EUROPESE
COMMISSIE

Brussel, 24.7.2019
COM(2019) 374 final

MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT EN DE RAAD

Gegevensbeschermingsregels als basis voor vertrouwen in de EU en daarbuiten - een inventarisatie

Mededeling van de Commissie aan het Europees Parlement en de Raad

Gegevensbeschermingsregels als basis voor vertrouwen in de EU en daarbuiten – een inventarisatie

I. Inleiding

De algemene verordening gegevensbescherming[1] (hierna te noemen "de verordening") is sinds meer dan een jaar van toepassing in de hele Europese Unie. Zij vormt het hart van een coherent en gemoderniseerd gegevensbeschermingslandschap van de EU, dat ook de richtlijn gegevensbescherming bij wetshandhaving[2] en de verordening gegevensbescherming voor EU-instellingen en -organen[3] omvat. Dit kader wordt gecompleteerd door de e-privacyverordening, die op dit moment het wetgevingsproces doorloopt.

Krachtige gegevensbeschermingsregels zijn essentieel voor het waarborgen van het grondrecht op bescherming van persoonsgegevens, zijn van groot belang voor een democratische maatschappij[4] en vormen een belangrijk onderdeel van een steeds grotere data-economie. De EU streeft ernaar de vele mogelijkheden van digitalisering op het gebied van diensten, banen en innovatie te benutten en tegelijkertijd de uitdagingen die deze met zich meebrengen, aan te gaan. Identiteitsdiefstal, het lekken van gevoelige gegevens, discriminatie van personen, ingebouwde vooroordelen, het delen van illegale content en de ontwikkeling van inbreuk makende bewakingssystemen zijn slechts enkele voorbeelden van kwesties die steeds vaker het onderwerp vormen van publiek debat en waarbij duidelijk is dat mensen verwachten dat hun gegevens worden beschermd.

---

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): https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32016R0679

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 of 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): https://eur-lex.europa.eu/legal-content/NL/ALL/?uri=celex:32016L0680. De richtlijn moest door de lidstaten uiterlijk op 6 mei 2018 zijn omgezet. De stand van zaken met betrekking tot de omzetting is te lezen in de verslagen van de veiligheidsunie.

3 Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG (PB L 295 van 21.11.2018, blz. 39): https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32018R1725. De verordening is van toepassing sinds 11 december 2018.

4 Het Hooggerechtshof van India heeft in een baanbrekende uitspraak van 24 augustus 2017 erkend dat privacy een grondrecht en een "essentieel facet van de waardigheid van de mens" is.

Gegevensbescherming is een waarlijk wereldwijd fenomeen geworden, omdat mensen uit de hele wereld de bescherming en beveiliging van hun gegevens steeds meer waarderen. Veel landen hebben uitgebreide gegevensbeschermingsregels vastgesteld of zijn bezig met de procedure hiervoor op basis van beginselen die vergelijkbaar zijn met die uit de verordening, wat leidt tot de wereldwijde convergentie van gegevensbeschermingsregels. Hierdoor ontstaan nieuwe mogelijkheden om gegevensstromen tussen commerciële marktdeelnemers of overheidsautoriteiten te vergemakkelijken en tegelijkertijd het beschermingsniveau van de persoonsgegevens in de EU en wereldwijd te verhogen.

Mensen nemen gegevensbescherming serieuzer dan ooit tevoren, wat veel gevolgen heeft voor verschillende belanghebbenden en sectoren. De Commissie is vastbesloten om de EU naar een succesvolle uitvoering van het nieuwe stelsel voor gegevensbescherming te leiden en ervoor te zorgen dat alle aspecten ervan volledig operationeel worden. Met deze mededeling inventariseert de Commissie de resultaten die tot op heden zijn behaald in verband met de consistente uitvoering van de gegevensbeschermingsregels in de hele EU, de werking van het nieuwe beheerssysteem, de gevolgen voor burgers en ondernemingen en de inspanningen van de EU om de wereldwijde convergentie van gegevensbeschermingsstelsels te bevorderen. Deze mededeling volgt op de mededeling van de Commissie voor de toepassing van de verordening van januari 2018[5] en is gebaseerd op informatie uit de werkzaamheden van de groep van diverse belanghebbenden[6], met name haar bijdrage aan de inventarisatie na een jaar en de discussies die zijn gehouden tijdens het evenement dat de Commissie op 13 juni 2019 heeft georganiseerd[7]. Deze mededeling is bovendien een bijdrage aan de toetsing die de Commissie uiterlijk in mei 2020 wil uitvoeren [8].

Het wetgevingskader voor gegevensbescherming van de EU is een hoeksteen van de Europese mensgerichte benadering van innovatie. Het wordt onderdeel van de regelgeving waar steeds meer beleidsmaatregelen op steunen, waaronder gezondheid en onderzoek, kunstmatige intelligentie, vervoer, energie, mededinging en wetshandhaving. De Commissie heeft consequent benadrukt hoe belangrijk de gedegen uitvoering en handhaving van de nieuwe gegevensbeschermingsregels zijn, zoals is aangegeven in haar mededeling voor de toepassing van de verordening uit januari 2018 en haar richtsnoeren voor het gebruik van persoonsgegevens in het kader van verkiezingen uit september 2018[9]. Op het moment van

---

5 Mededeling van de Commissie aan het Europees Parlement en de Raad "Betere bescherming, nieuwe mogelijkheden - Richtsnoeren Commissie voor de directe toepassing van de algemene verordening gegevensbescherming met ingang van 25 mei 2018" (COM(2018) 43 final): https://eur-lex.europa.eu/legal-content/NL/TXT/?qid=1517578296944&uri=CELEX%3A52018DC0043

6 De groep van diverse belanghebbenden op het gebied van de verordening die de Commissie heeft ingesteld, bestaat uit vertegenwoordigers van het maatschappelijk middenveld en het bedrijfsleven, academici en mensen uit de praktijk: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537&Lang=NL

7 http://europa.eu/rapid/press-release_IP-19-2956_nl.htm

8 Artikel 97 van de verordening.

9 "Richtsnoeren van de Commissie voor de toepassing van de EU-gegevensbeschermingswetgeving in het kader van verkiezingen"(COM(2018) 638 final): https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52018DC0638

deze mededeling is er veel vooruitgang geboekt met betrekking tot dit doel, hoewel er zeker meer werk moet worden verzet voordat de verordening volledig operationeel is.

II. Eén aanpak voor de gehele EU: het kader voor gegevensbescherming is in werking in de lidstaten

Eén van de hoofddoelen van de verordening was om een einde te maken aan het gefragmenteerde landschap met 28 verschillende nationale wetgevingen onder de vorige richtlijn gegevensbescherming[10] en het bieden van rechtszekerheid aan natuurlijke personen en ondernemingen in de hele EU. Dat doel is grotendeels behaald.

De harmonisatie van het rechtskader

Hoewel de verordening rechtstreeks toepasselijk is in de lidstaten, moest op nationaal niveau een aantal wettelijke maatregelen worden getroffen om nationale autoriteiten op het gebied van gegevensbescherming op te zetten en hen bevoegdheden toe te wijzen[11], regels over specifieke kwesties vast te stellen, bijvoorbeeld over het in overeenstemming brengen van de bescherming van persoonsgegevens met de vrijheid van meningsuiting en informatie, en sectorale wetgeving met gegevensbeschermingsaspecten te wijzigen of in te trekken. Op het moment van deze mededeling hadden alle lidstaten op drie na[12] hun nationale gegevensbeschermingswetgeving geactualiseerd. Aan de aanpassing van sectorale wetgeving wordt op nationaal niveau nog altijd gewerkt. Sinds de verordening is opgenomen in de Overeenkomst betreffende de Europese Economische Ruimte, is zij ook van toepassing op Noorwegen, IJsland en Liechtenstein, die ook hun nationale gegevensbeschermingswetgeving hebben vastgesteld.

Door belanghebbenden wordt echter opgeroepen om sommige gebieden nog verder te harmoniseren[13]. De verordening geeft de lidstaten inderdaad wat ruimte om de toepassing op bepaalde gebieden nader te specificeren, zoals de leeftijd voor toestemming door kinderen voor onlinediensten[14] of de verwerking van persoonsgegevens op het gebied van bijvoorbeeld geneeskunde en volksgezondheid. In dit geval gelden voor de maatregelen van de lidstaten twee elementen als kader:

---

[10] Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens: https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=celex:31995L0046

[11] Zoals de bevoegdheid om administratieve geldboeten op te leggen.

[12] Op 23 juli 2019 zijn Griekenland, Portugal en Slovenië nog steeds bezig met het vaststellen van hun nationale wetgeving.

[13] Zie het verslag van de groep van diverse belanghebbenden op het gebied van de verordening van 13 juni 2019: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670&Lang=NL

[14] 13 jaar voor België, Denemarken, Estland, Finland, Letland, Malta, Zweden en het Verenigd Koninkrijk; 14 jaar voor Oostenrijk, Bulgarije, Cyprus, Spanje, Italië en Litouwen; 15 jaar voor Tsjechië en Frankrijk; 16 jaar voor Duitsland, Hongarije, Kroatië, Ierland, Luxemburg, Nederland, Polen, Roemenië en Slowakije.

i) elke nader bepalende nationale wetgeving moet voldoen aan de vereisten van het Handvest van de grondrechten van de Europese Unie[15] (en aan de beperkingen uit de verordening die voortbouwt op het Handvest);
ii) de wetgeving mag geen afbreuk doen aan het vrije verkeer van persoonsgegevens binnen de EU[16].

In sommige gevallen hebben lidstaten voornamelijk door middel van sectorale wetgeving nationale eisen ingevoerd boven op de verordening, wat leidt tot fragmentatie en onnodige lasten. Eén voorbeeld van een extra eis die lidstaten boven op de verordening hebben ingevoerd, is de verplichting in Duitsland om in ondernemingen met ten minste twintig werknemers een functionaris voor gegevensbescherming aan te wijzen die zich permanent bezighoudt met de geautomatiseerde verwerking van persoonsgegevens.

Aanhoudende inspanningen voor meer harmonisatie

De Commissie houdt bilaterale dialogen met nationale autoriteiten, waarbij zij in het bijzonder aandacht besteedt aan de nationale maatregelen met betrekking tot:

- de daadwerkelijke onafhankelijkheid van gegevensbeschermingsautoriteiten, onder andere dankzij passende financiële, personele en technische middelen;
- de wijze waarop de nationale wetgeving de rechten van betrokkenen beperkt;
- het feit dat er in de nationale wetgeving geen vereisten, zoals aanvullende verwerkingsvoorwaarden, zouden moeten staan boven op de verordening als er geen ruimte voor specificatie is;
- de naleving van de verplichting om het recht op bescherming van persoonsgegevens in overeenstemming te brengen met de vrijheid van meningsuiting en informatie, met dien verstande dat deze verplichting niet mag worden misbruikt om journalistiek werk te ontmoedigen.

Het werk van de gegevensbeschermingsautoriteiten, die samenwerken in het kader van het Europees Comité voor gegevensbescherming ("het Comité"), is essentieel voor de consequente toepassing van de nieuwe regels: handhavingsmaatregelen die betrekking hebben op meerdere lidstaten, verlopen via het mechanisme voor samenwerking en coherentie[17] van het Comité en de door het Comité vastgestelde richtsnoeren dragen bij aan de geharmoniseerde interpretatie van de verordening. De belanghebbenden verwachten echter van de gegevensbeschermingsautoriteiten dat zij verder gaan in deze richting.

Het werk van de nationale gerechten en het Hof van Justitie van de Europese Unie helpt ook bij het creëren van een consistente interpretatie van de gegevensbeschermingsregels.

---

15 Artikel 8.
16 In overeenstemming met artikel 16, lid 2, van het Verdrag betreffende de werking van de Europese Unie.
17 Op grond van artikel 60 van de verordening werken gegevensbeschermingsautoriteiten samen om in concrete gevallen één interpretatie van de verordening toe te passen. In artikel 64 is bepaald dat het Comité in bepaalde gevallen advies zal uitbrengen om te waarborgen dat de verordening consequent wordt toegepast. Ten slotte heeft het Comité het recht om bindende besluiten vast te stellen als de gegevensbeschermingsautoriteiten het niet eens worden.

Nationale gerechten hebben onlangs bepalingen in de nationale wetgeving die afwijken van de verordening, ongeldig verklaard[18].

III. Alle stukjes van het nieuwe beheerssysteem vallen op hun plaats

Met de verordening is een nieuwe beheersstructuur gecreëerd, waarin de onafhankelijke nationale gegevensbeschermingsautoriteiten centraal staan als de handhavers van de verordening en het eerste contactpunt voor belanghebbenden. Hoewel de meeste gegevensbeschermingsautoriteiten het afgelopen jaar steeds meer middelen tot hun beschikking hebben gekregen, zijn er nog altijd grote verschillen tussen de lidstaten[19].

Gegevensbeschermingsautoriteiten gebruiken hun nieuwe bevoegdheden

Op grond van de verordening hebben gegevensbeschermingsautoriteiten krachtigere handhavingsbevoegdheden gekregen. Ondanks de zorgen die enkele belanghebbenden vóór mei 2018 hebben geuit, gebruiken de nationale gegevensbeschermingsautoriteiten hun handhavingsbevoegdheden evenwichtig. Zij hebben de nadruk gelegd op de dialoog en niet op sancties, voornamelijk voor de kleinste marktdeelnemers voor wie de verwerking van persoonsgegevens geen hoofdactiviteit is. Tegelijkertijd deinsden zij er niet voor terug om hun nieuwe bevoegdheden waar nodig doeltreffend te gebruiken, onder andere door onderzoek te doen op het gebied van sociale media[20] en administratieve geldboeten op te leggen die variëren van enkele duizenden tot enkele miljoenen euro's, afhankelijk van de ernst van de inbreuk op de gegevensbeschermingsregels.

Voorbeelden van boeten die door gegevensbeschermingsautoriteiten zijn opgelegd[21]:

- 5 000 EUR voor een café voor sportweddenschappen in Oostenrijk vanwege onrechtmatige videobewaking;
- 220 000 EUR voor een gegevensmakelaar in Polen, omdat hij had verzuimd mensen ervan in kennis te stellen dat hun gegevens werden verwerkt;
- 250 000 EUR voor de Spaanse voetbalcompetitie LaLiga, vanwege onvoldoende transparantie in het ontwerp van een smartphone-applicatie;
- 50 miljoen EUR voor Google in Frankrijk, vanwege de voorwaarden voor het verkrijgen van toestemming van gebruikers.

Het is essentieel dat gegevensbeschermingsautoriteiten hij het uitvoeren van onderzoeken in vaak complexe dossiers relevant bewijsmateriaal verzamelen, alle procedurele stappen uit hoofde van de nationale wetgeving naleven en een eerlijke rechtsbedeling waarborgen.

---

18 Dit is gebeurd in Duitsland en Spanje.

19 https://edpb.europa.eu/sites/edpb/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf

20 De Ierse commissie voor gegevensbescherming heeft bijvoorbeeld 15 formele onderzoeken geopend in verband met de naleving van de verordening door multinationale technologiebedrijven. Zie bladzijde 49 van het jaarverslag van de Ierse commissie voor gegevensbescherming voor 2018: https://www.dataprotection.ie/en/news-media/press-releases/dpc-publishes-annual-report-25-may-31-december-2018

21 Verschillende uitspraken waarin geldboeten worden opgelegd, worden nog rechterlijk getoetst.

Hiervoor is tijd en veel werk nodig, wat verklaart waarom de meeste onderzoeken die na de inwerkingtreding van de verordening zijn ingesteld, nog steeds lopen.

Dat gezegd hebbende, moet het succes van de verordening niet worden afgemeten aan het aantal opgelegde geldboeten, maar aan de verandering in de cultuur en het gedrag van alle betrokken actoren. In verband hiermee beschikken de gegevensbeschermingsautoriteiten over andere instrumenten, zoals het opleggen van een tijdelijke of definitieve verwerkingsbeperking, waaronder een verwerkingsverbod, of het opschorten van gegevensstromen naar een ontvanger in een derde land[22].

Enkele gegevensbeschermingsautoriteiten hebben nieuwe instrumenten gecreëerd, zoals hulplijnen en toolkits voor ondernemingen, terwijl andere nieuwe benaderingen hebben ontwikkeld, zoals regulatory sandboxes[23] om ondernemingen te helpen bij de naleving van de verordening. Een aantal belanghebbenden, voornamelijk kleine en middelgrote ondernemingen in enkele lidstaten, is echter nog steeds van mening dat het niet voldoende ondersteuning en informatie heeft ontvangen[24]. Om deze situatie te verbeteren, verleent de Commissie subsidies aan gegevensbeschermingsautoriteiten, zodat zij belanghebbenden, met name natuurlijke personen en kleine en middelgrote ondernemingen, kunnen bereiken[25].

Het Europees Comité voor gegevensbescherming is operationeel

De gegevensbeschermingsautoriteiten hebben hun werkzaamheden in het Europees Comité voor gegevensbescherming geïntensiveerd[26]. Dankzij deze intensieve werkzaamheden heeft het Comité circa twintig richtsnoeren over belangrijke aspecten van de verordening vastgesteld[27]. De toekomstige werkgebieden van het Comité worden in overeenstemming met de verordening gepresenteerd in een tweejarenprogramma[28].

In grensoverschrijdende gevallen is elke gegevensbeschermingsautoriteit niet langer slechts een nationale autoriteit, maar onderdeel van een EU-breed proces voor alle stadia, van het onderzoek tot de beslissing. Deze nauwe samenwerking is de dagelijkse praktijk geworden: eind juni 2019 waren er via het samenwerkingsmechanisme 516 grensoverschrijdende zaken beheerd.

---

22 Artikel 58, lid 2, onder f) en j).

23 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/09/ico-call-for-views-on-creating-a-regulatory-sandbox/

24 Zie het verslag van de groep van diverse belanghebbenden op het gebied van de AVG: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670&Lang=NL

25 In 2018 is 2 miljoen EUR toegekend aan negen gegevensbeschermingsautoriteiten voor activiteiten in de periode 2018-2019: België, Bulgarije, Denemarken, Hongarije, Litouwen, Letland, Nederland, Slovenië en IJsland: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai-ag-2017;
In 2019 wordt 1 miljoen EUR toegekend: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai-ag-2019

26 Het Comité beschikt over rechtspersoonlijkheid en bestaat uit de hoofden van de nationale toezichthoudende autoriteiten en de Europese Toezichthouder voor gegevensbescherming.

27 https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_nl

28 https://edpb.europa.eu/our-work-tools/our-documents/publication-type/work-program_nl

De Commissie draagt actief bij aan de werkzaamheden van het Comité[29] om de letter en de geest van de verordening uit te dragen en brengt de algemene beginselen van het EU-recht in herinnering[30].

Op naar een EU-cultuur van gegevensbescherming

Het potentieel van het nieuwe beheerssysteem is nog niet volledig ontplooid. Het is van belang dat het Comité zijn besluitvorming verder stroomlijnt en een gemeenschappelijke EU-cultuur van gegevensbescherming ontwikkelt onder zijn leden. De mogelijkheden voor gegevensbeschermingsautoriteiten om hun krachten te bundelen[31] voor kwesties waarbij meer dan één lidstaat betrokken is, bijvoorbeeld voor het uitvoeren van gezamenlijke onderzoeken en gezamenlijke handhavingsmaatregelen, kunnen hieraan bijdragen en tegelijkertijd een tegenwicht bieden aan de beperkingen van de middelen.

Veel belanghebbenden willen dat de nationale gegevensbeschermingsautoriteiten nog meer samenwerken en een uniforme aanpak hanteren[32]. Zij willen ook dat het advies van de gegevensbeschermingsautoriteiten consistenter is[33] en dat de nationale richtsnoeren en die van het Comité volledig op elkaar aansluiten. Sommige belanghebbenden verwachten ook meer opheldering over belangrijke concepten uit de verordening, zoals de op risico's gebaseerde aanpak, met speciale aandacht voor de zorgen van kleine en middelgrote ondernemingen.

In dit verband is het essentieel om belanghebbenden een grotere bijlage te laten leveren aan de werkzaamheden van het Comité. Daarom is de Commissie ingenomen met de systematische openbare raadpleging over richtsnoeren van het Comité. Dit gebruik zou samen met de organisatie van workshops voor belanghebbenden over gerichte onderwerpen in een vroeg stadium van de discussie moeten worden voortgezet en uitgebreid, zodat de werkzaamheden van het Comité transparant, inclusief en relevant zijn.

IV. Personen maken gebruik van hun rechten, maar de voorlichting moet doorgaan

Een ander hoofddoel van de verordening was het versterken van de rechten van personen. Burgerrechten- en consumentenorganisaties beschouwen de verordening als een belangrijke bijdrage aan een eerlijke digitale maatschappij die is gebaseerd op wederzijds vertrouwen.

---

29 Als deelnemer zonder stemrecht.

30 De Commissie heeft ook geholpen bij de soepele instelling van het Comité en ondersteunt de werking ervan door haar communicatiesysteem beschikbaar te stellen.

31 Artikel 62 van de verordening.

32 Zie het verslag van de groep van diverse belanghebbenden op het gebied van de verordening: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670&Lang=NL
Ondernemingen zijn bijvoorbeeld van mening dat de nationale lijsten van verwerkingsactiviteiten waarvoor uit hoofde van artikel 35 van de verordening een gegevensbeschermingseffectbeoordeling nodig is, beter geharmoniseerd zouden kunnen zijn.

33 Waaronder tussen de verschillende autoriteiten in federale staten.

Meer bekendheid van gegevensbeschermingsrechten

In de EU zijn steeds meer mensen op de hoogte van de gegevensbeschermingsregels en van hun rechten: 67 % van de respondenten van een Eurobarometer uit mei 2019[34] is op de hoogte van de verordening en 57 % weet dat er een nationale gegevensbeschermingsautoriteit is tot wie zij zich kunnen wenden voor informatie of om een klacht in te dienen. 73 % van hen heeft wel eens gehoord van ten minste één van de rechten die hun bij de verordening zijn toegekend. Een aanzienlijk deel van de inwoners van de EU treft echter nog altijd niet actief maatregelen om hun persoonsgegevens online te beschermen. Zo heeft 44 % de standaard-privacyinstellingen op sociale netwerken niet veranderd.

Steeds meer mensen oefenen hun rechten uit

Deze grotere kennis heeft ertoe geleid dat mensen hun rechten intensiever uitoefenen via klantvragen en door zich vaker tot de gegevensbeschermingsautoriteiten te wenden om te verzoeken om informatie of een klacht in te dienen[35]. In verschillende sectoren, zoals het bankwezen en de telecommunicatie, hebben ondernemingen ook aangegeven dat er meer om toegang tot persoonsgegevens wordt gevraagd. Bovendien hebben mensen hun toestemming vaker ingetrokken en vaker hun recht uitgeoefend om bezwaar te maken tegen commerciële communicatie[36].

Door verschillende marktdeelnemers is echter melding gemaakt van misverstanden over de gegevensbeschermingsregels, zoals het idee dat mensen toestemming moeten geven voor elke verwerking, of dat het recht op wissing absoluut is (terwijl marktdeelnemers persoonsgegevens soms moeten bewaren, bijvoorbeeld op basis van wettelijke verplichtingen)[37]. Maatschappelijke organisaties klagen op hun beurt over de lange wachttijd op antwoord van sommige ondernemingen en gegevensbeschermingsautoriteiten.

Het is belangrijk om te vermelden dat er na machtiging door personen die gebruikmaken van de nieuwe mogelijkheid uit hoofde van de verordening, meerdere representatieve vorderingen zijn ingediend door non-gouvernementele organisaties[38]. Het zou gemakkelijker zijn geweest om gebruik te maken van representatieve vorderingen als meer lidstaten de mogelijkheid uit de verordening hadden gebruikt om non-gouvernementele organisaties in staat te stellen om zonder machtiging vorderingen in te dienen[39].

---

34 https://europa.eu/rapid/press-release_IP-19-2956_nl.htm

35 https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr_in_numbers_1.pdf

36 Zie het verslag van de groep van diverse belanghebbenden op het gebied van de algemene verordening gegevensbescherming:

37 Zie het verslag van de groep van diverse belanghebbenden op het gebied van de algemene verordening gegevensbescherming:

38 Artikel 80, lid 1, van de verordening.

39 Artikel 80, lid 2, van de verordening.

De noodzaak om door te gaan met voorlichting

Daarom moet op nationaal en EU-niveau worden doorgegaan met de dialoog en de voorlichtingsinspanningen die zijn gericht op het publiek. Hiervoor heeft de Commissie in juli 2019 een nieuwe onlinecampagne gelanceerd[40] om mensen aan te moedigen om privacyverklaringen te lezen en hun privacyinstellingen te optimaliseren.

V. Ondernemingen passen hun werkwijzen aan

Met de verordening wordt beoogd om ondernemingen te ondersteunen in de digitale economie door toekomstbestendige oplossingen te bieden. Over het algemeen zijn ondernemingen blij met het verantwoordelijkheidsbeginsel dat anders is dan de vorige, tijdrovende *ex ante*-aanpak (schrappen van kennisgevingsverplichtingen, schaalbaarheid van verplichtingen en flexibiliteit van het beginsel van gegevensbescherming door ontwerp en door standaardinstellingen waardoor mededinging op basis van privacyvriendelijke oplossingen mogelijk is). Tegelijkertijd vragen sommige ondernemingen om meer rechtszekerheid en aanvullende of duidelijkere richtsnoeren van gegevensbeschermingsautoriteiten[41].

Gedegen gegevensbeheer

Door ondernemingen wordt een aantal uitdagingen gemeld waar zij bij de aanpassing aan de regels mee te maken hebben[42]. Anderzijds wordt door veel ondernemingen benadrukt dat het ook een gelegenheid was om gegevensbescherming onder de aandacht van de raad van bestuur te brengen, orde op zaken te stellen met betrekking tot de gegevens die zij bezitten, de veiligheid te verbeteren, beter voorbereid te zijn op incidenten, de blootstelling aan onnodige risico's te verlagen en relaties op basis van vertrouwen op te bouwen met hun klanten en commerciële partners. Wat betreft transparantie melden bedrijfs- en maatschappelijke organisaties dat het soms lastig is om een balans te vinden tussen het verstrekken van alle informatie waarom uit hoofde van de verordening is gevraagd en tegelijkertijd duidelijk en helder taalgebruik en een vorm te hanteren die mensen begrijpen. Hiervoor worden door de marktdeelnemers innovatieve oplossingen ontwikkeld.

Ondernemingen gaven doorgaans aan dat zij de nieuwe rechten voor betrokkenen konden invoeren, hoewel het soms een uitdaging was om de deadlines te halen vanwege het gestegen aantal verzoeken en de meer uiteenlopende aard ervan[43], of om de identiteit te controleren van de persoon die het verzoek doet.

---

40 Dit is een vervolg op een eerdere campagne die gericht was op het verspreiden van informatiemateriaal voor mensen en ondernemingen op: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_nl

41 Zie het verslag van de groep van diverse belanghebbenden op het gebied van de verordening.

42 Het actualiseren van het IT-systeem wordt vaak genoemd als een van de grootste uitdagingen, voornamelijk wat betreft de uitvoering van de beginselen van gegevensbescherming door ontwerp en door standaardinstellingen, het recht op wissing in back-ups enz.

43 Ook pleiten ondernemingen voor richtsnoeren van het Comité over ongegronde en buitensporige verzoeken.

Gevolgen voor innovatie

In de verordening wordt de ontwikkeling van nieuwe technologieën niet alleen toegestaan, maar zelfs aangemoedigd, terwijl het grondrecht op bescherming van persoonsgegevens in acht wordt genomen. Dit is het geval voor gebieden zoals kunstmatige intelligentie.

Ondernemingen zijn begonnen met het ontwikkelen van nieuwe, meer privacyvriendelijke diensten. Zo krijgen zoekmachines die gebruikers niet volgen of die niet gedragsgericht adverteren, in sommige lidstaten een steeds groter marktaandeel. Andere ondernemingen ontwikkelen diensten die voortbouwen op nieuwe rechten van personen, zoals de overdraagbaarheid van hun persoonsgegevens. Een groeiend aantal ondernemingen bevordert de inachtneming van persoonsgegevens als aanbeveling om zich te onderscheiden van de concurrentie. Deze ontwikkelingen zijn niet beperkt tot de EU, maar gelden ook voor innovatieve buitenlandse economieën[44].

De specifieke situatie van kleine en micro-ondernemingen met een "laag risico"

Hoewel de situatie tussen de lidstaten varieert, kwamen de meeste vragen over de toepassing van de verordening onder meer van kleine en micro-ondernemingen[45] waarvoor de verwerking van persoonsgegevens geen hoofdactiviteit is. Hoewel deze vragen gedeeltelijk voortkwamen uit een gebrek aan kennis van de gegevensbeschermingsregels, werden hun zorgen soms ook vergroot door campagnes van bureaus die betaald advies willen leveren, door de verspreiding van onjuiste informatie, bijvoorbeeld over de noodzaak systematisch toestemming te verkrijgen van personen[46], en door aanvullende voorwaarden op nationaal niveau.

In dit verband vragen kleine en micro-ondernemingen om richtsnoeren met praktische informatie die zijn afgestemd op hun specifieke situatie. Sommige gegevensbeschermingsautoriteiten hebben dit op nationaal niveau al gedaan[47]. In aanvulling op nationale initiatieven heeft de Commissie informatiemateriaal verstrekt om deze ondernemingen te helpen om via een reeks praktische stappen aan de nieuwe regels te voldoen[48].

Gebruikmaken van de instrumenten uit de verordening

In de verordening worden instrumenten aangeboden om aan te tonen dat de verordening wordt nageleefd, zoals standaardcontractbepalingen, gedragscodes en de nieuwe certificeringsmechanismen.

---

44 Volgens een verslag van de Israëlische vereniging voor de cyberbeveiligingsindustrie was de subsector "Gegevensbescherming en privacy" deels als gevolg van de inwerkingtreding van de AVG in 2018 de snelst groeiende subsector van de cyberbeveiliging.

45 Zoals gedefinieerd op: https://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_nl

46 De verordening baseert zich in feite niet uitsluitend op toestemming, maar bevat verschillende rechtsgronden voor de verwerking van persoonsgegevens.

47 Bijvoorbeeld deze gids van de Franse gegevensbeschermingsautoriteit: https://www.cnil.fr/fr/la-cnil-et-bpifrance-sassocient-pour-accompagner-les-tpe-et-pme-dans-leur-appropriation-du-reglement

48 https://ec.europa.eu/commission/sites/beta-political/files/ds-02-18-544-nl-n.pdf

Standaardcontractbepalingen zijn modelbepalingen die vrijwillig kunnen worden opgenomen in een contract, bijvoorbeeld tussen een verwerkingsverantwoordelijke en een verwerker, en waarin de verplichtingen van de contracterende partijen uit hoofde van de verordening staan. Overeenkomstig de verordening kunnen de standaardcontractbepalingen zowel voor internationale doorgiften als binnen de EU worden gebruikt[49]. Op het gebied van internationale doorgiften blijkt uit het wijdverbreide gebruik ervan[50] dat ze erg nuttig zijn voor ondernemingen die de verordening willen naleven en met name voor ondernemingen die niet de middelen hebben om met al hun contractanten die gegevens verwerken, te onderhandelen over individuele contracten.

In een aantal sectoren wordt het vaststellen van standaardcontractbepalingen gezien als een nuttige manier om harmonisatie te bevorderen, met name als de Commissie dit doet. De Commissie zal samenwerken met belanghebbenden om gebruik te maken van de mogelijkheden uit de verordening en om bestaande bepalingen te actualiseren.

De naleving van gedragscodes is een ander operationeel en praktisch instrument waarover de bedrijfstak beschikt om gemakkelijker aan te tonen dat de verordening wordt nageleefd[51]. Deze codes moeten worden ontwikkeld door brancheverenigingen of organen die categorieën van de verwerkingsverantwoordelijken en verwerkers vertegenwoordigen, en hierin moet worden beschreven hoe de gegevensbeschermingsregels in een bepaalde sector kunnen worden ingevoerd. Doordat deze het ijkpunt vormen van de verplichtingen en de risico's[52], zouden ze voor kleine en middelgrote ondernemingen een nuttige en kosteneffectieve manier kunnen zijn om aan hun verplichtingen te voldoen.

Ten slotte kan certificering ook een nuttig instrument zijn om aan te tonen dat bepaalde voorwaarden uit de verordening worden nageleefd. Hierdoor kan de rechtszekerheid voor ondernemingen worden vergroot en de verordening wereldwijd worden ondersteund. Met de richtsnoeren voor certificering en accreditatie[53] die het Europees Comité voor gegevensbescherming onlangs heeft vastgesteld, is het mogelijk om in de EU certificeringsregelingen te ontwikkelen. De Commissie houdt deze ontwikkelingen in de gaten en zal indien nodig gebruikmaken van de bevoegdheid uit de verordening om certificeringsvereisten op te stellen. De Commissie heeft ook het recht om voor elementen die

---

49 Zie artikel 28 van de verordening. Door de Commissie vastgestelde standaardcontractbepalingen zijn geldig in de hele EU. De bepalingen die uit hoofde van artikel 28, lid 8, zijn vastgesteld door een gegevensbeschermingsautoriteit, zijn daarentegen uitsluitend bindend voor de autoriteit die deze heeft vastgesteld, en kunnen daarom volgens artikelen 55 en 56 als standaardcontractbepalingen worden gebruikt voor verwerkingen die onder de jurisdictie van die autoriteit vallen.

50 Standaardcontractbepalingen zijn het belangrijkste instrument dat ondernemingen inzetten voor de uitvoer van gegevens.

51 Het Europees Comité voor gegevensbescherming heeft op 4 juni 2019 richtsnoeren voor gedragscodes vastgesteld. Zij vormen een toelichting op de regels en procedures rond de indiening, goedkeuring en bekendmaking van codes op nationaal en Europees niveau.

52 Overweging 98 van de verordening.

53 https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_en; https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42018-accreditation-certification-bodies-under_en

relevant zijn voor de verordening, normalisatieverzoeken in te dienen bij de normalisatie-instellingen van de EU.

VI. De opwaartse convergentie neemt internationaal toe

Niet alleen in de EU wordt er gevraagd om de bescherming van persoonsgegevens. Zoals blijkt uit een recent wereldwijd onderzoek over internetbeveiliging is er over de hele wereld een groeiend gebrek aan vertrouwen, waardoor mensen zich online anders gaan gedragen[54]. Steeds meer bedrijven nemen deze zorgen weg door vrijwillig de rechten die voortkomen uit de verordening, ook toe te kennen aan hun klanten die buiten de EU gevestigd zijn.

Nu landen over de hele wereld vergelijkbare uitdagingen steeds meer aanpakken, worden in toenemende mate gegevensbeschermingsregels opgesteld of bestaande regels geactualiseerd. Deze wetten vertonen vaak een aantal overeenkomsten met het stelsel voor gegevensbescherming van de EU, zoals overkoepelende wetgeving in plaats van regels per bedrijfstak, afdwingbare individuele rechten en een onafhankelijke toezichthoudende autoriteit. Deze tendens is echt wereldwijd te zien, van Zuid-Korea tot Brazilië, van Chili tot Thailand en van India tot Indonesië. Het groeiende, wereldwijde lidmaatschap van "Verdrag 108" van de Raad van Europa[55] – dat onlangs is geactualiseerd[56] met een aanzienlijke bijdrage van de Commissie – is een ander duidelijk teken van deze tendens van opwaartse convergentie.

Het bevorderen van veilige en vrije gegevensstromen onder andere door middel van adequaatheidsbesluiten

Deze groeiende convergentie biedt nieuwe mogelijkheden voor het bevorderen van gegevensstromen, en daarmee ook de handel en samenwerking tussen overheidsautoriteiten, terwijl de gegevens van personen in de EU als deze worden doorgegeven naar het buitenland, tegelijkertijd beter worden beschermd.

---

[54] Zie 2019 CIGI-Ipsos Global Survey on Internet Security and Trust. Volgens dat onderzoek maakte 78 % van de onderzochte personen zich zorgen over hun online privacy, waarbij 49 % aangaf dat dit wantrouwen ervoor had gezorgd dat ze online minder persoonsgegevens openbaar maakten, terwijl 43 % aangaf hun apparaat zorgvuldiger te beveiligen en 39 % antwoordde naast andere voorzorgsmaatregelen selectiever gebruik te maken van internet. Het onderzoek werd uitgevoerd in 25 economieën: Australië, Brazilië, Canada, China, Duitsland, Egypte, Frankrijk, Groot-Brittannië, Hongkong, India, Indonesië, Italië, Japan, Kenia, Mexico, Nigeria, Pakistan, Polen, Rusland, Tunesië, Turkije, Verenigde Staten, Zuid-Afrika, Zuid-Korea en Zweden.

[55] Verdrag van de Raad van Europa van 28 januari 1981 tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (ETS nr. 108) en Aanvullend Protocol van 2001 bij het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens inzake toezichthoudende autoriteiten en grensoverschrijdend verkeer van gegevens (ETS nr. 181). Dit is het enige bindende internationale instrument op het gebied van gegevensbescherming. Meest recent is het verdrag geratificeerd door Argentinië, Mexico, Kaapverdië en Marokko.

[56] Protocol tot wijziging van het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (ETS nr. 108), zoals op 17-18 mei 2018 te Helsingør, Denemarken, is overeengekomen tijdens de 128e zitting van het Comité van Ministers. De geconsolideerde tekst van het geactualiseerde Verdrag 108 is te vinden op: https://rm.coe.int/16808ade9d

Bij de uitvoering van de strategie uit haar mededeling uit 2017 betreffende de uitwisseling en bescherming van persoonsgegevens in een geglobaliseerde wereld[57] heeft de Commissie haar overleg met derde landen en andere internationale partners geïntensiveerd, waarbij werd voortgebouwd op de convergentie tussen privacysystemen en deze verder werd ontwikkeld. Dit omvat onder andere het nagaan of er met bepaalde derde landen adequaatheidsvaststellingen kunnen worden gedaan[58]. Dit werk heeft belangrijke resultaten opgeleverd, voornamelijk de inwerkingtreding van de wederzijdse adequaatheidsregeling tussen de EU en Japan in februari 2019, waarmee de grootste ruimte voor vrije en veilige gegevensstromen ter wereld werd gecreëerd. De adequaatheidsonderhandelingen met Zuid-Korea zijn in een gevorderd stadium en er worden verkennende werkzaamheden uitgevoerd met het oog op het voeren van gesprekken over adequaatheid met verschillende Latijns-Amerikaanse landen, zoals Chili of Brazilië, afhankelijk van de voltooiing van lopende wetgevingsprocessen. Er zijn ook veelbelovende ontwikkelingen in enkele delen van Azië, zoals India, Indonesië en Taiwan, en in Oost- en Zuid-Europa, die wellicht leiden tot toekomstige adequaatheidsbesluiten.

Tegelijkertijd is de Commissie ingenomen met het feit dat andere landen die doorgifte-instrumenten hebben ingesteld die vergelijkbaar zijn met de adequaatheid van de verordening, hebben erkend dat de EU en landen die de EU als "adequaat" heeft erkend, het vereiste beschermingsniveau waarborgen[59]. Hierdoor kan mogelijk een netwerk van landen worden gecreëerd waarbinnen vrijelijk gegevens kunnen worden doorgegeven.

Bovendien wordt er intensief samengewerkt met andere derde landen, zoals Canada, Nieuw-Zeeland, Argentinië en Israël, om de continuïteit van adequaatheidsbesluiten die zijn vastgesteld op basis van de gegevensbeschermingsrichtlijn uit 1995 onder de verordening te waarborgen. Het is intussen aangetoond dat het EU-VS-privacyschild met meer dan 4 700 deelnemende ondernemingen een nuttig instrument is om trans-Atlantische gegevensstromen een hoog beschermingsniveau te bieden[60]. Dankzij de jaarlijkse toetsing wordt de werking van het kader regelmatig gecontroleerd en kunnen nieuwe problemen tijdig worden aangepakt.

Aangezien er geen standaardoplossing voor gegevensstromen bestaat, werkt de Commissie ook samen met belanghebbenden en het Comité om het volledige potentieel van de instrumenten voor internationale doorgiften uit de verordening te benutten. Deze instrumenten zijn onder andere standaardcontractbepalingen, de ontwikkeling van certificeringsregelingen, gedragscodes of administratieve regelingen voor publieke instanties. In dat opzicht is de Commissie geïnteresseerd in de uitwisseling van ervaringen en best practices met andere systemen die mogelijk een specifieke expertise hebben ontwikkeld voor sommige van deze instrumenten. De Commissie zal overwegen gebruik te maken van de bevoegdheden die uit

---

[57] Mededeling van de Commissie aan het Europees Parlement en de Raad "Uitwisseling en bescherming van persoonsgegevens in een geglobaliseerde wereld" (COM(2017) 7 final).

[58] Dankzij de verordening is er ook een mogelijkheid gecreëerd voor adequaatheidsvaststellingen met betrekking tot internationale organisaties, als onderdeel van de inspanningen van de EU om de uitwisseling van gegevens met dergelijke entiteiten te vergemakkelijken.

[59] Deze aanpak wordt onder andere in Argentinië, Colombia, Israël en Zwitserland gehanteerd.

[60] Dit betekent dat het privacyschild in de eerste drie jaar van zijn bestaan meer deelnemende ondernemingen heeft dan zijn voorganger Safe Harbour na dertien jaar had.

hoofde van de verordening zijn toegekend met betrekking tot die doorgifte-instrumenten, en dan met name de standaardcontractbepalingen.

Het zou de moeite waard kunnen zijn om naast puur bilaterale instrumenten te onderzoeken of gelijkgestemde landen op dit gebied een multinationaal kader zouden kunnen vormen, in een tijd waarin gegevensstromen een steeds essentiëler deel van de handel, communicatie en sociale interactie vormen. Met een dergelijk instrument zouden gegevens vrijelijk door de contracterende partijen kunnen worden doorgegeven, waarbij tevens het vereiste beschermingsniveau wordt gewaarborgd op basis van gedeelde waarden en convergerende systemen. Dit zou bijvoorbeeld kunnen worden ontwikkeld op basis van het geactualiseerde Verdrag 108 of het begin dit jaar door Japan gestarte initiatief "Data Free Flow with Trust".

Het ontwikkelen van nieuwe synergieën tussen de handel en gegevensbeschermingsinstrumenten

Terwijl de Commissie de convergentie van gegevensbeschermingsnormen op internationaal niveau bevordert, stelt zij ook alles in het werk om digitaal protectionisme te voorkomen. Hiervoor heeft zij specifieke bepalingen over gegevensstromen en gegevensbescherming in handelsovereenkomsten ontwikkeld die zij tijdens bilaterale en multilaterale onderhandelingen, zoals de huidige gesprekken van de WTO over e-handel, systematisch aan de orde stelt. Met deze horizontale bepalingen worden puur protectionistische maatregelen, zoals voorschriften voor verplichte gegevenslokalisatie, uitgesloten, terwijl de partijen de regelgevende autonomie behouden om het grondrecht op gegevensbescherming te beschermen.

Hoewel gesprekken over gegevensbescherming en handelsbesprekingen een ander verloop hebben, kunnen ze elkaar aanvullen. De wederzijdse adequaatheidsregeling tussen de EU en Japan is het beste voorbeeld van een dergelijke synergie: hierdoor worden commerciële uitwisselingen vergemakkelijkt, waardoor de voordelen van de economische partnerschapsovereenkomst worden versterkt. Dit soort convergentie, die is gebaseerd op gedeelde waarden en hoge normen en wordt ondersteund door doeltreffende handhaving, zorgt in feite voor de sterkste basis voor de uitwisseling van persoonsgegevens. Steeds meer internationale partners erkennen dit ook[61]. Aangezien ondernemingen steeds vaker grensoverschrijdend actief zijn en bij voorkeur in de hele wereld soortgelijke regels toepassen, draagt een dergelijke convergentie bij aan een klimaat dat bevorderlijk is voor directe investeringen, waardoor de handel wordt vergemakkelijkt en er meer vertrouwen tussen handelspartners bestaat.

De uitwisseling van informatie vergemakkelijken om criminaliteit en terrorisme tegen te gaan op basis van passende waarborgen

Als gegevensbeschermingsstelsels beter op elkaar zijn afgestemd, wordt de hoognodige uitwisseling van informatie tussen de Europese en buitenlandse regelgevende, politiële en

[61] Zoals bijvoorbeeld blijkt uit de verwijzing naar het concept "Data Free Flow with Trust" uit de verklaring van de G20-leiders van Osaka: https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf

justitiële autoriteiten veel gemakkelijker, waardoor er effectiever en sneller kan worden samengewerkt op het gebied van wetshandhaving[62]. Daarom overweegt de Commissie de mogelijkheid om adequaatheidsbesluiten vast te stellen uit hoofde van de richtlijn wetshandhaving en zo de samenwerking met belangrijke partners voor het bestrijden van criminaliteit en terrorisme te verdiepen. Bovendien kan de "raamovereenkomst" tussen de EU en de VS[63], die in februari 2017 van kracht is geworden, als model dienen voor vergelijkbare overeenkomsten met andere belangrijke veiligheidspartners.

Andere voorbeelden die wijzen op het belang van hoge normen voor gegevensbescherming als basis voor stabiele samenwerking op het gebied van wetshandhaving met derde landen, zijn de overdracht van persoonsgegevens van passagiers (PNR-gegevens)[64] en de uitwisseling van operationele informatie tussen Europol en belangrijke internationale partners. In dit opzicht zijn er momenteel onderhandelingen over internationale overeenkomsten gaande of op het punt van beginnen met verschillende landen van het Zuidelijk Nabuurschap[65].

Sterke waarborgen voor gegevensbescherming zullen ook een essentieel onderdeel zijn van toekomstige overeenkomsten voor grensoverschrijdende toegang tot elektronisch bewijsmateriaal in strafrechtelijke onderzoeken op bilateraal (overeenkomst tussen de EU en de VS) of multilateraal niveau (tweede aanvullend protocol bij het Verdrag van Boedapest van de Raad van Europa inzake cybercriminaliteit)[66].

Het bevorderen van samenwerking tussen handhavingsinstanties

Nu problemen met de inachtneming van privacy of veiligheidsincidenten gevolgen kunnen hebben voor een groot aantal personen in verschillende rechtsgebieden tegelijk, kunnen nauwere samenwerkingsvormen tussen toezichthoudende autoriteiten op internationaal niveau ervoor zorgen dat individuele rechten doeltreffender worden beschermd en dat er een stabiel klimaat voor ondernemers bestaat. Tegen deze achtergrond en in nauw overleg met het Comité werkt de Commissie aan manieren om samenwerking op het gebied van handhaving en wederzijdse bijstand tussen de Europese en buitenlandse toezichthoudende autoriteiten te

---

62 Zie de mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's "De Europese veiligheidsagenda" (COM(2015) 185 final).

63 Overeenkomst tussen de EU en de VS over de bescherming van persoonsgegevens die worden doorgegeven en verwerkt met het oog op het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, waaronder terrorisme, in het kader van politiële en justitiële samenwerking in strafzaken. https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=celex:22016A1210(01) (de "raamovereenkomst"). De raamovereenkomst vormt de eerste bilaterale internationale overeenkomst op het gebied van wetshandhaving met daarin een veelomvattend overzicht van gegevensbeschermingsrechten en -verplichtingen conform het EU-acquis. Het is een succesvol voorbeeld van hoe de samenwerking op het gebied van wetshandhaving met een belangrijke internationale partner kan worden verbeterd door te onderhandelen over sterke gegevensbeschermingswaarborgen.

64 In resolutie 2396 van de Veiligheidsraad van de Verenigde Naties van 21 december 2017 worden alle lidstaten van de VN opgeroepen om het vermogen te ontwikkelen om PNR-gegevens te verzamelen, verwerken en analyseren met volledige inachtneming van de mensenrechten en fundamentele vrijheden. Zie ook de mededeling van de Commissie "De Europese veiligheidsagenda" (COM(2015) 185 final): http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52015DC0185

65 https://ec.europa.eu/home-affairs/news/security-union-strengthening-europols-cooperation-third-countries-fight-terrorism-and-serious_en

66 http://europa.eu/rapid/press-release_IP-19-2891_en.htm

vergemakkelijken, onder meer door gebruik te maken van de nieuwe bevoegdheden op grond van de verordening[67]. Daarbij zou het kunnen gaan om verschillende samenwerkingsvormen, variërend van het ontwikkelen van gemeenschappelijke praktische of interpretatiehulpmiddelen[68] tot het uitwisselen van informatie over lopende onderzoeken.

Ten slotte is de Commissie ook voornemens om de dialoog met regionale organisaties en netwerken te intensiveren, zoals de Associatie van Zuidoost-Aziatische staten (ASEAN), de Afrikaanse Unie, het Asia Pacific Privacy Authorities forum (APPA) of het Ibero-American Data Protection Network, organisaties die een steeds grotere rol spelen bij het opstellen van gemeenschappelijke normen voor gegevensbescherming, het bevorderen van de uitwisseling van best practices en het stimuleren van de samenwerking tussen handhavingsinstanties. Bovendien zal de Commissie samenwerken met de Organisatie voor Economische Samenwerking en Ontwikkeling en de Asian-Pacific Economic Cooperation Organisation voor meer convergentie met het oog op een hoog niveau van gegevensbescherming.

VII. Gegevensbeschermingswetgeving als integraal onderdeel van zeer uiteenlopende beleidsregels

De bescherming van persoonsgegevens is in verschillende beleidsregels van de Unie gewaarborgd en opgenomen.

Diensten op het gebied van telecommunicatie en elektronische communicatie

De Commissie heeft haar voorstel voor een Verordening betreffende privacy en elektronische communicatie in januari 2017 aangenomen[69]. Het doel van het voorstel was het beschermen van de vertrouwelijkheid van communicatie, zoals is vastgesteld in het Handvest van de grondrechten, maar ook om persoonsgegevens te beschermen die onderdeel zijn van communicatie en eindapparatuur van gebruikers.

De voorgestelde e-privacyverordening is dankzij de specifieke regels voor de bovenstaande doeleinden een specificatie van en aanvulling op de verordening. De verordening is een modernisering van de huidige e-privacyregels van de EU[70] met het oog op technologische en juridische ontwikkelingen. De privacy van personen wordt verbeterd, omdat de nieuwe regels ook gelden voor over-the-top communicatiediensten, waardoor een gelijk speelveld wordt gecreëerd voor alle elektronische-communicatiediensten. Hoewel het Europees Parlement in oktober 2017 een mandaat heeft vastgesteld om trialogen te beginnen, heeft de Raad nog geen overeenstemming bereikt over een algemene aanpak. De Commissie blijft zich volledig

---

67 Zie artikel 50 van de verordening over internationale samenwerking op het gebied van gegevensbescherming. Dit artikel heeft betrekking op uiteenlopende samenwerkingsvormen, van informatie over gegevensbeschermingswetgeving tot de doorverwijzing van klachten en bijstand bij onderzoeken.

68 Zoals gemeenschappelijke templates voor kennisgevingen van inbreuken.

69 https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A52017PC0010

70 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).

inzetten voor de e-privacyverordening en ondersteunt de medewetgevers bij hun inspanningen om de voorgestelde verordening snel vast te stellen.

Gezondheid en onderzoek

Het vergemakkelijken van de uitwisseling van gezondheidsgegevens, die uit hoofde van de verordening gevoelige gegevens zijn, tussen lidstaten is om redenen van algemeen belang steeds belangrijker op het gebied van volksgezondheid. Een aantal van deze redenen zijn het verlenen van gezondheidszorg of behandelingen, bescherming tegen ernstige grensoverschrijdende bedreigingen van de gezondheid en het waarborgen van hoge normen inzake kwaliteit en veiligheid van de gezondheidszorg en van geneesmiddelen of medische hulpmiddelen. In de verordening staan de regels die zorgen voor de wettige en betrouwbare verwerking en uitwisseling van gezondheidsgegevens in de EU. Deze regels zijn ook van toepassing op de toegang tot de medische gegevens van patiënten door derden, met inbegrip van patiëntgegevens, e-recepten en op de lange termijn veelomvattende elektronische medische dossiers, en het gebruik hiervan voor wetenschappelijk onderzoek. Voor klinische proeven heeft de Commissie ook specifieke vragen en antwoorden opgesteld over de wisselwerking tussen de verordening betreffende klinische proeven[71] en de algemene verordening gegevensbescherming:[72].

Kunstmatige intelligentie ("KI")

Omdat KI van steeds groter strategisch belang is, is het noodzakelijk om wereldwijde regels op te stellen voor de ontwikkeling en het gebruik ervan. Bij de bevordering van de ontwikkeling en het gebruik van KI heeft de Commissie gekozen voor een mensgerichte benadering, wat betekent dat KI-toepassingen de grondrechten moeten eerbiedigen[73]. In deze context vormen de regels uit de verordening een algemeen kader met specifieke verplichtingen en rechten die met name relevant zijn voor de verwerking van persoonsgegevens in KI. Zo bevat de verordening het recht om niet te worden onderworpen aan uitsluitend geautomatiseerde besluitvorming, met uitzondering van bepaalde situaties[74]. Bovendien bevat de verordening specifieke voorschriften voor transparantie met betrekking tot het gebruik van geautomatiseerde besluitvorming, te weten de verplichting om kennis te geven van het bestaan van dergelijke besluiten en het verstrekken van nuttige informatie en uitleg over het belang en de verwachte gevolgen van de verwerking voor de betrokkene[75]. De

---

71 https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=celex%3A32014R0536

72 https://ec.europa.eu/health/sites/health/files/files/documents/qa_clinicaltrials_gdpr_en.pdf

73 Mededeling van de Commissie van 8 april 2019 "Vertrouwen kweken in mensgerichte kunstmatige intelligentie": https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2019:0168:FIN:NL:PDF Ethische richtsnoeren voor betrouwbare KI van de deskundigengroep op hoog niveau (HLEG) van 8 april 2019: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60434. Zie ook de aanbeveling van de OESO-raad betreffende kunstmatige intelligentie: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449, de AI-beginselen van de G20 die zijn ondersteund door de verklaring van de G20-leiders van Osaka: https://www.g20.org/pdf/documents/en/annex_08.pdf en de ministeriële verklaring van de G20 betreffende handel en digitale economie: https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf

74 Artikel 22 van de verordening.

75 Artikel 13, lid 2, onder f), van de verordening.

deskundigengroep op hoog niveau inzake KI[76], de Organisatie voor Economische Samenwerking en Ontwikkeling[77] en de G20[78] hebben erkend dat de kernbeginselen van de verordening zeer relevant zijn voor het aanpakken van de uitdagingen en mogelijkheden die uit KI voortkomen. Het Europees Comité voor gegevensbescherming heeft KI aangemerkt als één van de mogelijke onderwerpen voor het Werkprogramma voor 2019-2020[79].

Vervoer

De ontwikkeling van verbonden voertuigen en intelligente steden is steeds meer afhankelijk van de verwerking en uitwisseling van grote hoeveelheden persoonsgegevens tussen meerdere partijen, waaronder auto's, autofabrikanten, dienstverleners op het gebied van telematica en overheidsautoriteiten die verantwoordelijk zijn voor de wegeninfrastructuur. Door de betrokkenheid van meerdere partijen is er sprake van een bepaalde complexiteit voor de toekenning van de rollen en verantwoordelijkheden aan de verschillende actoren die betrokken zijn bij de verwerking van persoonsgegevens en voor het waarborgen van de rechtmatigheid van de verwerking door alle actoren. De naleving van de verordening en de e-privacywetgeving zijn essentieel om intelligente vervoerssystemen succesvol in te zetten in alle vervoerswijzen en de verspreiding van digitale hulpmiddelen en diensten waardoor personen en zaken mobieler zijn[80].

Energie

De ontwikkeling van digitale oplossingen in de energiesector is steeds meer afhankelijk van de verwerking van persoonsgegevens. De wetgeving die is vastgesteld als onderdeel van het pakket Schone energie voor alle Europeanen[81], bevat nieuwe bepalingen om de digitalisering van de elektriciteitssector mogelijk te maken en regels over toegang tot gegevens, gegevensbeheer en interoperabiliteit die toestaan dat de realtimegegevens van consumenten worden behandeld met het oog op besparingen en het bevorderen van zelfopwekking en participatie op de energiemarkt. Daarom is het voor de succesvolle uitvoering van deze bepalingen van groot belang dat de gegevensbeschermingsregels worden nageleefd.

---

76 https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence

77 Aanbeveling van de Raad betreffende kunstmatige intelligentie: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

78 Ministeriële verklaring van de G20 betreffende handel en digitale economie: https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf

79 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12plen-2.1edpb_work_program_en.pdf

80 Bijvoorbeeld door de planning en het gebruik van verschillende vervoerswijzen tijdens hun reis te vergemakkelijken.

81 Met name de elektriciteitsrichtlijn: https://eur-lex.europa.eu/legal-content/NL/ALL/?uri=CELEX%3A32009L0072

Mededinging

De verwerking van persoonsgegevens is een element waarmee steeds meer rekening moet worden gehouden in mededingingsbeleid[82]. Aangezien gegevensbeschermingsautoriteiten de enige autoriteiten zijn die een schending van de gegevensbeschermingsregels mogen beoordelen, werken autoriteiten op het gebied van mededinging, consumenten en gegevensbescherming samen op het snijpunt van hun respectieve bevoegdheden. De Commissie stimuleert deze samenwerking en volgt de ontwikkelingen nauwlettend.

Verkiezingen

In de Richtsnoeren voor het gebruik van persoonsgegevens in het kader van verkiezingen[83], die in september 2018 zijn gepubliceerd als onderdeel van het verkiezingspakket[84], heeft de Commissie de aandacht gevestigd op regels die van belang zijn voor de bij verkiezingen betrokken actoren, waaronder problemen in verband met de micro-targeting van kiezers. Deze richtsnoeren komen terug in een verklaring van het Europees Comité voor gegevensbescherming[85], en door een aantal gegevensbeschermingsautoriteiten zijn op nationaal niveau richtsnoeren gepubliceerd. In het verkiezingspakket worden alle lidstaten bovendien opgeroepen om een nationaal electoraal samenwerkingsnetwerk op te zetten van bevoegde autoriteiten op het gebied van verkiezingskwesties en autoriteiten die verantwoordelijk zijn voor het toezicht op en de handhaving van de regels, zoals gegevensbescherming, voor online activiteiten die relevant zijn voor de verkiezingen. Er zijn tevens nieuwe maatregelen vastgesteld voor het invoeren van sancties voor de overtreding van de gegevensbeschermingsregels door Europese politieke partijen en stichtingen. De Commissie heeft de lidstaten aanbevolen op nationaal niveau dezelfde aanpak te volgen. Ook bij de evaluatie van de verkiezingen voor het Europees Parlement in 2019, die in oktober 2019 wordt gepubliceerd, wordt rekening gehouden met gegevensbeschermingsaspecten.

Wetshandhaving

Een doeltreffende, echte veiligheidsunie kan uitsluitend worden opgezet op basis van de volledige naleving van de grondrechten die zijn vastgelegd in het EU-handvest en de secundaire EU-wetgeving, met inbegrip van passende gegevensbeschermingswaarborgen om de veilige uitwisseling van persoonsgegevens ten behoeve van de wetshandhaving te garanderen. De noodzaak en evenredigheid van alle beperkingen van het grondrecht op privacy en gegevensbescherming worden streng getoetst.

---

82 Bijvoorbeeld zaak M.8788 – Apple/Shazam en zaak M.8124 – Microsoft/LinkedIn.

83 https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52018DC0638

84 http://europa.eu/rapid/press-release_IP-18-5681_nl.htm

85 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf

VIII. Conclusie

Op basis van de op dit moment beschikbare informatie en de dialoog met belanghebbenden is de Commissie vooralsnog van oordeel dat de toepassing van de verordening in het eerste jaar over het algemeen positief was. Zoals uit deze mededeling blijkt, moet er op een aantal gebieden echter vooruitgang worden geboekt.

Het ten uitvoer leggen en aanvullen van het rechtskader:

- De drie lidstaten die hun nationale gegevensbeschermingswet nog niet hebben geactualiseerd, moeten dit met spoed doen. Alle lidstaten moeten hun sectorale wetgeving volledig afstemmen op de voorschriften van de verordening.

- De Commissie zal alle instrumenten waarover zij beschikt, waaronder inbreukprocedures, gebruiken om ervoor te zorgen dat de lidstaten de verordening naleven en om de fragmentatie van het kader voor gegevensbescherming te beperken.

Zorgen dat het nieuwe beheersysteem volledig wordt ontplooid:

- De lidstaten moeten de nationale gegevensbeschermingsautoriteiten voldoende personele, financiële en technische middelen verstrekken.

- De gegevensbeschermingsautoriteiten moeten hun samenwerking intensiveren, bijvoorbeeld door gezamenlijke onderzoeken uit te voeren. De lidstaten moeten de uitvoering van dergelijke onderzoeken vergemakkelijken.

- Het Comité moet een EU-cultuur van gegevensbescherming blijven ontwikkelen en volledig gebruik maken van de instrumenten uit de verordening om te waarborgen dat de regels geharmoniseerd worden toegepast. Het moet aan richtsnoeren blijven werken, met name voor kleine en middelgrote ondernemingen.

- De deskundigheid van het secretariaat van het Comité moet worden versterkt zodat de werkzaamheden van het Comité effectiever kunnen worden ondersteund en geleid.

- De Commissie blijft gegevensbeschermingsautoriteiten en het Comité ondersteunen, voornamelijk door actief deel te nemen aan de werkzaamheden van het Comité en zijn aandacht te vestigen op de voorschriften van het EU-recht tijdens de uitvoering van de verordening.

- De Commissie zal de interactie tussen gegevensbeschermingsautoriteiten en andere autoriteiten ondersteunen, met name op het gebied van mededinging, met volledige inachtneming van hun respectieve bevoegdheden.

Het ondersteunen en betrekken van belanghebbenden:

- Het Comité moet belanghebbenden beter bij zijn werkzaamheden betrekken. De Commissie blijft gegevensbeschermingsautoriteiten financieel ondersteunen, zodat zij belanghebbenden kunnen bereiken.

- De Commissie zet haar voorlichtingsactiviteiten en haar werk met belanghebbenden voort.

Het bevorderen van internationale convergentie:

- De Commissie intensiveert onder andere op het gebied van wetshandhaving haar dialoog met in aanmerking komende belangrijke partners betreffende adequaatheid. Zij streeft er in het bijzonder naar om de lopende onderhandelingen met Zuid-Korea de komende maanden af te ronden. In 2020 brengt zij verslag uit over de evaluatie van de elf adequaatheidsbesluiten die uit hoofde van de gegevensbeschermingsrichtlijn zijn vastgesteld.
- De Commissie zet haar werkzaamheden voort, onder andere door middel van technische bijstand, de uitwisseling van informatie en best practices met landen die interesse hebben in het vaststellen van moderne privacywetgeving, en de bevordering van samenwerking met de toezichthoudende autoriteiten van derde landen en regionale organisaties.
- De Commissie zal als initiatiefnemer voor handel en samenwerking samenwerken met multilaterale en regionale organisaties voor de bevordering van hoge normen voor gegevensbescherming (bijvoorbeeld onder het initiatief "Data Free Flow with Trust" dat Japan in het kader van de G20 is gestart).

Volgens de verordening[86] is de Commissie verplicht om in 2020 verslag uit te brengen over de uitvoering. Dit is een gelegenheid om de geboekte vooruitgang te beoordelen en om te bekijken of de verschillende onderdelen van het nieuwe gegevensbeschermingsstelsel na twee jaar volledig operationeel zijn. De Commissie zal hiervoor samenwerken met het Europees Parlement, de Raad, de lidstaten, het Europees Comité voor gegevensbescherming, relevante belanghebbenden en burgers.

[86] Artikel 97 van de verordening.