is in overeenstemming met de EU-wetgeving inzake de bescherming van persoonsgegevens en de privacy van communicatie en eindapparatuur en voorziet in aanvullende waarborgen voor de toegang tot persoonsgegevens, en voor gevallen die onder intellectuele-eigendomsrechten vallen.

In hoofdstuk II wordt een hoog niveau van consumentenbescherming versterkt met het nieuwe recht op toegang tot door gebruikers gegenereerde data in situaties die voorheen niet onder het EU-recht vielen. Het recht om rechtmatig verkregen eigendom te gebruiken en erover te beschikken wordt versterkt met een recht op toegang tot data die zijn gegenereerd door het gebruik van een voorwerp dat behoort tot het internet der dingen. Op deze manier hebben eigenaren een betere gebruikerservaring en kunnen zij gebruikmaken van een breder scala aan bijvoorbeeld reparatie- en onderhoudsdiensten. In het kader van de consumentenbescherming verdienen de rechten van kinderen als kwetsbare consumenten bijzondere aandacht en zullen de regels van de dataverordening bijdragen tot duidelijkheid over de toegang tot en het gebruik van data.

Wanneer derden op verzoek van de gebruiker toegang krijgen tot data die worden gegenereerd via het internet der dingen, beperkt dit de vrijheid van ondernemerschap en de contractvrijheid van de fabrikant of ontwerper van een product of gerelateerde dienst. De beperking hiervan is gerechtvaardigd om de consumentenbescherming te verbeteren, met name om de economische belangen van de consument te bevorderen. De fabrikant of ontwerper van een product of gerelateerde dienst heeft doorgaans exclusieve zeggenschap over het gebruik van data die door het gebruik van een product of gerelateerde dienst worden gegenereerd, wat bijdraagt tot lock-in-effecten en de toegang tot de markt belemmert voor spelers die aftermarketdiensten aanbieden. Het recht op toegang tot data die worden gegenereerd via het internet der dingen pakt deze situatie aan door consumenten die producten of gerelateerde diensten gebruiken, in staat te stellen op zinvolle wijze te bepalen hoe de data die door hun gebruik van het product of de gerelateerde dienst worden gegenereerd, worden gebruikt en door innovatie door meer marktdeelnemers mogelijk te maken. Consumenten krijgen dus een ruimere keuze op het gebied van aftermarketdiensten, zoals reparatie en onderhoud, en zijn niet meer afhankelijk van de diensten van de fabrikant. Het voorstel vergemakkelijkt de overdraagbaarheid van de data van gebruikers aan derden en maakt aldus een concurrerend aanbod van aftermarketdiensten mogelijk, evenals bredere op data gebaseerde innovatie en de ontwikkeling van producten of diensten die geen verband houden met die welke oorspronkelijk door gebruikers zijn gekocht of waar zij een abonnement op hebben genomen.

De beperking van de vrijheid van de fabrikant of ontwerper om contracten aan te gaan en zaken te doen, is evenredig en wordt beperkt door het onaangetaste vermogen van de fabrikant of ontwerper om de data ook te gebruiken, voor zover dit in overeenstemming is met de toepasselijke wetgeving en de overeenkomst met de gebruiker. Bovendien zal de fabrikant of ontwerper ook het recht hebben om een vergoeding te eisen voor het verlenen van toegang aan derden. Het toegangsrecht doet geen afbreuk aan de bestaande rechten inzake toegang en overdraagbaarheid voor betrokkenen uit hoofde van de AVG. Aanvullende waarborgen zorgen voor een evenredig gebruik van de data door de derde partij.

Hoofdstuk IV omvat een eerlijk en doeltreffend systeem voor bescherming tegen oneerlijke contractvoorwaarden voor het delen van data, ten bate van micro-, kleine en middelgrote bedrijven. Deze bepaling beperkt de contractuele vrijheid van bedrijven in het toepassingsgebied tot op zekere hoogte, aangezien zij alleen van toepassing is op oneerlijke

contractvoorwaarden in verband met de toegang tot en het gebruik van data die eenzijdig door één contractpartij aan een micro-, klein of middelgroot bedrijf worden opgelegd. Dit is gerechtvaardigd omdat kleine en middelgrote bedrijven doorgaans in een zwakkere onderhandelingspositie verkeren en vaak geen andere keuze hebben dan de contractvoorwaarden te aanvaarden, of het contract te laten lopen. De contractvrijheid blijft grotendeels onverlet, aangezien alleen buitensporige en oneerlijke bedingen ongeldig worden verklaard en de gesloten overeenkomst, indien mogelijk, geldig blijft zonder de oneerlijke bedingen. Bovendien kunnen de partijen nog steeds individueel onderhandelen over een specifiek contractueel beding[55].

In hoofdstuk V zullen de bepalingen met betrekking tot het delen van data tussen bedrijven en overheden op basis van een uitzonderlijke noodzaak de capaciteit van overheidsinstanties vergroten om actie te ondernemen ten behoeve van het algemeen belang, bijvoorbeeld om te reageren op een algemene noodsituatie, die te voorkomen of bij te dragen aan het herstel achteraf. De particuliere sector heeft ook baat bij de stroomlijning van de procedures voor verzoeken om data.

In hoofdstuk VI versterken de bepalingen inzake het overstappen naar een andere aanbieder van dataverwerkingsdiensten de positie van zakelijke klanten en waarborgen zij hun keuze om van aanbieder te veranderen. De beperking van het recht van een bedrijf om dataverwerkingsdiensten aan te bieden is gerechtvaardigd, omdat de nieuwe regels betrekking hebben op lock-in-effecten op de cloud- en edgemarkt en zakelijke gebruikers en personen met betrekking tot dataverwerkingsdiensten meer keuze bieden.

In hoofdstuk X beperkt de interventie betreffende het recht sui generis van de databankrichtlijn de bescherming van intellectuele eigendom daarin niet. Het draagt veeleer bij tot de rechtszekerheid in gevallen waarin de bescherming van het recht sui generis voorheen onduidelijk was.

4. GEVOLGEN VOOR DE BEGROTING

Dit voorstel heeft geen gevolgen voor de begroting.

5. OVERIGE ELEMENTEN

- **Uitvoeringsplanning en regelingen betreffende controle, evaluatie en rapportage**

Op sectoraal en macro-economisch niveau zal de lopende studie inzake de monitoring van de datamarkten helpen het economische effect van het huidige voorstel op de groei van de datamarkt in de EU te volgen.

De effecten voor kleine en middelgrote bedrijven, met name hun perceptie van problemen in verband met de toegang tot en het gebruik van data, zal vijf jaar na de goedkeuring van de dataverordening worden beoordeeld door middel van een raadpleging van het mkb-panel.

Gezien de centrale rol van de gemeenschappelijke Europese dataruimten bij de uitvoering van de Europese datastrategie zullen veel van de effecten van dit initiatief worden gemonitord op het niveau van de sectorale dataruimten en de inzichten die worden verzameld door het ondersteuningscentrum voor dataruimten dat in het kader van het programma Digitaal Europa zal worden gefinancierd. De regelmatige interactie tussen de diensten van de Commissie, het

[55] Voor meer uitleg over de oneerlijkheidstoets en het beginsel van contractvrijheid, zie de effectbeoordeling, bijlage 11.

ondersteuningscentrum en de Europese raad voor data-innovatie (op te richten na de inwerkingtreding van de datagovernanceverordening) moet dienen als een betrouwbare informatiebron aan de hand waarvan de vooruitgang kan worden beoordeeld.

Ten slotte zal vier jaar na de goedkeuring van de dataverordening worden geëvalueerd en zo nodig zullen verdere maatregelen worden voorbereid.

- **Artikelsgewijze toelichting**

Hoofdstuk I omschrijft het onderwerp en het toepassingsgebied van de verordening en bevat de definities die in de rechtshandeling worden gebruikt.

Hoofdstuk II vergroot de rechtszekerheid voor consumenten en bedrijven om toegang te krijgen tot data die worden gegenereerd door de producten of daaraan gerelateerde diensten die zij bezitten, huren of leasen. Fabrikanten en ontwerpers moeten de producten zodanig ontwerpen dat de data standaard gemakkelijk toegankelijk zijn, en zij moeten transparant zijn over welke data toegankelijk zullen zijn en hoe zij er toegang toe kunnen krijgen. De bepalingen van dit hoofdstuk doen geen afbreuk aan de mogelijkheid voor fabrikanten om, indien overeengekomen met de gebruiker, toegang te krijgen tot en gebruik te maken van data van producten of aanverwante diensten die zij aanbieden. De datahouder is verplicht dergelijke data op verzoek van de gebruiker ter beschikking van derden te stellen. Gebruikers hebben het recht de datahouder toestemming te verlenen om toegang tot de data te verlenen aan derde dienstverleners, zoals aanbieders van aftermarketdiensten. Micro- en kleine bedrijven zullen van deze verplichtingen worden vrijgesteld.

Hoofdstuk III bevat algemene regels die van toepassing zijn op de verplichting om data beschikbaar te stellen. Wanneer een datahouder verplicht is data beschikbaar te stellen aan een ontvanger van data als bedoeld in hoofdstuk II of in andere EU-wetgeving of wetgeving van de lidstaat, heeft het algemene kader betrekking op de voorwaarden waaronder data beschikbaar worden gesteld en de vergoeding voor het beschikbaar stellen van data. Alle voorwaarden moeten eerlijk en niet-discriminerend zijn en elke compensatie moet redelijk zijn, zonder dat dit belet dat andere EU-wetgeving of nationale wetgeving tot uitvoering van het EU-recht compensatie uitsluit of voorziet in een lagere vergoeding voor het beschikbaar stellen van data. De compensatie voor kleine en middelgrote bedrijven mag niet hoger zijn dan de kosten voor het beschikbaar stellen van de data, tenzij in sectorale wetgeving anders is bepaald. Door de lidstaten gecertificeerde geschillenbeslechtingsorganen kunnen partijen die het oneens zijn over de compensatie of de voorwaarden om tot een overeenkomst te komen, helpen.

Hoofdstuk IV behandelt het oneerlijke karakter van contractvoorwaarden in data-uitwisselingsovereenkomsten tussen bedrijven, in situaties waarin een contractvoorwaarde eenzijdig door een partij wordt opgelegd aan een micro-, klein of middelgroot bedrijf. Dit hoofdstuk garandeert dat in contractuele overeenkomsten inzake de toegang tot en het gebruik van data geen misbruik wordt gemaakt van onevenwichtigheden in de onderhandelingspositie tussen de contractpartijen. Het instrument van een oneerlijkheidstoets omvat een algemene bepaling waarin het oneerlijke karakter van een contractuele bepaling over het delen van data wordt gedefinieerd, aangevuld met een lijst van bedingen die altijd oneerlijk zijn of geacht worden oneerlijk te zijn. In situaties van ongelijke onderhandelingspositie beschermt dit criterium de zwakkere contractpartij, en voorkomt zo oneerlijke overeenkomsten. Dergelijke oneerlijkheid zou het gebruik van data door beide contractpartijen belemmeren. Op die manier

zorgen de bepalingen voor een eerlijkere waardeverdeling in de data-economie[56]. Door de Commissie aanbevolen modelcontractvoorwaarden kunnen commerciële partijen helpen contracten op basis van eerlijke voorwaarden te sluiten.

Hoofdstuk V creëert een geharmoniseerd kader voor het gebruik van data die in handen zijn van ondernemingen in bepaalde situaties waarin er sprake is van een uitzonderlijke behoefte aan data door overheidsinstanties en EU-instellingen, -agentschappen of -organen. Het kader is gebaseerd op een verplichting om data beschikbaar te stellen en zou alleen van toepassing zijn in het geval van algemene noodsituaties of in situaties waarin overheidsinstanties bepaalde data uitzonderlijk moeten gebruiken, maar die data niet tijdig op de markt kunnen worden verkregen door nieuwe wetgeving vast te stellen of door middel van bestaande rapportageverplichtingen. In geval van een uitzonderlijke noodzaak om te reageren op algemene noodsituaties, zoals noodsituaties op het gebied van de volksgezondheid, grote natuurrampen of door de mens veroorzaakte rampen, worden de data gratis ter beschikking gesteld. In andere gevallen van uitzonderlijke noodzaak, onder meer om een algemene noodsituatie te voorkomen of het herstel erna te ondersteunen, moet de datahouder die de data beschikbaar stelt, recht hebben op een vergoeding van de kosten voor het beschikbaar stellen van de relevante data, vermeerderd met een redelijke marge. Om ervoor te zorgen dat het recht om data op te vragen niet wordt misbruikt en dat de overheidssector verantwoordelijk blijft voor het gebruik ervan, moeten de verzoeken om data evenredig zijn, moet daarin duidelijk worden aangegeven welk doel moet worden bereikt en rekening worden gehouden met de belangen van de onderneming die de data beschikbaar stelt. De bevoegde autoriteiten zouden ervoor zorgen dat alle verzoeken transparant en openbaar toegankelijk zijn. Zij zouden ook eventuele daaruit voortvloeiende klachten behandelen.

Hoofdstuk VI introduceert minimale regelgevingsvereisten van contractuele, commerciële en technische aard, die worden opgelegd aan aanbieders van cloud-, edge- en andere dataverwerkingsdiensten, om het overstappen tussen dergelijke diensten mogelijk te maken. Het voorstel zorgt er met name voor dat klanten de functionele gelijkwaardigheid van de dienst (een minimumniveau van functionaliteit) behouden nadat zij naar een andere dienstverlener zijn overgestapt. Het voorstel bevat een uitzondering op grond van technische onhaalbaarheid, maar legt de bewijslast in dit verband bij de dienstverlener. Het voorstel schrijft geen specifieke technische normen of interfaces voor. Het vereist echter wel dat diensten compatibel zijn met Europese normen of technische open interoperabiliteitsspecificaties, indien deze bestaan.

Hoofdstuk VII heeft betrekking op onrechtmatige toegang van derden tot niet-persoonsgebonden data die in de EU zijn opgeslagen door op de EU-markt aangeboden dataverwerkingsdiensten. Het voorstel heeft geen gevolgen voor de rechtsgrondslag van verzoeken om toegang tot data die in handen zijn van EU-burgers of -bedrijven, en laat het EU-kader voor databescherming en privacy onverlet. Het biedt specifieke waarborgen, doordat aanbieders alle redelijke technische, juridische en organisatorische maatregelen moeten nemen om te voorkomen dat die toegang in strijd is met concurrerende verplichtingen tot bescherming van dergelijke data uit hoofde van het EU-recht, tenzij aan strikte voorwaarden is voldaan. De verordening is in overeenstemming met de internationale verbintenissen van de EU in het kader van de WTO en in bilaterale handelsovereenkomsten.

Hoofdstuk VIII voorziet in essentiële eisen inzake interoperabiliteit voor exploitanten van dataruimten en aanbieders van dataverwerkingsdiensten, alsook in essentiële eisen voor

[56] Zie bijlage 11 bij de effectbeoordeling voor meer uitleg over de oneerlijkheidstoets, onder meer over de werking in de praktijk.

slimme contracten. Dit hoofdstuk maakt ook open interoperabiliteitsspecificaties en Europese normen voor de interoperabiliteit van dataverwerkingsdiensten mogelijk om een naadloze cloudomgeving met meerdere aanbieders te bevorderen.

Hoofdstuk IX bevat het uitvoerings- en handhavingskader met de bevoegde autoriteiten in elke lidstaat, waaronder een klachtenmechanisme. De Commissie beveelt vrijwillige modelcontractvoorwaarden aan inzake de toegang tot en het gebruik van data. Voor inbreuken op van deze verordening gelden sancties.

Hoofdstuk X bevat een bepaling die inhoudt dat het in Richtlijn 96/9/EG vastgestelde recht sui generis niet van toepassing is op databanken die data bevatten die zijn verkregen van of gegenereerd door het gebruik van een product of een gerelateerde dienst, teneinde de daadwerkelijke uitoefening van het recht van gebruikers op toegang tot en het gebruik van data overeenkomstig artikel 4 van deze verordening of van het recht om dergelijke data overeenkomstig artikel 5 van deze verordening met derden te delen, te belemmeren.

Hoofdstuk XI biedt de Commissie de mogelijkheid gedelegeerde handelingen vast te stellen om een toezichtmechanisme in te voeren voor het overstappen naar een andere aanbieder van dataverwerkingsdiensten, de essentiële eisen inzake interoperabiliteit nader te specificeren en referenties voor open interoperabiliteitsspecificaties en Europese normen voor de interoperabiliteit van dataverwerkingsdiensten te publiceren. De verordening voorziet ook in de comitéprocedure voor het vaststellen van uitvoeringshandelingen om het bepalen van gemeenschappelijke specificaties voor interoperabiliteit en slimme contracten te vergemakkelijken wanneer er geen geharmoniseerde normen bestaan of deze onvoldoende zijn om de conformiteit met de essentiële eisen te waarborgen. Het voorstel verduidelijkt ook het verband met andere EU-rechtshandelingen betreffende rechten en verplichtingen inzake het delen van data.

2022/0047 (COD)

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

betreffende geharmoniseerde regels inzake eerlijke toegang tot en eerlijk gebruik van data (Dataverordening)

(Voor de EER relevante tekst)

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 114,

Gezien het voorstel van de Europese Commissie,

Na toezending van het ontwerp van wetgevingshandeling aan de nationale parlementen,

Gezien het advies van het Europees Economisch en Sociaal Comité[57],

Gezien het advies van het Comité van de Regio's[58],

Handelend volgens de gewone wetgevingsprocedure,

Overwegende hetgeen volgt:

(1) De afgelopen jaren hebben datagestuurde technologieën alle sectoren van de economie grondig getransformeerd. Met name de verspreiding van producten die verband houden met het internet der dingen heeft het volume en de potentiële waarde van data voor consumenten, bedrijven en de samenleving vergroot. Hoogwaardige en interoperabele data uit verschillende domeinen vergroten het concurrentievermogen en de innovatie en zorgen voor duurzame economische groei. Dezelfde dataset kan voor verschillende doeleinden onbeperkt worden gebruikt en hergebruikt, zonder dat dit invloed heeft op de kwaliteit of kwantiteit ervan.

(2) Belemmeringen voor het delen van data staan een optimale verdeling van data in het belang van de samenleving in de weg. Deze belemmeringen zijn onder meer een gebrek aan stimulansen voor datahouders om vrijwillig data-uitwisselingscontracten te sluiten, onzekerheid over de rechten en plichten met betrekking tot data, de kosten van het contracteren en implementeren van technische interfaces, de hoge mate van versnippering van informatie in datasilo's, slecht beheer van metadata, het ontbreken van normen voor semantische en technische interoperabiliteit, knelpunten die de toegang tot data belemmeren, een gebrek aan gemeenschappelijke praktijken voor het delen van data en misbruik van contractuele onevenwichtigheden met betrekking tot de toegang tot en het gebruik van data.

(3) In sectoren die worden gekenmerkt door de aanwezigheid van micro-, kleine en middelgrote ondernemingen, is er vaak een gebrek aan digitale capaciteiten en vaardigheden om data te verzamelen, te analyseren en te gebruiken, en is de toegang

[57] PB C , blz. .
[58] PB C , blz. .

vaak beperkt doordat één partij deze in het systeem houdt, of door een gebrek aan interoperabiliteit tussen data, tussen datadiensten of over de grenzen heen.

(4) Om tegemoet te komen aan de behoeften van de digitale economie en om belemmeringen voor een goed functionerende interne datamarkt weg te nemen, moet er een geharmoniseerd kader worden vastgesteld waarin wordt gespecificeerd wie, anders dan de fabrikant of andere datahouder, recht heeft op toegang tot de door producten of aanverwante diensten gegenereerde data, onder welke voorwaarden en op welke basis. Bijgevolg mogen de lidstaten geen aanvullende nationale voorschriften vaststellen of handhaven met betrekking tot de aangelegenheden die binnen het toepassingsgebied van deze verordening vallen, tenzij uitdrukkelijk in deze verordening bepaald, aangezien dit gevolgen zou hebben voor de rechtstreekse en uniforme toepassing van deze verordening.

(5) Deze verordening waarborgt dat gebruikers van een product of gerelateerde dienst in de EU tijdig toegang hebben tot de data die door het gebruik van dat product of die gerelateerde dienst worden gegenereerd en dat deze gebruikers de data kunnen gebruiken, onder meer door deze te delen met derden van hun keuze. De verordening verplicht de datahouder om data onder bepaalde omstandigheden ter beschikking te stellen van gebruikers en door de gebruikers aangewezen derden. Het zorgt er ook voor dat datahouders hun data op eerlijke, redelijke en niet-discriminerende voorwaarden en op transparante wijze ter beschikking stellen van ontvangers van data in de EU. Privaatrechtelijke regels zijn van cruciaal belang in het algemene kader van data-uitwisseling. Daarom past deze verordening de regels van het verbintenissenrecht aan en voorkomt zij misbruik van contractuele onevenwichtigheden die een eerlijke toegang tot en een eerlijk gebruik van data door micro-, kleine en middelgrote ondernemingen belemmeren in de zin van Aanbeveling 2003/361/EG. Deze verordening zorgt er ook voor dat datahouders de data die nodig zijn voor de uitvoering van taken in het algemeen belang, beschikbaar stellen aan overheidsinstanties van de lidstaten en aan EU-instellingen, -agentschappen of -organen, indien er sprake is van een uitzonderlijke noodzaak. Daarnaast beoogt deze verordening het overstappen tussen dataverwerkingsdiensten te vergemakkelijken en de interoperabiliteit van mechanismen en diensten voor het delen en uitwisselen van data in de EU te verbeteren. Deze verordening mag niet worden uitgelegd als het erkennen of creëren van een rechtsgrondslag voor datahouders om data in handen te hebben, er toegang toe te hebben of ze te verwerken, of als het verlenen van een nieuw recht aan datahouders om data te gebruiken die door het gebruik van een product of gerelateerde dienst zijn gegenereerd. In plaats daarvan gaat de verordening uit van de daadwerkelijke controle die de datahouder feitelijk of rechtens heeft over data die door producten of gerelateerde diensten worden gegenereerd.

(6) Het genereren van data is het resultaat van acties van ten minste twee actoren: de ontwerper of fabrikant van een product en de gebruiker van dat product. Het roept vragen op over eerlijkheid in de digitale economie, omdat de door dergelijke producten of gerelateerde diensten geregistreerde data belangrijke input vormen voor aftermarketdiensten, ondersteunende en andere diensten. Om de belangrijke economische voordelen van data als een niet-concurrerend goed voor de economie en de samenleving te realiseren, is een algemene benadering van de toekenning van toegangs- en gebruiksrechten voor data te verkiezen boven de toekenning van exclusieve toegangs- en gebruiksrechten.

(7) Het grondrecht op bescherming van persoonsgegevens wordt met name gewaarborgd door Verordening (EU) 2016/679 en Verordening (EU) 2018/1725. Richtlijn

2002/58/EG beschermt bovendien het privéleven en de vertrouwelijkheid van communicatie, onder meer door voorwaarden te stellen aan de opslag van en de toegang tot persoonsgegevens en niet-persoonsgebonden data in eindapparatuur. Deze instrumenten vormen de basis voor duurzame en verantwoorde dataverwerking, ook wanneer datasets een mix van persoonsgegevens en niet-persoonsgebonden data bevatten. Deze verordening vormt een aanvulling op en doet geen afbreuk aan het EU-recht inzake gegevensbescherming en privacy, met name Verordening (EU) 2016/679 en Richtlijn 2002/58/EG. Geen enkele bepaling van deze verordening mag zodanig worden toegepast of uitgelegd dat het recht op bescherming van persoonsgegevens of het recht op privacy en vertrouwelijkheid van communicatie wordt beperkt.

(8) De beginselen van minimale gegevensverwerking en gegevensbescherming door ontwerp en door standaardinstellingen zijn van essentieel belang wanneer de verwerking aanzienlijke risico's inhoudt voor de grondrechten van personen. Rekening houdend met de stand van de techniek moeten alle partijen bij het delen van data, ook wanneer dat binnen het toepassingsgebied van deze verordening valt, technische en organisatorische maatregelen nemen om deze rechten te beschermen. Dergelijke maatregelen omvatten niet alleen pseudonimisering en encryptie, maar ook het gebruik van steeds meer beschikbare technologie waarmee algoritmen op de data kunnen worden toegepast, waarmee waardevolle inzichten kunnen worden verkregen zonder overdracht tussen partijen of onnodig kopiëren van de ruwe of gestructureerde data zelf.

(9) Deze verordening vormt een aanvulling op en doet geen afbreuk aan het EU-recht dat erop gericht is de belangen van consumenten te behartigen en een hoog niveau van consumentenbescherming te waarborgen en hun gezondheid, veiligheid en economische belangen te beschermen, met name Richtlijn 2005/29/EG van het Europees Parlement en de Raad[59], Richtlijn 2011/83/EU van het Europees Parlement en de Raad[60] en Richtlijn 93/13/EEG van het Europees Parlement en de Raad[61].

(10) Deze verordening doet geen afbreuk aan EU-rechtshandelingen die voorzien in het delen van, de toegang tot en het gebruik van data met het oog op preventie van, onderzoek naar, opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen, of voor douane- en belastingdoeleinden, ongeacht de rechtsgrondslag uit hoofde van het Verdrag betreffende de werking van de Europese Unie op grond waarvan zij zijn vastgesteld. Dergelijke handelingen omvatten Verordening (EU) 2021/784 van het Europees Parlement en de Raad van 29 april 2021 om de verspreiding van terroristische online-inhoud aan te pakken, de [voorstellen inzake elektronisch bewijsmateriaal [COM (2018) 225 en 226] zodra deze zijn vastgesteld],

---

[59] Richtlijn 2005/29/EG van het Europees Parlement en de Raad van 11 mei 2005 betreffende oneerlijke handelspraktijken van ondernemingen jegens consumenten op de interne markt en tot wijziging van Richtlijn 84/450/EEG van de Raad, Richtlijnen 97/7/EG, 98/27/EG en 2002/65/EG van het Europees Parlement en de Raad en van Verordening (EG) nr. 2006/2004 van het Europees Parlement en de Raad ("Richtlijn oneerlijke handelspraktijken") (PB L 149 van 11.6.2005, blz. 22).

[60] Richtlijn 2011/83/EU van het Europees Parlement en de Raad van 25 oktober 2011 betreffende consumentenrechten, tot wijziging van Richtlijn 93/13/EEG van de Raad en van Richtlijn 1999/44/EG van het Europees Parlement en de Raad en tot intrekking van Richtlijn 85/577/EEG en van Richtlijn 97/7/EG van het Europees Parlement en de Raad.

[61] Richtlijn 93/13/EEG van de Raad van 5 april 1993 betreffende oneerlijke bedingen in consumentenovereenkomsten. Richtlijn (EU) 2019/2161 van het Europees Parlement en de Raad van 27 november 2019 tot wijziging van Richtlijn 93/13/EEG van de Raad en Richtlijnen 98/6/EG, 2005/29/EG en 2011/83/EU van het Europees Parlement en de Raad wat betreft betere handhaving en modernisering van de regels voor consumentenbescherming in de Unie.

het [voorstel voor] een verordening van het Europees Parlement en de Raad betreffende een eengemaakte markt voor digitale diensten (wet inzake digitale diensten) en tot wijziging van Richtlijn 2000/31/EG, alsmede internationale samenwerking in dit verband, met name op basis van het Verdrag van de Raad van Europa van 2001 inzake cybercriminaliteit („Verdrag van Boedapest"). Deze verordening doet geen afbreuk aan de bevoegdheden van de lidstaten met betrekking tot activiteiten op het gebied van openbare veiligheid, defensie en nationale veiligheid overeenkomstig het EU-recht, en activiteiten van de douane op het gebied van risicobeheer en in het algemeen de controle op de naleving van het douanewetboek door marktdeelnemers.

(11) Deze verordening mag geen afbreuk doen aan het EU-recht tot vaststelling van fysieke ontwerp- en datavereisten voor producten die in de EU in de handel worden gebracht.

(12) Deze verordening vormt een aanvulling op en doet geen afbreuk aan het EU-recht tot vaststelling van toegankelijkheidseisen voor bepaalde producten en diensten, met name Richtlijn 2019/882[62].

(13) Deze verordening doet geen afbreuk aan de bevoegdheden van de lidstaten met betrekking tot activiteiten op het gebied van openbare veiligheid, defensie en nationale veiligheid overeenkomstig het EU-recht, en activiteiten van de douane op het gebied van risicobeheer en in het algemeen de controle op de naleving van het douanewetboek door marktdeelnemers.

(14) Fysieke producten die door middel van hun componenten data over hun prestaties, gebruik of omgeving verkrijgen, genereren of verzamelen en die via een openbare elektronische-communicatiedienst (vaak het internet der dingen genoemd) kunnen communiceren, moeten onder deze verordening vallen. Elektronische-communicatiediensten omvatten vaste telefoonnetwerken, televisiekabelnetwerken, satellietnetwerken en NFC-netwerken (Near Field Communication). Dergelijke producten kunnen voertuigen, huishoudelijke apparatuur en consumptiegoederen, medische en gezondheidsapparatuur of landbouw- en industriële machines omvatten. De data vertegenwoordigen de digitalisering van handelingen van de gebruiker en gebeurtenissen en moeten daarom toegankelijk zijn voor de gebruiker, terwijl informatie die is afgeleid of herleid van deze data, indien rechtmatig in handen, niet mag worden geacht binnen het toepassingsgebied van deze verordening te vallen. Dergelijke data zijn potentieel waardevol voor de gebruiker en ondersteunen innovatie en de ontwikkeling van digitale en andere diensten die het milieu, de gezondheid en de circulaire economie beschermen, met name door het onderhoud en de reparatie van de producten in kwestie te vergemakkelijken.

(15) Bepaalde producten die in de eerste plaats zijn ontworpen om inhoud weer te geven of af te spelen, of om inhoud vast te leggen en door te geven, onder meer voor gebruik door een onlinedienst, mogen daarentegen niet onder deze verordening vallen. Dergelijke producten zijn bijvoorbeeld pc's, servers, tablets en smartphones, camera's, webcams, geluidsopnamesystemen en tekstscanners. Zij vereisen menselijke input om verschillende vormen van inhoud te produceren, zoals tekstdocumenten, geluidsbestanden, videobestanden, spellen en digitale kaarten.

(16) Er moeten regels worden vastgesteld die van toepassing zijn op verbonden producten die op zo'n manier een dienst bevatten of daarmee verbonden zijn, dat het product zijn

[62] Richtlijn (EU) 2019/882 van het Europees Parlement en de Raad van 17 april 2019 betreffende de toegankelijkheidsvoorschriften voor producten en diensten (PB L 151 van 7.6.2019, blz. 70).

functies niet kan vervullen wanneer de dienst ontbreekt. Dergelijke gerelateerde diensten kunnen deel uitmaken van de verkoop-, huur- of leaseovereenkomst, of gebruikelijk zijn voor goederen van hetzelfde type en de gebruiker kan deze diensten redelijkerwijs verwachten, gezien de aard van het product en rekening houdend met publiekelijk gedane mededelingen van of namens de verkoper, verhuurder, leasegever of andere personen in eerdere schakels van de transactieketen, waaronder de producent. Deze gerelateerde diensten kunnen zelf data genereren die voor de gebruiker waardevol zijn, onafhankelijk van de dataverzamelingscapaciteit van het product waarmee zij verbonden zijn. Deze verordening moet ook van toepassing zijn op gerelateerde diensten die niet door de verkoper, verhuurder of lease-aanbieder zelf worden verleend, maar die in het kader van de verkoop-, huur- of leaseovereenkomst door een derde worden verleend. In geval van twijfel over de vraag of de dienst deel uitmaakt van de verkoop-, huur- of leaseovereenkomst, dient deze verordening van toepassing te zijn.

(17) Data die door het gebruik van een product of gerelateerde dienst worden gegenereerd, omvatten o.a. data die opzettelijk door de gebruiker zijn geregistreerd. Dergelijke data omvatten ook data die als bijproduct van de handeling van de gebruiker worden gegenereerd, zoals diagnostische data, en data die worden geregistreerd zonder enige handeling van de gebruiker, zoals wanneer het product zich in de „stand-bystand" bevindt of tijdens perioden waarin het product is uitgeschakeld. Dergelijke data moeten data omvatten in de vorm en het formaat waarin zij door het product worden gegenereerd, maar mogen geen betrekking hebben op data die voortvloeien uit een softwareproces dat afgeleide data uit dergelijke data berekent, aangezien een dergelijk softwareproces onderworpen kan zijn aan intellectuele-eigendomsrechten.

(18) Onder gebruiker van een product moet worden verstaan de natuurlijke of rechtspersoon, zoals een onderneming of consument, die het product heeft gekocht, gehuurd of geleased. Afhankelijk van de wettelijke benaming waaronder gebruikers een product gebruiken, dragen zij de risico's en de voordelen van het gebruik van het verbonden product en moeten zij ook toegang hebben tot de data die het product genereert. De gebruiker moet daarom het recht hebben voordeel te halen uit de gegevens die door dat product en alle gerelateerde diensten worden gegenereerd.

(19) In de praktijk zijn niet alle door producten of gerelateerde diensten gegenereerde data gemakkelijk toegankelijk voor de gebruikers ervan en zijn er vaak beperkte mogelijkheden voor de overdraagbaarheid van data die zijn gegenereerd door producten die verbonden zijn met het internet der dingen. Vaak kunnen gebruikers niet de data verkrijgen die nodig zijn om gebruik te maken van aanbieders van reparatie- en andere diensten, en kunnen bedrijven geen innovatieve, efficiëntere en gemakkelijkere diensten lanceren. In veel sectoren zijn fabrikanten vaak in staat om door hun controle over het technische ontwerp van het product of de gerelateerde diensten te bepalen welke data worden gegenereerd en hoe deze kunnen worden geraadpleegd, ook al hebben zij geen wettelijk recht op de data. Daarom moet ervoor worden gezorgd dat producten zodanig worden ontworpen en vervaardigd en dat gerelateerde diensten op zodanige wijze worden aangeboden dat de door het gebruik ervan gegenereerde data altijd gemakkelijk toegankelijk zijn voor de gebruiker.

(20) Indien meerdere personen of entiteiten eigenaar zijn van een product of partij zijn bij een lease- of huurovereenkomst en toegang hebben tot een gerelateerde dienst, moeten bij het ontwerp van het product of de gerelateerde dienst of de relevante interface redelijke inspanningen worden geleverd om ervoor te zorgen dat alle personen toegang hebben tot de data die zij genereren. Gebruikers van producten die data genereren,

moeten doorgaans een gebruikersaccount aanmaken. Hierdoor kan de gebruiker door de fabrikant worden geïdentificeerd en kan worden gecommuniceerd om verzoeken om toegang tot data uit te verwerken en uit te voeren. Fabrikanten of ontwerpers van een product dat gewoonlijk door meerdere personen wordt gebruikt, moeten een mechanisme opzetten om afzonderlijke gebruikersaccounts voor individuele personen, indien relevant, of de mogelijkheid voor meerdere personen om hetzelfde gebruikersaccount te gebruiken, mogelijk te maken. De gebruiker moet op eenvoudig verzoek toegang krijgen tot mechanismen die automatische uitvoering mogelijk maken, zonder dat daarvoor een onderzoek of machtiging van de fabrikant of de datahouder vereist is. Dit betekent dat data alleen beschikbaar mogen worden gesteld wanneer de gebruiker dit daadwerkelijk wenst. Wanneer geautomatiseerde uitvoering van het verzoek om toegang tot data niet mogelijk is, bijvoorbeeld via een gebruikersaccount of een bij het product of de dienst gevoegde mobiele applicatie, moet de fabrikant de gebruiker informeren hoe toegang tot de data kan worden verkregen.

(21) Producten kunnen worden ontworpen om bepaalde data rechtstreeks beschikbaar te stellen via een gegevensopslag op het apparaat of een server op afstand waaraan de data worden doorgegeven. De toegang tot de gegevensopslag op het toestel kan mogelijk worden gemaakt via al dan niet draadloze lokale netwerken die verbonden zijn met een openbare elektronische-communicatiedienst of een mobiel netwerk. De server kan de eigen lokale servercapaciteit van de fabrikant zijn of die van een derde partij of een aanbieder van clouddiensten die als datahouder fungeert. Zij kunnen zo worden ontworpen dat de gebruiker of een derde de data op het product of op een computing instance van de fabrikant kan verwerken.

(22) Virtuele assistenten spelen een steeds grotere rol bij de digitalisering van consumentenomgevingen en fungeren als een gebruiksvriendelijke interface om inhoud af te spelen, informatie te verkrijgen of fysieke objecten te activeren die verbonden zijn met het internet der dingen. Virtuele assistenten kunnen als één toegangspoort fungeren, bijvoorbeeld binnen een slimme thuisomgeving, en aanzienlijke hoeveelheden relevante data registreren over de manier waarop gebruikers interageren met producten die verbonden zijn met het internet der dingen, waaronder producten die door andere partijen zijn vervaardigd, en kunnen het gebruik van door fabrikanten geleverde interfaces, zoals touchscreens of smartphone-apps, vervangen. Het is mogelijk dat de gebruiker dergelijke data ter beschikking wil stellen van derde fabrikanten om nieuwe slimme thuisdiensten mogelijk te maken. Dergelijke virtuele assistenten moeten onder het recht op toegang tot data vallen waarin deze verordening voorziet, ook met betrekking tot data die vóór de activering van de virtuele assistent door het activeringswoord van de virtuele assistent zijn geregistreerd en data die worden gegenereerd wanneer een gebruiker via een virtuele assistent contact maakt met een product dat door een andere entiteit dan de fabrikant van het product wordt verstrekt. Echter, alleen de data die voortvloeien uit de interactie tussen de gebruiker en het product via de virtuele assistent vallen binnen het toepassingsgebied van deze verordening. Data die zijn geproduceerd door de virtuele assistent die geen verband houden met het gebruik van een product, vallen niet onder deze verordening.

(23) Alvorens een contract te sluiten voor de aankoop, huur of leasing van een product of de verlening van een gerelateerde dienst, moet de gebruiker duidelijke en voldoende informatie worden verstrekt over de wijze waarop toegang kan worden verkregen tot de gegenereerde data. Deze verplichting zorgt voor transparantie over de gegenereerde data en bevordert de toegang voor de gebruiker. Deze verplichting om informatie te

verstrekken doet geen afbreuk aan de verplichting van de verwerkingsverantwoordelijke om de betrokkene informatie te verstrekken overeenkomstig artikel 12, 13 en 14 van Verordening (EG) nr. 2016/679.

(24) Deze verordening legt datahouders de verplichting op om in bepaalde omstandigheden data beschikbaar te stellen. Voor zover persoonsgegevens worden verwerkt, dient de houder van deze data een verwerkingsverantwoordelijke te zijn in de zin van Verordening (EU) 2016/679. Wanneer gebruikers betrokkenen zijn, moeten datahouders worden verplicht hun toegang tot hun data te verlenen en de data overeenkomstig deze verordening ter beschikking te stellen van derden naar keuze van de gebruiker. Deze verordening schept echter geen rechtsgrondslag op grond van Verordening (EU) 2016/679 voor de datahouder om op verzoek van een gebruiker die geen betrokkene is, toegang te verlenen tot persoonsgegevens of deze beschikbaar te stellen aan een derde, en mag niet worden opgevat als een verlening van een nieuw recht aan de datahouder om data te gebruiken die door het gebruik van een product of een gerelateerde dienst zijn gegenereerd. Dit geldt met name wanneer de fabrikant de datahouder is. In dat geval moet een contractuele overeenkomst tussen de fabrikant en de gebruiker de basis vormen voor het gebruik van niet-persoonsgebonden data. Deze overeenkomst kan deel uitmaken van de verkoop-, huur- of leaseovereenkomst met betrekking tot het product. Elke contractuele bepaling in de overeenkomst die bepaalt dat de datahouder de door de gebruiker van een product of gerelateerde dienst gegenereerde data mag gebruiken, moet transparant zijn voor de gebruiker, ook wat betreft het doel waarvoor de datahouder de data zal gebruiken. Deze verordening mag geen beletsel vormen voor contractuele voorwaarden die tot gevolg hebben dat het gebruik van de data, of bepaalde categorieën daarvan, door de datahouder wordt uitgesloten of beperkt. Deze verordening mag evenmin in de weg staan voor sectorspecifieke regelgevingsvereisten uit hoofde van EU-recht, of nationale wetgeving die verenigbaar is met het EU-recht, die het gebruik van bepaalde data door de datahouder om duidelijk omschreven redenen van openbare orde zouden uitsluiten of beperken.

(25) In sectoren die worden gekenmerkt door de concentratie van een klein aantal fabrikanten die aan eindgebruikers leveren, hebben gebruikers slechts beperkte mogelijkheden om data met die fabrikanten te delen. Onder dergelijke omstandigheden kunnen contractuele overeenkomsten ontoereikend zijn om de doelstelling van empowerment van gebruikers te verwezenlijken. De data blijven doorgaans onder controle van de fabrikanten, waardoor het voor gebruikers moeilijk is om waarde te verkrijgen uit de data die worden gegenereerd door de apparatuur die zij kopen of leasen. Bijgevolg is er een beperkt potentieel voor kleinere innovatieve bedrijven om concurrerende op data gebaseerde oplossingen aan te bieden, en voor een diverse data-economie in Europa. Deze verordening moet daarom voortbouwen op recente ontwikkelingen in specifieke sectoren, zoals de gedragscode voor het delen van landbouwdata op basis van een contractuele overeenkomst. Sectorale wetgeving kan worden voorgesteld om tegemoet te komen aan sectorspecifieke behoeften en doelstellingen. Voorts mag de datahouder geen door het gebruik van het product of de gerelateerde dienst gegenereerde data gebruiken om inzicht te verkrijgen in de economische situatie van de gebruiker, zijn of haar activa of productiemethoden of het gebruik op een andere wijze die de commerciële positie van de gebruiker op de markten waarop hij of zij actief is, zou kunnen ondermijnen. Dit zou bijvoorbeeld inhouden dat kennis over de algemene prestaties van een bedrijf of een landbouwbedrijf wordt gebruikt in contractuele onderhandelingen met de gebruiker over de mogelijke aankoop van producten of landbouwproducten van de gebruiker ten

nadele van de gebruiker, of bijvoorbeeld dat dergelijke informatie wordt gebruikt om in grotere databanken over bepaalde markten in het aggregaat (bv. databanken over oogstopbrengsten voor het komende oogstseizoen) te voorzien, aangezien een dergelijk gebruik op indirecte wijze negatieve gevolgen voor de gebruiker kan hebben. De gebruiker moet de nodige technische interface krijgen om vergunningen te beheren, bij voorkeur met gedetailleerde toestemmingsopties (zoals „eenmaal toestaan" of „toestaan bij het gebruik van deze app of dienst"), waaronder de optie om de toestemming in te trekken.

(26) In overeenkomsten tussen een datahouder en een consument als gebruiker van een product of gerelateerde dienst die data genereert, is Richtlijn 93/13/EEG van toepassing op de voorwaarden van de overeenkomst om ervoor te zorgen dat een consument niet onderworpen is aan oneerlijke contractvoorwaarden. Voor oneerlijke contractvoorwaarden die eenzijdig worden opgelegd aan een micro-, kleine of middelgrote onderneming in de zin van artikel 2 van de bijlage bij Aanbeveling 2003/361/EG[63], bepaalt deze verordening dat dergelijke oneerlijke bedingen niet bindend mogen zijn voor die onderneming.

(27) De datahouder kan een passende gebruikersidentificatie verlangen om na te gaan of de gebruiker recht heeft op toegang tot de data. In het geval van persoonsgegevens die namens de verwerkingsverantwoordelijke door een andere verwerkende partij worden verwerkt, dient de datahouder ervoor te zorgen dat het verzoek om toegang door de verwerkende partij wordt ontvangen en behandeld.

(28) Het moet de gebruiker vrij staan de data voor elk rechtmatig doel te gebruiken. Dit houdt onder meer in dat de data die de gebruiker in het kader van de uitoefening van het recht uit hoofde van deze verordening heeft ontvangen, worden verstrekt aan een derde die een aftermarketdienst aanbiedt die mogelijk concurreert met een door de datahouder verleende dienst, of de datahouder daartoe opdracht geeft. De datahouder dient ervoor te zorgen dat de aan de derde ter beschikking gestelde data even nauwkeurig, volledig, betrouwbaar, relevant en actueel zijn als de data waartoe de datahouder zelf toegang heeft of kan hebben op basis van het gebruik van het product of de gerelateerde dienst. Bedrijfsgeheimen of intellectuele-eigendomsrechten moeten bij de verwerking van de data in acht worden genomen. Het is belangrijk om stimulansen te behouden om te investeren in producten met functionaliteiten die gebaseerd zijn op het gebruik van data van sensoren die in dat product zijn ingebouwd. Het doel van deze verordening moet dienovereenkomstig worden opgevat als het bevorderen van de ontwikkeling van nieuwe, innovatieve producten of aanverwante diensten, het stimuleren van innovatie op aftermarkets, maar ook het stimuleren van de ontwikkeling van volledig nieuwe diensten die gebruikmaken van de data, onder meer op basis van data van uiteenlopende producten of gerelateerde diensten. Tegelijkertijd mogen de investeringsprikkels voor het soort product waarvan de data afkomstig zijn, bijvoorbeeld door het gebruik van data om een concurrerend product te ontwikkelen, niet worden ondermijnd.

(29) Een derde partij aan wie data ter beschikking worden gesteld, kan een onderneming, een onderzoeksorganisatie of een non-profitorganisatie zijn. Bij het beschikbaar stellen van de data aan de derde mag de datahouder geen misbruik maken van zijn positie om een concurrentievoordeel te verkrijgen op markten waar de datahouder en de derde mogelijk rechtstreeks met elkaar concurreren. Daarom mag de datahouder ook geen

[63] Aanbeveling 2003/361/EG van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen.

door het gebruik van het product of de gerelateerde dienst gegenereerde data gebruiken om inzicht te verkrijgen in de economische situatie van de derde, zijn of haar activa of productiemethoden of het gebruik op een andere wijze die de commerciële positie van de derde op de markten waarop hij of zij actief is, zou kunnen ondermijnen.

(30) Het gebruik van een product of gerelateerde dienst kan, met name wanneer de gebruiker een natuurlijke persoon is, data genereren die betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon (betrokkene). De verwerking van dergelijke data is onderworpen aan de regels van Verordening (EU) 2016/679, ook wanneer persoonsgegevens en niet-persoonsgebonden data in een dataset onlosmakelijk met elkaar verbonden zijn[64]. De betrokkene kan de gebruiker of een andere natuurlijke persoon zijn. Persoonsgegevens mogen alleen worden opgevraagd door een verwerkingsverantwoordelijke of een betrokkene. Een gebruiker die de betrokkene is, heeft op grond van Verordening (EU) 2016/679 onder bepaalde omstandigheden recht op toegang tot hem betreffende persoonsgegevens, en deze verordening laat deze rechten onverlet. Op grond van deze verordening heeft de gebruiker die een natuurlijke persoon is ook recht op toegang tot alle door het product gegenereerde, al dan niet persoonlijke data. Wanneer de gebruiker niet de betrokkene is, maar een onderneming, waaronder een eenmanszaak, en niet in geval van gedeeld huishoudelijk gebruik van het product, is de gebruiker een verwerkingsverantwoordelijke in de zin van Verordening (EU) 2016/679. Bijgevolg moet een gebruiker als verwerkingsverantwoordelijke die van plan is persoonsgegevens op te vragen die zijn gegenereerd door het gebruik van een product of een gerelateerde dienst, beschikken over een rechtsgrondslag voor de verwerking van de data op grond van artikel 6, lid 1, van Verordening (EU) 2016/679, zoals toestemming van de betrokkene of gerechtvaardigd belang. Deze gebruiker moet ervoor zorgen dat de betrokkene naar behoren wordt geïnformeerd over de gespecificeerde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden voor de verwerking van die data en over de wijze waarop de betrokkene zijn rechten daadwerkelijk kan uitoefenen. Wanneer de datahouder en de gebruiker gezamenlijke verwerkingsverantwoordelijken zijn in de zin van artikel 26 van Verordening (EU) 2016/679, zijn zij verplicht om door middel van een onderlinge regeling op transparante wijze hun respectieve verantwoordelijkheden voor de naleving van die verordening vast te stellen. Het moet duidelijk zijn dat een dergelijke gebruiker, zodra data beschikbaar zijn gesteld, op zijn beurt datahouder kan worden, indien hij aan de criteria van deze verordening voldoet en dus onderworpen wordt aan de verplichtingen om data beschikbaar te stellen uit hoofde van deze verordening.

(31) Data die door het gebruik van een product of verwante dienst worden gegenereerd, mogen alleen op verzoek van de gebruiker aan een derde ter beschikking worden gesteld. Deze verordening vormt een aanvulling op het recht in artikel 20 van Verordening (EU) 2016/679. Dat artikel voorziet in een recht van betrokkenen om hun persoonsgegevens in een gestructureerd, algemeen gebruikt en machineleesbaar formaat te ontvangen en deze gegevens door te geven aan andere verwerkingsverantwoordelijken, wanneer die gegevens worden verwerkt op basis van artikel 6, lid 1, punt a), of artikel 9, lid 2, punt a), of van een overeenkomst uit hoofde van artikel 6, lid 1, punt b). Betrokkenen moeten het recht hebben om de data direct van een verwerkingsverantwoordelijke naar een andere verwerkingsverantwoordelijke te laten overdragen. In artikel 20 wordt gespecificeerd dat dit betrekking heeft op door

64 PB L 303 van 28.11.2018, blz. 59.

de betrokkene verstrekte data, maar wordt niet gespecificeerd of dit een actief gedrag van de zijde van de betrokkene vereist, dan wel of het ook van toepassing is op situaties waarin een product of een gerelateerde dienst door zijn ontwerp het gedrag van een betrokkene of andere informatie met betrekking tot een betrokkene op passieve wijze observeert. Het recht uit hoofde van deze verordening vormt op verschillende manieren een aanvulling op het recht om persoonsgegevens te ontvangen en over te dragen uit hoofde van artikel 20 van Verordening (EU) 2016/679. Het verleent gebruikers het recht op toegang tot en beschikbaarstelling aan derden van data die worden gegenereerd door het gebruik van een product of gerelateerde dienst, ongeacht of het persoonsgegevens betreft, en of het actief verstrekte of passief waargenomen data betreft en ongeacht de rechtsgrondslag van de verwerking. In tegenstelling tot de technische verplichtingen waarin artikel 20 van Verordening (EU) 2016/679 voorziet, voorziet deze verordening in de technische haalbaarheid van toegang van derden voor alle soorten data die binnen het toepassingsgebied van de verordening vallen, ongeacht of het persoonsgegevens of niet-persoonsgebonden data zijn. Het biedt de datahouder ook de mogelijkheid een redelijke vergoeding vast te stellen die door derden, maar niet door de gebruiker, moet worden betaald voor de kosten die voortvloeien uit het verlenen van rechtstreekse toegang tot de door het product van de gebruiker gegenereerde data. Indien een datahouder en een derde partij niet in staat zijn overeenstemming te bereiken over de voorwaarden voor een dergelijke rechtstreekse toegang, mag de betrokkene op geen enkele wijze worden belet de in Verordening (EU) 2016/679 vervatte rechten, waaronder het recht op overdraagbaarheid van data, uit te oefenen door overeenkomstig die verordening rechtsmiddelen in te stellen. In deze context moet worden begrepen dat, overeenkomstig Verordening (EU) 2016/679, de verwerking van bijzondere categorieën persoonsgegevens door de datahouder of de derde op grond van een contractuele overeenkomst niet is toegestaan.

(32) De toegang tot alle op eindapparatuur opgeslagen of via die eindapparatuur toegankelijke data is onderworpen aan Richtlijn 2002/58/EG en vereist de toestemming van de abonnee of gebruiker in de zin van die richtlijn, tenzij dit strikt noodzakelijk is voor de levering van een uitdrukkelijk door de gebruiker of abonnee gevraagde dienst van de informatiemaatschappij (of uitsluitend met het oog op de doorgifte van een communicatie). Richtlijn 2002/58/EG („e-privacyrichtlijn”) (en de voorgestelde e-privacyverordening) beschermt de integriteit van de eindapparatuur van de gebruiker wat betreft het gebruik van verwerkings- en opslagmogelijkheden en het verzamelen van informatie. Apparatuur voor het internet der dingen wordt als eindapparatuur beschouwd indien deze direct of indirect verbonden is met een openbaar communicatienetwerk.

(33) Om uitbuiting van gebruikers te voorkomen, mogen derden aan wie data op verzoek van de gebruiker beschikbaar zijn gesteld, de data alleen verwerken voor de met de gebruiker overeengekomen doeleinden en deze alleen met een andere derde delen indien dit noodzakelijk is om de door de gebruiker gevraagde dienst te verlenen.

(34) Overeenkomstig het beginsel van minimale gegevensverwerking mag de derde partij alleen toegang hebben tot aanvullende informatie die nodig is voor de levering van de door de gebruiker gevraagde dienst. Nadat toegang tot data is verkregen, mag de derde deze uitsluitend verwerken voor de met de gebruiker overeengekomen doeleinden, zonder inmenging van de datahouder. Het moet voor de gebruiker even gemakkelijk zijn om toegang van de derde tot de data te weigeren of stop te zetten als het voor de gebruiker is om toegang te verlenen. De derde mag de gebruiker op geen enkele

manier dwingen, bedriegen of manipuleren door de autonomie, besluitvorming of keuzes van de gebruiker te ondermijnen of te beperken, onder meer door middel van een digitale interface met de gebruiker. In dit verband mogen derden zich bij het ontwerpen van hun digitale interfaces niet baseren op zogenaamde donkere patronen. Donkere patronen zijn ontwerptechnieken die consumenten aanzetten tot of misleiden in beslissingen die negatieve gevolgen voor hen hebben. Deze manipulatietechnieken kunnen worden gebruikt om gebruikers, met name kwetsbare consumenten, te overtuigen zich ongewenst te gedragen en gebruikers door nudging te misleiden zodat zij bepaalde beslissingen over de toegang tot hun data nemen of om hun beslissingen op onredelijke wijze te sturen, waardoor hun autonomie, besluitvorming en keuze worden ondermijnd en beperkt. Gangbare en legitieme handelspraktijken die in overeenstemming zijn met het EU-recht, mogen op zichzelf niet als donkere patronen worden beschouwd. Derden moeten voldoen aan hun verplichtingen uit hoofde van het toepasselijke EU-recht, met name de vereisten van Richtlijn 2005/29/EG, Richtlijn 2011/83/EU, Richtlijn 2000/31/EG en Richtlijn 98/6/EG.

(35) De derde mag de data ook niet gebruiken om personen te profileren, tenzij deze verwerkingsactiviteiten strikt noodzakelijk zijn om de door de gebruiker gevraagde dienst te verlenen. De verplichting om data te wissen wanneer deze niet langer nodig zijn voor het met de gebruiker overeengekomen doel, vormt een aanvulling op het recht van de betrokkene om de data te wissen overeenkomstig artikel 17 van Verordening (EG) nr. 2016/679. Wanneer de derde een aanbieder van een databemiddelingsdienst in de zin van [de datagovernanceverordening] is, zijn de waarborgen voor de betrokkene waarin die verordening voorziet, van toepassing. De derde partij mag de data gebruiken om een nieuw en innovatief product of een nieuwe innovatieve dienst te ontwikkelen, maar niet om een concurrerend product te ontwikkelen.

(36) Start-ups, kleine en middelgrote ondernemingen en bedrijven uit traditionele sectoren met minder ontwikkelde digitale mogelijkheden hebben moeite om toegang te krijgen tot relevante data. Deze verordening heeft tot doel de toegang tot data voor deze entiteiten te vergemakkelijken, en er tegelijkertijd voor te zorgen dat de overeenkomstige verplichtingen zo proportioneel mogelijk worden afgebakend om overschrijding van de reikwijdte te voorkomen. Tegelijkertijd is een klein aantal zeer grote ondernemingen ontstaan met niet alleen een aanzienlijke economische macht in de digitale economie door de accumulatie en aggregatie van grote hoeveelheden data, maar ook met de technologische infrastructuur om deze te gelde te maken. Tot deze ondernemingen behoren ondernemingen die kernplatformdiensten aanbieden die alle platformecosystemen in de digitale economie controleren en die bestaande of nieuwe marktdeelnemers niet kunnen aanvechten of betwisten. De [verordening betreffende betwistbare en eerlijke markten in de digitale sector (wet inzake digitale markten)] heeft tot doel deze inefficiënties en onevenwichtigheden te verhelpen door de Commissie toe te staan een aanbieder als „poortwachter” aan te wijzen, en legt een aantal verplichtingen op aan die aangewezen poortwachters, waaronder een verbod om bepaalde data zonder toestemming te combineren en een verplichting om te zorgen voor effectieve rechten op overdraagbaarheid van data uit hoofde van artikel 20 van Verordening (EU) 2016/679. In overeenstemming met de [verordening inzake betwistbare en eerlijke markten in de digitale sector (wet inzake digitale markten)] en gezien het ongeëvenaarde vermogen van deze ondernemingen om data te verkrijgen, zou het niet nodig zijn om de doelstelling van deze verordening te verwezenlijken, en zou het derhalve onevenredig zijn om datahouders te verplichten om dergelijke poortwachterondernemingen op te nemen als begunstigden van het recht op toegang

tot data. Dit betekent dat een onderneming die kernplatformdiensten aanbiedt en als poortwachter is aangewezen, geen toegang kan vragen tot of toegang kan krijgen tot data van gebruikers die zijn gegenereerd door het gebruik van een product of gerelateerde dienst of door een virtuele assistent op basis van de bepalingen van hoofdstuk II van deze verordening. Een onderneming die kernplatformdiensten aanbiedt die overeenkomstig de wet inzake digitale markten als poortwachter is aangewezen, moet worden geacht alle juridische entiteiten van een groep ondernemingen te omvatten wanneer één juridische entiteit een kernplatformdienst aanbiedt. Bovendien mogen derden aan wie op verzoek van de gebruiker data ter beschikking worden gesteld, de data niet ter beschikking stellen van een aangewezen poortwachter. De derde mag bijvoorbeeld de dienstverlening niet uitbesteden aan een poortwachter. Derden mogen echter wel gebruikmaken 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.

(37) Gezien de huidige stand van de technologie is het te belastend om verdere ontwerpverplichtingen op te leggen met betrekking tot producten die worden vervaardigd of ontworpen en gerelateerde diensten die worden verleend door micro- en kleine ondernemingen. Dit is echter niet het geval wanneer de vervaardiging of het ontwerp van een product aan een micro- of kleine onderneming wordt uitbesteed. In dergelijke situaties kan de onderneming die deze taak aan de micro- of kleine onderneming heeft uitbesteed, de onderaannemer op passende wijze vergoeden. Een micro- of kleine onderneming kan niettemin als datahouder onderworpen zijn aan de vereisten van deze verordening, wanneer zij niet de fabrikant van het product of een aanbieder van gerelateerde diensten is.

(38) Deze verordening bevat algemene toegangsregels wanneer een datahouder wettelijk verplicht is data beschikbaar te stellen aan een ontvanger van data. Die toegang moet gebaseerd zijn op eerlijke, redelijke, niet-discriminerende en transparante voorwaarden, om te zorgen voor consistentie van de praktijken op het gebied van het delen van data op de interne markt, in alle sectoren, en om eerlijke praktijken voor het delen van data aan te moedigen en te bevorderen, zelfs op gebieden waar een dergelijk recht op toegang tot data niet wordt verleend. Deze algemene toegangsregels zijn niet van toepassing op verplichtingen om data beschikbaar te stellen uit hoofde van Verordening (EU) 2016/679. Deze regels hebben geen gevolgen voor het vrijwillig delen van data.

(39) Op basis van het beginsel van contractvrijheid moeten de partijen vrij kunnen blijven onderhandelen over de precieze voorwaarden voor het beschikbaar stellen van data in hun overeenkomsten, binnen het kader van de algemene regels voor het beschikbaar stellen van data.

(40) Om ervoor te zorgen dat de voorwaarden voor verplichte toegang tot data voor beide partijen eerlijk zijn, moeten de algemene regels inzake het recht op toegang tot data verwijzen naar de regel inzake het vermijden van oneerlijke contractvoorwaarden.

(41) Om het gebrek aan informatie over de voorwaarden van verschillende contracten te compenseren, waardoor het voor de ontvanger van de data moeilijk is om te beoordelen of de voorwaarden voor het beschikbaar stellen van de data niet discriminerend zijn, moet de datahouder aantonen dat een contractueel beding niet discriminerend is. Er is geen sprake van onrechtmatige discriminatie wanneer een

datahouder verschillende contractvoorwaarden gebruikt om data beschikbaar te stellen of verschillende vergoedingen, indien deze verschillen om objectieve redenen gerechtvaardigd zijn. Deze verplichtingen laten Richtlijn (EU) 2016/679 onverlet.

(42) Als stimulans om te blijven investeren in het genereren van waardevolle data, waaronder investeringen in relevante technische instrumenten, bevat deze verordening het beginsel dat de datahouder een redelijke vergoeding kan vragen wanneer hij wettelijk verplicht is data beschikbaar te stellen aan de ontvanger van de data. Deze bepalingen mogen niet worden opgevat als het betalen voor de data zelf, maar in het geval van micro-, kleine of middelgrote ondernemingen, voor de gemaakte kosten en investeringen die nodig zijn om de data beschikbaar te stellen.

(43) In gerechtvaardigde gevallen, onder andere wanneer het noodzakelijk is om de deelname van de consument en de mededinging te waarborgen of innovatie op bepaalde markten te bevorderen, kan het EU-recht of de nationale wetgeving tot uitvoering van het EU-recht gereguleerde compensatie opleggen voor het beschikbaar stellen van specifieke soorten data.

(44) Om micro-, kleine en middelgrote ondernemingen te beschermen tegen buitensporige economische lasten die het voor hen commercieel te moeilijk zouden maken om innovatieve bedrijfsmodellen te ontwikkelen en uit te voeren, mag de compensatie voor het beschikbaar stellen van data niet hoger zijn dan de directe kosten van het beschikbaar stellen van de data en niet-discriminerend zijn.

(45) Directe kosten voor het beschikbaar stellen van data zijn de kosten die nodig zijn voor de reproductie, elektronische verspreiding en opslag, maar niet die voor het verzamelen of produceren van data. De directe kosten voor het beschikbaar stellen van data moeten beperkt blijven tot het aandeel dat kan worden toegeschreven aan de individuele verzoeken, rekening houdend met het feit dat de datahouder permanent de nodige technische interfaces of bijbehorende software en connectiviteit zal moeten opzetten. Bij regelmatige of herhaalde transacties in een zakelijke relatie kunnen de kosten in verband met het beschikbaar stellen van de data dalen wanneer houders en ontvangers van data langetermijnregelingen sluiten, bijvoorbeeld via een abonnementsmodel.

(46) Het is niet nodig in te grijpen in het geval van het delen van data tussen grote ondernemingen of wanneer de datahouder een kleine of middelgrote onderneming is en de ontvanger van de data een grote onderneming is. In dergelijke gevallen worden de ondernemingen geacht in staat te zijn te onderhandelen over een redelijke vergoeding, rekening houdend met factoren zoals de omvang, het formaat, de aard of het aanbod van en de vraag naar de data, alsmede de kosten voor het verzamelen en ter beschikking stellen van de data aan de ontvanger van de data.

(47) Transparantie is een belangrijk beginsel om ervoor te zorgen dat de door de datahouder gevraagde vergoeding redelijk is, of, indien de ontvanger van de data een micro-, kleine of middelgrote onderneming is, dat de vergoeding niet hoger is dan de kosten die rechtstreeks verband houden met het beschikbaar stellen van de data aan de ontvanger en toe te schrijven is aan het individuele verzoek. Om de ontvanger van de data in staat te stellen te beoordelen en na te gaan of de vergoeding voldoet aan de vereisten van deze verordening, moet de datahouder de ontvanger voldoende gedetailleerde informatie verstrekken voor de berekening van de vergoeding.

(48) Het waarborgen van toegang tot alternatieve manieren om binnenlandse en grensoverschrijdende geschillen in verband met het beschikbaar stellen van data op te

lossen, moet ten goede komen aan houders en ontvangers van data en aldus het vertrouwen in het delen van data versterken. In gevallen waarin de partijen het niet eens kunnen worden over eerlijke, redelijke en niet-discriminerende voorwaarden voor het beschikbaar stellen van data, moeten de geschillenbeslechtingsorganen de partijen een eenvoudige, snelle en goedkope oplossing bieden.

(49) Om te voorkomen dat voor hetzelfde geschil twee of meer geschillenbeslechtingsorganen worden aangezocht, met name in een grensoverschrijdende context, moet een geschillenbeslechtingsorgaan een verzoek om beslechting van een geschil dat reeds voor een ander geschillenbeslechtingorgaan of voor een rechterlijke instantie van een lidstaat is gebracht, kunnen afwijzen.

(50) Partijen bij geschillenbeslechtingsprocedures mogen niet worden belet hun grondrechten op een doeltreffende voorziening in rechte en op een onpartijdig gerecht uit te oefenen. Daarom mag het besluit om een geschil aan een geschillenbeslechtingsorgaan voor te leggen die partijen niet het recht ontnemen om verhaal te halen bij een rechterlijke instantie van een lidstaat.

(51) Wanneer de ene partij zich in een sterkere onderhandelingspositie bevindt, bestaat het risico dat die partij die positie kan inzetten ten nadele van de andere overeenkomstsluitende partij bij de onderhandelingen over toegang tot data en de toegang tot data commercieel minder levensvatbaar en soms onbetaalbaar kan maken. Dergelijke contractuele onevenwichtigheden schaden met name het vermogen van micro-, kleine en middelgrote ondernemingen om te onderhandelen over de voorwaarden voor toegang tot data, die vaak geen andere keuze hebben dan contractvoorwaarden te aanvaarden, of het contract te laten schieten. Oneerlijke contractvoorwaarden die de toegang tot en het gebruik van data of de aansprakelijkheid en rechtsmiddelen in geval van schending of beëindiging van datagerelateerde verplichtingen regelen, mogen derhalve niet bindend zijn voor micro-, kleine of middelgrote ondernemingen wanneer deze eenzijdig aan hen zijn opgelegd.

(52) In de regels inzake contractvoorwaarden moet rekening worden gehouden met het beginsel van contractvrijheid als essentieel concept in de relaties tussen ondernemingen. Daarom moeten niet alle contractuele bedingen aan een oneerlijkheidstoets worden onderworpen, maar alleen bedingen die eenzijdig aan micro-, kleine en middelgrote ondernemingen worden opgelegd. Het gaat om situaties waarin een partij een bepaald contractueel beding voorstelt en de micro-, kleine of middelgrote onderneming geen invloed kan uitoefenen op de inhoud van dat beding, ondanks een poging om erover te onderhandelen. Een contractueel beding dat door één partij wordt voorgesteld en door de micro-, kleine of middelgrote onderneming is aanvaard, of een beding waarover is onderhandeld en dat vervolgens in gewijzigde vorm tussen de contractpartijen is overeengekomen, mag niet als eenzijdig opgelegd worden beschouwd.

(53) Daarnaast moeten de regels inzake oneerlijke contractvoorwaarden alleen van toepassing zijn op de elementen van een overeenkomst die verband houden met het beschikbaar stellen van data, dat wil zeggen contractuele voorwaarden betreffende de toegang tot en het gebruik van data, alsook aansprakelijkheid of rechtsmiddelen in geval van schending en beëindiging van datagerelateerde verplichtingen. Andere delen van hetzelfde contract die geen verband houden met het beschikbaar stellen van data, mogen niet worden onderworpen aan de in deze verordening vastgestelde oneerlijkheidstoets.

(54) Criteria voor het vaststellen van oneerlijke contractuele bedingen mogen alleen worden toegepast op buitensporige contractuele bedingen, waarbij misbruik wordt gemaakt van een sterkere onderhandelingspositie. De overgrote meerderheid van de contractuele voorwaarden die commercieel gunstiger zijn voor de ene partij dan voor de andere, waaronder voorwaarden die normaal zijn in overeenkomsten tussen ondernemingen, zijn een normale uitdrukking van het beginsel van contractvrijheid en blijven van toepassing.

(55) Indien een contractueel beding niet voorkomt in de lijst van bedingen die altijd als oneerlijk worden beschouwd of die geacht worden oneerlijk te zijn, is de algemene oneerlijkheidsbepaling van toepassing. In dit verband moeten de als oneerlijk aangemerkte bedingen als maatstaf dienen voor de interpretatie van de algemene oneerlijkheidsbepaling. Ten slotte kunnen door de Commissie te ontwikkelen en aanbevolen modelcontractvoorwaarden voor data-uitwisselingsovereenkomsten tussen ondernemingen ook nuttig zijn voor commerciële partijen bij de onderhandelingen over contracten.

(56) In situaties van uitzonderlijke noodzaak kan het nodig zijn dat overheidsinstanties of EU-instellingen, -agentschappen of -organen data die een onderneming in handen heeft, gebruiken om te reageren op algemene noodsituaties of in andere uitzonderlijke gevallen. Onderzoeksinstellingen en organisaties die onderzoek financieren, zouden ook als overheidsinstanties of overheidsondernemingen kunnen worden georganiseerd. Om de lasten voor het bedrijfsleven te beperken, moeten micro- en kleine ondernemingen worden vrijgesteld van de verplichting om in uitzonderlijke gevallen data te verstrekken aan overheidsinstanties en EU-instellingen, -agentschappen of -organen.

(57) In het geval van algemene noodsituaties, zoals noodsituaties op het gebied van de volksgezondheid, grote milieu- en natuurrampen, waaronder door de klimaatverandering verergerde rampen en door de mens veroorzaakte grote rampen, zoals grote cyberincidenten, zal het algemeen belang dat voortvloeit uit het gebruik van de data zwaarder wegen dan het belang van de datahouders om vrijelijk over hun data te beschikken. In dat geval moeten datahouders verplicht worden de data op verzoek beschikbaar te stellen aan overheidsinstanties of aan EU-instellingen, -agentschappen of -organen. Of er al dan niet sprake is van een algemene noodsituatie, wordt bepaald volgens de respectieve procedures in de lidstaten of van relevante internationale organisaties.

(58) Een uitzonderlijke noodzaak kan zich ook voordoen wanneer een overheidsinstantie kan aantonen dat de data nodig zijn om een algemene noodsituatie te voorkomen of om bij te dragen aan het herstel achteraf, in omstandigheden die zich in een redelijke verhouding tot de algemene noodsituatie in kwestie bevinden. Wanneer de uitzonderlijke noodzaak niet wordt gerechtvaardigd door de noodzaak om te reageren op, te voorkomen of bij te dragen aan het herstel na een algemene noodsituatie, moet de overheidsinstantie of de EU-instelling, het EU-agentschap of het EU-orgaan aantonen dat het door het gebrek aan tijdige toegang tot en gebruik van de gevraagde data niet in staat is een specifieke taak in het algemeen belang waarin uitdrukkelijk bij wet is voorzien, doeltreffend te vervullen. Een dergelijke uitzonderlijke noodzaak kan zich ook voordoen in andere situaties, bijvoorbeeld in verband met het tijdig opstellen van officiële statistieken wanneer data niet anderszins beschikbaar zijn of wanneer de lasten voor de statistische respondenten aanzienlijk zullen worden verminderd. Tegelijkertijd moet de overheidsinstantie of de EU-instelling, het EU-agentschap of het EU-orgaan, indien er geen sprake is van reactie op, voorkomen van of bijstand bij

herstel na een algemene noodsituatie, aantonen dat er geen alternatieve manieren zijn om de gevraagde data te verkrijgen en dat de data niet tijdig kunnen worden verkregen door de nodige verplichtingen tot het verstrekken van data in nieuwe wetgeving vast te leggen.

(59) Deze verordening mag niet van toepassing zijn op, noch vooruitlopen op vrijwillige regelingen voor het uitwisselen van data tussen particuliere entiteiten en overheidsinstanties. Deze verordening mag geen afbreuk doen aan de verplichtingen van datahouders om data te verstrekken op basis van behoeften van niet-uitzonderlijke aard, met name wanneer het scala aan data en datahouders bekend is en het datagebruik regelmatig kan plaatsvinden, zoals in het geval van rapportageverplichtingen en internemarktverplichtingen. Deze verordening mag evenmin van invloed zijn op de vereisten inzake toegang tot data om de naleving van de toepasselijke regels te controleren, onder andere in gevallen waarin overheidsinstanties de controle op de naleving toevertrouwen aan andere entiteiten dan overheidsinstanties.

(60) Voor de uitoefening van hun taken op het gebied van het voorkomen, het onderzoek, de opsporing en de vervolging van strafbare en administratieve overtredingen, de tenuitvoerlegging van strafrechtelijke en administratieve sancties en het verzamelen van data voor belasting- of douanedoeleinden, moeten overheidsinstanties en EU-instellingen, -agentschappen of -organen gebruikmaken van hun bevoegdheden uit hoofde van de sectorale wetgeving. Deze verordening doet derhalve geen afbreuk aan instrumenten voor het delen van, de toegang tot en het gebruik van data op die gebieden.

(61) Een evenredig, beperkt en voorspelbaar kader op EU-niveau is noodzakelijk voor het beschikbaar stellen van data door datahouders, in geval van uitzonderlijke noodzaak, aan de overheidsinstanties en EU-instellingen, -agentschappen of -organen, zowel om rechtszekerheid te waarborgen als om de administratieve lasten voor bedrijven tot een minimum te beperken. Daartoe moeten verzoeken om data van overheidsinstanties en EU-instellingen, -agentschappen en -organen aan datahouders transparant en evenredig zijn wat betreft de inhoud en de gedetailleerdheid ervan. Het doel van het verzoek en het beoogde gebruik van de gevraagde data moeten specifiek en duidelijk worden toegelicht, waarbij de verzoekende entiteit voldoende flexibiliteit moet worden geboden om haar taken in het algemeen belang uit te voeren. In het verzoek moet ook rekening worden gehouden met de legitieme belangen van de bedrijven waaraan het verzoek is gericht. De lasten voor datahouders moeten tot een minimum worden beperkt door de verzoekende entiteiten te verplichten het eenmaligheidsbeginsel in acht te nemen, dat voorkomt dat dezelfde data meer dan eens worden opgevraagd door meer dan één overheidsinstantie of EU-instelling, -agentschap of -orgaan wanneer die data nodig zijn om te reageren op een algemene noodsituatie. Om de transparantie te waarborgen, moeten verzoeken om data van overheidsinstanties en EU-instellingen, -agentschappen of -organen zonder onnodige vertraging openbaar worden gemaakt door de entiteit die om de data verzoekt en moeten alle verzoeken die door een algemene noodsituatie worden gerechtvaardigd online worden gepubliceerd.

(62) Het doel van de verplichting om de data te verstrekken is ervoor te zorgen dat overheidsinstanties en EU-instellingen, -agentschappen of -organen over de nodige kennis beschikken om te reageren op noodsituaties in de openbare sector, deze te voorkomen of ervan te herstellen of om de capaciteit te behouden om specifieke taken te vervullen waarin de wet uitdrukkelijk voorziet. De door deze entiteiten verkregen data kunnen commercieel gevoelig zijn. Richtlijn (EU) 2019/1024 van het Europees

Parlement en de Raad[65] mag derhalve niet van toepassing zijn op data die uit hoofde van deze verordening beschikbaar worden gesteld en deze data mogen niet worden beschouwd als open data die beschikbaar zijn voor hergebruik door derde partijen. Dit mag echter geen afbreuk doen aan de toepasselijkheid van Richtlijn (EU) 2019/1024 op het hergebruik van officiële statistieken voor de productie waarvan op grond van deze verordening verkregen data zijn gebruikt, mits het hergebruik geen betrekking heeft op de onderliggende data. Bovendien mag dit geen afbreuk doen aan de mogelijkheid om data te delen voor het verrichten van onderzoek of voor het opstellen van officiële statistieken, mits aan de voorwaarden van deze verordening is voldaan. Het moet overheidsinstanties ook worden toegestaan om op grond van deze verordening verkregen data uit te wisselen met andere overheidsinstanties om tegemoet te komen aan de uitzonderlijke noodzaak waarvoor de data zijn opgevraagd.

(63) datahouders moeten de mogelijkheid hebben om binnen een termijn van 5 of 15 werkdagen te vragen om een wijziging of intrekking van het verzoek van een overheidsinstantie of EU-instelling, -agentschap of -orgaan, afhankelijk van de aard van de uitzonderlijke noodzaak waarop het verzoek betrekking heeft. In het geval van verzoeken op grond van een algemene noodsituatie, moet er een gegronde reden zijn om de data niet beschikbaar te stellen indien kan worden aangetoond dat het verzoek vergelijkbaar is met of identiek is aan een eerder ingediend verzoek voor hetzelfde doel van een andere overheidsinstantie of van een andere EU-instelling, -agentschap of -orgaan. Een datahouder die het verzoek afwijst of om wijziging verzoekt, moet de onderliggende motivering voor deze afwijzing meedelen aan de overheidsinstantie of aan de EU-instelling, het EU-agentschap of -orgaan die om de data verzoekt. Indien de databankrechten sui generis uit hoofde van Richtlijn 96/6/EG van het Europees Parlement en de Raad[66] van toepassing zijn op de gevraagde datasets, moeten de datahouders hun rechten uitoefenen op een wijze die de overheidsinstantie of de EU-instelling, het EU-agentschap of -orgaan niet belet de data overeenkomstig deze verordening te verkrijgen of te delen.

(64) Wanneer het strikt noodzakelijk is persoonsgegevens op te nemen in de data die ter beschikking worden gesteld van een overheidsinstantie of EU-instelling, -agentschap of -orgaan, moeten de toepasselijke regels inzake de bescherming van persoonsgegevens worden nageleefd en moet het beschikbaar stellen van de data en het daaropvolgende gebruik ervan vergezeld gaan van waarborgen voor de rechten en belangen van de personen op wie die data betrekking hebben. De instantie die de data opvraagt, moet de strikte noodzaak en de specifieke en beperkte doeleinden van de verwerking aantonen. De datahouder moet redelijke inspanningen leveren om de data te anonimiseren of, indien een dergelijke anonimisering onmogelijk blijkt, moet de datahouder technologische middelen, zoals pseudonimisering en aggregatie, toepassen alvorens de data beschikbaar te stellen.

(65) Data die op basis van een uitzonderlijke noodzaak ter beschikking worden gesteld van overheidsinstanties en EU-instellingen, -agentschappen en -organen, mogen alleen worden gebruikt voor het doel waarvoor zij werden gevraagd, tenzij de datahouder die de data beschikbaar heeft gesteld, uitdrukkelijk heeft ingestemd met het gebruik van de data voor andere doeleinden. De data moeten worden vernietigd zodra zij niet

---

65 Richtlijn (EU) 2019/1024 van het Europees Parlement en de Raad van 20 juni 2019 inzake open data en het hergebruik van overheidsinformatie (PB L 172 van 26.6.2019, blz. 56).

66 Richtlijn 96/9/EG van het Europees Parlement en de Raad van 11 maart 1996 betreffende de rechtsbescherming van databanken (PB L 77 van 27.3.1996, blz. 20).

langer nodig zijn voor het in het verzoek vermelde doel, tenzij anders overeengekomen, en de datahouder moet daarvan in kennis worden gesteld.

(66) Bij het hergebruik van door datahouders verstrekte data moeten overheidsinstanties, EU-instellingen, -agentschappen en -organen zowel de bestaande toepasselijke wetgeving als de contractuele verplichtingen die op de datahouder van toepassing zijn, eerbiedigen. Wanneer de openbaarmaking van bedrijfsgeheimen van de datahouder aan overheidsinstanties of aan EU-instellingen, -agentschappen of -organen strikt noodzakelijk is voor het doel waarvoor de data zijn opgevraagd, moet de datahouder de garantie krijgen dat die openbaarmaking vertrouwelijk zal gebeuren.

(67) Wanneer de bescherming van een aanzienlijk algemeen belang in het geding is, zoals het reageren op algemene noodsituaties, mag van overheidsinstanties of EU-instellingen, -agentschappen of -organen niet worden verwacht dat zij ondernemingen voor de verkregen data vergoeden. Algemene noodsituaties zijn zeldzame gebeurtenissen en niet al deze noodsituaties vereisen het gebruik van data die in het handen zijn van ondernemingen. De zakelijke activiteiten van de datahouders zullen daarom waarschijnlijk niet negatief worden beïnvloed als gevolg van het feit dat overheidsinstanties of EU-instellingen, -agentschappen of -organen een beroep doen op deze verordening. Aangezien er echter vaker sprake kan zijn van een uitzonderlijke noodzaak dan enkel om te reageren op een algemene noodsituatie, waaronder gevallen van preventie of herstel van een algemene noodsituatie, moeten datahouders in dergelijke gevallen recht hebben op een redelijke vergoeding die niet hoger mag zijn dan de technische en organisatorische kosten die zijn gemaakt om aan het verzoek te voldoen en de redelijke marge die nodig is om de data beschikbaar te stellen aan de overheidsinstantie of de EU-instelling, het EU-agentschap of het EU-orgaan. De vergoeding mag noch worden opgevat als een betaling voor de data zelf, noch als een verplichte vergoeding.

(68) De overheidsinstanties of EU-instellingen, agentschappen of organen mogen de data die zij op grond van het verzoek hebben verkregen, delen met andere entiteiten of personen wanneer dit nodig is om wetenschappelijk onderzoek of analyses uit te voeren die zij niet zelf kunnen uitvoeren. Dergelijke data kunnen onder dezelfde omstandigheden ook worden gedeeld met de nationale bureaus voor de statistiek en Eurostat voor het opstellen van officiële statistieken. Dergelijke onderzoeksactiviteiten moeten echter verenigbaar zijn met het doel waarvoor de data zijn opgevraagd en de datahouder moet worden geïnformeerd over het delen van de door hem verstrekte data met andere entiteiten. Personen die onderzoek verrichten of onderzoeksorganisaties waarmee deze data kunnen worden gedeeld, moeten handelen zonder winstoogmerk of in het kader van een door de staat erkende taak van algemeen belang. Organisaties waarop commerciële ondernemingen een beslissende invloed uitoefenen, waardoor dergelijke ondernemingen zeggenschap kunnen uitoefenen vanwege structurele situaties die zouden kunnen leiden tot preferentiële toegang tot de resultaten van het onderzoek, mogen voor de toepassing van deze verordening niet als onderzoeksorganisaties worden beschouwd.

(69) De mogelijkheid voor klanten van dataverwerkingsdiensten, waaronder cloud- en edgediensten, om over te stappen van de ene op de andere dataverwerkingsdienst, met behoud van een minimale functionaliteit van de dienst, is een essentiële voorwaarde voor een meer concurrerende markt met lagere toetredingsdrempels voor nieuwe dienstverleners.

(70) Verordening (EU) 2018/1807 van het Europees Parlement en de Raad moedigt dienstverleners aan om doeltreffende zelfregulerende gedragscodes te ontwikkelen en uit te voeren die beste werkwijzen bevatten voor onder meer een gemakkelijkere overstap naar een andere aanbieder van dataverwerkingsdiensten en het overdragen van data. Gezien de beperkte doeltreffendheid van de als reactie daarop ontwikkelde zelfreguleringskaders en het algemene gebrek aan open normen en interfaces, is het noodzakelijk een reeks minimale wettelijke verplichtingen voor aanbieders van dataverwerkingsdiensten vast te stellen om contractuele, economische en technische belemmeringen voor een doeltreffende overstap tussen dataverwerkingsdiensten uit de weg te ruimen.

(71) Dataverwerkingsdiensten moeten betrekking hebben op diensten die toegang op aanvraag en brede toegang op afstand mogelijk maken tot een schaalbare en elastische pool van gedeelde en gedistribueerde computerbronnen. Deze computerbronnen omvatten onder andere netwerken, servers of andere virtuele of fysieke infrastructuur, besturingssystemen, software, waaronder softwareontwikkelingsinstrumenten, opslag, toepassingen en diensten. Het vermogen van de gebruiker van dataverwerkingsdiensten om eenzijdig zelfvoorzienend te zijn, zoals servertijd of netwerkopslag, zonder enige menselijke interactie door de dienstverlener, zou kunnen worden omschreven als beheer op verzoek. Met “brede toegang op afstand” wordt bedoeld: de computercapaciteit wordt via het netwerk aangeboden en is toegankelijk via mechanismen die het gebruik van heterogene thin- of thick-client-platforms bevorderen (van webbrowsers, mobiele telefoons, tot werkstations). Met “schaalbaar” wordt bedoeld: computercapaciteit die, ongeacht de geografische locatie van de capaciteit, op flexibele wijze door aanbieders van dataverwerkingsdiensten wordt toegewezen om schommelingen in de vraag te kunnen opvangen Met “elastische groep” wordt bedoeld: de computercapaciteit die, afhankelijk van de vraag, ter beschikking wordt gesteld en wordt vrijgegeven om deze beschikbare capaciteit snel te kunnen verhogen of verlagen naargelang van het werkvolume. Met “gedeeld” wordt bedoeld: de computercapaciteit die ter beschikking wordt gesteld van meerdere gebruikers die een gemeenschappelijke toegang tot de dienst hebben, maar waarbij de verwerking voor elke gebruiker afzonderlijk plaatsvindt, hoewel de dienst door middel van dezelfde elektronische apparatuur wordt verleend. Met “gedistribueerd” wordt bedoeld: de computercapaciteit die zich op verschillende netwerkcomputers of -toestellen bevindt en die onderling communiceert en coördineert door middel van het doorgeven van berichten. De term „sterk gedistribueerd” wordt gebruikt om dataverwerkingsdiensten te beschrijven die betrekking hebben op dataverwerking dichter bij de plaats waar data worden gegenereerd of verzameld, bijvoorbeeld in een verbonden dataverwerkingsapparaat. Edge computing, een vorm van dergelijke sterk gedistribueerde dataverwerking, zal naar verwachting nieuwe bedrijfsmodellen en modellen voor de levering van clouddiensten genereren, die van meet af aan open en interoperabel moeten zijn.

(72) Deze verordening heeft tot doel de overstap tussen dataverwerkingsdiensten te vergemakkelijken, inclusief alle voorwaarden en acties waarmee klanten een contractuele overeenkomst van een dataverwerkingsdienst kunnen beëindigen, een of meerdere nieuwe contracten kunnen afsluiten met verschillende aanbieders van dataverwerkingsdiensten, al hun digitale activa, waaronder hun data, aan de betrokken andere aanbieders over kunnen dragen en deze in de nieuwe omgeving kunnen blijven gebruiken en tegelijkertijd te profiteren van functionele gelijkwaardigheid. Digitale activa hebben betrekking op elementen in digitaal formaat waarvoor de klant het gebruiksrecht heeft, waaronder data, toepassingen, virtuele machines en andere

uitingen van virtualiseringstechnologieën, zoals containers. Functionele gelijkwaardigheid betekent het handhaven van een minimumniveau van functionaliteit van een dienst na het overstappen, dit moet technisch haalbaar worden geacht wanneer zowel de oorspronkelijke als de nieuwe dataverwerkingsdienst (geheel of gedeeltelijk) hetzelfde type dienst bestrijken. Metadata die door het gebruik van een dienst door de klant worden gegenereerd, moeten ook overdraagbaar zijn overeenkomstig de bepalingen van deze verordening inzake het overstappen.

(73) Wanneer aanbieders van dataverwerkingsdiensten op hun beurt klant zijn van dataverwerkingsdiensten die door een derde aanbieder worden verleend, zullen zij zelf profiteren van doeltreffender overstappen, terwijl zij tegelijkertijd nog steeds gebonden zijn aan de verplichtingen van deze verordening voor wat hun eigen dienstenaanbod betreft.

(74) Aanbieders van dataverwerkingsdiensten moeten worden verplicht alle bijstand en ondersteuning te bieden die nodig zijn om het overstapproces succesvol en doeltreffend te maken, zonder dat van deze aanbieders wordt verlangd dat zij binnen of op basis van de IT-infrastructuur van verschillende aanbieders van dataverwerkingsdiensten nieuwe categorieën diensten ontwikkelen om functionele gelijkwaardigheid in een andere omgeving dan hun eigen systemen te waarborgen. Niettemin zijn dienstverleners verplicht alle bijstand en ondersteuning te bieden die nodig zijn om het overstapproces doeltreffend te laten verlopen. Bestaande rechten in verband met de beëindiging van contracten, waaronder de rechten die zijn ingevoerd bij Verordening (EU) 2016/679 en Richtlijn (EU) 2019/770 van het Europees Parlement en de Raad[67], moeten onverlet worden gelaten.

(75) Om het overstappen tussen dataverwerkingsdiensten te vergemakkelijken, moeten aanbieders van dataverwerkingsdiensten het gebruik van implementatie- en/of nalevingsinstrumenten overwegen, met name die welke door de Commissie zijn gepubliceerd in de vorm van een rulebook voor clouddiensten. Met name modelcontractbepalingen zijn nuttig om het vertrouwen in dataverwerkingsdiensten te vergroten, een evenwichtigere relatie tussen gebruikers en dienstverleners tot stand te brengen en de rechtszekerheid te verbeteren met betrekking tot de voorwaarden die gelden voor de overstap naar andere dataverwerkingsdiensten. In dit licht moeten gebruikers en dienstverleners overwegen gebruik te maken van modelcontractbepalingen die zijn ontwikkeld door relevante organen of deskundigengroepen die krachtens het EU-recht zijn opgericht.

(76) Open interoperabiliteitsspecificaties en -normen die zijn ontwikkeld overeenkomstig de punten 3 en 4 van bijlage II bij Verordening (EU) nr. 1025/2021 op het gebied van interoperabiliteit en overdraagbaarheid, maken een naadloze cloudomgeving met diverse verkopers mogelijk, wat een belangrijke vereiste is voor open innovatie in de Europese data-economie. Aangezien niet is gebleken dat marktgestuurde processen leiden tot het vaststellen van technische specificaties of normen die doeltreffende cloudinteroperabiliteit op het PaaS-niveau (platform-as-a-service) en SaaS (software as-a-service) bevorderen, moet de Commissie op basis van deze verordening en in overeenstemming met Verordening (EU) nr. 1025/2012 Europese normalisatie-instellingen kunnen verzoeken dergelijke normen te ontwikkelen, met name voor soorten diensten waarvoor dergelijke normen nog niet bestaan. Daarnaast zal de

[67] Richtlijn (EU) 2019/770 van het Europees Parlement en de Raad van 20 mei 2019 betreffende bepaalde aspecten van overeenkomsten voor de levering van digitale inhoud en digitale diensten (PB L 136 van 22.5.2019, blz. 1).

Commissie de marktpartijen aanmoedigen relevante open interoperabiliteitsspecificaties te ontwikkelen. De Commissie kan door middel van gedelegeerde handelingen het gebruik van Europese normen voor interoperabiliteit of open interoperabiliteitsspecificaties voor specifieke soorten diensten voorschrijven, door middel van een verwijzing in een centraal register voor EU-normen voor de interoperabiliteit van dataverwerkingsdiensten. Er wordt alleen naar Europese normen en open interoperabiliteitsspecificaties verwezen indien deze in overeenstemming zijn met de in deze verordening gespecificeerde criteria, die dezelfde betekenis hebben als de eisen in de punten 3 en 4 van bijlage II bij Verordening (EU) nr. 1025/2021 en de interoperabiliteitsfacetten zoals gedefinieerd in ISO/IEC 19941:2017.

(77) Derde landen mogen wetten, voorschriften en andere rechtshandelingen vaststellen die gericht zijn op het rechtstreeks overdragen van of het verlenen van toegang door de overheid tot niet-persoonsgebonden data die zich buiten hun grenzen, waaronder in de EU, bevinden. Rechterlijke uitspraken of besluiten van andere juridische of administratieve instanties, waaronder van rechtshandhavingsinstanties van derde landen die vereisen dat persoonsgegevens worden overgedragen of dat er toegang tot die gegevens wordt verschaft, moeten afdwingbaar zijn indien zij gebaseerd zijn op een internationale overeenkomst, zoals een verdrag inzake wederzijdse rechtshulp, tussen het verzoekende derde land en de EU of een lidstaat. In andere gevallen kunnen zich situaties voordoen waarin een verzoek om overdracht van of het verlenen van toegang tot niet-persoonsgebonden data op grond van het recht van een derde land in strijd is met een verplichting om die data te beschermen op grond van het EU-recht of het nationale recht, met name wat betreft de bescherming van de grondrechten van het individu, zoals het recht op veiligheid en het recht op een doeltreffende voorziening in rechte, of de fundamentele belangen van een lidstaat in verband met nationale veiligheid of defensie, alsmede de bescherming van commercieel gevoelige data, inclusief de bescherming van bedrijfsgeheimen, en de bescherming van intellectuele-eigendomsrechten, waaronder zijn contractuele verbintenissen inzake vertrouwelijkheid in overeenstemming met dat recht. Bestaan er geen internationale overeenkomsten die dergelijke kwesties regelen, dan mag overdracht of toegang worden toegestaan indien gecontroleerd is dat het systeem van het derde land voorschrijft dat de redenen voor en de evenredigheid van het besluit worden toegelicht, dat het vonnis of het besluit van de rechtbank een specifiek karakter heeft, en dat het met redenen omklede bezwaar van de geadresseerde wordt getoetst door een bevoegde rechtbank in het derde land die gemachtigd is om rekening te houden met de relevante juridische belangen van de dataverstrekker. Indien mogelijk op grond van de voorwaarden van het verzoek om toegang tot data van de autoriteit van het derde land, moet de aanbieder van dataverwerkingsdiensten de klant wiens data worden opgevraagd hierover kunnen informeren om na te gaan of er sprake is van een mogelijk conflict van een dergelijke toegang met EU- of nationale voorschriften, zoals die inzake de bescherming van commercieel gevoelige data, waaronder de bescherming van bedrijfsgeheimen en intellectuele-eigendomsrechten en de contractuele verbintenissen inzake vertrouwelijkheid.

(78) Om het vertrouwen in de data te vergroten, is het belangrijk dat de waarborgen met betrekking tot de EU-burgers, de overheidssector en het bedrijfsleven zo veel mogelijk worden toegepast om de controle over hun data te waarborgen. Daarnaast moeten het EU-recht, de EU-waarden en de EU-normen in acht worden genomen op het gebied van (maar niet beperkt tot) veiligheid, gegevensbescherming en privacy, en consumentenbescherming. Om onrechtmatige toegang tot niet-persoonsgebonden data te voorkomen, moeten aanbieders van dataverwerkingsdiensten die onder dit

instrument vallen, zoals cloud- en edgediensten, alle redelijke maatregelen nemen om de toegang tot de systemen waar niet-persoonsgebonden data worden opgeslagen te voorkomen, onder meer, in voorkomend geval, door middel van versleuteling van data, frequente audits, de geverifieerde naleving van relevante certificeringsregelingen voor veiligheidsgaranties en de wijziging van het bedrijfsbeleid.

(79) Normalisatie en semantische interoperabiliteit moeten een sleutelrol spelen bij het bieden van technische oplossingen om interoperabiliteit te waarborgen. Om de conformiteit met de interoperabiliteitseisen te vergemakkelijken, moet worden voorzien in een vermoeden van conformiteit voor interoperabiliteitsoplossingen die voldoen aan geharmoniseerde normen of delen daarvan, overeenkomstig Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad. De Commissie moet gemeenschappelijke specificaties vaststellen op gebieden waar geen geharmoniseerde normen bestaan of waar deze ontoereikend zijn voor betere interoperabiliteit van de gemeenschappelijke Europese dataruimten, applicatieprogramma-interfaces, overstappen naar andere clouddiensten en slimme contracten. Daarnaast kunnen er nog gemeenschappelijke specificaties in de verschillende sectoren worden vastgesteld, overeenkomstig de sectorale wetgeving van de EU of de lidstaten, op basis van de specifieke behoeften van die sectoren. Herbruikbare datastructuren en -modellen (in de vorm van kernvocabularia), ontologieën, toepassingsprofielen van metadata, referentiedata in de vorm van kernvocabulaire, taxonomieën, codelijsten, autoriteitstabellen en thesauri moeten ook deel uitmaken van de technische specificaties voor semantische interoperabiliteit. Daarnaast moet de Commissie in staat worden gesteld opdracht te geven tot het ontwikkelen van geharmoniseerde normen voor de interoperabiliteit van dataverwerkingsdiensten.

(80) Om de interoperabiliteit van slimme contracten in toepassingen voor data-uitwisseling te bevorderen, moeten essentiële eisen worden vastgesteld voor slimme contracten voor professionals die slimme contracten voor anderen sluiten of dergelijke slimme contracten integreren in toepassingen die de uitvoering van overeenkomsten voor het delen van data ondersteunen. Om de conformiteit van dergelijke slimme contracten met die essentiële eisen te vergemakkelijken, moet worden voorzien in een vermoeden van conformiteit voor interoperabiliteitsoplossingen die voldoen aan geharmoniseerde normen of delen daarvan, overeenkomstig Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad.

(81) Met het oog op een efficiënte uitvoering van deze verordening moeten de lidstaten hiervoor een of meer bevoegde autoriteiten aanwijzen. Indien een lidstaat meer dan één bevoegde autoriteit aanwijst, moet hij ook een coördinerende bevoegde autoriteit aanwijzen. De bevoegde autoriteiten moeten met elkaar samenwerken. De autoriteiten die verantwoordelijk zijn voor het toezicht op de naleving van gegevensbescherming en de bevoegde autoriteiten die krachtens sectorale wetgeving zijn aangewezen, moeten verantwoordelijk zijn voor de toepassing van deze verordening op hun bevoegdheidsgebieden.

(82) Om hun rechten uit hoofde van deze verordening te doen gelden, moeten natuurlijke en rechtspersonen het recht hebben verhaal te halen voor inbreuken op hun rechten uit hoofde van deze verordening door een klacht in te dienen bij de bevoegde autoriteiten. Die autoriteiten moeten worden verplicht samen te werken om ervoor te zorgen dat de klacht naar behoren wordt behandeld en opgelost. Om gebruik te maken van het samenwerkingsnetwerkmechanisme voor consumentenbescherming en om representatieve vorderingen mogelijk te maken, wijzigt deze verordening de bijlagen

bij Verordening (EU) 2017/2394 van het Europees Parlement en de Raad[68] en Richtlijn (EU) 2020/1828 van het Europees Parlement en de Raad[69].

(83) De bevoegde autoriteiten van de lidstaten moeten ervoor zorgen dat inbreuken op de in deze verordening vastgestelde verplichtingen worden bestraft met sancties. Daarbij moeten zij rekening houden met de aard, de ernst, de frequentie en de duur van de inbreuk, het algemeen belang, de omvang en de aard van de verrichte activiteiten, alsmede de economische draagkracht van de inbreukpleger. Zij moeten er rekening mee houden of de inbreukpleger systematisch of herhaaldelijk zijn of haar verplichtingen uit hoofde van deze verordening niet nakomt. Om ondernemingen te helpen contracten op te stellen en daarover te onderhandelen, moet de Commissie niet-verplichte modelcontractvoorwaarden voor data-uitwisselingsovereenkomsten tussen ondernemingen ontwikkelen en aanbevelen, indien nodig rekening houdend met de voorwaarden in specifieke sectoren en de bestaande praktijken met vrijwillige mechanismen voor data-uitwisseling. Deze modelcontractvoorwaarden moeten in de eerste plaats een praktisch instrument zijn om met name kleinere ondernemingen te helpen een contract te sluiten. Wanneer deze modelcontractvoorwaarden op grote schaal en integraal worden gebruikt, moeten zij ook het gunstige effect hebben dat zij van invloed zijn op de opzet van contracten inzake de toegang tot en het gebruik van data en derhalve in bredere zin leiden tot eerlijkere contractuele betrekkingen bij de toegang tot en het delen van data.

(84) Om het risico weg te nemen dat houders van data in databanken die zijn verkregen of gegenereerd door middel van fysieke componenten, zoals sensoren, van een verbonden product en een gerelateerde dienst, aanspraak maken op het recht sui generis uit hoofde van artikel 7 van Richtlijn 96/9/EG wanneer dergelijke databanken niet in aanmerking komen voor het recht sui generis, en daardoor de daadwerkelijke uitoefening van het recht van gebruikers op toegang tot en gebruik van data en het recht om data met derde partijen te delen uit hoofde van deze verordening belemmeren, moet in deze verordening worden verduidelijkt dat het recht sui generis niet van toepassing is op dergelijke databanken aangezien niet aan de vereisten voor bescherming zou zijn voldaan.

(85) Teneinde rekening te houden met de technische aspecten van dataverwerkingsdiensten, moet aan de Commissie de bevoegdheid worden overgedragen om overeenkomstig artikel 290 VWEU handelingen vast te stellen om deze verordening aan te vullen met het oog op de invoering van een monitoringmechanisme voor overstapkosten die door aanbieders van dataverwerkingsdiensten op de markt wordt opgelegd, tot nadere bepaling van de essentiële eisen inzake interoperabiliteit voor exploitanten van dataruimten en aanbieders van dataverwerkingsdiensten en tot publicatie van de referentie van open interoperabiliteitsspecificaties en Europese normen voor de interoperabiliteit van dataverwerkingsdiensten. Het is van bijzonder belang dat de Commissie bij haar voorbereidende werkzaamheden tot passende raadplegingen overgaat, onder meer op deskundigenniveau, en dat die raadplegingen geschieden in overeenstemming met de

[68] Verordening (EU) 2017/2394 van het Europees Parlement en de Raad van 12 december 2017 betreffende samenwerking tussen de nationale autoriteiten die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming en tot intrekking van Verordening (EG) nr. 2006/2004 (PB L 345 van 27.12.2017, blz. 1).

[69] Richtlijn (EU) 2020/1828 van het Europees Parlement en de Raad van 25 november 2020 betreffende representatieve vorderingen ter bescherming van de collectieve belangen van consumenten en tot intrekking van Richtlijn 2009/22/EG (PB L 409 van 4.12.2020, blz. 1).

beginselen van het Interinstitutioneel Akkoord over beter wetgeven van 13 april 2016[70]. Met name om te zorgen voor gelijke deelname aan de voorbereiding van gedelegeerde handelingen ontvangen het Europees Parlement en de Raad alle documenten op hetzelfde tijdstip als de deskundigen van de lidstaten, en hebben hun deskundigen systematisch toegang tot de vergaderingen van de deskundigengroepen van de Commissie die zich bezighouden met de voorbereiding van de gedelegeerde handelingen.

(86) Om eenvormige voorwaarden voor de uitvoering van deze verordening te waarborgen, moeten aan de Commissie uitvoeringsbevoegdheden worden toegekend om deze verordening aan te vullen, zodat zij gemeenschappelijke specificaties kan vaststellen met het oog op de interoperabiliteit van gemeenschappelijke Europese dataruimten en datadeling, het overstappen tussen dataverwerkingsdiensten, de interoperabiliteit van slimme contracten en technische middelen, zoals applicatieprogramma-interfaces, teneinde de transmissie van data tussen partijen mogelijk te maken, ook continu of realtime en voor kernvocabularia van semantische interoperabiliteit, en zodat zij gemeenschappelijke specificaties voor slimme contracten kan vaststellen. Die bevoegdheden moeten worden uitgeoefend overeenkomstig Verordening (EU) nr. 182/2011 van het Europees Parlement en de Raad[71].

(87) Deze verordening mag geen afbreuk doen aan specifieke bepalingen van EU-handelingen op het gebied van data-uitwisseling tussen bedrijven, tussen bedrijven en consumenten en tussen bedrijven en overheidsinstanties die vóór de datum van vaststelling van deze verordening zijn vastgesteld. Met het oog op de samenhang en de soepele werking van de interne markt moet de Commissie, in voorkomend geval, het verband tussen deze verordening en de handelingen tot regeling van het delen van data die zijn vastgesteld vóór de datum van vaststelling van deze verordening evalueren, om na te gaan of die specifieke bepalingen in overeenstemming moeten worden gebracht met deze verordening. Deze verordening mag geen afbreuk doen aan regels die gericht zijn op specifieke behoeften van afzonderlijke sectoren of gebieden van algemeen belang. Dergelijke regels kunnen aanvullende vereisten omvatten met betrekking tot technische aspecten van de toegang tot data, zoals interfaces voor de toegang tot data, of de wijze waarop toegang tot data kan worden verleend, bijvoorbeeld rechtstreeks vanuit het product of via databemiddelingsdiensten. Dergelijke regels kunnen ook beperkingen omvatten van de rechten van datahouders om toegang te krijgen tot of gebruik te maken van gebruikersdata, of andere aspecten dan de toegang tot en het gebruik van data, zoals governance-aspecten. Deze verordening mag evenmin afbreuk doen aan specifiekere regels in het kader van de ontwikkeling van gemeenschappelijke Europese dataruimten.

(88) Deze verordening doet geen afbreuk aan de toepassing van de mededingingsregels, met name niet aan de artikelen 101 en 102 van het Verdrag. De maatregelen van deze verordening mogen niet worden gebruikt om de mededinging te beperken op een wijze die strijdig is met het Verdrag.

(89) Om de economische actoren in staat te stellen zich aan te passen aan de nieuwe regels van deze verordening, moeten zij een jaar na de inwerkingtreding van de verordening van toepassing worden.

---

70 PB L 123 van 12.5.2016, blz. 1

71 Verordening (EU) nr. 182/2011 van het Europees Parlement en de Raad van 16 februari 2011 tot vaststelling van de algemene voorschriften en beginselen die van toepassing zijn op de wijze waarop de lidstaten de uitoefening van de uitvoeringsbevoegdheden door de Commissie controleren (PB L 55 van 28.2.2011, blz. 13).

(90) Overeenkomstig artikel 42 van Verordening (EU) 2018/1725 zijn de Europese Toezichthouder voor gegevensbescherming en het Europees Comité voor gegevensbescherming geraadpleegd, en op [XX XX 2022] hebben zij hun gezamenlijke advies uitgebracht,

HEBBEN DE VOLGENDE VERORDENING VASTGESTELD:

HOOFDSTUK 1
ALGEMENE BEPALINGEN

Artikel 1
Onderwerp en toepassingsgebied

1. Bij deze verordening worden geharmoniseerde regels vastgesteld voor het beschikbaar stellen van data die zijn gegenereerd door het gebruik van een product of een gerelateerde dienst door de gebruiker van dat product of die dienst, het beschikbaar stellen van data door datahouders aan data-ontvangers, en het beschikbaar stellen van data door datahouders aan overheidsinstanties of EU-instellingen, -agentschappen of -organen, indien er een uitzonderlijke noodzaak bestaat voor de uitvoering van een taak van algemeen belang.

2. Deze verordening is van toepassing op:

   (a) fabrikanten van producten en leveranciers van gerelateerde diensten die in de EU in de handel worden gebracht en de gebruikers van dergelijke producten of diensten;

   (b) datahouders die data ter beschikking stellen van data-ontvangers in de EU;

   (c) data-ontvangers in de EU aan wie data ter beschikking worden gesteld;

   (d) overheidsinstanties en EU-instellingen, -agentschappen of -organen die datahouders verzoeken om data beschikbaar te stellen wanneer er een uitzonderlijke noodzaak bestaat om die data te gebruiken voor de uitvoering van een taak in het algemeen belang en de datahouders die deze data in antwoord op een dergelijk verzoek verstrekken;

   (e) aanbieders van dataverwerkingsdiensten die dergelijke diensten aan klanten in de EU aanbieden.

3. Het EU-recht inzake de bescherming van persoonsgegevens, de persoonlijke levenssfeer en de vertrouwelijkheid van communicatie en de integriteit van eindapparatuur is van toepassing op persoonsgegevens die worden verwerkt in verband met de in deze verordening vastgestelde rechten en verplichtingen. Deze richtlijn doet geen afbreuk aan het EU-recht betreffende de bescherming van persoonsgegevens, met name Verordening (EU) 2016/679 en Richtlijn 2002/58/EG, met inbegrip van de bevoegdheden van toezichthoudende autoriteiten. Wat de in hoofdstuk II van deze verordening vastgestelde rechten betreft, en wanneer gebruikers betrokkenen zijn van persoonsgegevens waarop de rechten en verplichtingen uit hoofde van dat hoofdstuk van toepassing zijn, vormen de bepalingen van deze verordening een aanvulling op het recht op overdraagbaarheid van data uit hoofde van artikel 20 van Verordening (EU) 2016/679.

4. Deze verordening doet geen afbreuk aan rechtshandelingen van de EU en haar lidstaten die voorzien in het delen van, de toegang tot en het gebruik van data met het oog op het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van Verordening (EU) 2021/784 van het Europees Parlement en de Raad[72] en de [voorstellen inzake elektronisch bewijsmateriaal [COM (2018) 225 en 226] zodra deze zijn vastgesteld, en internationale samenwerking op dit gebied. Deze verordening doet geen afbreuk aan het verzamelen, delen, raadplegen en gebruiken van data uit hoofde van Richtlijn (EU) 2015/849 van het Europees Parlement en de Raad tot voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld en de financiering van terrorisme en Verordening (EU) 2015/847 van het Europees Parlement en de Raad betreffende bij geldovermakingen te voegen informatie. Deze verordening doet geen afbreuk aan de bevoegdheden van de lidstaten met betrekking tot activiteiten op het gebied van openbare veiligheid, defensie, nationale veiligheid, douane- en belastingadministratie en de gezondheid en veiligheid van de burgers overeenkomstig het EU-recht.

Artikel 2
Definities

Voor de toepassing van deze verordening wordt verstaan onder:

(1) "data": elke digitale weergave van handelingen, feiten of informatie en elke compilatie van dergelijke handelingen, feiten of informatie, ook in de vorm van geluidsopnames of visuele of audiovisuele opnames;

(2) „product": een tastbaar, roerend goed, ook wanneer dit deel uitmaakt van een onroerend goed, dat data over het gebruik of de omgeving ervan verkrijgt, genereert of verzamelt, en dat data kan doorgeven via een openbare elektronische-communicatiedienst en waarvan de hoofdfunctie niet het opslaan en verwerken van data is;

(3) „gerelateerde dienst": een digitale dienst, met inbegrip van software, die zodanig in een product is geïntegreerd of daarmee verbonden is dat de afwezigheid ervan het product zou beletten een van zijn functies uit te voeren;

(4) „virtuele assistent": software die opdrachten, taken of vragen kan verwerken, onder meer op basis van audio, schriftelijke input, gebaren of bewegingen, en die op basis van die opdrachten, taken of vragen toegang biedt tot eigen diensten en diensten van derde partijen of controle uitoefent op eigen apparatuur en apparaten van derde partijen;

(5) „gebruiker": een natuurlijke of rechtspersoon die een product in eigendom heeft, huurt of leaset of een dienst ontvangt;

(6) „datahouder": een rechtspersoon of natuurlijke persoon die overeenkomstig deze verordening, het toepasselijke EU-recht of de nationale wetgeving tot uitvoering van het EU-recht, of, in het geval van niet-persoonsgebonden data en door controle over het technische ontwerp van het product en de bijbehorende diensten, het recht of de verplichting heeft om bepaalde data beschikbaar te stellen;

[72] Verordening (EU) 2021/784 van het Europees Parlement en de Raad van 29 april 2021 inzake het tegengaan van de verspreiding van terroristische online-inhoud (PB L 172 van 17.5.2021, blz. 79).

(7) „ontvanger van data”: een rechtspersoon of natuurlijke persoon die handelt voor doeleinden die verband houden met zijn handels-, bedrijfs-, ambachts- of beroepsactiviteit, die niet de gebruiker van een product of gerelateerde dienst is en aan wie data beschikbaar worden gesteld door de datahouder, met inbegrip van een derde partij op verzoek van de gebruiker aan de datahouder of in overeenstemming met een wettelijke verplichting uit hoofde van EU-recht of nationale wetgeving tot omzetting van het EU-recht;

(8) "bedrijf" (of "onderneming"): iedere natuurlijke persoon of rechtspersoon die handelt volgens onder deze verordening vallende overeenkomsten en praktijken, voor doeleinden die gerelateerd zijn aan diens handels-, bedrijfs-, ambachts- of beroepsactiviteit;

(9) "overheidsinstantie": nationale, regionale en lokale autoriteiten van de lidstaten, publiekrechtelijke instellingen van de lidstaten of samenwerkingsverbanden bestaande uit één of meer van deze autoriteiten of één of meer van deze instellingen;

(10) „algemene noodsituatie”: een uitzonderlijke situatie die negatieve gevolgen heeft voor de EU-bevolking, een lidstaat of een deel daarvan, met een risico op ernstige en blijvende gevolgen voor de levensomstandigheden of de economische stabiliteit, of een aanzienlijke verslechtering van de economische activa in de EU of in de betrokken lidstaat of lidstaten;

(11) „verwerking” : een bewerking of een geheel van bewerkingen die al dan niet op geautomatiseerde wijze op data of datasets in elektronische vorm worden uitgevoerd, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, bekendmaken door middel van doorgeven, verspreiden of anderszins ter beschikking stellen, op een lijn brengen of combineren, afschermen, wissen of vernietigen van data;

(12) „dataverwerkingsdienst”: een andere digitale dienst dan een online-inhoudsdienst als gedefinieerd in artikel 2, lid 5, van Verordening (EU) 2017/1128, die aan een klant wordt aangeboden en die administratie op aanvraag en brede toegang op afstand tot een schaalbare en elastische pool van gedeelde computercapaciteit van gecentraliseerde, gedistribueerde of sterk gedistribueerde aard mogelijk maakt;

(13) „type dienst”: een reeks dataverwerkingsdiensten met dezelfde primaire doelstelling en hetzelfde basismodel voor dataverwerkingsdiensten;

(14) „functionele gelijkwaardigheid”: het handhaven van een minimumniveau van functionaliteit in de omgeving van een nieuwe dataverwerkingsdienst na het overstapproces, in die mate dat de dienst van bestemming, als reactie op een inputactie van de gebruiker op kernelementen van de dienst, dezelfde output zal leveren met dezelfde prestaties en met hetzelfde niveau van veiligheid, operationele veerkracht en kwaliteit van de dienst als de oorspronkelijke dienst op het moment van beëindiging van het contract;

(15) „open interoperabiliteitsspecificaties”: technische ICT-specificaties, zoals gedefinieerd in Verordening (EU) nr. 1025/2012, die wat betreft prestaties gericht zijn op het bereiken van interoperabiliteit tussen dataverwerkingsdiensten;

(16) „slim contract”: een computerprogramma dat is opgeslagen in een elektronisch-registersysteem waarin het resultaat van de uitvoering van het programma in het elektronische register wordt geregistreerd;

(17) „elektronisch register”: een elektronisch register in de zin van artikel 3, punt 53, van Verordening (EU) nr. 910/2014;

(18) “gemeenschappelijke specificaties”: een document dat geen norm is en dat technische oplossingen bevat om te voldoen aan bepaalde voorschriften en verplichtingen zoals vastgesteld in deze verordening;

(19) „interoperabiliteit”: het vermogen van twee of meer dataruimten of communicatienetwerken, -systemen, -producten, -toepassingen of -componenten om data uit te wisselen en te gebruiken teneinde hun functies te vervullen;

(20) “geharmoniseerde norm”: geharmoniseerde norm zoals gedefinieerd in artikel 2, lid 1, punt c), van Verordening (EU) nr. 1025/2012.

HOOFDSTUK II
DATA DELEN TUSSEN BEDRIJVEN EN CONSUMENTEN EN TUSSEN BEDRIJVEN ONDERLING

Artikel 3
Verplichting om door het gebruik van producten of gerelateerde diensten gegenereerde data toegankelijk te maken

1. Producten worden zodanig ontworpen en vervaardigd, en gerelateerde diensten worden zodanig verleend, dat de door het gebruik ervan gegenereerde data standaard gemakkelijk, veilig en, waar relevant en passend, rechtstreeks toegankelijk zijn voor de gebruiker.

2. Alvorens een contract te sluiten voor de aankoop, huur of leasing van een product of een gerelateerde dienst, krijgt de gebruiker op een duidelijke en begrijpelijke manier minstens de volgende informatie:

   (a) de aard en het volume van de data die waarschijnlijk zullen worden gegenereerd door het gebruik van het product of de gerelateerde dienst;

   (b) of de data waarschijnlijk continu en in realtime zullen worden gegenereerd;

   (c) de manier waarop de gebruiker toegang kan krijgen tot die data;

   (d) of de fabrikant van het product of de dienstverlener die de gerelateerde dienst verleent van plan is de data zelf te gebruiken of een derde partij toe te staan de data te gebruiken en, zo ja, voor welke doeleinden die data zullen worden gebruikt;

   (e) of de verkoper, verhuurder of lease-aanbieder de datahouder is en, zo niet, de identiteit van de datahouder, zoals diens handelsnaam en het geografische adres van de datahouder;

   (f) de communicatiemiddelen waarmee de gebruiker snel contact met de datahouder kan opnemen en efficiënt met hem of haar kan communiceren;

   (g) hoe de gebruiker kan verzoeken om de data te delen met een derde;

   (h) het recht van de gebruiker om bij de in artikel 31 bedoelde bevoegde autoriteit een klacht in te dienen over een schending van de bepalingen van dit hoofdstuk.

Artikel 4

Het recht van gebruikers op toegang tot en gebruik van de door het gebruik van producten of gerelateerde diensten gegenereerde data

1. Wanneer de gebruiker geen rechtstreekse toegang heeft tot de data via het product, stelt de datahouder de data die door het gebruik van een product of een gerelateerde dienst worden gegenereerd, onverwijld, kosteloos en, indien van toepassing, continu en in realtime ter beschikking van de gebruiker. Dit gebeurt op eenvoudig elektronisch verzoek, voor zover dit technisch haalbaar is.

2. De datahouder verlangt van de gebruiker geen informatie die verder gaat dan wat nodig is om de gebruiker als zodanig te verifiëren overeenkomstig lid 1. De datahouder bewaart geen informatie over de toegang van de gebruiker tot de gevraagde data die verder gaat dan nodig is voor de goede uitvoering van het toegangsverzoek van de gebruiker en voor de beveiliging en het onderhoud van de data-infrastructuur.

3. Bedrijfsgeheimen worden alleen bekendgemaakt op voorwaarde dat alle specifieke noodzakelijke maatregelen worden genomen om de vertrouwelijkheid van bedrijfsgeheimen te waarborgen, met name ten aanzien van derden. De datahouder en de gebruiker kunnen maatregelen overeenkomen om de vertrouwelijkheid van de gedeelde data te waarborgen, met name ten aanzien van derden.

4. De gebruiker gebruikt de data die zijn verkregen naar aanleiding van een in lid 1 bedoeld verzoek niet om een product te ontwikkelen dat concurreert met het product waaruit de data afkomstig zijn.

5. Wanneer de gebruiker geen betrokkene is, worden persoonsgegevens die door het gebruik van een product of een gerelateerde dienst zijn gegenereerd, door de datahouder alleen ter beschikking gesteld van de gebruiker indien er een geldige rechtsgrondslag bestaat uit hoofde van artikel 6, lid 1, van Verordening (EU) 2016/679 en, in voorkomend geval, indien aan de voorwaarden van artikel 9 van Verordening (EU) 2016/679 is voldaan.

6. De datahouder gebruikt uitsluitend niet-persoonsgebonden data die zijn gegenereerd door het gebruik van een product of gerelateerde dienst op basis van een contractuele overeenkomst met de gebruiker. De datahouder gebruikt geen door het gebruik van het product of de gerelateerde dienst gegenereerde data om inzicht te verkrijgen in de economische situatie, de activa of de productiemethoden van de gebruiker of het gebruik van het product of de dienst door de gebruiker die de commerciële positie van de gebruiker op de markten waarop hij of zij actief is, zou kunnen ondermijnen.

Artikel 5

Het recht om data te delen met derden

1. Op verzoek van een gebruiker of van een namens een gebruiker optredende partij stelt de datahouder de door het gebruik van een product of gerelateerde dienst gegenereerde data onverwijld en zonder kosten voor de gebruiker ter beschikking aan een derde partij, met dezelfde kwaliteit als die waarover de datahouder beschikt en, indien van toepassing, continu en in realtime.

2. Een onderneming die kernplatformdiensten aanbiedt en die voor een of meer van dergelijke diensten als poortwachter is aangewezen overeenkomstig artikel [...] van [Verordening XXX inzake betwistbare en eerlijke markten in de digitale sector (wet

inzake digitale markten)[73]], is geen in aanmerking komende derde partij op grond van dit artikel en mag derhalve niet:

(a) een gebruiker op enigerlei wijze vragen of commercieel stimuleren, onder meer door financiële of andere vergoedingen te bieden, om data die de gebruiker heeft verkregen naar aanleiding van een verzoek uit hoofde van artikel 4, lid 1, beschikbaar te stellen voor een van zijn diensten;

(b) een gebruiker verzoeken of commercieel stimuleren om de datahouder te verzoeken data beschikbaar te stellen aan een van zijn diensten overeenkomstig lid 1 van dit artikel;

(c) van een gebruiker data ontvangen die de gebruiker heeft verkregen naar aanleiding van een verzoek uit hoofde van artikel 4, lid 1.

3. Van de gebruiker of derde partij wordt geen informatie verlangd die verder gaat dan wat nodig is om de gebruiker of derde partij als zodanig te verifiëren overeenkomstig lid 1. De datahouder bewaart geen informatie over de toegang van de derde partij tot de gevraagde data die verder gaat dan nodig is voor de goede uitvoering van het toegangsverzoek van de derde partij en voor de beveiliging en het onderhoud van de data-infrastructuur.

4. De derde partij mag geen dwangmiddelen inzetten of misbruik maken van kennelijke leemten in de technische infrastructuur van de datahouder die bedoeld is om de data te beschermen, teneinde toegang tot data te verkrijgen.

5. De datahouder gebruikt geen niet-persoonsgebonden data die zijn gegenereerd door het gebruik van het product of de gerelateerde dienst om inzicht te verkrijgen in de economische situatie, activa en productiemethoden van of gebruik door de derde partij die de commerciële positie van de derde partij op de markten waarop de derde actief is, zouden kunnen ondermijnen, tenzij de derde partij met dat gebruik heeft ingestemd en de technische mogelijkheid heeft om die toestemming te allen tijde in te trekken.

6. Wanneer de gebruiker geen betrokkene is, worden persoonsgegevens die door het gebruik van een product of een gerelateerde dienst zijn gegenereerd, door de datahouder alleen ter beschikking gesteld indien er een geldige rechtsgrondslag bestaat uit hoofde van artikel 6, lid 1, van Verordening (EU) 2016/679 en, in voorkomend geval, indien aan de voorwaarden van artikel 9 van Verordening (EU) 2016/679 is voldaan.

7. Het verzuim van de datahouder en de derde partij om regelingen voor het doorgeven van de data overeen te komen, mag de uitoefening van de rechten van de betrokkene uit hoofde van Verordening (EU) 2016/679 en met name het recht op overdraagbaarheid van data uit hoofde van artikel 20 van die verordening, niet belemmeren, beletten of verstoren.

8. Bedrijfsgeheimen worden alleen bekendgemaakt aan derde partijen voor zover deze strikt noodzakelijk zijn om het tussen de gebruiker en de derde partij overeengekomen doel te verwezenlijken en voor zover alle tussen de datahouder en de derde partij overeengekomen specifieke noodzakelijke maatregelen door de derde partij worden genomen om de vertrouwelijkheid van het bedrijfsgeheim te waarborgen. In dat geval worden de aard van de data als bedrijfsgeheimen en de

[73] PB [...].

maatregelen ter bescherming van de vertrouwelijkheid gespecificeerd in de overeenkomst tussen de datahouder en de derde partij.

9. Het in lid 1 bedoelde recht doet geen afbreuk aan het recht op gegevensbescherming van anderen.

Artikel 6

Verplichtingen van derde partijen die op verzoek van de gebruiker data ontvangen

1. Een derde partij verwerkt de hem overeenkomstig artikel 5 ter beschikking gestelde data uitsluitend voor de doeleinden en onder de voorwaarden die met de gebruiker zijn overeengekomen, en met inachtneming van de rechten van de betrokkene wat persoonsgegevens betreft, en wist de data wanneer zij niet langer noodzakelijk zijn voor het overeengekomen doel.

2. De derde partij mag niet:

   (a) de gebruiker op enigerlei wijze dwingen, misleiden of manipuleren door de autonomie, besluitvorming of keuzes van de gebruiker te ondermijnen of te beperken, onder meer door middel van een digitale interface met de gebruiker;

   (b) de ontvangen data gebruiken voor de profilering van natuurlijke personen in de zin van artikel 4, lid 4, van Verordening (EU) 2016/679, tenzij dit noodzakelijk is om de door de gebruiker gevraagde dienst te verlenen;

   (c) de ontvangen data in ruwe, geaggregeerde of afgeleide vorm ter beschikking stellen van een andere derde partij, tenzij dit noodzakelijk is om de door de gebruiker gevraagde dienst te verlenen;

   (d) de ontvangen data beschikbaar stellen aan een onderneming die kernplatformdiensten aanbiedt en die voor een of meer van dergelijke diensten als poortwachter is aangewezen overeenkomstig artikel [...] van [verordening inzake betwistbare en eerlijke markten in de digitale sector (wet inzake digitale markten)];

   (e) de ontvangen data gebruiken om een product te ontwikkelen dat concurreert met het product waaruit de ontvangen data afkomstig zijn, of de data voor dat doel met een andere derde partij delen;

   (f) beletten dat de gebruiker, onder meer door middel van contractuele verbintenissen, de door hem ontvangen data ter beschikking stelt van andere partijen.

Artikel 7

Reikwijdte van de verplichtingen tot het delen van data tussen bedrijven en consumenten en tussen bedrijven onderling

1. De verplichtingen van dit hoofdstuk zijn niet van toepassing op data die zijn gegenereerd door het gebruik van producten die zijn vervaardigd of gerelateerde diensten die worden verleend door ondernemingen die micro- of kleine ondernemingen zijn in de zin van artikel 2 van de bijlage bij Aanbeveling 2003/361/EG, mits die ondernemingen geen partnerondernemingen of verbonden ondernemingen in de zin van artikel 3 van de bijlage bij Aanbeveling 2003/361/EG hebben die niet als micro- of kleine onderneming worden aangemerkt.

2. Wanneer in deze verordening wordt verwezen naar producten of gerelateerde diensten, wordt die verwijzing ook geacht virtuele assistenten te omvatten, voor zover deze worden gebruikt om toegang te krijgen tot of controle uit te oefenen op een product of gerelateerde dienst.

HOOFDSTUK III
VERPLICHTINGEN VOOR DATAHOUDERS DIE WETTELIJK VERPLICHT ZIJN OM DATA BESCHIKBAAR TE STELLEN

Artikel 8

Voorwaarden waaronder datahouders data ter beschikking stellen aan ontvangers van data

1. Wanneer een datahouder verplicht is data aan een ontvanger van data beschikbaar te stellen op grond van artikel 5 of krachtens andere EU-wetgeving of nationale wetgeving tot uitvoering van het EU-recht, doet hij dit onder eerlijke, redelijke en niet-discriminerende voorwaarden en op transparante wijze overeenkomstig de bepalingen van dit hoofdstuk en hoofdstuk IV.

2. Een datahouder komt met een ontvanger van data de voorwaarden voor het beschikbaar stellen van de data overeen. Een contractuele bepaling betreffende de toegang tot en het gebruik van de data of de aansprakelijkheid en rechtsmiddelen voor de inbreuk op of de beëindiging van datagerelateerde verplichtingen is niet bindend indien zij voldoet aan de voorwaarden van artikel 13 of indien zij de toepassing uitsluit van, afwijkt van of de gevolgen wijzigt van de rechten van de gebruiker uit hoofde van hoofdstuk II.

3. Een datahouder mag bij het beschikbaar stellen van data geen onderscheid maken tussen vergelijkbare categorieën ontvangers van data, met inbegrip van partnerondernemingen of verbonden ondernemingen, zoals gedefinieerd in artikel 3 van de bijlage bij Aanbeveling 2003/361/EG, van de datahouder. Wanneer een ontvanger van data van mening is dat de voorwaarden voor het beschikbaar stellen van de data discriminerend zijn, dient de datahouder aan te tonen dat er geen sprake is van discriminatie.

4. Een datahouder stelt de data niet op exclusieve basis ter beschikking aan een ontvanger van data, tenzij de gebruiker daarom uit hoofde van hoofdstuk II verzoekt.

5. Van houders en ontvangers van data wordt niet verlangd dat zij informatie verstrekken die verder gaat dan wat nodig is om na te gaan of wordt voldaan aan de contractuele voorwaarden die zijn overeengekomen voor het beschikbaar stellen van data, of aan hun verplichtingen uit hoofde van deze verordening of andere toepasselijke EU-wetgeving of nationale wetgeving tot uitvoering van het EU-recht.

6. Tenzij anders bepaald in het EU-recht, met inbegrip van artikel 6 van deze verordening, of in nationale wetgeving tot omzetting van het EU-recht, leidt een verplichting om data ter beschikking te stellen aan een ontvanger van data niet tot een verplichting tot de openbaarmaking van bedrijfsgeheimen in de zin van Richtlijn (EU) 2016/943.

Artikel 9
Vergoeding voor het beschikbaar stellen van data

1. Elke vergoeding die tussen een houder en een ontvanger van data is overeengekomen voor het beschikbaar stellen van data, dient redelijk te zijn.

2. Wanneer de ontvanger van de data een micro-, kleine of middelgrote onderneming is in de zin van artikel 2 van de bijlage bij Aanbeveling 2003/361/EG, mag de overeengekomen vergoeding niet hoger zijn dan de kosten die rechtstreeks verband houden met het beschikbaar stellen van de data aan de ontvanger van de data en die aan het verzoek zijn toe te schrijven. Artikel 8, lid 3, is van overeenkomstige toepassing.

3. Dit artikel belet niet dat andere EU-wetgeving of nationale wetgeving tot uitvoering van het EU-recht een vergoeding voor het beschikbaar stellen van data uitsluit of voorziet in een lagere vergoeding.

4. De datahouder verstrekt de ontvanger van data voldoende gedetailleerde informatie over de grondslag voor de berekening van de vergoeding, zodat de ontvanger van de data kan nagaan of aan de vereisten van lid 1 en, indien van toepassing, lid 2 is voldaan.

Artikel 10
Geschillenbeslechting

1. Houders en ontvangers van data hebben toegang tot overeenkomstig lid 2 van dit artikel gecertificeerde geschillenbeslechtingsorganen om geschillen te beslechten met betrekking tot het vaststellen van eerlijke, redelijke en niet-discriminerende voorwaarden voor en transparante wijze van het beschikbaar stellen van data overeenkomstig de artikelen 8 en 9.

2. De lidstaat waar het geschillenbeslechtingsorgaan is gevestigd, certificeert dat orgaan op verzoek van dat orgaan, indien het heeft aangetoond dat het aan alle volgende voorwaarden voldoet:

   (a) het is onpartijdig en onafhankelijk en neemt zijn besluiten volgens een duidelijk en eerlijk reglement van orde;

   (b) het beschikt over de nodige deskundigheid met betrekking tot het vaststellen van eerlijke, redelijke en niet-discriminerende voorwaarden voor en transparante wijze van het beschikbaar stellen van data, zodat het die voorwaarden doeltreffend kan bepalen;

   (c) het is gemakkelijk toegankelijk via elektronische communicatietechnologie;

   (d) het kan snel, doeltreffend en kosteneffectief en in ten minste een van de officiële EU-talen een besluit uitvaardigen.

   Indien uiterlijk op [datum van toepassing van de verordening] geen geschillenbeslechtingsorgaan in een lidstaat is gecertificeerd, richt die lidstaat een geschillenbeslechtingsorgaan op dat voldoet aan de voorwaarden van de punten a) tot en met d) van dit lid en certificeert dat orgaan.

3. De lidstaten stellen de Commissie in kennis van de overeenkomstig lid 2 gecertificeerde geschillenbeslechtingsorganen. De Commissie publiceert een lijst van deze organen op een speciale website en houdt deze actueel.

4. De geschillenbeslechtingsorganen stellen de betrokken partijen in kennis van de vergoedingen of van de mechanismen om de vergoedingen vast te stellen, voordat die partijen om een besluit verzoeken.

5. Geschillenbeslechtingsorganen weigeren een verzoek om beslechting van een geschil dat al voor een ander geschillenbeslechtingsorgaan of voor een rechterlijke instantie van een lidstaat is gebracht.

6. De geschillenbeslechtingsorganen bieden de partijen de mogelijkheid om binnen een redelijke termijn hun standpunt over aangelegenheden die zij bij die instanties aanhangig hebben gemaakt, kenbaar te maken. In dat verband verstrekken de geschillenbeslechtingsorganen deze partijen de opmerkingen van de andere partij en eventuele deskundigenverklaringen. De organen bieden de partijen de mogelijkheid op deze opmerkingen en verklaringen te reageren.

7. De geschillenbeslechtingsorganen nemen hun besluit uiterlijk 90 dagen nadat het verzoek om een besluit is ingediend. Deze besluiten worden schriftelijk of op een duurzame drager opgesteld en worden met een motivering gestaafd.

8. Het besluit van het geschillenbeslechtingsorgaan is alleen bindend voor de partijen indien de partijen vóór aanvang van de geschillenbeslechtingsprocedure uitdrukkelijk hebben ingestemd met het bindende karakter ervan.

9. Dit artikel doet geen afbreuk aan het recht van de partijen om een doeltreffende voorziening in rechte in te stellen bij een rechterlijke instantie van een lidstaat.

Artikel 11

Technische beschermingsmaatregelen en bepalingen inzake ongeoorloofd gebruik of ongeoorloofde openbaarmaking van data

1. De datahouder kan passende technische beschermingsmaatregelen treffen, zoals slimme contracten, om ongeoorloofde toegang tot de data te voorkomen en de naleving van de artikelen 5, 6, 9 en 10 en van de overeengekomen contractuele voorwaarden voor het beschikbaar stellen van data te waarborgen. Dergelijke technische beschermingsmaatregelen mogen niet worden gebruikt als middel om het recht van de gebruiker te belemmeren om op doeltreffende wijze data aan derde partijen te verstrekken overeenkomstig artikel 5 of enig recht van een derde partij uit hoofde van het EU-recht of nationale wetgeving tot uitvoering van het EU-recht als bedoeld in artikel 8, lid 1.

2. Een ontvanger van data die met het oog op het verkrijgen van data onjuiste of valse informatie aan de datahouder heeft verstrekt, bedrieglijke of dwingende middelen heeft ingezet of kennelijke leemten in de technische infrastructuur van de datahouder ter bescherming van de data heeft misbruikt, de data die ter beschikking zijn gesteld voor ongeoorloofde doeleinden heeft gebruikt of deze data zonder toestemming van de datahouder aan een andere partij heeft verstrekt, doet onverwijld het volgende, tenzij de datahouder of de gebruiker anderszins instructies geeft:

   (a) de door de datahouder beschikbaar gestelde data en kopieën daarvan vernietigen;

   (b) een einde maken aan het produceren, aanbieden, in de handel brengen of gebruiken van goederen, afgeleide data of diensten die zijn geproduceerd op basis van de via die data verkregen kennis, of aan het invoeren, uitvoeren of

opslaan van inbreukmakende goederen voor die doeleinden, en inbreukmakende goederen vernietigen.

3. Lid 2, punt b), is niet van toepassing in de volgende gevallen:

   (a) het gebruik van de data heeft de datahouder geen ernstige schade berokkend;

   (b) het zou onevenredig zijn, gezien de belangen van de datahouder.

Artikel 12

Reikwijdte van de verplichtingen voor datahouders die wettelijk verplicht zijn om data beschikbaar te stellen

1. Dit hoofdstuk is van toepassing wanneer een datahouder krachtens artikel 5 of krachtens het EU-recht of krachtens nationale wetgeving tot uitvoering van het EU-recht verplicht is data ter beschikking te stellen aan een ontvanger van data.

2. Contractuele voorwaarden in een overeenkomst inzake het delen van data die, ten nadele van een partij of, in voorkomend geval, ten nadele van de gebruiker, de toepassing van dit hoofdstuk uitsluiten, daarvan afwijken of de gevolgen ervan wijzigen, zijn voor die partij niet bindend.

3. Dit hoofdstuk is alleen van toepassing op verplichtingen om data beschikbaar te stellen uit hoofde van het EU-recht of van nationale wetgeving tot omzetting van het EU-recht, die in werking treden na [datum van toepassing van de verordening].

HOOFDSTUK IV
ONEERLIJKE BEDINGEN MET BETREKKING TOT DE TOEGANG TOT EN HET GEBRUIK VAN DATA TUSSEN ONDERNEMINGEN

Artikel 13

Oneerlijke contractuele bedingen die eenzijdig worden opgelegd aan een micro-, kleine of middelgrote onderneming

1. Een contractueel beding betreffende de toegang tot en het gebruik van data of de aansprakelijkheid en rechtsmiddelen in geval van schending of beëindiging van datagerelateerde verplichtingen die eenzijdig door een onderneming zijn opgelegd aan een micro-, kleine of middelgrote onderneming in de zin van artikel 2 van de bijlage bij Aanbeveling 2003/361/EG, is niet bindend voor laatstgenoemde onderneming indien deze oneerlijk is.

2. Een contractueel beding is oneerlijk wanneer het beding van dien aard is dat het gebruik ervan sterk afwijkt van de goede handelspraktijken bij de toegang tot en het gebruik van data, en indruist tegen de beginselen van goede trouw en billijke handel.

3. Een contractueel beding is oneerlijk in de zin van dit artikel indien dat beding het volgende tot doel of gevolg heeft:

   (a) de partij die het beding eenzijdig heeft opgelegd, draagt geen of beperkte aansprakelijkheid voor opzettelijke handelingen of grove nalatigheid;

   (b) de partij aan wie het beding eenzijdig is opgelegd, wordt uitgesloten van de rechtsmiddelen waarover deze beschikt in geval van niet-nakoming van contractuele verplichtingen of de partij die het beding eenzijdig heeft opgelegd,

draagt geen aansprakelijkheid in geval van niet-nakoming van die verplichtingen;

(c) de partij die het beding eenzijdig heeft opgelegd beschikt over het exclusieve recht om te bepalen of de verstrekte data in overeenstemming zijn met de overeenkomst of om een bepaling van de overeenkomst uit te leggen.

4. Een contractueel beding wordt geacht oneerlijk te zijn in de zin van dit artikel indien het ertoe strekt of tot gevolg heeft dat:

(a) de rechtsmiddelen in geval van niet-nakoming van contractuele verplichtingen of de aansprakelijkheid in geval van niet-nakoming van die verplichtingen op ongepaste wijze worden beperkt;

(b) de partij die het beding eenzijdig heeft opgelegd, toegang kan krijgen tot en gebruik kan maken van data van de andere overeenkomstsluitende partij op een wijze die de rechtmatige belangen van de andere overeenkomstsluitende partij aanzienlijk schaadt;

(c) de partij aan wie het beding eenzijdig is opgelegd, wordt verhinderd de door die partij tijdens de looptijd van de overeenkomst aangeleverde of gegenereerde data te gebruiken, of het gebruik van dergelijke data in die mate wordt beperkt dat die partij niet het recht heeft deze data te gebruiken, te verzamelen, er toegang toe te geven of de waarde van die data op evenredige wijze te exploiteren;

(d) de partij aan wie het beding eenzijdig is opgelegd, wordt verhinderd tijdens de looptijd van de overeenkomst of binnen een redelijke termijn na de beëindiging van de overeenkomst een kopie van de door die partij aangeleverde of gegenereerde data te verkrijgen;

(e) de partij die de termijn eenzijdig heeft opgelegd, de overeenkomst met een onredelijk korte termijn kan opzeggen, rekening houdend met de redelijke mogelijkheden van de andere overeenkomstsluitende partij om over te schakelen op een alternatieve en vergelijkbare dienst en met de financiële schade die door deze beëindiging wordt berokkend, tenzij er gewichtige redenen zijn om dit te doen.

5. Een beding in een overeenkomst wordt geacht eenzijdig te zijn opgelegd in de zin van dit artikel indien het door een van de overeenkomstsluitende partijen is gesteld en de andere partij ondanks een poging om daarover te onderhandelen geen invloed op de inhoud ervan heeft kunnen uitoefenen. De overeenkomstsluitende partij die een contractueel beding heeft gesteld, moet bewijzen dat dit beding niet eenzijdig is opgelegd.

6. Wanneer het oneerlijke beding van de overeenkomst kan worden gescheiden van de overige bedingen van de overeenkomst, blijven die resterende bedingen bindend.

7. Dit artikel is niet van toepassing op contractuele bedingen waarin het eigenlijke onderwerp van de overeenkomst wordt omschreven, noch op contractuele voorwaarden die de te betalen prijs bepalen.

8. De partijen bij een overeenkomst als bedoeld in lid 1 mogen de toepassing van dit artikel niet uitsluiten, daarvan afwijken of de gevolgen ervan wijzigen.

HOOFDSTUK V
DATA BESCHIKBAAR STELLEN AAN

OVERHEIDSINSTANTIES EN EU-INSTELLINGEN, -AGENTSCHAPPEN OF -ORGANEN OP GROND VAN UITZONDERLIJKE NOODZAAK

Artikel 14

Verplichting om data beschikbaar te stellen op grond van uitzonderlijke noodzaak

1. Een datahouder stelt op verzoek data ter beschikking aan een overheidsinstantie of een EU-instelling, -agentschap of -orgaan wanneer is aangetoond dat er een uitzonderlijke noodzaak bestaat om de gevraagde data te gebruiken.

2. Dit hoofdstuk is niet van toepassing op kleine en micro-ondernemingen in de zin van artikel 2 van de bijlage bij Aanbeveling 2003/361/EG.

Artikel 15

Uitzonderlijke noodzaak om data te gebruiken

Een uitzonderlijke noodzaak om data te gebruiken in de zin van dit hoofdstuk wordt geacht te bestaan wanneer er sprake is van een van de volgende omstandigheden:

(a) wanneer de gevraagde data noodzakelijk zijn om te reageren op een algemene noodsituatie;

(b) wanneer het verzoek om data beperkt is in tijd en reikwijdte en noodzakelijk is om een algemene noodsituatie te voorkomen of om het herstel na een algemene noodsituatie te ondersteunen;

(c) wanneer het gebrek aan beschikbare data de overheidsinstantie of de EU-instelling, het EU-agentschap of het EU-orgaan belet een specifieke taak van algemeen belang te vervullen waarin de wet uitdrukkelijk voorziet; en

(1) de overheidsinstantie of de EU-instelling, het EU-agentschap of het EU-orgaan niet in staat is geweest dergelijke data met alternatieve middelen te verkrijgen, onder meer door de data op de markt tegen markttarieven aan te kopen of door gebruik te maken van bestaande verplichtingen om data beschikbaar te stellen, en de vaststelling van nieuwe wetgevingsmaatregelen de tijdige beschikbaarheid van de data niet kan waarborgen; of

(2) het verkrijgen van de data volgens de procedure van dit hoofdstuk de administratieve lasten voor datahouders of andere ondernemingen aanzienlijk zou verminderen.

Artikel 16

Verband met andere verplichtingen om data beschikbaar te stellen aan overheidsinstanties en EU-instellingen, -agentschappen en -organen

1. Dit hoofdstuk doet geen afbreuk aan de in het EU-recht of het nationale recht vastgestelde verplichtingen met betrekking tot rapportage, het voldoen aan informatieverzoeken of het aantonen of verifiëren van de naleving van wettelijke verplichtingen.

2. De rechten uit hoofde van dit hoofdstuk worden niet uitgeoefend door overheidsinstanties en EU-instellingen, -agentschappen en -organen om activiteiten

uit te voeren met het oog op het voorkomen, onderzoeken, opsporen en vervolgen van strafrechtelijke of administratieve inbreuken of de tenuitvoerlegging van straffen, of ten behoeve van de douane- of belastingadministratie. Dit hoofdstuk doet geen afbreuk aan het toepasselijke EU-recht en het toepasselijke nationale recht inzake het voorkomen, onderzoeken, opsporen en vervolgen van strafrechtelijke of administratieve inbreuken of de tenuitvoerlegging van strafrechtelijke of administratieve sancties, of inzake de douane- of belastingadministratie.

Artikel 17
Verzoeken om data beschikbaar te stellen

1. Wanneer overheidsinstanties of EU-instellingen, -agentschappen of -organen om data overeenkomstig artikel 14, lid 1, verzoeken:

   (a) specificeren zij welke data vereist zijn;

   (b) tonen zij aan dat het verzoek om data gebeurt op grond van een uitzonderlijke noodzaak;

   (c) lichten zij het doel van het verzoek, het beoogde gebruik van de gevraagde data en de duur van dat gebruik toe;

   (d) vermelden zij de rechtsgrondslag voor het opvragen van de data;

   (e) specificeren zij binnen welke termijn de data beschikbaar moeten worden gesteld of binnen welke termijn de datahouder de overheidsinstantie, de EU-instelling, het EU-agentschap of -orgaan kan verzoeken het verzoek te wijzigen of in te trekken.

2. Een verzoek om data op grond van lid 1 van dit artikel:

   (a) wordt uitgedrukt in duidelijke, beknopte en eenvoudige taal die voor de datahouder begrijpelijk is;

   (b) staat in verhouding tot de uitzonderlijke noodzaak, wat betreft de mate van detail en het volume van de gevraagde data en de frequentie van de toegang tot de gevraagde data;

   (c) eerbiedigt de legitieme doelstellingen van de datahouder, rekening houdend met de bescherming van bedrijfsgeheimen en de kosten en inspanningen die nodig zijn om de data beschikbaar te stellen;

   (d) heeft voor zover mogelijk betrekking op niet-persoonsgebonden data;

   (e) stelt de datahouder in kennis van de sancties die overeenkomstig artikel 33 door een in artikel 31 bedoelde bevoegde autoriteit worden opgelegd in geval van niet-naleving van het verzoek;

   (f) wordt onverwijld online beschikbaar gesteld voor het publiek.

3. Een overheidsinstantie of een EU-instelling, -agentschap of -orgaan stelt de op grond van dit hoofdstuk verkregen data niet beschikbaar voor hergebruik in de zin van Richtlijn (EU) 2019/1024. Richtlijn (EU) 2019/1024 is niet van toepassing op de data die overheidsinstanties op grond van dit hoofdstuk in handen hebben gekregen.

4. Lid 3 belet een overheidsinstantie of een EU-instelling, -agentschap of -orgaan niet om op grond van dit hoofdstuk verkregen data uit te wisselen met een andere overheidsinstantie of een EU-instelling, -agentschap of -orgaan, met het oog op de vervulling van de taken in artikel 15, of om de data beschikbaar te stellen aan een

derde partij in gevallen waarin het door middel van een openbaar beschikbare overeenkomst technische inspecties of andere taken aan die derde partij heeft uitbesteed. De verplichtingen van overheidsinstanties, EU-instellingen, -agentschappen of -organen uit hoofde van artikel 19 zijn van toepassing.

Wanneer overheidsinstanties of EU-instellingen, -agentschappen of -organen data uit hoofde van dit lid doorgeeft of beschikbaar stelt, stellen zijde datahouder van wie de data zijn ontvangen daarvan in kennis.

Artikel 18
Naleving van verzoeken om data

1. Een datahouder die een verzoek om toegang tot data uit hoofde van dit hoofdstuk ontvangt, stelt de data onverwijld ter beschikking van de verzoekende overheidsinstantie of EU-instelling, -agentschap of -orgaan.

2. Onverminderd specifieke noodzaak in verband met de beschikbaarheid van data als omschreven in sectorale wetgeving, kan de datahouder het verzoek afwijzen of verzoeken om wijziging van het verzoek, en dit binnen vijf werkdagen na ontvangst van een verzoek om de data die noodzakelijk zijn om te reageren op een algemene noodsituatie, en binnen 15 werkdagen in andere gevallen van uitzonderlijke noodzaak, om een van de volgende redenen:

   (a) de data zijn niet beschikbaar;

   (b) het verzoek voldoet niet aan de voorwaarden van artikel 17, lid 1 en 2.

3. In geval van een verzoek om data die nodig zijn om te reageren op een algemene noodsituatie, kan de datahouder het verzoek ook afwijzen of vragen om wijziging ervan, indien de datahouder de gevraagde data reeds heeft verstrekt in antwoord op een eerder ingediend verzoek met hetzelfde doel door een andere overheidsinstantie of een andere EU-instelling, -agentschap of -orgaan en de datahouder niet in kennis is gesteld van de vernietiging van de data overeenkomstig artikel 19, lid 1, punt c).

4. Indien de datahouder besluit het verzoek af te wijzen of te verzoeken het te wijzigen overeenkomstig lid 3, vermeldt hij de identiteit van de overheidsinstantie of de EU-instelling, het EU-agentschap of EU-orgaan dat of die eerder een verzoek met hetzelfde doel heeft ingediend.

5. Indien persoonsgegevens moeten worden verstrekt om het verzoek om data van een overheidsinstantie of een EU-instelling, -agentschap of -orgaan in te willigen, levert de datahouder redelijke inspanningen om de data te pseudonimiseren, voor zover aan het verzoek kan worden voldaan met gepseudonimiseerde data.

6. Indien de overheidsinstantie of de EU-instelling, het EU-agentschap of -orgaan de weigering van een datahouder om de gevraagde data te verstrekken of diens verzoek tot wijziging van het verzoek wil aanvechten, of indien de datahouder het verzoek wenst aan te vechten, wordt de zaak voorgelegd aan de in artikel 31 bedoelde bevoegde autoriteit.

Artikel 19
Verplichtingen van overheidsinstanties en EU-instellingen, -agentschappen en -organen

1. Overheidsinstanties of EU-instellingen, -agentschappen of -organen die op grond van een verzoek uit hoofde van artikel 14 data hebben ontvangen:

(a) gebruiken de data niet op een wijze die onverenigbaar is met het doel waarvoor zij zijn gevraagd;

(b) treffen, voor zover de verwerking van persoonsgegevens noodzakelijk is, technische en organisatorische maatregelen die de rechten en vrijheden van de betrokkenen waarborgen;

(c) vernietigen de data zodra zij niet langer nodig zijn voor het aangegeven doel en stellen de datahouder ervan in kennis stellen dat de data zijn vernietigd.

2. De openbaarmaking van bedrijfsgeheimen of vermeende bedrijfsgeheimen aan een overheidsinstantie of een EU-instelling, -agentschap of -orgaan is alleen vereist voor zover dit strikt noodzakelijk is om het doel van het verzoek te verwezenlijken. In dat geval neemt de overheidsinstantie of de EU-instelling, het EU-agentschap of -orgaan passende maatregelen om de vertrouwelijkheid van die bedrijfsgeheimen te waarborgen.

Artikel 20
Compensatie in geval van uitzonderlijke noodzaak

1. Data die beschikbaar worden gesteld met als doel te reageren op een algemene noodsituatie overeenkomstig artikel 15, punt a), worden kosteloos verstrekt.

2. Indien de datahouder een vergoeding eist voor het beschikbaar stellen van data naar aanleiding van een verzoek overeenkomstig artikel 15, punt b) of c), mag die vergoeding niet hoger zijn dan de technische en organisatorische kosten die zijn gemaakt om aan het verzoek te voldoen, met inbegrip van, indien nodig, de kosten van anonimisering en technische aanpassing, vermeerderd met een redelijke marge. Op verzoek van de overheidsinstantie of de EU-instelling, het EU-agentschap of -orgaan die of dat om de data verzoekt, verstrekt de datahouder informatie over de grondslag voor de berekening van de kosten en de redelijke marge.

Artikel 21
Bijdrage van onderzoeksorganisaties of bureaus voor de statistiek in de context van een uitzonderlijke noodzaak

1. Een overheidsinstantie of een EU-instelling, -agentschap of -orgaan heeft het recht uit hoofde van dit hoofdstuk ontvangen data te delen met personen of organisaties met het oog op het uitvoeren van wetenschappelijk onderzoek of analyses die verenigbaar zijn met het doel waarvoor de data werden gevraagd, of aan nationale bureaus voor de statistiek en Eurostat voor het opstellen van officiële statistieken.

2. Personen of organisaties die de data overeenkomstig lid 1 ontvangen, handelen zonder winstoogmerk of in het kader van een in het EU-recht of het nationale recht van een lidstaat erkende taak van algemeen belang. Hieronder vallen niet organisaties waarop commerciële ondernemingen een beslissende invloed uitoefenen of die kunnen leiden tot preferentiële toegang tot de resultaten van het onderzoek.

3. Personen of organisaties die de data overeenkomstig lid 1 ontvangen, voldoen aan de bepalingen van artikel 17, lid 3, en artikel 19.

4. Wanneer een overheidsinstantie of een EU-instelling, -agentschap of -orgaan data uit hoofde van lid 1 doorgeeft of beschikbaar stelt, stelt deze de datahouder van wie de data zijn ontvangen daarvan in kennis.

Artikel 22

Wederzijdse bijstand en grensoverschrijdende samenwerking

1. Overheidsinstanties of EU-instellingen, -agentschappen of -organen werken samen en staan elkaar bij om dit hoofdstuk op consistente wijze uit te voeren.

2. Alle data die in het kader van de verzochte bijstand worden uitgewisseld en verstrekt overeenkomstig lid 1, worden uitsluitend gebruikt voor het doel waarvoor zij zijn aangevraagd.

3. Wanneer een overheidsinstantie voornemens is data op te vragen van een datahouder die in een andere lidstaat is gevestigd, stelt deze eerst de in artikel 31 bedoelde bevoegde autoriteit van die lidstaat van dat voornemen in kennis. Dit vereiste geldt ook voor verzoeken van EU-instellingen, -agentschappen en -organen.

4. Nadat de relevante bevoegde autoriteit overeenkomstig lid 3 in kennis is gesteld, adviseert deze de verzoekende overheidsinstantie over de eventuele noodzaak om samen te werken met overheidsinstanties van de lidstaat waar de datahouder is gevestigd, teneinde de administratieve lasten voor de datahouder bij de uitvoering van het verzoek te verlichten. De verzoekende overheidsinstantie houdt rekening met het advies van de relevante bevoegde autoriteit.

HOOFDSTUK VI

OVERSTAPPEN NAAR ANDERE DATAVERWERKINGSDIENSTEN

Artikel 23

Belemmeringen voor een doeltreffende overstap naar andere aanbieders van dataverwerkingsdiensten wegnemen

1. Aanbieders van dataverwerkingsdiensten nemen de in de artikelen 24, 25 en 26 bedoelde maatregelen om ervoor te zorgen dat de klanten van hun dienst kunnen overstappen naar een andere dataverwerkingsdienst van hetzelfde type die door een andere dienstverlener wordt verleend. Aanbieders van dataverwerkingsdiensten dienen met name commerciële, technische, contractuele en organisatorische belemmeringen weg te nemen die klanten beletten:

   (a) na een opzegtermijn van maximaal 30 kalenderdagen de contractuele overeenkomst van de dienst op te zeggen;

   (b) nieuwe contractuele overeenkomsten met een andere aanbieder van dataverwerkingsdiensten voor hetzelfde soort diensten te sluiten;

   (c) zijn of haar data, toepassingen en andere digitale activa aan een andere aanbieder van dataverwerkingsdiensten over te dragen;

   (d) de functionele gelijkwaardigheid van de dienst in de IT-omgeving van de verschillende aanbieders van dataverwerkingsdiensten voor hetzelfde type dienst te handhaven, overeenkomstig artikel 26.

2. Lid 1 is alleen van toepassing op belemmeringen die verband houden met de diensten, contractuele overeenkomsten of handelspraktijken van de oorspronkelijke aanbieder.

Artikel 24

Contractvoorwaarden betreffende een overstap naar andere aanbieders van dataverwerkingsdiensten

1. De rechten van de klant en de verplichtingen van de aanbieder van een dataverwerkingsdienst met betrekking tot het overstappen naar andere aanbieders van dergelijke diensten worden duidelijk vastgelegd in een schriftelijk contract. Onverminderd Richtlijn (EU) 2019/770 omvat dit contract ten minste het volgende:

   (a) bepalingen op grond waarvan de klant, op verzoek, kan overstappen naar een dataverwerkingsdienst die wordt aangeboden door een andere aanbieder van dataverwerkingsdiensten of op grond waarvan de klant alle data, toepassingen en digitale activa die direct of indirect door de klant worden gegenereerd, kan overdragen naar een on-premise-systeem, met name de vaststelling van een verplichte maximale overgangsperiode van 30 kalenderdagen, waarbinnen de aanbieder van dataverwerkingsdiensten:

      (1) het overstapproces ondersteunt en, indien technisch haalbaar, voltooit;

      (2) zorgt voor volledige continuïteit bij de verlening van de respectieve functies of diensten;

   (b) een volledige specificatie van alle data- en toepassingscategorieën die tijdens het overstapproces exporteerbaar zijn, waaronder ten minste alle data die door de klant bij het aangaan van de dienstenovereenkomst zijn ingevoerd en alle data en metadata die in de periode waarin de dienst werd verleend door de klant en door het gebruik van de dienst zijn gecreëerd, waaronder, maar niet beperkt tot, configuratieparameters, beveiligingsinstellingen, toegangsrechten en toegangslogs voor de dienst;

   (c) een minimumtermijn voor het opvragen van data van ten minste 30 kalenderdagen, beginnend na de beëindiging van de overgangsperiode die is overeengekomen tussen de klant en de dienstverlener, overeenkomstig lid 1, punt a), en lid 2.

2. Wanneer de verplichte overgangsperiode als gedefinieerd in lid 1, punten a) en c), van dit artikel technisch niet haalbaar is, stelt de aanbieder van dataverwerkingsdiensten de klant daarvan in kennis binnen 7 werkdagen na het overstapverzoek , met een gedetailleerde motivering van de technische onhaalbaarheid en met vermelding van een alternatieve overgangsperiode, die niet langer mag zijn dan 6 maanden. Overeenkomstig lid 1 van dit artikel wordt de volledige continuïteit van de dienstverlening gewaarborgd gedurende de gehele alternatieve overgangsperiode tegen verlaagde tarieven, als bedoeld in artikel 25, lid 2.

Artikel 25

Geleidelijke afschaffing van de overstapkosten

1. Vanaf [datum X + 3 jaar] brengen aanbieders van dataverwerkingsdiensten de klant geen kosten in rekening voor het overstapproces.

2. Vanaf [datum X, de datum van inwerkingtreding van de dataverordening] tot en met [datum X + 3 jaar] kunnen aanbieders van dataverwerkingsdiensten de klant lagere kosten voor het overstapproces opleggen.

3. De in lid 2 bedoelde kosten mogen niet hoger zijn dan de kosten van de aanbieder van dataverwerkingsdiensten die rechtstreeks verband houden met het betrokken overstapproces.

4. De Commissie is bevoegd overeenkomstig artikel 38 gedelegeerde handelingen vast te stellen teneinde deze verordening aan te vullen met het oog op de invoering van een toezichtmechanisme waarmee de Commissie toezicht kan houden op de door aanbieders van dataverwerkingsdiensten op de markt opgelegde overstaptarieven om ervoor te zorgen dat de in lid 1 van dit artikel beschreven afschaffing van de overstaptarieven binnen de in hetzelfde lid vastgestelde termijn wordt verwezenlijkt.

Artikel 26
Technische aspecten van een overstap

1. Aanbieders van dataverwerkingsdiensten die betrekking hebben op schaalbare en elastische computermiddelen die beperkt zijn tot infrastructurele elementen zoals servers, netwerken en de virtuele hulpbronnen die nodig zijn voor de exploitatie van de infrastructuur, maar die geen toegang bieden tot de operationele diensten, software en toepassingen die worden opgeslagen, anderszins verwerkt of op die infrastructurele elementen worden ingezet, zorgen ervoor dat de klant, nadat hij of zij overschakelt op een dienst van hetzelfde type die door een andere aanbieder van dataverwerkingsdiensten wordt aangeboden, functionele gelijkwaardigheid geniet bij het gebruik van de nieuwe dienst.

2. Voor dataverwerkingsdiensten die niet onder lid 1 vallen, stellen aanbieders van dataverwerkingsdiensten open interfaces kosteloos ter beschikking.

3. Voor andere dataverwerkingsdiensten dan die welke onder lid 1 vallen, zorgen aanbieders van dataverwerkingsdiensten voor compatibiliteit met open interoperabiliteitsspecificaties of Europese interoperabiliteitsnormen die zijn vastgesteld overeenkomstig artikel 29, lid 5, van deze verordening.

4. Wanneer de in lid 3 bedoelde open interoperabiliteitsspecificaties of Europese normen voor het betrokken type dienst niet bestaan, exporteert de aanbieder van dataverwerkingsdiensten op verzoek van de klant alle gegenereerde of medegegenereerde data, met inbegrip van de relevante dataformaten en datastructuren, in een gestructureerd, algemeen gebruikt en machineleesbaar formaat.

HOOFDSTUK VII
INTERNATIONALE CONTEXTEN MET BETREKKING TOT NIET-PERSOONSGEBONDEN DATA

Artikel 27
Internationale toegang en overdracht

1. Aanbieders van dataverwerkingsdiensten nemen alle redelijke technische, juridische en organisatorische maatregelen, waaronder contractuele regelingen, om internationale overdracht of toegang van de overheid tot niet-persoonsgebonden data die in de EU zijn opgeslagen, te voorkomen wanneer die doorgifte of toegang in strijd zou zijn met het EU-recht of het nationale recht van de betrokken lidstaat, onverminderd lid 2 of lid 3.

2. Elk besluit of elke rechterlijke uitspraak en elke beslissing van een administratieve autoriteit van een derde land op grond waarvan een verlener van dataverwerkingsdiensten niet-persoonsgebonden data die binnen het toepassingsgebied van deze verordening vallen en in de EU zijn opgeslagen, moet overdragen of er toegang toe moet verlenen, mag alleen op enigerlei wijze worden erkend of afdwingbaar zijn indien het besluit, de uitspraak of de beslissing gebaseerd is op een internationale overeenkomst, zoals een verdrag inzake wederzijdse rechtsbijstand, die van kracht is tussen het verzoekende derde land en de EU of op een dergelijke overeenkomst tussen het verzoekende derde land en een lidstaat.

3. Indien een dergelijke internationale overeenkomst ontbreekt en een aanbieder van dataverwerkingsdiensten de geadresseerde is van een besluit van een rechterlijke instantie of een administratieve autoriteit van een derde land om niet-persoonsgebonden data die binnen het toepassingsgebied van deze verordening vallen en in de EU worden bewaard, over te dragen of er toegang toe te geven en de naleving van een dergelijk besluit de geadresseerde in strijd zou kunnen brengen met het EU-recht of het nationale recht van de betrokken lidstaat, mag de overdracht van die data aan of de toegang tot die data door die autoriteit van het derde land alleen plaatsvinden:

   (a) wanneer het systeem van het derde land voorschrijft dat de redenen voor en de evenredigheid van het besluit worden toegelicht, en dat het vonnis of besluit van de rechtbank, al naargelang het geval, een specifiek karakter heeft, bijvoorbeeld door een voldoende verband te leggen met bepaalde verdachten of inbreuken;

   (b) wanneer het met redenen omklede bezwaar van de geadresseerde wordt getoetst door een bevoegde rechterlijke instantie in het derde land; en

   (c) wanneer in die context de bevoegde rechterlijke instantie die het besluit of vonnis velt of het besluit van een administratieve autoriteit toetst, uit hoofde van het recht van dat land gemachtigd is om rekening te houden met de relevante juridische belangen van de verstrekker van de data die door het EU-recht of het toepasselijke recht van de lidstaat worden beschermd.

De geadresseerde van het besluit kan de relevante bevoegde instanties of autoriteiten uit hoofde van deze verordening om advies vragen om te bepalen of aan deze voorwaarden is voldaan, met name wanneer hij of zij van mening is dat het besluit betrekking kan hebben op commercieel gevoelige data of afbreuk kan doen aan de nationale veiligheids- of defensiebelangen van de EU of haar lidstaten.

De bij Verordening [xxx — DGA] opgerichte Europese raad voor gegevensinnovatie adviseert en assisteert de Commissie bij het opstellen van richtsnoeren voor de beoordeling van de vraag of aan deze voorwaarden is voldaan.

4. Indien aan de voorwaarden van lid 2 of lid 3 is voldaan, verstrekt de aanbieder van dataverwerkingsdiensten de minimaal toegestane hoeveelheid data in antwoord op een verzoek, op basis van een redelijke interpretatie daarvan.

5. De aanbieder van dataverwerkingsdiensten stelt de datahouder in kennis van het bestaan van een verzoek van een administratieve autoriteit in een derde land om toegang tot zijn of haar data te krijgen, alvorens aan dit verzoek te voldoen, behalve in gevallen waarin het verzoek rechtshandhavingsdoeleinden dient en zolang dit noodzakelijk is om de doeltreffendheid van de rechtshandhavingsactiviteiten te waarborgen.

HOOFDSTUK VIII
INTEROPERABILITEIT

Artikel 28
Essentiële eisen inzake interoperabiliteit

1. Exploitanten van dataruimten voldoen aan de volgende essentiële eisen om de interoperabiliteit van data, mechanismen en diensten voor data-uitwisseling te vergemakkelijken:

   (a) de inhoud van de dataset, gebruiksbeperkingen, licenties, dataverzamelingsmethoden, datakwaliteit en onzekerheid worden voldoende beschreven om de ontvanger in staat te stellen de data te vinden, te raadplegen en te gebruiken;

   (b) de datastructuren, dataformaten, vocabularia, classificatieschema's, taxonomieën en codelijsten worden op een voor het publiek toegankelijke en consistente wijze beschreven;

   (c) de technische middelen om toegang te krijgen tot de data, zoals applicatieprogramma-interfaces, en de gebruiksvoorwaarden en de kwaliteit van de dienstverlening worden voldoende beschreven om automatische toegang tot en overdracht van data tussen partijen mogelijk te maken, ook continu of in realtime in een machineleesbaar formaat;

   (d) er wordt voorzien in de middelen om de interoperabiliteit van slimme contracten binnen hun diensten en activiteiten mogelijk te maken.

Deze eisen kunnen een generiek karakter hebben of betrekking hebben op specifieke sectoren, waarbij ten volle rekening wordt gehouden met de samenhang met eisen die voortvloeien uit andere sectorale wetgeving van de EU of de lidstaten.

2. De Commissie is bevoegd overeenkomstig artikel 38 gedelegeerde handelingen tot aanvulling van deze richtlijn vast te stellen door de essentiële eisen in lid 1 van dit artikel verder te specificeren.

3. Exploitanten van dataruimten die voldoen aan de geharmoniseerde normen of delen daarvan die onder verwijzing in het Publicatieblad van de Europese Unie zijn bekendgemaakt, worden geacht in overeenstemming te zijn met de in lid 1 van dit artikel bedoelde essentiële eisen, voor zover die normen deze eisen dekken.

4. De Commissie kan overeenkomstig artikel 10 van Verordening (EU) nr. 1025/2012 een of meer Europese normalisatieorganisaties verzoeken geharmoniseerde normen op te stellen die voldoen aan de essentiële eisen in lid 1 van dit artikel.

5. De Commissie stelt door middel van uitvoeringshandelingen gemeenschappelijke specificaties vast wanneer er geen geharmoniseerde normen als bedoeld in lid 4 van dit artikel bestaan of indien zij van oordeel is dat de relevante geharmoniseerde normen ontoereikend zijn om de conformiteit met de essentiële eisen in lid 1 van dit artikel te waarborgen, indien nodig met betrekking tot een of meer van de in lid 1 van dit artikel vastgestelde eisen. Die uitvoeringshandelingen worden volgens de in artikel 39, lid 2, bedoelde onderzoeksprocedure vastgesteld.

6. De Commissie kan richtsnoeren aannemen waarin interoperabiliteitsspecificaties voor de werking van gemeenschappelijke Europese dataruimten worden vastgesteld, zoals architectuurmodellen en technische normen tot uitvoering van wettelijke

voorschriften en regelingen tussen partijen die de uitwisseling van data bevorderen, bijvoorbeeld met betrekking tot het recht op toegang en technische vertaling van instemming of toestemming.

Artikel 29

Interoperabiliteit voor dataverwerkingsdiensten

1. Open interoperabiliteitsspecificaties en Europese normen voor de interoperabiliteit van dataverwerkingsdiensten voldoen aan het volgende:

   (a) zij zijn wat betreft prestaties gericht op het bereiken van interoperabiliteit tussen verschillende dataverwerkingsdiensten die hetzelfde type dienst bestrijken;

   (b) zij verbeteren de overdraagbaarheid van digitale activa tussen verschillende dataverwerkingsdiensten die hetzelfde type dienst bestrijken;

   (c) zij garanderen voor zover technisch haalbaar, de functionele gelijkwaardigheid tussen verschillende dataverwerkingsdiensten die hetzelfde type dienst bestrijken.

2. Open interoperabiliteitsspecificaties en Europese normen voor de interoperabiliteit van dataverwerkingsdiensten hebben betrekking op:

   (a) de aspecten van cloudinteroperabiliteit in het vervoer, syntactische interoperabiliteit, semantische data-interoperabiliteit, gedragsinteroperabiliteit en beleidsinteroperabiliteit;

   (b) de overdraagbaarheidsaspecten van clouddata inzake syntactische overdraagbaarheid, semantische overdraagbaarheid van data en overdraagbaarheid van het databeleid;

   (c) de cloudtoepassingsaspecten van applicatiesyntactische overdraagbaarheid, applicatie-instructieportabiliteit, overdraagbaarheid van applicatiemetadata, overdraagbaarheid van applicatiegedrag en overdraagbaarheid van het applicatiebeleid.

3. Open interoperabiliteitsspecificaties voldoen aan de punten 3 en 4 van bijlage II bij Verordening (EU) nr. 1025/2012.

4. De Commissie kan overeenkomstig artikel 10 van Verordening (EU) nr. 1025/2012 een of meer Europese normalisatieorganisaties verzoeken om Europese normen op te stellen die van toepassing zijn op specifieke diensttypes van dataverwerkingsdiensten.

5. Voor de toepassing van artikel 26, lid 3, van deze verordening is de Commissie bevoegd overeenkomstig artikel 38 gedelegeerde handelingen vast te stellen om de referentie bekend te maken van open interoperabiliteitsspecificaties en Europese normen voor de interoperabiliteit van dataverwerkingsdiensten in een centrale register voor EU-normen voor de interoperabiliteit van dataverwerkingsdiensten, indien deze voldoen aan de criteria van de leden 1 en 2 van dit artikel.

Artikel 30

Essentiële eisen met betrekking tot slimme contracten voor het delen van data

1. De verkoper van een applicatie die gebruik maakt van slimme contracten of, bij het ontbreken daarvan, de persoon wiens handels-, bedrijfs- of beroepsactiviteit de

invoering van slimme contracten voor anderen in het kader van een overeenkomst voor het beschikbaar stellen van data inhoudt, voldoet aan de volgende essentiële eisen:

(a) robuustheid: ervoor zorgen dat het slimme contract zo is ontworpen dat het een zeer hoge mate van robuustheid biedt om functionele fouten te voorkomen en manipulatie door derden te weerstaan;

(b) veilige beëindiging en onderbreking: ervoor zorgen dat er een mechanisme bestaat om de doorlopende uitvoering van transacties te beëindigen: het slimme contract omvat interne functies die het contract kunnen resetten of de opdracht kunnen geven de verrichting stop te zetten of te onderbreken om toekomstige (accidentele) uitvoering ervan te voorkomen;

(c) archivering en continuïteit van data: indien een slim contract moet worden beëindigd of gedeactiveerd, de mogelijkheid bieden om transactiedata, de slimme-contractlogica en -code te archiveren om de verrichtingen die in het verleden met betrekking tot de data zijn uitgevoerd, te registreren (controleerbaarheid); en

(d) toegangscontrole: een slim contract wordt beschermd door middel van strikte toegangscontrolemechanismen in de beheers- en slimme-contractlagen.

2. De verkoper van een slim contract of, bij het ontbreken daarvan, de persoon wiens handels-, bedrijfs- of beroepsactiviteit de invoering van slimme contracten voor anderen in het kader van een overeenkomst voor het beschikbaar stellen van data inhoudt, voert een conformiteitsbeoordeling uit om aan de essentiële eisen van lid 1 te voldoen en geeft, wanneer aan de eisen is voldaan, een EU-conformiteitsverklaring af.

3. Door een EU-conformiteitsverklaring af te geven is de verkoper van een applicatie die gebruik maakt van slimme contracten of, bij het ontbreken daarvan, de persoon wiens handels-, bedrijfs- of beroepsactiviteit de invoering van slimme contracten voor anderen in het kader van een overeenkomst voor het beschikbaar stellen van data inhoudt, verantwoordelijk voor de conformiteit met de eisen in lid 1.

4. Een slim contract dat voldoet aan de geharmoniseerde normen of de relevante delen daarvan die in het Publicatieblad van de Europese Unie zijn bekendgemaakt, worden geacht in overeenstemming te zijn met de essentiële eisen in lid 1 van dit artikel, voor zover die normen deze eisen dekken.

5. De Commissie kan overeenkomstig artikel 10 van Verordening (EU) nr. 1025/2012 een of meer Europese normalisatieorganisaties verzoeken geharmoniseerde normen op te stellen die voldoen aan de essentiële eisen in lid 1 van dit artikel.

6. Wanneer er geen geharmoniseerde normen als bedoeld in lid 4 van dit artikel bestaan of wanneer de Commissie van oordeel is dat de desbetreffende geharmoniseerde normen niet volstaan om de conformiteit met de essentiële eisen in lid 1 van dit artikel in een grensoverschrijdende context te waarborgen, kan de Commissie door middel van uitvoeringshandelingen gemeenschappelijke specificaties vaststellen met betrekking tot de in lid 1 van dit artikel bedoelde essentiële eisen. Die uitvoeringshandelingen worden volgens de in artikel 39, lid 2, bedoelde onderzoeksprocedure vastgesteld.

HOOFDSTUK IX
UITVOERING EN HANDHAVING

Artikel 31
Bevoegde autoriteiten

1. Elke lidstaat wijst een of meer voor de uitvoering en handhaving van deze verordening bevoegde autoriteiten aan. De lidstaten kunnen een of meer nieuwe autoriteiten oprichten of een beroep doen op bestaande autoriteiten.

2. Onverminderd lid 1 van dit artikel:

   (a) zijn de onafhankelijke toezichthoudende autoriteiten die belast zijn met het toezicht op de toepassing van Verordening (EU) 2016/679 verantwoordelijk voor het toezicht op de toepassing van deze verordening wat de bescherming van persoonsgegevens betreft. De hoofdstukken VI en VII van Verordening (EG) 2016/679 zijn mutatis mutandis van toepassing. De taken en bevoegdheden van de toezichthoudende autoriteiten worden uitgeoefend met betrekking tot de verwerking van persoonsgegevens;

   (b) wordt de bevoegdheid van de sectorale autoriteiten voor specifieke sectorale data-uitwisselingskwesties in verband met de uitvoering van deze verordening geëerbiedigd;

   (c) heeft de nationale bevoegde autoriteit die verantwoordelijk is voor de toepassing en handhaving van hoofdstuk VI van deze verordening ervaring op het gebied van data en elektronische-communicatiediensten.

3. De lidstaten zorgen ervoor dat de respectieve taken en bevoegdheden van de overeenkomstig lid 1 van dit artikel aangewezen bevoegde autoriteiten duidelijk omschreven zijn en het volgende omvatten:

   (a) de bewustmaking over de rechten en verplichtingen uit hoofde van deze verordening bevorderen bij gebruikers en entiteiten die binnen het toepassingsgebied van deze verordening vallen;

   (b) klachten over vermeende inbreuken op deze verordening behandelen, de inhoud van de klacht onderzoeken in de mate waarin dat gepast is en de klager binnen een redelijke termijn in kennis stellen van de vooruitgang en het resultaat van het onderzoek, met name indien verder onderzoek of coördinatie met een andere bevoegde autoriteit noodzakelijk is;

   (c) onderzoek verrichten naar zaken die betrekking hebben op de toepassing van deze verordening, onder meer op basis van informatie die van een andere bevoegde autoriteit of een andere overheidsinstantie is ontvangen;

   (d) afschrikwekkende financiële sancties opleggen door middel van administratieve procedures, waaronder dwangsommen en sancties met terugwerkende kracht, of het inleiden van een gerechtelijke procedure voor het opleggen van geldboetes;

   (e) toezicht houden op technologische ontwikkelingen die relevant zijn voor het beschikbaar stellen en gebruiken van data;

   (f) samenwerken met de bevoegde autoriteiten van andere lidstaten om de consistente toepassing van deze verordening te waarborgen, waaronder het

elektronisch uitwisselen van alle relevante informatie, zonder onnodige vertraging;

(g) waarborgen dat verzoeken om toegang tot data van overheidsinstanties in het geval van algemene noodsituaties uit hoofde van hoofdstuk V beschikbaar zijn voor het publiek;

(h) samenwerken met alle relevante bevoegde autoriteiten om ervoor te zorgen dat de verplichtingen van hoofdstuk VI worden gehandhaafd in overeenstemming met andere EU-wetgeving en zelfregulering die van toepassing zijn op aanbieders van dataverwerkingsdiensten;

(i) ervoor zorgen dat de kosten voor het overstappen naar andere aanbieders van dataverwerkingsdiensten overeenkomstig artikel 25 worden ingetrokken.

4. Wanneer een lidstaat meer dan één bevoegde autoriteit aanwijst, werken de bevoegde autoriteiten bij de uitoefening van de hun krachtens lid 3 van dit artikel toegewezen taken en bevoegdheden met elkaar samen, onder meer, in voorkomend geval, met de toezichthoudende autoriteit die verantwoordelijk is voor het toezicht op de toepassing van Verordening (EU) 2016/679, teneinde de consistente toepassing van deze verordening te waarborgen. In dergelijke gevallen wijzen de betrokken lidstaten een coördinerende bevoegde autoriteit aan.

5. De lidstaten delen de naam van de aangewezen bevoegde autoriteiten en hun respectieve taken en bevoegdheden en, indien van toepassing, de naam van de coördinerende bevoegde autoriteit mee aan de Commissie. De Commissie houdt een openbaar register van deze autoriteiten bij.

6. Bij de uitvoering van hun taken en de uitoefening van hun bevoegdheden overeenkomstig deze verordening blijven de bevoegde autoriteiten vrij van enige invloed van buitenaf, direct of indirect, en vragen noch aanvaarden zij instructies van andere overheidsinstanties of particuliere partijen.

7. De lidstaten zorgen ervoor dat de aangewezen bevoegde autoriteiten over de nodige middelen beschikken om hun taken overeenkomstig deze verordening naar behoren uit te voeren.

Artikel 32
Recht om klacht in te dienen bij een bevoegde autoriteit

1. Onverminderd andere mogelijkheden van administratief beroep of beroep in rechte hebben natuurlijke en rechtspersonen het recht om individueel of, in voorkomend geval, collectief een klacht in te dienen bij de relevante bevoegde autoriteit in de lidstaat waar zij hun gewone verblijfplaats, werkplek of vestiging hebben, indien zij van mening zijn dat hun rechten uit hoofde van deze verordening zijn geschonden.

2. De bevoegde autoriteit waarbij de klacht is ingediend, stelt de klager in kennis van het verloop van de procedure en van het genomen besluit.

3. De bevoegde autoriteiten werken samen om klachten zonder onnodige vertraging te behandelen en op te lossen, onder meer door alle relevante informatie elektronisch uit te wisselen. Deze samenwerking doet geen afbreuk aan het specifieke samenwerkingsmechanisme waarin de hoofdstukken VI en VII van Verordening (EU) 2016/679 voorzien.

Artikel 33
Sancties

1. De lidstaten stellen voorschriften vast ten aanzien van de sancties die van toepassing zijn op inbreuken op deze verordening en nemen alle nodige maatregelen om ervoor te zorgen dat deze sancties worden uitgevoerd. De vastgestelde sancties moeten doeltreffend, evenredig en afschrikwekkend zijn.

2. De lidstaten stellen de Commissie uiterlijk op [toepassingsdatum van deze verordening] in kennis van die voorschriften en maatregelen en delen haar onverwijld alle latere wijzigingen daarvan mee.

3. Voor inbreuken op de verplichtingen in hoofdstuk II, III en V van deze verordening kunnen de in artikel 51 van Verordening (EU) 2016/679 bedoelde toezichthoudende autoriteiten binnen hun bevoegdheidssfeer administratieve geldboetes opleggen overeenkomstig artikel 83 van Verordening (EU) 2016/679, welke kunnen oplopen tot het in artikel 83, lid 5, van die verordening bedoelde bedrag.

4. Voor inbreuken op de verplichtingen in hoofdstuk V kan de in artikel 52 van Verordening (EU) 2018/1725 bedoelde toezichthoudende autoriteit binnen haar bevoegdheidssfeer administratieve geldboetes opleggen overeenkomstig artikel 66 van Verordening (EU) 2018/1725, die kunnen oplopen tot het in artikel 66, lid 3, van die verordening bedoelde bedrag.

Artikel 34
Modelcontractvoorwaarden

De Commissie ontwikkelt niet-bindende modelcontractvoorwaarden inzake de toegang tot en het gebruik van data en beveelt deze aan teneinde partijen bij te staan bij het opstellen van en onderhandelen over contracten met evenwichtige contractuele rechten en verplichtingen.

HOOFDSTUK X
RECHT SUI GENERIS KRACHTENS RICHTLIJN 1996/9/EG

Artikel 35
Databanken die bepaalde data bevatten

Het in artikel 7 van Richtlijn 96/9/EG bedoelde recht sui generis is niet van toepassing op databanken die data bevatten die zijn verkregen uit of gegenereerd door het gebruik van een product of een gerelateerde dienst, om de uitoefening van het recht van gebruikers op toegang tot en gebruik van dergelijke data overeenkomstig artikel 4 van deze verordening of van het recht op het delen van dergelijke data met derden overeenkomstig artikel 5 van deze verordening, niet te belemmeren.

HOOFDSTUK XI
SLOTBEPALINGEN

Artikel 36
Wijziging van Verordening (EU) nr. 2017/2394

Aan de bijlage bij Verordening (EU) nr. 2017/2394 wordt het volgende punt toegevoegd:

"29. [Verordening (EU) XXX van het Europees Parlement en de Raad [Dataverordening]]."

Artikel 37
Wijziging van Richtlijn (EU) 2020/1828

In de bijlage bij Richtlijn (EU) 2020/1828 wordt het volgende punt toegevoegd:

"67. [Verordening (EU) XXX van het Europees Parlement en de Raad [Dataverordening]]"

Artikel 38
Uitoefening van de bevoegdheidsdelegatie

1. De bevoegdheid om gedelegeerde handelingen vast te stellen, wordt aan de Commissie toegekend onder de in dit artikel neergelegde voorwaarden.

2. De in artikel 25, lid 4, artikel 28, lid 2 en artikel 29, lid 5 bedoelde bevoegdheid om gedelegeerde handelingen vast te stellen, wordt aan de Commissie toegekend voor onbepaalde tijd met ingang van [...].

3. Het Europees Parlement of de Raad kan de in artikel 25, lid 4, artikel 28, lid 2, en artikel 29, lid 5 bedoelde bevoegdheidsdelegatie te allen tijde intrekken. Het besluit tot intrekking beëindigt de delegatie van de in dat besluit genoemde bevoegdheid. Het wordt van kracht op de dag na die van de bekendmaking ervan in het Publicatieblad van de Europese Unie of op een daarin genoemde latere datum. Het laat de geldigheid van de reeds van kracht zijnde gedelegeerde handelingen onverlet.

4. Vóór de vaststelling van een gedelegeerde handeling raadpleegt de Commissie de door elke lidstaat aangewezen deskundigen overeenkomstig de beginselen die zijn neergelegd in het Interinstitutioneel Akkoord over beter wetgeven van 13 april 2016.

5. Zodra de Commissie een gedelegeerde handeling heeft vastgesteld, doet zij daarvan gelijktijdig kennisgeving aan het Europees Parlement en de Raad.

6. Een op grond van artikel 25, lid 4, artikel 28, lid 2, en artikel 29, lid 5 vastgestelde gedelegeerde handeling treedt alleen in werking indien noch het Europees Parlement, noch de Raad daartegen binnen een termijn van drie maanden na de kennisgeving van de handeling aan het Europees Parlement en aan de Raad bezwaar heeft gemaakt, of indien zowel het Europees Parlement als de Raad voor het verstrijken van die termijn de Commissie heeft medegedeeld dat zij daartegen geen bezwaar zullen maken. Die termijn wordt op initiatief van het Europees Parlement of de Raad met drie maanden verlengd.

Artikel 39
Comitéprocedure

1. De Commissie wordt bijgestaan door een comité. Dat comité is een comité in de zin van Verordening (EU) nr. 182/2011.

2. Wanneer naar dit lid wordt verwezen, is artikel 5 van Verordening (EU) nr. 182/2011 van toepassing.

Artikel 40
Andere EU-rechtshandelingen betreffende rechten en verplichtingen inzake de toegang tot en het gebruik van data

1. De specifieke verplichtingen voor het beschikbaar stellen van data tussen bedrijven, tussen bedrijven en consumenten, en bij wijze van uitzondering tussen bedrijven en overheidsinstanties, in EU-rechtshandelingen die op of vóór [xx XXX xxx] in

werking zijn getreden, en de daarop gebaseerde gedelegeerde of uitvoeringshandelingen, blijven onverlet.

2. Deze verordening doet geen afbreuk aan EU-wetgeving waarin, gezien de behoeften van een sector, een gemeenschappelijke Europese dataruimte of een gebied van algemeen belang, verdere vereisten worden vastgesteld, met name met betrekking tot:

   (a) technische aspecten van de toegang tot data;

   (b) beperkingen van het recht van datahouders op toegang tot of gebruik van bepaalde door gebruikers verstrekte data;

   (c) aspecten die verder gaan dan de toegang tot en het gebruik van data.

Artikel 41
Evaluatie en herziening

Uiterlijk op [*twee jaar na de datum van toepassing van deze verordening*] voert de Commissie een evaluatie van deze verordening uit en brengt zij over de belangrijkste bevindingen verslag uit aan het Europees Parlement, de Raad en het Europees Economisch en Sociaal Comité. In het kader van deze evaluatie wordt met name het volgende beoordeeld:

(a) andere categorieën of soorten data die toegankelijk moeten worden gemaakt;

(b) de uitsluiting van bepaalde categorieën ondernemingen als begunstigden op grond van artikel 5;

(c) andere situaties die voor de toepassing van artikel 15 als uitzonderlijke noodzaak moeten worden beschouwd;

(d) veranderingen in de contractuele praktijken van aanbieders van dataverwerkingsdiensten en of dit leidt tot voldoende naleving van artikel 24;

(e) verlaging van de kosten die aanbieders van dataverwerkingsdiensten voor het overstapproces opleggen, in overeenstemming met de geleidelijke afschaffing van de overstaptarieven overeenkomstig artikel 25.

Artikel 42
Inwerkingtreding en toepassing

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Zij is van toepassing met ingang van [12 maanden na de inwerkingtreding van deze verordening].

Gedaan te Brussel,

Voor het Europees Parlement	*Voor de Raad*
De Voorzitter	*De Voorzitter*