VERORDENING (EU) 2018/1807 VAN HET EUROPEES PARLEMENT EN DE RAAD

van 14 november 2018

inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie

(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 ([1]),

Na raadpleging van het Comité van de Regio's,

Handelend volgens de gewone wetgevingsprocedure ([2]),

Overwegende hetgeen volgt:

(1) De digitalisering van de economie versnelt. Informatie- en communicatietechnologie is geen geïsoleerde sector meer, maar vormt de basis van alle moderne innovatieve economische systemen en samenlevingen. Elektronische gegevens vormen de kern van die systemen en kunnen grote waarde genereren wanneer zij worden geanalyseerd of gecombineerd met diensten en producten. Tegelijkertijd brengen de snelle ontwikkeling van de gegevenseconomie en opkomende technologieën zoals kunstmatige intelligentie, producten en diensten met betrekking tot het internet der dingen, autonome systemen en 5G nieuwe juridische kwesties met zich mee op het gebied van de toegang tot en het hergebruik van gegevens, alsmede op het gebied van aansprakelijkheid, ethiek en solidariteit. Vooral aan aansprakelijkheidskwesties zal naar verwachting, met name door de toepassing van zelfregulerende gedragscodes en andere beste praktijken, veel aandacht moeten worden besteed en zal daarbij in alle stadia van de waardeketen van gegevensverwerking rekening moeten worden gehouden met aanbevelingen, besluiten en maatregelen die zonder menselijke interactie worden genomen. Werk op dit gebied kan daarnaast onder meer betrekking hebben op passende mechanismen voor het bepalen van de aansprakelijkheid, voor het overdragen van verantwoordelijkheden tussen samenwerkende diensten, voor verzekeringen en voor controles.

(2) Datawaardeketens zijn opgebouwd uit verschillende gegevensactiviteiten: het creëren en verkrijgen van gegevens; het combineren en organiseren van gegevens; het verwerken van gegevens; het analyseren, marketen en verspreiden van gegevens; het gebruiken en hergebruiken van gegevens. Een essentiële schakel in elke datawaardeketen is een effectief en efficiënt verloop van gegevensverwerking. Het effectieve en efficiënte verloop van gegevensverwerking en de ontwikkeling van de gegevenseconomie in de Unie worden echter in het bijzonder belemmerd door twee soorten obstakels voor de gegevensmobiliteit en voor de interne markt: door de instanties van de lidstaten ingevoerde gegevenslokalisatievereisten en afhankelijkheid van één aanbieder in praktijken in de privésector.

(3) De vrijheid van vestiging en de vrijheid van dienstverrichting krachtens het Verdrag betreffende de werking van de Europese Unie („VWEU") gelden voor gegevensverwerkingsdiensten. Het verrichten van die diensten wordt echter bemoeilijkt en in sommige gevallen verhinderd door nationale, regionale of lokale voorschriften inzake de territoriale lokalisatie van de gegevens.

(4) Dergelijke obstakels voor het vrije verkeer ten aanzien van gegevensverwerkingsdiensten en voor het recht van vestiging van dienstverleners vloeien voort uit wettelijke voorschriften van de lidstaten die bepalen dat gegevens binnen een specifiek geografisch gebied of een grondgebied gelokaliseerd moeten zijn om te worden verwerkt. Andere regels of administratieve werkmethoden hebben een vergelijkbaar effect doordat zij specifieke eisen stellen die het moeilijker maken om gegevens buiten een welbepaald geografisch gebied of een grondgebied binnen de Unie te verwerken, zoals eisen inzake het gebruik van technologische voorzieningen die binnen een specifieke lidstaat zijn gecertificeerd of erkend. De keuzevrijheid van marktdeelnemers en de overheid inzake de plaats waar gegevens worden verwerkt, wordt verder ingeperkt door rechtsonzekerheid over de reikwijdte van al dan niet legitieme gegevenslokalisatievereisten. Deze verordening beperkt geenszins de vrijheid van bedrijven om overeenkomsten aan te gaan waarin wordt bepaald waar de gegevens moeten worden gelokaliseerd. Deze verordening heeft louter tot doel deze keuzevrijheid te waarborgen door ervoor te zorgen dat een overeengekomen locatie zich eender waar in de Unie kan bevinden.

([1]) PB C 227 van 28.6.2018, blz. 78.
([2]) Standpunt van het Europees Parlement van 4 oktober 2018 (nog niet bekendgemaakt in het Publicatieblad) en besluit van de Raad van 6 november 2018.

(5) Daarnaast wordt de gegevensmobiliteit binnen de Unie ook belemmerd door privaatrechtelijke beperkingen van juridische, contractuele en technische aard die gebruikers van gegevensverwerkingsdiensten belemmeren of verhinderen om hun gegevens van de ene dienstverlener naar de andere of naar hun eigen informatietechnologie (IT)-systemen over te dragen, zelfs na het beëindigen van hun overeenkomst met een dienstverlener.

(6) De combinatie van die obstakels heeft geleid tot een gebrek aan concurrentie tussen verleners van clouddiensten in de Unie, verscheidene problemen met betrekking tot afhankelijkheid van één aanbieder, en een ernstig gebrek aan gegevensmobiliteit. Evenzo heeft het gegevenslokalisatiebeleid afbreuk gedaan aan het vermogen van onderzoeks- en ontwikkelingsbedrijven om de samenwerking tussen bedrijven, universiteiten en andere onderzoeksorganisaties te vergemakkelijken teneinde hun eigen innovatie te stimuleren.

(7) Ter wille van de rechtszekerheid en om in de Unie gelijke mededingingsvoorwaarden te garanderen, is een voor alle marktdeelnemers geldend uniform pakket regels van cruciaal belang voor de werking van de interne markt. Om de belemmeringen voor het handelsverkeer en de concurrentieverstoringen die voortvloeien uit verschillen tussen nationale wetten weg te nemen en te voorkomen dat er nog meer belemmeringen voor het handelsverkeer en aanzienlijke concurrentieverstoringen ontstaan, moeten daarom uniforme regels worden vastgesteld die in alle lidstaten van toepassing zijn.

(8) Deze verordening doet geen afbreuk aan het rechtskader inzake de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens en inzake de eerbiediging van het privéleven en de bescherming van persoonsgegevens in elektronische communicatie, en met name Verordening (EU) 2016/679 van het Europees Parlement en de Raad ([1]) en de Richtlijnen (EU) 2016/680 ([2]) en 2002/58/EG ([3]) van het Europees Parlement en de Raad.

(9) Het snel groeiende internet der dingen, kunstmatige intelligentie en machine-learning zijn belangrijke bronnen van niet-persoonsgebonden gegevens, zoals deze bijvoorbeeld in geautomatiseerde industriële productieprocessen worden ingezet. Onder niet-persoonsgebonden gegevens vallen bijvoorbeeld geaggregeerde en geanonimiseerde gegevenssets die worden gebruikt voor bigdata-analyses, gegevens over precisielandbouw waarmee het gebruik van pesticiden en water kan worden gemonitord en geoptimaliseerd, en gegevens over de onderhoudsbehoeften van industriële machines. Als technologische ontwikkelingen het mogelijk maken om geanonimiseerde niet-persoonsgebonden gegevens om te vormen tot persoonsgegevens, moeten dergelijke gegevens worden behandeld als persoonsgegevens en moet Verordening (EU) 2016/679 dus van toepassing zijn.

(10) Verordening (EU) 2016/679 bepaalt dat het vrije verkeer van persoonsgegevens in de Unie noch beperkt noch verboden mag worden om redenen die verband houden met de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens. Bij deze verordening wordt hetzelfde beginsel toegepast op het vrije verkeer van niet-persoonsgebonden gegevens binnen de Unie, uitgezonderd wanneer een beperking of een verbod om redenen van openbare veiligheid gerechtvaardigd zou zijn. Verordening (EU) 2016/679 en deze verordening voorzien in een samenhangend geheel van regels inzake het vrije verkeer van verschillende soorten gegevens. Voorts legt deze verordening geen verplichting op om de verschillende soorten gegevens gescheiden op te slaan.

(11) Om een omgeving tot stand te brengen waarin niet-persoonsgebonden gegevens vrij kunnen circuleren binnen de Unie, de gegevenseconomie zich verder kan ontwikkelen en het bedrijfsleven van de Unie beter kan concurreren, dient een helder, alomvattend en voorspelbaar rechtskader te worden geschapen voor het verwerken van andere dan persoonsgegevens in de interne markt. Een op beginselen gebaseerde benadering die voorziet in samenwerking tussen de lidstaten en zelfregulering moet een zodanig flexibel kader garanderen dat rekening kan worden gehouden met de veranderende behoeften van gebruikers, dienstverleners en nationale autoriteiten in de Unie. Om overlapping met bestaande mechanismen en daarmee meer lasten voor zowel de lidstaten als het bedrijfsleven te voorkomen, hoeven er geen gedetailleerde technische voorschriften te worden uitgevaardigd.

(12) Deze verordening moet gegevensverwerking die wordt verricht als onderdeel van niet onder het Unierecht vallende activiteiten onverlet laten. Meer bepaald moet in herinnering worden gebracht dat de nationale veiligheid, overeenkomstig artikel 4 van het Verdrag betreffende de Europese Unie („VEU"), de exclusieve verantwoordelijkheid is van elke lidstaat.

([1]) Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1).

([2]) Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad (PB L 119 van 4.5.2016, blz. 89).

([3]) Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (PB L 201 van 31.7.2002, blz. 37).

(13) Het vrije verkeer van gegevens in de Unie zal een belangrijke rol spelen bij het bewerkstelligen van gegevensgestuurde groei en innovatie. Evenals bedrijven en consumenten kunnen de overheden en publiekrechtelijke instellingen van de lidstaten profiteren van een grotere keuzevrijheid inzake gegevensgestuurde dienstverleners, meer concurrerende prijzen en een doeltreffendere dienstverlening aan de burgers. Gezien de grote hoeveelheden gegevens die overheden en publiekrechtelijke instellingen verwerken, is het van het grootste belang dat zij het goede voorbeeld geven door gegevensverwerkingsdiensten te gaan gebruiken en dat zij geen gegevenslokalisatiebeperkingen opleggen wanneer zij gebruikmaken van gegevensverwerkingsdiensten. Daarom dienen overheden en publiekrechtelijke instellingen onder deze verordening te vallen. In dit verband moet het in deze verordening neergelegde beginsel van vrij verkeer van niet-persoonsgebonden gegevens ook van toepassing zijn op administratieve werkmethoden van algemene en consistente aard en andere gegevenslokalisatievereisten op het gebied van overheidsopdrachten, onverminderd Richtlijn 2014/24/EU van het Europees Parlement en de Raad ([1]).

(14) Net zoals Richtlijn 2014/24/EU geldt deze verordening onverminderd de wettelijke en bestuursrechtelijke bepalingen die verband houden met de interne organisatie van de lidstaten en die bevoegdheden en verantwoordelijkheden op het gebied van gegevensverwerking onder overheden en publiekrechtelijke instellingen verdelen zonder contractuele vergoeding van prestaties van particuliere partijen, en onverminderd de wettelijke en bestuursrechtelijke bepalingen van de lidstaten die voorzien in de uitvoering van die bevoegdheden en verantwoordelijkheden. Hoewel overheden en publiekrechtelijke instellingen worden aangespoord om de economische en andere voordelen van uitbesteding aan externe dienstverleners in overweging te nemen, kunnen zij legitieme redenen hebben om ervoor te kiezen diensten zelf te verlenen of in te besteden. Derhalve zijn de lidstaten uit hoofde van deze verordening geenszins verplicht om af te zien van de verlening van diensten die zij zelf willen verlenen of om deze door externe partijen uit te laten voeren of anders dan via overheidsopdrachten te regelen.

(15) Deze verordening moet van toepassing zijn op natuurlijke personen of rechtspersonen die gegevensverwerkingsdiensten aanbieden aan gebruikers die in de Unie verblijven of er een vestiging hebben, met inbegrip van personen die in de Unie gegevensverwerkingsdiensten aanbieden zonder er een vestiging te hebben. Deze verordening mag derhalve niet van toepassing zijn op gegevensverwerkingsdiensten die buiten de Unie worden verricht en evenmin op de met die gegevens verband houdende gegevenslokalisatievereisten.

(16) Deze verordening bevat geen regels voor de bepaling van het toepasselijk recht in handelszaken en geldt daarmee onverminderd Verordening (EG) nr. 593/2008 van het Europees Parlement en de Raad ([2]). In het bijzonder wordt een dienstverleningsovereenkomst, voor zover het op de overeenkomst toepasselijke recht niet volgens die verordening gekozen is, in principe geregeld door het recht van het land waar de dienstverlener zijn gewone verblijfplaats heeft.

(17) Deze verordening moet van toepassing zijn op gegevensverwerking in de ruimst mogelijke zin en het gebruik omvatten van alle soorten IT-systemen, ongeacht of zij zich bij de gebruiker zelf bevinden of aan een dienstverlener zijn uitbesteed. Zij moet alle gradaties van gegevensverwerking omvatten, van gegevensopslag („Infrastructure-as-a-Service (IaaS)") tot de verwerking van gegevens op platformen („Platform-as-a-Service (PaaS)") of in applicaties („Softwareas-a-Service (SaaS)").

(18) Gegevenslokalisatievereisten vormen een onmiskenbaar obstakel voor het vrij verlenen van gegevensverwerkingsdiensten in de Unie en voor de interne markt. Om die reden moeten zij als dusdanig worden verboden, tenzij zij gerechtvaardigd zijn uit hoofde van de bescherming van de openbare veiligheid in de zin van het Unierecht, in het bijzonder in de zin van artikel 52 VWEU, en in overeenstemming zijn met het evenredigheidsbeginsel van artikel 5 VEU. Om het beginsel van het vrije grensoverschrijdende verkeer van niet-persoonsgebonden gegevens in de praktijk te brengen, om ervoor te zorgen dat bestaande gegevenslokalisatievereisten snel worden opgeheven en om op operationele gronden de verwerking van gegevens op verschillende plaatsen in de Unie mogelijk te maken, en omdat deze verordening in maatregelen voorziet die de toegankelijkheid van gegevens voor wettelijke controles waarborgt, mogen de lidstaten enkel de openbare veiligheid kunnen inroepen voor gegevenslokalisatievereisten.

(19) Het begrip „openbare veiligheid" in de zin van artikel 52 VWEU en zoals uitgelegd door het Hof van Justitie omvat zowel de interne als de externe veiligheid van een lidstaat, alsmede vraagstukken in verband met de openbare veiligheid, met name om ruimte te bieden voor onderzoek, opsporing en vervolging van strafbare feiten. Het veronderstelt dat er sprake is van een reële en voldoende ernstige bedreiging voor een van de fundamentele belangen van de samenleving, zoals een bedreiging voor het functioneren van de instellingen en de essentiële openbare diensten en voor het overleven van de bevolking, het risico van een ernstige verstoring van de externe betrekkingen of van de vreedzame co-existentie van de volkeren, alsook de aantasting van militaire belangen. Overeenkomstig het evenredigheidsbeginsel moeten gegevenslokalisatievereisten die om redenen van openbare veiligheid gerechtvaardigd zijn, geschikt zijn om het nagestreefde doel te bereiken en mogen zij niet verder gaan dan wat nodig is om dat doel te bereiken.

([1]) Richtlijn 2014/24/EU van het Europees Parlement en de Raad van 26 februari 2014 betreffende het plaatsen van overheidsopdrachten en tot intrekking van Richtlijn 2004/18/EG (PB L 94 van 28.3.2014, blz. 65).

([2]) Verordening (EG) nr. 593/2008 van het Europees Parlement en de Raad van 17 juni 2008 inzake het recht dat van toepassing is op verbintenissen uit overeenkomst (Rome I) (PB L 177 van 4.7.2008, blz. 6).

(20) Om de doeltreffende toepassing van het beginsel van het vrije grensoverschrijdende verkeer van niet-persoonsgebonden gegevens te garanderen en te voorkomen dat er nieuwe belemmeringen voor een goede werking van de interne markt ontstaan, dienen de lidstaten de Commissie onmiddellijk in kennis te stellen van elke ontwerphandeling die een nieuw gegevenslokalisatievereiste bevat of een bestaand gegevenslokalisatievereiste wijzigt. Die ontwerphandelingen worden ingediend en beoordeeld volgens Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad ([1]).

(21) Bovendien dienen de lidstaten met het oog op het wegnemen van eventuele belemmeringen tijdens een overgangsperiode van 24 maanden na de datum van inwerkingtreding van deze verordening de bestaande wettelijke en bestuursrechtelijke bepalingen van algemene aard waarin gegevenslokalisatievereisten zijn vastgelegd aan een onderzoek te onderwerpen en dergelijke gegevenslokalisatievereisten die naar hun mening stroken met deze verordening, alsmede de rechtvaardiging daarvoor, mee te delen aan de Commissie. Dit moet de Commissie in staat stellen de gegrondheid van resterende gegevenslokalisatievereisten te bestuderen. De Commissie moet waar passend bevoegd zijn om aan de betrokken lidstaat opmerkingen te richten. Die opmerkingen kunnen een aanbeveling bevatten om het gegevenslokalisatievereiste te wijzigen of in te trekken.

(22) De in deze verordening neergelegde verplichtingen om bestaande gegevenslokalisatievereisten en ontwerphandelingen aan de Commissie mee te delen, moeten gelden voor wettelijke gegevenslokalisatievereisten en ontwerphandelingen van algemene aard, maar niet voor besluiten die tot een welbepaalde natuurlijke of rechtspersoon zijn gericht.

(23) Ter wille van de transparantie van in wettelijke en bestuursrechtelijke bepalingen van algemene aard neergelegde gegevenslokalisatievereisten in de lidstaten voor natuurlijke en rechtspersonen, zoals dienstverleners en gebruikers van gegevensverwerkingsdiensten, moeten de lidstaten informatie over dergelijke vereisten bekendmaken op één centraal nationaal online-informatiepunt en die informatie regelmatig bijwerken. Als alternatief moeten de lidstaten bijgewerkte informatie over dergelijke vereisten verstrekken aan een centraal informatiepunt dat bij een andere Uniehandeling is ingesteld. Met het oog op passende voorlichting van natuurlijke en rechtspersonen over in de Unie geldende gegevenslokalisatievereisten, dienen de lidstaten de adresgegevens van dergelijke centrale informatiepunten aan de Commissie mee te delen. De Commissie moet deze gegevens op haar eigen website publiceren, samen met een regelmatig bijgewerkte geconsolideerde lijst van alle gegevenslokalisatievereisten die in de lidstaten van kracht zijn, met inbegrip van beknopte informatie over die vereisten.

(24) Vaak ligt aan gegevenslokalisatievereisten een gebrek aan vertrouwen in grensoverschrijdende gegevensverwerking ten grondslag dat voortkomt uit de veronderstelling dat gegevens niet toegankelijk zullen zijn voor de bevoegde autoriteiten van de lidstaten, zoals voor inspectie- en toezichtdoeleinden en voor wettelijk voorgeschreven controles. Het louter nietig verklaren van contractuele bepalingen die bevoegde autoriteiten verbieden om op rechtmatige wijze toegang te verkrijgen tot gegevens om hun officiële taken te kunnen verrichten, volstaat niet om dit vertrouwen terug te winnen. Bijgevolg moet deze verordening uitdrukkelijk bepalen dat zij geen afbreuk doet aan de bevoegdheid van die autoriteiten om toegang tot gegevens te vragen of te krijgen overeenkomstig het Unierecht of het nationale recht, alsook dat de bevoegde autoriteiten de toegang tot gegevens niet mag worden geweigerd op grond van het feit dat de gegevens in een andere lidstaat worden verwerkt. Bevoegde autoriteiten kunnen functionele vereisten opleggen ter ondersteuning van de toegang tot gegevens, zoals het vereiste dat systeemdefinities in de betrokken lidstaat moeten worden bewaard.

(25) Natuurlijke of rechtspersonen die onderworpen zijn aan verplichtingen om aan bevoegde autoriteiten gegevens te verstrekken, kunnen aan die verplichtingen voldoen door de bevoegde autoriteiten effectieve en tijdige elektronische toegang tot de gegevens te bieden en te waarborgen, ongeacht op het grondgebied van welke lidstaat de gegevens worden verwerkt. Dergelijke toegang kan worden gegarandeerd door opname van uitdrukkelijke bepalingen in overeenkomsten tussen de tot toegangsverlening gehouden natuurlijke of rechtspersoon en de dienstverlener.

(26) Wanneer een natuurlijke of rechtspersoon onderworpen is aan een verplichting tot het verstrekken van toegang tot gegevens en die verplichting niet nakomt, moet de bevoegde autoriteit bijstand kunnen vragen van bevoegde autoriteiten in andere lidstaten. In dergelijke gevallen maken de bevoegde autoriteiten afhankelijk van het onderwerp gebruik van de specifieke Unierechtelijke of krachtens internationale overeenkomsten opgezette

([1]) Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij (PB L 241 van 17.9.2015, blz. 1).

samenwerkingsinstrumenten, bijvoorbeeld op het gebied van politiesamenwerking, samenwerking in strafzaken, civiele zaken of administratieve aangelegenheden, Kaderbesluit 2006/960/JBZ van de Raad ([1]), Richtlijn 2014/41/EU van het Europees Parlement en de Raad ([2]), het Verdrag van de Raad van Europa inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken ([3]), Verordening (EG) nr. 1206/2001 van de Raad ([4]), Richtlijn 2006/112/EG van de Raad ([5]) en Verordening (EU) nr. 904/2010 van de Raad ([6]). Indien dergelijke specifieke samenwerkingsmechanismen ontbreken, moeten de bevoegde autoriteiten onderling samenwerken om toegang te krijgen tot de desbetreffende gegevens door middel van aangewezen centrale aanspreekpunten.

(27) Wanneer een verzoek om bijstand met zich brengt dat de aangezochte autoriteit toegang krijgt tot gebouwen van een natuurlijke of rechtspersoon en tot gegevensverwerkingsapparatuur en -media, dient zulks te gebeuren met inachtneming van het Unierecht of het nationale procesrecht, met inbegrip van het eventuele vereiste om voorafgaande rechterlijke machtiging te verkrijgen.

(28) Deze verordening mag gebruikers niet toestaan om de toepassing van het nationale recht te omzeilen. Daarom moet deze verordening voorzien in de oplegging van doeltreffende, evenredige en afschrikkende sancties door de lidstaten aan gebruikers die de bevoegde autoriteiten de toegang ontzeggen tot hun gegevens die zij nodig hebben om hun officiële Unie- en nationaalrechtelijke taken te verrichten. In dringende gevallen, wanneer een gebruiker misbruik maakt van zijn recht, moeten de lidstaten strikt evenredige voorlopige maatregelen kunnen nemen. Voorlopige maatregelen die de relokalisatie van gegevens gedurende meer dan 180 dagen vanaf het begin van de relokalisatie vereisen, zouden afwijken van het beginsel van het vrije verkeer van gegevens voor langere duur en zouden derhalve aan de Commissie moeten worden meegedeeld, zodat kan worden bepaald of zij verenigbaar zijn met het Unierecht.

(29) Onbelemmerde gegevensportabiliteit is cruciaal voor de keuze van de gebruiker en voor doeltreffende mededinging op de markt voor gegevensverwerkingsdiensten. De reële of aangevoelde moeilijkheid om gegevens over de grens over te dragen, vermindert ook het vertrouwen van professionele gebruikers in aanbiedingen in het buitenland en daarmee hun vertrouwen in de interne markt. Terwijl individuele consumenten beter zijn geworden van het bestaande Unierecht, is het voor zakelijke of professionele gebruikers niet gemakkelijker om van dienstverlener te veranderen. Ook consistente, Uniebrede technische vereisten dragen, ongeacht of zij betrekking hebben op technische harmonisatie, wederzijdse erkenning of vrijwillige harmonisatie, bij aan de ontwikkeling van een concurrerende interne markt voor gegevensverwerkingsdiensten.

(30) Om volop van de concurrentieomgeving te kunnen profiteren, moeten professionele gebruikers geïnformeerde keuzes kunnen maken en de verschillende componenten van op de interne markt aangeboden gegevensverwerkingsdiensten, zoals de contractbepalingen inzake gegevensportabiliteit bij de beëindiging van een overeenkomst, vlot met elkaar kunnen vergelijken. Vanwege het innoverende vermogen van de markt en gelet op de ervaring en de deskundigheid van de dienstverleners en de professionele gebruikers van gegevensverwerkingsdiensten, is het dienstig dat de gedetailleerde voorlichtings- en operationele vereisten inzake gegevensportabiliteit via zelfregulering door de marktdeelnemers — hierbij aangespoord, ondersteund en gemonitord door de Commissie — worden vastgesteld in de vorm van Uniegedragscodes die contractuele modelbepalingen kunnen omvatten.

(31) Teneinde ervoor te zorgen dat dergelijke gedragscodes doeltreffend zijn en om het voor gebruikers gemakkelijker te maken om van dienstverlener te veranderen en om gegevens over te dragen, moeten deze gedragscodes alomvattend zijn en ten minste een aantal essentiële zaken omvatten die belangrijk zijn tijdens de gegevensoverdracht, zoals processen voor en de locatie van databack-ups, de beschikbare gegevensformaten en -supports, de vereiste IT-configuratie en minimale netwerkbandbreedte, de in acht te nemen wachttijd voordat het overdrachtsproces kan worden ingezet en de termijn waarbinnen de gegevens voor overdracht beschikbaar blijven, en de waarborgen inzake toegang tot de gegevens voor het geval de dienstverlener failliet zou gaan. De gedragscodes moeten bovendien duidelijk maken dat afhankelijkheid van één aanbieder geen aanvaardbare bedrijfspraktijk is, moeten voorzien in technologieën die het vertrouwen vergroten, en moeten regelmatig worden bijgewerkt om aan te sluiten bij de technologische ontwikkelingen. De Commissie moet erop toezien dat alle betrokken belanghebbenden, met inbegrip van associaties van kleine en middelgrote ondernemingen en start-ups, gebruikers en verleners van clouddiensten tijdens het hele proces worden geraadpleegd. De Commissie moet de ontwikkeling en de doeltreffendheid van de tenuitvoerlegging van dergelijke gedragscodes evalueren.

([1]) Kaderbesluit 2006/960/JBZ van de Raad van 18 december 2006 betreffende de vereenvoudiging van de uitwisseling van informatie en inlichtingen tussen de rechtshandhavingsautoriteiten van de lidstaten van de Europese Unie (PB L 386 van 29.12.2006, blz. 89).

([2]) Richtlijn 2014/41/EU van het Europees Parlement en de Raad van 3 april 2014 betreffende het Europees onderzoeksbevel in strafzaken (PB L 130 van 1.5.2014, blz. 1).

([3]) Verdrag van de Raad van Europa, CETS nr. 185.

([4]) Verordening (EG) nr. 1206/2001 van de Raad van 28 mei 2001 betreffende de samenwerking tussen de gerechten van de lidstaten op het gebied van bewijsverkrijging in burgerlijke en handelszaken (PB L 174 van 27.6.2001, blz. 1).

([5]) Richtlijn 2006/112/EG van de Raad van 28 november 2006 betreffende het gemeenschappelijke stelsel van belasting over de toegevoegde waarde (PB L 347 van 11.12.2006, blz. 1).

([6]) Verordening (EU) nr. 904/2010 van de Raad van 7 oktober 2010 betreffende de administratieve samenwerking en de bestrijding van fraude op het gebied van de belasting over de toegevoegde waarde (PB L 268 van 12.10.2010, blz. 1).

(32) Bevoegde autoriteiten van een lidstaat die bijstand van een andere lidstaat wensen om op grond van deze verordening toegang tot gegevens te krijgen, richten daartoe via een aangewezen centraal aanspreekpunt een naar behoren gemotiveerd verzoek aan het centrale aanspreekpunt van die andere lidstaat en nemen daarin een schriftelijke toelichting op van de rechtvaardiging voor en rechtsgrondslag van de wens om toegang tot gegevens te verkrijgen. Het centrale aanspreekpunt van de aangezochte lidstaat faciliteert het doorsturen van het verzoek naar de autoriteit die in de aangezochte lidstaat bevoegd is. De autoriteit waarnaar het verzoek wordt doorgestuurd, verleent met het oog op een doeltreffende samenwerking onverwijld bijstand in antwoord op het verzoek of verstrekt informatie over moeilijkheden om een dergelijk verzoek in te willigen of over de redenen waarom het verzoek wordt afgewezen.

(33) Het vergroten van het vertrouwen in de beveiliging van grensoverschrijdende gegevensverwerking moet de neiging van marktdeelnemers en de overheid om gegevenslokalisatie als substituut voor gegevensbeveiliging te gebruiken, verminderen. Ook moet het ondernemingen meer rechtszekerheid geven inzake de naleving van de geldende beveiligingseisen wanneer zij hun gegevensverwerking uitbesteden aan dienstverleners, waaronder die in een andere lidstaat.

(34) Beveiligingsvereisten met betrekking tot gegevensverwerking die worden toegepast op een gerechtvaardigde en evenredige manier op grond van het Unierecht of het nationale recht in overeenstemming met het Unierecht in de lidstaat van verblijf of vestiging van de natuurlijke of rechtspersoon waarvan gegevens betrokken zijn, dienen onverminderd van toepassing te blijven op de verwerking van die gegevens in een andere lidstaat. Deze natuurlijke of rechtspersonen moeten zelf dan wel via bedingen in overeenkomsten met dienstverleners aan dergelijke vereisten kunnen voldoen.

(35) Op nationaal niveau vastgestelde beveiligingsvereisten moeten noodzakelijk zijn en in verhouding staan tot de risico's voor de veiligheid van gegevensverwerking binnen het toepassingsgebied van het nationale recht waarin deze vereisten zijn gesteld.

(36) Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad ([1]) voorziet in wettelijke maatregelen om het algemene cyberbeveiligingsniveau in de Unie op te trekken. Gegevensverwerkingsdiensten behoren tot de digitale diensten die onder die richtlijn vallen. Overeenkomstig die richtlijn zorgen de lidstaten ervoor dat de verleners van digitale diensten de risico's voor de beveiliging van netwerk- en informatiesystemen die zij gebruiken identificeren en passende en evenredige technische en organisatorische maatregelen nemen om die risico's te beheersen. Zulke maatregelen moeten zorgen voor een beveiligingsniveau dat is afgestemd op de risico's die zich voordoen en moeten rekening houden met de beveiliging van systemen en voorzieningen, de behandeling van incidenten, het beheer van de bedrijfscontinuïteit, toezicht, controle en testen, en inachtneming van de internationale normen. Deze aspecten worden nader gespecificeerd in uitvoeringshandelingen die de Commissie op grond van de richtlijn vaststelt.

(37) De Commissie moet een verslag over de tenuitvoerlegging van deze verordening indienen, met name om na te gaan of deze moet worden gewijzigd in het licht van technologische of marktontwikkelingen. Dat verslag moet met name een evaluatie bevatten van deze verordening, in het bijzonder van de toepassing ervan op gegevenssets die bestaan uit zowel persoonsgegevens als niet-persoonsgebonden gegevens, alsook van de toepassing van de uitzondering in verband met de openbare veiligheid. Alvorens deze verordening van toepassing wordt, moet de Commissie ook richtsnoeren publiceren over de manier waarop moet worden omgegaan met gegevenssets die bestaan uit zowel persoonsgegevens als niet-persoonsgebonden gegevens, zodat bedrijven, met inbegrip van kleine en middelgrote ondernemingen, de wisselwerking tussen deze verordening en Verordening (EU) 2016/679 beter begrijpen en om ervoor te zorgen dat beide verordeningen worden nageleefd.

(38) Deze verordening eerbiedigt de grondrechten en neemt de beginselen in acht die met name in het Handvest van de grondrechten van de Europese Unie zijn erkend en dient te worden uitgelegd en toegepast overeenkomstig die rechten en beginselen, waaronder het recht op bescherming van persoonsgegevens, de vrijheid van meningsuiting en van informatie en de vrijheid van ondernemerschap.

(39) Daar de doelstelling van deze richtlijn, namelijk vrij verkeer van gegevens, anders dan persoonsgebonden gegevens, binnen de Unie, niet voldoende door de lidstaten kan worden verwezenlijkt, maar vanwege de omvang of de gevolgen ervan beter door de Unie kan worden verwezenlijkt, kan de Unie, overeenkomstig het in artikel 5 VEU neergelegde subsidiariteitsbeginsel, maatregelen nemen. Overeenkomstig het in hetzelfde artikel neergelegde evenredigheidsbeginsel gaat deze verordening niet verder dan nodig is om dat doel te verwezenlijken,

([1]) Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (PB L 194 van 19.7.2016, blz. 1).

HEBBEN DE VOLGENDE VERORDENING VASTGESTELD:

Artikel 1

Onderwerp

Deze verordening beoogt het vrije verkeer van niet-persoonsgebonden gegevens binnen de Unie te waarborgen door regels vast te leggen met betrekking tot gegevenslokalisatievereisten, de beschikbaarheid van gegevens voor bevoegde autoriteiten en de portabiliteit van gegevens voor professionele gebruikers.

Artikel 2

Werkingssfeer

1. Deze verordening is van toepassing op de verwerking van elektronische niet-persoonsgebonden gegevens in de Unie die:

a) als dienst wordt verleend aan gebruikers die in de Unie verblijven of er een vestiging hebben, ongeacht of de dienstverlener in de Unie is gevestigd, of

b) wordt verricht door een natuurlijke persoon of een rechtspersoon die in de Unie verblijft of er een vestiging heeft, voor eigen intern gebruik.

2. Indien een gegevensset bestaat uit zowel persoonsgegevens als niet-persoonsgebonden gegevens is deze verordening van toepassing op het deel niet-persoonsgebonden gegevens van de gegevensset. Wanneer persoonsgegevens en niet-persoonsgebonden gegevens in een set onlosmakelijk met elkaar verbonden zijn, laat deze verordening de toepassing van Verordening (EU) 2016/679 onverlet.

3. Deze verordening is niet van toepassing op activiteiten die niet onder de werkingssfeer van het Unierecht vallen.

Deze verordening doet geen afbreuk aan de wettelijke en bestuursrechtelijke bepalingen die verband houden met de interne organisatie van de lidstaten, waarbij de bevoegdheden en verantwoordelijkheden voor gegevensverwerking worden verdeeld onder of toegekend aan overheidsinstanties of publiekrechtelijke instellingen als gedefinieerd in artikel 2, lid 1, punt 4), van Richtlijn 2014/24/EU zonder contractuele vergoeding van particuliere partijen, en doet evenmin afbreuk aan de wettelijke en bestuursrechtelijke bepalingen van de lidstaten die voorzien in de toepassing van die bevoegdheden en verantwoordelijkheden.

Artikel 3

Definities

In deze verordening wordt verstaan onder:

1. „gegevens": andere gegevens dan persoonsgegevens als gedefinieerd in artikel 4, punt 1), van Verordening (EU) 2016/679;

2. „verwerking": een bewerking of een geheel van bewerkingen die al dan niet op geautomatiseerde wijze met betrekking tot gegevens of een geheel van gegevens in elektronische vorm zijn uitgevoerd, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, bekendmaken door middel van doorzending, verspreiden of anderszins ter beschikking stellen, op een lijn brengen of combineren, afschermen, wissen of vernietigen van gegevens;

3. „ontwerphandeling": een tekst die is uitgewerkt met de bedoeling deze als een wettelijke of bestuursrechtelijke bepaling van algemene strekking vast te stellen of uiteindelijk te doen vaststellen en die zich in een stadium bevindt waarin nog belangrijke wijzigingen kunnen worden aangebracht;

4. „dienstverlener": een natuurlijke of rechtspersoon die gegevensverwerkingsdiensten verleent;

5. „gegevenslokalisatievereiste": elke verplichting, verbodsbepaling, voorwaarde, beperking die of ander vereiste dat is vastgelegd in de wettelijke en bestuursrechtelijke bepalingen van een lidstaat of voortvloeit uit een algemene en vaste publiekrechtelijke praktijk in een lidstaat en binnen publiekrechtelijke instellingen, ook op het gebied van overheidsopdrachten, onverminderd Richtlijn 2014/24/EU, die gegevensverwerking op het grondgebied van een welbepaalde lidstaat verplicht stelt of die gegevensverwerking in een andere lidstaat belemmert;

6. „bevoegde autoriteit": een instantie van een lidstaat of een andere entiteit die krachtens het nationaal recht bevoegd is om een openbare functie te bekleden of openbaar gezag uit te oefenen, die uit hoofde van haar taken op grond van het Unie- of nationale recht bevoegd is om toegang te hebben tot gegevens die worden verwerkt door een natuurlijke of rechtspersoon;

7. „gebruiker": een natuurlijke of rechtspersoon, met inbegrip van een openbaar lichaam of een publiekrechtelijke instelling, die gebruikmaakt van of verzoekt om een gegevensverwerkingsdienst;

8. „professionele gebruiker": een natuurlijke of rechtspersoon, met inbegrip van een openbaar lichaam of een publiekrechtelijke instelling, die gebruikmaakt van of verzoekt om een gegevensverwerkingsdienst voor zijn handel, bedrijf, ambacht, beroep of taak.

Artikel 4

Vrij verkeer van gegevens binnen de Unie

1. Gegevenslokalisatievereisten zijn verboden, behalve wanneer zij in overeenstemming met het evenredigheidsbeginsel om redenen van openbare veiligheid gerechtvaardigd zijn.

De eerste alinea van dit lid geldt onverminderd lid 3 en onverminderd gegevenslokalisatievereisten die op basis van het bestaande Unierecht zijn vastgesteld.

2. De lidstaten delen onverwijld elke ontwerphandeling waarbij een nieuw gegevenslokalisatievereiste wordt ingevoerd of een bestaand gegevenslokalisatievereiste wordt gewijzigd, mee aan de Commissie overeenkomstig de procedures waarin de artikelen 5, 6 en 7 van Richtlijn (EU) 2015/1535 voorzien.

3. De lidstaten doen het nodige opdat alle bestaande in een wettelijke of bestuursrechtelijke bepaling van algemene strekking vastgelegde gegevenslokalisatievereisten die niet in overeenstemming zijn met lid 1 van dit artikel uiterlijk op 30 mei 2021 worden ingetrokken.

Bestaande maatregelen die gegevenslokalisatievereisten bevatten en die volgens een lidstaat in overeenstemming zijn met lid 1 van dit artikel en bijgevolg van toepassing kunnen blijven, dienen met opgave van de redenen daarvoor uiterlijk op 30 mei 2021 aan de Commissie te worden meegedeeld. Onverminderd artikel 258 VWEU beoordeelt de Commissie binnen zes maanden na ontvangst van een dergelijke mededeling of die maatregel in overeenstemming is met lid 1 van dit artikel en maakt zij ten aanzien van de betrokken lidstaat waar passend opmerkingen, waaronder zo nodig in de vorm van aanbevelingen tot wijziging of intrekking van de maatregel.

4. De lidstaten maken de details van de in een wettelijke of bestuursrechtelijke bepaling van algemene strekking vastgelegde gegevenslokalisatievereisten, die op hun grondgebied van toepassing zijn, voor het publiek beschikbaar door middel van een centraal nationaal online-informatiepunt waarvan zij de actualiteit bewaken, of voorzien een overeenkomstig een andere Uniehandeling ingesteld centraal informatiepunt van actuele informatie over deze gegevensvereisten.

5. De lidstaten delen de Commissie het adres mee van hun in lid 4 bedoelde centrale informatiepunt. De Commissie zet de koppeling(en) naar dit informatiepunt/deze informatiepunten op haar website, samen met een regelmatig bijgewerkte, geconsolideerde lijst van alle gegevenslokalisatievereisten als bedoeld in lid 4, met beknopte informatie over die vereisten.

Artikel 5

Beschikbaarheid van gegevens voor bevoegde autoriteiten

1. Deze verordening doet geen afbreuk aan de bevoegdheid van de bevoegde autoriteiten om met het oog op de uitvoering van hun taken om toegang tot gegevens te verzoeken en deze te verkrijgen overeenkomstig het Unierecht of het nationale recht. De toegang tot gegevens mag bevoegde autoriteiten niet worden geweigerd op grond van het feit dat de gegevens in een andere lidstaat worden verwerkt.

2. Wanneer een bevoegde autoriteit geen toegang tot gebruikersgegevens krijgt nadat zij hierom heeft verzocht, en indien er op grond van het Unierecht of internationale overeenkomsten geen specifiek samenwerkingsmechanisme bestaat voor de uitwisseling van gegevens tussen bevoegde autoriteiten van verschillende lidstaten, mag die bevoegde autoriteit overeenkomstig de in artikel 7 uiteengezette procedure om bijstand van een autoriteit in een andere lidstaat verzoeken.

3. Wanneer een verzoek om bijstand met zich brengt dat de aangezochte autoriteit zich toegang moet verschaffen tot gebouwen van een natuurlijke of rechtspersoon, met inbegrip van dataverwerkingsapparatuur en -media, dient zulks te gebeuren met inachtneming van het Unierecht of het nationale procesrecht.

4. De lidstaten mogen overeenkomstig het Unie- en nationale recht voorzien in doeltreffende, evenredige en afschrikkende sancties voor de niet-nakoming van een verplichting om gegevens te verstrekken.

In het geval van rechtsmisbruik door een gebruiker mogen de lidstaten ten aanzien van die gebruiker, rekening houdend met de belangen van de betrokken partijen, strikt evenredige voorlopige maatregelen nemen, wanneer dit wordt gerechtvaardigd door de spoedeisendheid om toegang te verkrijgen tot de gegevens. Indien een voorlopige maatregel de relokalisatie van gegevens gedurende meer dan 180 dagen vanaf het begin van de relokalisatie oplegt, wordt deze binnen de periode van 180 dagen aan de Commissie meegedeeld. De Commissie bestudeert de maatregel en de verenigbaarheid ervan met het Unierecht zo spoedig mogelijk en neemt in voorkomend geval de nodige maatregelen. De Commissie wisselt informatie over ervaringen op dit gebied uit met de in artikel 7 bedoelde centrale aanspreekpunten van de lidstaten.

Artikel 6

Gegevensportabiliteit

1. De Commissie zal het opstellen van zelfregulerende gedragscodes op Unieniveau („gedragscodes") bevorderen en faciliteren, om bij te dragen aan een concurrerende gegevenseconomie op basis van de beginselen van transparantie en interoperabiliteit en terdege rekening houdend met open normen over onder meer de volgende aspecten:

a) beste praktijken ter vergemakkelijking van het veranderen van dienstverlener en gegevensportabiliteit in een gestructureerde, algemeen gangbare en machineleesbare vorm, met inbegrip van open standaardformaten als dat noodzakelijk is of als de dienstverlener die de gegevens ontvangt, daarom verzoekt;

b) minimale informatievereisten om ervoor te zorgen dat professionele gebruikers voor de sluiting van een gegevensverwerkingsovereenkomst voldoende gedetailleerde, duidelijke en transparante informatie krijgen over de toepasselijke processen, technische vereisten, termijnen en kosten wanneer professionele gebruikers van dienstverlener willen veranderen of gegevens terug naar hun eigen IT-systemen willen overdragen;

c) benaderingen van certificeringsregelingen voor producten en diensten op het gebied van gegevensverwerking, teneinde professionele gebruikers de mogelijkheid te geven om de kwaliteit van deze producten en diensten beter te vergelijken, waarbij rekening wordt gehouden met gevestigde nationale of internationale normen; dergelijke benaderingen kunnen betrekking hebben op onder meer kwaliteitsbeheer, beheer van de informatiebeveiliging, beheer van de bedrijfscontinuïteit en milieubeheer;

d) multidisciplinaire stappenplannen voor communicatie, teneinde de gedragscodes bij de betrokken belanghebbenden onder de aandacht te brengen.

2. De Commissie ziet erop toe dat de gedragscodes worden uitgewerkt in nauwe samenwerking met alle relevante belanghebbenden, met inbegrip van samenwerkingsverbanden van kleine en middelgrote ondernemingen en start-ups, gebruikers en verleners van clouddiensten.

3. De Commissie spoort dienstverleners aan om de ontwikkeling van de gedragscodes uiterlijk op 29 november 2019 te voltooien en deze uiterlijk op 29 mei 2020 op doeltreffende wijze ten uitvoer te leggen.

Artikel 7

Procedure voor samenwerking tussen autoriteiten

1. Elke lidstaat wijst een centraal aanspreekpunt aan dat voor de uitvoering van deze verordening samenwerkt met de aanspreekpunten van de andere lidstaten en met de Commissie. De lidstaten delen de Commissie mee welke instantie zij als centraal aanspreekpunt hebben aangewezen en brengen wijzigingen ter kennis van de Commissie.

2. Bevoegde autoriteiten van een lidstaat die op grond van artikel 5, lid 2, bijstand van een andere lidstaat wensen om toegang tot gegevens te krijgen, dienen daartoe een gemotiveerd verzoek in bij het centrale aanspreekpunt van die andere lidstaat. Dit verzoek omvat een schriftelijke toelichting van de rechtvaardiging voor en rechtsgrondslag van de wens om toegang tot gegevens te verkrijgen.

3. Het centrale aanspreekpunt gaat na welke autoriteit in zijn lidstaat bevoegd is en stuurt het in lid 2 bedoelde verzoek door naar die autoriteit.

4. Zo spoedig mogelijk en binnen een termijn die in verhouding staat tot de urgentie van het verzoek verstrekt de aldus aangezochte bevoegde autoriteit een antwoord, waarin ofwel de gevraagde gegevens worden meegedeeld, ofwel aan de verzoekende bevoegde autoriteit wordt meegedeeld dat de aangezochte autoriteit van oordeel is dat het verzoek niet aan de uit deze verordening voortvloeiende voorwaarden voor verzoeken om bijstand voldoet.

5. Alle informatie die in het kader van de verzochte bijstand wordt uitgewisseld en verstrekt overeenkomstig artikel 5, lid 2, wordt uitsluitend gebruikt ten behoeve van de aangelegenheid waarvoor zij is aangevraagd.

6. De centrale aanspreekpunten verstrekken gebruikers algemene informatie over deze verordening, waaronder over de gedragscodes.

Artikel 8

Evaluatie en richtsnoeren

1. Uiterlijk op 29 november 2022 dient de Commissie een verslag in bij het Europees Parlement, bij de Raad en bij het Europees Economisch en Sociaal Comité, waarin zij de tenuitvoerlegging van deze verordening evalueert, met name wat betreft:

a) de toepassing van deze verordening, in het bijzonder de toepassing ervan op gegevenssets die bestaan uit zowel persoonsgegevens als niet-persoonsgebonden gegevens, met name in het licht van markt- en technologische ontwikkelingen waardoor meer mogelijkheden kunnen ontstaan om de anonimiteit van gegevens op te heffen;

b) de tenuitvoerlegging van artikel 4, lid 1, door de lidstaten, en met name de uitzondering in verband met de openbare veiligheid, en

c) de ontwikkeling en doeltreffende tenuitvoerlegging van de gedragscodes en de doeltreffende verstrekking van informatie door dienstverleners.

2. De lidstaten verstrekken de Commissie de informatie die noodzakelijk is om het in lid 1 bedoelde verslag op te stellen.

3. De Commissie publiceert uiterlijk op 29 mei 2019 richtsnoeren inzake de wisselwerking tussen deze verordening en Verordening (EU) 2016/679 wat betreft gegevenssets die bestaan uit zowel persoonsgegevens als niet-persoonsgebonden gegevens.

Artikel 9

Slotbepalingen

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

Deze verordening wordt zes maanden na de bekendmaking ervan van toepassing.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Straatsburg, 14 november 2018.

Voor het Europees Parlement	*Voor de Raad*
De voorzitter	*De voorzitter*
A. TAJANI	K. EDTSTADLER