Advies 14/2021 betreffende het ontwerp van uitvoeringsbesluit van de Europese Commissie overeenkomstig Verordening (EU) 2016/679 betreffende de adequate bescherming van persoonsgegevens in het Verenigd Koninkrijk

Vastgesteld op 13 april 2021

Translations proofread by EDPB Members.
This language version has not yet been proofread.

INHOUDSOPGAVE

Het Europees Comité voor gegevensbescherming

Gezien artikel 70, lid 1, punt s), van 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 (hierna "AVG" genoemd),

Gezien de Overeenkomst betreffende de Europese Economische Ruimte (hierna "EER" genoemd), en met name bijlage XI en Protocol 37, als gewijzigd bij Besluit nr. 154/2018 van het Gemengd Comité van de EER van 6 juli 2018[1],

Gezien de artikelen 12 en 22 van zijn Reglement,

HEEFT HET VOLGENDE ADVIES VASTGESTELD:

1. SAMENVATTING

1. De Europese Commissie heeft op 19 februari 2021 haar ontwerpuitvoeringsbesluit (hierna "ontwerpbesluit" genoemd) over de adequate bescherming van persoonsgegevens door het Verenigd Koninkrijk (hierna "VK" genoemd) overeenkomstig de AVG goedgekeurd[2]. Vervolgens heeft de Europese Commissie het proces voor de formele vaststelling ervan ingeleid.

2. Op dezelfde datum heeft de Europese Commissie het Europees Comité voor gegevensbescherming (hierna "EDPB" genoemd) om advies gevraagd[3]. De EDPB heeft de adequaatheid van het in het VK geboden beschermingsniveau beoordeeld op basis van de bestudering van het ontwerpbesluit zelf, alsmede op basis van een analyse van de door de Europese Commissie beschikbaar gestelde documentatie.

3. De EDPB heeft zich toegespitst op de beoordeling van zowel de algemene AVG-aspecten van het ontwerpbesluit als op de toegang van overheidsinstanties tot persoonsgegevens die vanuit de EER worden doorgegeven met het oog op rechtshandhaving en nationale veiligheid, met inbegrip van de rechtsmiddelen die personen in de EER ter beschikking staan. De EDPB heeft ook nagegaan of de waarborgen waarin het Britse rechtskader voorziet van kracht zijn.

4. De EDPB heeft voor dit werk gebruikgemaakt van zijn AVG-adequaatheidsreferentie[4], die in februari 2018 is vastgesteld, en de Aanbevelingen 02/2020 over de Europese essentiële garanties voor surveillancemaatregelen[5].

[1] Met "lidstaten" worden in dit advies "EER-lidstaten" bedoeld.
[2] Zie persmededeling van de Europese Commissie, Gegevensbescherming: Europese Commissie start proces voor persoonsgegevensverkeer naar het VK, 19 februari 2021, https://ec.europa.eu/commission/presscorner/detail/nl/ip_21_661
[3] Idem.
[4] Zie Groep gegevensbescherming artikel 29, Adequaatheidsreferentie, vastgesteld op 28 november 2017, laatstelijk gewijzigd en vastgesteld op 6 februari 2018, WP254 rev.01 (bekrachtigd door de EDPB, zie https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines); (hierna "*AVG-adequaatheidsreferentie*" genoemd).
[5] Zie aanbevelingen 02/2020 van de EDPB over de Europese essentiële garanties voor surveillancemaatregelen, vastgesteld op 10 november 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_nl

1.1. Convergentiegebieden

5. De EDPB heeft als hoofddoel de Europese Commissie advies te bieden over de adequaatheid van het beschermingsniveau dat personen in het Verenigd Koninkrijk wordt geboden. Het is van belang te erkennen dat de EDPB niet verwacht dat het Britse rechtskader identiek is aan de Europese gegevensbeschermingswetgeving.

6. De EDPB wijst er echter op dat in artikel 45 AVG en in de jurisprudentie van het Hof van Justitie van de Europese Unie (hierna "HvJ-EU" genoemd) is bepaald dat de wetgeving van het derde land in overeenstemming moet zijn met de wezenlijke inhoud van de in de AVG verankerde grondbeginselen, wil zij geacht worden een passend beschermingsniveau te bieden. Het gegevensbeschermingskader van het Verenigd Koninkrijk is grotendeels gebaseerd op het gegevensbeschermingskader van de EU (met name de AVG en Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad, hierna "Richtlijn gegevensbescherming bij rechtshandhaving" genoemd), wat voortvloeit uit het feit dat het Verenigd Koninkrijk tot 31 januari 2020 een lidstaat van de EU was. Bovendien wordt in de Britse Data Protection Act 2018, die op 23 mei 2018 in werking is getreden en waarbij de Britse Data Protection Act 1998 is ingetrokken, de toepassing van de AVG in de Britse wetgeving verder gespecificeerd, naast de omzetting van de Richtlijn gegevensbescherming bij rechtshandhaving, en worden er bevoegdheden verleend en taken opgelegd aan de nationale toezichthoudende autoriteit voor gegevensbescherming, het Britse Information Commissioner's Office (hierna "ICO" genoemd). Daarom erkent de EDPB dat het Verenigd Koninkrijk de AVG grotendeels heeft overgenomen in zijn gegevensbeschermingskader.

7. **Bij de analyse van de wetgeving en praktijk van een derde land dat tot voor kort een EU-lidstaat was, is het duidelijk dat de EDPB veel aspecten als in grote lijnen overeenkomstig heeft aangemerkt.**

8. De EDPB merkt op het gebied van gegevensbescherming op dat het AVG-kader en het Britse rechtskader wat bepaalde kernbepalingen betreft sterk op elkaar zijn afgestemd, zoals bijvoorbeeld de begrippen (bv. "persoonsgegevens"; "verwerking van persoonsgegevens"; "verwerkingsverantwoordelijke"); gronden voor behoorlijke en rechtmatige verwerking voor legitieme doeleinden; doelbinding; kwaliteit en evenredigheid van de gegevens; bewaring van gegevens; beveiliging en vertrouwelijkheid; transparantie; bijzondere categorieën persoonsgegevens; direct marketing; geautomatiseerde besluitvorming en profilering.

1.2. Uitdagingen

9. Het Verenigd Koninkrijk was tot voor kort een lidstaat van de EU; daarom heeft de EDPB, bij de analyse van zijn wetgeving en praktijk, verschillende aspecten als in grote lijnen overeenkomstig aangemerkt. Tezelfdertijd heeft de EDPB, gelet op zijn rol in het vaststellen van een adequaatheidsbesluit, maar ook op de tijdsdruk, besloten zijn aandacht toe te spitsen op de aspecten die zijns inziens nadere bestudering en grondiger onderzoek behoeven.

10. Desalniettemin blijven er uitdagingen bestaan en de EDPB is van mening dat de volgende punten nader moeten worden onderzocht om ervoor te zorgen dat het in grote lijnen overeenkomstige beschermingsniveau wordt bereikt en dat de Europese Commissie in het VK nauwlettend moet toezien op de naleving ervan.

1.2.1. Algemeen

11. De eerste uitdaging is van algemene aard en heeft betrekking op het volgen van de ontwikkeling van het Britse rechtsstelsel inzake gegevensbescherming in het algemeen. Hoewel de Britse regering haar voornemen te kennen heeft gegeven om een afzonderlijk en onafhankelijk beleid inzake gegevensbescherming te ontwikkelen, met de mogelijke bedoeling om af te wijken van de EU-wetgeving inzake gegevensbescherming, hebben dergelijke politieke verklaringen nog geen concrete vorm gekregen in het Britse rechtskader. Deze mogelijke toekomstige **afwijking zou echter risico's kunnen inhouden voor de handhaving van het beschermingsniveau dat wordt geboden aan persoonsgegevens die vanuit de EU worden doorgegeven. Daarom wordt de Europese Commissie verzocht deze ontwikkelingen vanaf de inwerkingtreding van haar adequaatheidsbesluit nauwlettend te volgen en zo nodig de nodige maatregelen te nemen, onder meer door het besluit te wijzigen en/of op te schorten.**

1.2.2. Algemene aspecten van gegevensbescherming

12. Ten eerste is de zogenaamde "**afwijking op het gebied van immigratie**", die is vastgelegd in **punt 4, deel 1, van bijlage 2 bij de Data Protection Act 2018**, **vrij "ruim" geformuleerd**. Zij geldt met name ook wanneer persoonsgegevens niet met het oog op immigratiecontrole door een verwerkingsverantwoordelijke worden verzameld, maar door deze laatste ter beschikking worden gesteld van een andere verwerkingsverantwoordelijke die deze persoonsgegevens verwerkt met het oog op immigratiecontrole.

13. De EDPB verzoekt de Europese Commissie na te gaan wat de stand van zaken is in de procedure *Open Rights Group & Anor, R (On the Application Of) tegen Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin)* en, aangezien dit arrest niet definitief is (*res judicata*), na te gaan of het door het arrest in hoger beroep wordt bevestigd of herzien, en daarbij rekening te houden met een eventuele actualisering in dit verband, en deze in het besluit te vermelden. **De EDPB verzoekt de Europese Commissie voorts om in het adequaatheidsbesluit nadere informatie te verstrekken over de afwijking op het gebied van immigratie[6], met name met betrekking tot de noodzaak en de evenredigheid van een dergelijke ruime afwijking in de Britse wetgeving, vooral gelet op het ruime toepassingsgebied *ratione personae*.** Tezelfdertijd verzoekt de EDPB de Europese Commissie nader te onderzoeken of er in het Britse rechtskader extra waarborgen bestaan of denkbaar zijn, bijvoorbeeld door middel van juridisch bindende instrumenten die de afwijking op het gebied van immigratie zouden aanvullen door de voorspelbaarheid ervan en de waarborgen voor de betrokkenen te versterken, en die ook een betere en snellere beoordeling van en toezicht op de vereisten inzake de noodzakelijkheid en de evenredigheid mogelijk zouden maken.

14. Ten tweede, hoewel de EDPB erkent dat het VK hoofdstuk V AVG grotendeels heeft overgenomen in zijn gegevensbeschermingskader, heeft de EDPB vastgesteld dat bepaalde aspecten van het Britse rechtskader **met betrekking tot verdere doorgifte** het beschermingsniveau voor persoonsgegevens die vanuit de EER worden doorgegeven, zouden kunnen ondermijnen.

[6] Ook als resultaat van de lopende evaluatie van het gebruik van de afwijking op het gebied van immigratie waarnaar wordt verwezen op blz. 5 van het Explanatory Framework for Adequacy Discussions, Section E3: Schedule 2 Restrictions van de Britse regering, 13 maart 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf

15. In artikel 44 AVG[7] is namelijk bepaald dat doorgiften en verdere doorgiften van persoonsgegevens alleen mogen plaatsvinden als het door de AVG voor natuurlijke personen gewaarborgde beschermingsniveau niet wordt ondermijnd. **Dit betekent dat niet alleen de Britse wetgeving "in grote lijnen overeenkomt" met de EU-wetgeving met betrekking tot de verwerking van persoonsgegevens die in het kader van het toekomstige adequaatheidsbesluit naar het VK worden doorgegeven, maar ook dat de in het VK geldende regels met betrekking tot de verdere doorgifte van die gegevens naar derde landen ervoor moeten zorgen dat een in grote lijnen overeenkomstig beschermingsniveau wordt gehandhaafd.**

16. De EDPB neemt er weliswaar kennis van dat het Verenigd Koninkrijk op grond van zijn rechtskader gebieden kan erkennen als gebieden die een passend niveau van gegevensbescherming bieden in het licht van het gegevensbeschermingskader van het Verenigd Koninkrijk, maar wil er toch op wijzen dat deze gebieden tot op heden wellicht niet in aanmerking komen voor een door de Europese Commissie afgegeven adequaatheidsbesluit en geen beschermingsniveau waarborgen dat "in grote lijnen overeenkomt" met het in de EER gewaarborgde niveau. Dit kan ertoe leiden dat er risico's ontstaan voor de bescherming van persoonsgegevens die vanuit de EER worden doorgegeven, vooral als het gegevensbeschermingskader van het Verenigd Koninkrijk in de toekomst afwijkt van het EU-acquis. Voorts heeft het Verenigd Koninkrijk de derde landen waarvoor de Europese Commissie uit hoofde van Richtlijn 95/46/EG[8] een adequaatheidsbesluit heeft verleend reeds als adequaat erkend. De Europese Commissie zal deze besluiten echter binnenkort herzien en de conclusies van deze herziening zijn nog niet bekend.

17. **Voor de bovengenoemde situaties moet de Europese Commissie haar toezichthoudende rol vervullen, en indien het in grote lijnen overeenkomstige beschermingsniveau voor persoonsgegevens die vanuit de EER worden doorgegeven niet wordt gehandhaafd, moet de Europese Commissie overwegen het adequaatheidsbesluit te wijzigen om specifieke waarborgen voor gegevens die vanuit de EER worden doorgegeven in te voeren en/of het adequaatheidsbesluit op te schorten.**

18. **Wat de internationale overeenkomsten tussen het VK en derde landen betreft,** wordt de Europese Commissie verzocht de wisselwerking tussen het gegevensbeschermingskader van het Verenigd Koninkrijk en zijn internationale verbintenissen, buiten de overeenkomst inzake toegang tot elektronische gegevens ten behoeve van de bestrijding van zware criminaliteit die tussen het VK en de Verenigde Staten van Amerika (hierna "VS" genoemd)[9] is gesloten (hierna "overeenkomst VK-VS in het kader van de Amerikaanse CLOUD Act" genoemd), te onderzoeken, met name om de

[7] "*Persoonsgegevens die worden verwerkt of die zijn bestemd om na doorgifte aan een derde land of een internationale organisatie te worden verwerkt, mogen slechts worden doorgegeven indien, onverminderd de overige bepalingen van deze verordening, de verwerkingsverantwoordelijke en de verwerker aan de in dit hoofdstuk neergelegde voorwaarden hebben voldaan; dit geldt ook voor verdere doorgiften van persoonsgegevens vanuit het derde land of een internationale organisatie aan een ander derde land of een andere internationale organisatie. Alle bepalingen van dit hoofdstuk worden toegepast opdat het door deze verordening voor natuurlijke personen gewaarborgde beschermingsniveau niet wordt ondermijnd.*"

[8] 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 (PB L 281 van 23.11.1995, blz. 31).

[9] Zie Overeenkomst tussen de regering van het Verenigd Koninkrijk van Groot-Brittannië en Noord-Ierland en de regering van de Verenigde Staten van Amerika over de toegang tot elektronische gegevens met het oog op de bestrijding van zware criminaliteit, Washington DC, VS, 3 oktober 2019, https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019.

continuïteit van het beschermingsniveau te waarborgen wanneer persoonsgegevens op grond van het adequaatheidsbesluit voor het VK van de EU naar het VK worden doorgegeven en vervolgens verder worden doorgegeven naar andere derde landen; en om voortdurend toezicht te houden op en zo nodig actie te nemen ingeval het sluiten van internationale overeenkomsten tussen het VK en derde landen het in de EU geboden beschermingsniveau voor persoonsgegevens dreigt te ondermijnen.

19. Voorts wordt de Europese Commissie verzocht na te gaan of de overeenkomst VK-VS in het kader van de Amerikaanse CLOUD Act passende aanvullende waarborgen biedt, rekening houdend met de mate van gevoeligheid van de betrokken gegevenscategorieën en de enige vereisten van de doorgifte van elektronisch bewijsmateriaal rechtstreeks door dienstverleners in plaats van tussen autoriteiten, en tevens te beoordelen onder welke omstandigheden waarborgen kunnen worden geboden door een passende uitvoering van de aanpassing van de raamovereenkomst tussen de EU en de VS[10].

20. De EDPB merkt voorts op dat verdere doorgiften vanuit het VK naar een ander derde land ook kunnen plaatsvinden op basis van **doorgifte-instrumenten overeenkomstig de in het VK toepasselijke wetgeving inzake gegevensbescherming[11]**. Naar aanleiding van *Schrems II*[12] verzoekt de EDPB de Europese Commissie om in het adequaatheidsbesluit de zekerheid te bieden dat de nodige waarborgen daadwerkelijk zullen worden ingebouwd, mede rekening houdend met de wetgeving van het ontvangende derde land.

21. Met betrekking tot het ontbreken **van bescherming op grond van artikel 48 AVG** in de Britse wetgeving, verzoekt de EDPB de Europese Commissie om verdere garanties en specifieke verwijzingen naar de Britse wetgeving die ervoor zorgen dat het beschermingsniveau op grond van het Britse rechtskader in grote lijnen overeenkomt met het in de EER gewaarborgde beschermingsniveau.

22. Wat de **procedurele en handhavingsmechanismen** betreft, merkt de EDPB op dat het bestaan en de doeltreffende werking van een onafhankelijke toezichthoudende autoriteit, het bestaan van een systeem dat een goed nalevingsniveau, en een systeem van toegang tot passende verhaalmechanismen dat personen in de EER de middelen verschaft om hun rechten uit te oefenen en verhaal te zoeken zonder op omslachtige belemmeringen voor administratief en gerechtelijk beroep te stuiten, essentiële elementen zijn die een gegevensbeschermingskader moeten kenmerken dat met het Europese kader overeenstemt.

23. De EDPB erkent dat het VK de desbetreffende bepalingen van de AVG op de meeste punten heeft weerspiegeld in de Britse AVG en in de Britse Data Protection Act 2018; desalniettemin wordt de Europese Commissie verzocht voortdurend toe te zien op alle ontwikkelingen in het Britse rechtskader en de Britse praktijk, die nadelige gevolgen voor deze gebieden zouden kunnen hebben.

[10] Zie Overeenkomst tussen de Verenigde Staten van Amerika en de Europese Unie over de bescherming van persoonlijke informatie in verband met de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten, december 2016 (hierna de "raamovereenkomst tussen de EU en de VS" genoemd), https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=LEGISSUM:3104_8

[11] Zie artikelen 46 en 47 Britse AVG.

[12] Zie *Schrems II*.

1.2.3. Betreffende de toegang die overheidsinstanties hebben tot gegevens die zijn doorgegeven naar het VK

24. De EDPB constateert dat het Britse rechtskader voor veiligheids- en inlichtingendiensten ingrijpend is gewijzigd, met name wat betreft de interceptie en verwerving van communicatiegegevens. De EDPB meent te begrijpen dat deze wijzigingen onder meer een reactie zijn op de procedures die zijn ingeleid voor het HvJ-EU en het Europees Hof voor de Rechten van de Mens (hierna "EHRM" genoemd) en hun recente arresten in dit verband.

25. De EDPB is met name ingenomen met het feit dat het Verenigd Koninkrijk het Investigatory Powers Tribunal (hierna "IPT" genoemd) heeft opgericht. Het IPT is niet alleen bevoegd om zaken te behandelen inzake het gebruik van onderzoeksbevoegdheden door rechtshandhavingsinstanties, maar ook door inlichtingendiensten. De EDPB gaat er derhalve van uit dat het IPT functioneert als een echte rechterlijke instantie in de zin van artikel 47 Handvest van de grondrechten van de Europese Unie (hierna "EU-Handvest" genoemd).

26. Voorts merkt de EDPB in positieve zin op dat de introductie van "Judicial Commissioners" in de Investigatory Powers Act 2016 (hierna "IPA 2016" genoemd) een belangrijke verbetering is. Hij begrijpt dat een belangrijke functie van de Judicial Commissioners erin bestaat in individuele gevallen *vooraf* verschillende surveillancemaatregelen goed te keuren, waaronder de gerichte interceptie en bulkverwerving van communicatiegegevens (de zogenaamde "dubbele-lockprocedure").

27. De EDPB ziet evenwel in dat, om de doeltreffendheid van dit extra niveau van toezicht te beoordelen, verder moet worden verduidelijkt voor welke scenario's een rechtmatige interceptie zonder goedkeuring van de Investigatory Powers Commissioner (hierna "IPC" genoemd) of de Judicial Commissioners mogelijk is, en verzoekt de Europese Commissie nader te beoordelen en aan te tonen dat, zelfs in gevallen waarin de dubbele-lockprocedure niet van toepassing is, het Britse rechtskader in passende waarborgen voorziet, onder meer door middel van doeltreffend toezicht *achteraf* en verhaalsmogelijkheden voor individuele personen, en aldus een beschermingsniveau waarborgt dat in grote lijnen overeenkomt met het in de EU geboden niveau.

28. Voorts verzoekt de EDPB de Europese Commissie nader te onderzoeken onder welke voorwaarden een beroep kan worden gedaan op urgentie en verduidelijking te geven over de mogelijke manieren waarop de betrokkenen hun rechten kunnen uitoefenen en de mogelijke rechtsmiddelen die hun worden aangereikt in het kader van de interferentie met apparatuur, met name in het geval van een afwijking van de dubbele-lockprocedure.

29. Daarnaast is de EDPB van mening dat er behoefte bestaat aan verdere verduidelijking en beoordeling van bulkinterceptie, met name wat betreft de selectie en toepassing van de selecteurs, om te verduidelijken in hoeverre de toegang tot persoonsgegevens voldoet aan de door het HvJ-EU vastgestelde drempel, en welke waarborgen er bestaan ter bescherming van de grondrechten van personen wier gegevens in deze context worden onderschept, onder meer wat betreft de bewaartermijnen van de gegevens. Daarbij zou een onafhankelijke beoordeling door de bevoegde Britse toezichthoudende autoriteiten bijzonder nuttig zijn. De EDPB benadrukt voorts dat het des te kritieker lijkt dat "overzeese communicaties" die binnen de werkingssfeer van bulkinterceptiepraktijken vallen, lijkt te impliceren dat het VK binnen de EU gegevens rechtstreeks zou kunnen onderscheppen en in bulk zou kunnen verzamelen, met inbegrip van gegevens tijdens de doorvoer tussen de EU en het VK , hetgeen binnen de werkingssfeer van het ontwerpbesluit zou vallen. Vanwege het belang van dit aspect roept de EDPB de Europese Commissie op de ontwikkelingen op dit gebied nauwlettend te volgen.

30. Nog steeds wat bulkinterceptie betreft, wijst de EDPB op de consequente beoordeling door het EHRM en het HvJ-EU, en wijst hij op de bedenkingen die zijn geuit met betrekking tot secundaire gegevens, die vanwege hun gevoeligheid specifieke waarborgen moeten genieten. De EDPB verzoekt de Europese Commissie daarom zorgvuldig na te gaan of de waarborgen die de Britse wetgeving voor een dergelijke categorie persoonsgegevens biedt, een beschermingsniveau waarborgen dat in grote lijnen overeenkomt met het in de EER gewaarborgde niveau.

31. In dit verband is de EDPB zich ervan bewust dat het openbare verslag van het Intelligence and Security Committee van 2016 over het gebruik van bulkbevoegdheden[13] betrekking heeft op praktijken onder het vorige rechtskader, dat vervolgens werd vervangen door de IPA 2016. Nochtans ziet hij de noodzaak in van een verdere onafhankelijke beoordeling van en toezicht op het gebruik van geautomatiseerde verwerkingsinstrumenten door de bevoegde Britse toezichthoudende autoriteiten, en verzoekt hij de Europese Commissie een nadere beoordeling te maken van deze kwestie en de waarborgen die in dit verband aan de betrokkenen in de EER zouden en/of kunnen worden geboden.

32. De EDPB deelt de mening van de IPC dat verdere toetsing en toezicht nodig zijn om ervoor te zorgen dat de waarborgen die in de praktijk door de bevoegde autoriteiten op het gebied van nationale veiligheid en inlichtingen worden toegepast om onregelmatigheden bij de toepassing van de desbetreffende wetgeving te verhelpen, worden gehandhaafd en verder zullen worden verbeterd. De EDPB is tevens ingenomen met het feit dat de IPC bijgevolg in 2019 zijn aanpak van de inspecties van bulkinterceptie heeft herzien, "*waarbij onder meer zorgvuldig is gekeken naar de technisch complexe manieren waarop bulkinterceptie daadwerkelijk wordt uitgevoerd*", en heeft toegezegd "*een grondig onderzoek van de selecteurs en de zoekcriteria waarop het EHRM hierboven heeft gezinspeeld*" te zullen opnemen in de inspecties van bulkinterceptie vanaf 2020. Gezien het belang van dit aspect is de EDPB bezorgd over het feit dat de IPC nog geen gedetailleerd onderzoek naar de selecteurs en de zoekcriteria heeft verricht, en verzoekt hij de Europese Commissie de ontwikkelingen op dit gebied van nabij te volgen, temeer daar de concrete vorm van een dergelijk toezicht nog moet worden verduidelijkt.

33. Met betrekking tot openbaarmaking overzee benadrukt de EDPB dat de toepassing van de vrijstelling ten behoeve van de nationale veiligheid waarin de Britse wetgeving voorziet ertoe kan leiden dat er geen waarborgen zijn die garanderen dat de beginselen van doelbinding, noodzakelijkheid en de evenredigheid ook worden nageleefd, of die ervoor zorgen dat in het derde land van bestemming ook voldoende rechten van de personen, toezicht en verhaalsmogelijkheden worden geboden of geëerbiedigd. De EDPB beveelt de Europese Commissie dan ook aan om de algemene waarborgen die de Britse wetgeving biedt als het gaat om openbaarmaking overzee nader te onderzoeken, met name in het licht van de toepassing van vrijstellingen ten behoeve van de nationale veiligheid.

34. Ten slotte heeft de EDPB bedenkingen bij andere vormen van informatie-uitwisseling en -verstrekking gebaseerd op andere instrumenten, met name de verschillende internationale overeenkomsten die het VK met andere derde landen heeft gesloten, vooral wanneer deze instrumenten ontoegankelijk blijven voor het publiek, zoals de Brits-Amerikaanse overeenkomst inzake communicatie-inlichtingen. Een dergelijke overeenkomst zou kunnen leiden tot een omzeiling van de waarborgen die zijn vastgesteld met betrekking tot de toegang tot en het gebruik van

[13] Zie Report of the Bulk Powers Review van de Independent Reviewer of Terrorism Legislation, augustus 2016, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf

persoonsgegevens voor nationale veiligheidsdoeleinden. De EDPB is van mening dat het sluiten van bilaterale of multilaterale overeenkomsten met derde landen met het oog op samenwerking op inlichtingengebied, waarbij een rechtsgrondslag wordt verschaft voor de rechtstreekse interceptie en verwerving van persoonsgegevens of de doorgifte van persoonsgegevens naar deze landen, eveneens aanzienlijke gevolgen kan hebben voor de voorwaarden voor het verdere gebruik van de verzamelde informatie, aangezien dergelijke overeenkomsten waarschijnlijk gevolgen zullen hebben voor het gegevensbeschermingskader van het Verenigd Koninkrijk dat wordt beoordeeld.

1.3. Conclusie

35. De EDPB is van mening dat de beoordeling van de adequaatheid van het VK uniek is vanwege de voormalige status van het VK als lidstaat van de EU. Overigens zou het ook het eerste adequaatheidsbesluit zijn dat een vervalclausule bevat.

36. Daarom erkent de EDPB dat er op veel gebieden sprake is van convergentie tussen de gegevensbeschermingskaders van het Verenigd Koninkrijk en de EU. Tezelfdertijd en na een zorgvuldige analyse van het ontwerpbesluit van de Europese Commissie en de Britse wetgeving inzake gegevensbescherming, heeft de EDPB echter een aantal uitdagingen vastgesteld, die in dit advies uitvoerig worden behandeld. De EDPB wenst in dit verband de nadruk te leggen op de uiterst belangrijke rol van de Europese Commissie bij het volgen van alle relevante ontwikkelingen in het Verenigd Koninkrijk.

37. Gezien het bovenstaande beveelt de EDPB de Europese Commissie aan de in dit advies genoemde uitdagingen aan te pakken. Tevens verzoekt de EDPB de Europese Commissie om alle relevante ontwikkelingen in het Verenigd Koninkrijk die gevolgen kunnen hebben voor de vraag of het beschermingsniveau voor persoonsgegevens in feite overeenkomt met dat van de EU op de voet te volgen en zo nodig snel passende maatregelen te nemen.

2. INLEIDING

2.1. Gegevensbeschermingskader van het Verenigd Koninkrijk

38. Het gegevensbeschermingskader van het Verenigd Koninkrijk is grotendeels gebaseerd op het gegevensbeschermingskader van de EU (met name de AVG en de richtlijn gegevensbescherming bij rechtshandhaving), wat een gevolg is van het feit dat het Verenigd Koninkrijk tot 31 januari 2020 een lidstaat van de EU was. Bovendien wordt in de Britse Data Protection Act 2018, die op 23 mei 2018 in werking is getreden en waarbij de Britse Data Protection Act 1998 is ingetrokken, de toepassing van de AVG in de Britse wetgeving verder gespecificeerd, naast de omzetting van de Richtlijn gegevensbescherming bij rechtshandhaving, en worden er bevoegdheden verleend en taken opgelegd aan de nationale toezichthoudende autoriteit voor gegevensbescherming, het Britse ICO.

39. Zoals vermeld in overweging 12 van het ontwerpbesluit van de Europese Commissie, heeft de regering van het Verenigd Koninkrijk de wet van 2018 betreffende de terugtrekking uit de Europese Unie uitgevaardigd, waarmee de rechtstreeks toepasselijke EU-wetgeving in het recht van het Verenigd Koninkrijk wordt opgenomen. Krachtens deze wet hebben de ministers van het VK de bevoegdheid om via wettelijke instrumenten secundaire wetgeving in te voeren, om na de terugtrekking van het VK uit de EU de nodige wijzigingen in de overgenomen EU-wetgeving aan te brengen, zodat deze in de binnenlandse context past.

40. Bijgevolg bestaat het desbetreffende rechtskader dat na het einde van de overgangsperiode[14] in het Verenigd Koninkrijk van toepassing is uit:

- de algemene verordening gegevensbescherming van het Verenigd Koninkrijk (hierna "Britse AVG" genoemd), zoals opgenomen in het recht van het Verenigd Koninkrijk krachtens de wet van 2018 betreffende de terugtrekking uit de Europese Unie, zoals gewijzigd bij de DPPEC (Data Protection, Privacy and Electronic Communications (Amendment Etc.) (EU Exit)) Regulations 2019;
- de Data Protection Act 2018 (hierna "DPA 2018" genoemd), zoals gewijzigd door de DPPEC Regulations 2019, en de Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020; en
- de IPA 2016.

(gezamenlijk "het gegevensbeschermingskader van het Verenigd Koninkrijk").

2.2. Reikwijdte van de beoordeling van de EDPB

41. Het ontwerpbesluit van de Europese Commissie is het resultaat van een beoordeling van het gegevensbeschermingskader van het Verenigd Koninkrijk, gevolgd door besprekingen met de Britse regering. Overeenkomstig artikel 70, lid 1, punt s), AVG wordt van de EDPB verwacht dat hij een onafhankelijk advies uitbrengt over de bevindingen van de Europese Commissie, eventuele onvolkomenheden in het adequaatheidskader aanwijst en zich inspant om voorstellen te doen om deze te verhelpen.

42. In de AVG-adequaatheidsreferentie staat: "*de door de Europese Commissie verstrekte informatie moet in elk geval uitputtend zijn en het EDPB in staat stellen zelf het niveau van gegevensbescherming in het derde land te beoordelen*"[15].

43. Hierbij moet worden opgemerkt dat de EDPB de documenten die van belang zijn voor het onderzoek van het Britse rechtskader slechts ten dele tijdig heeft ontvangen. De EDPB heeft het merendeel van de Britse wetgeving waarnaar in het ontwerpbesluit wordt verwezen ontvangen via links waarnaar in dit besluit wordt verwezen. De Europese Commissie was niet in de gelegenheid om de EDPB schriftelijke toelichtingen en toezeggingen van het Verenigd Koninkrijk te verstrekken met betrekking tot de uitwisselingen tussen de Britse autoriteiten en de Europese Commissie die voor deze exercitie van belang zijn[16].

---

[14] De overgangsperiode loopt tot 31 december 2020, waarna de EU-wetgeving niet langer van toepassing is in het VK. De "overbruggingsperiode" loopt tot uiterlijk 30 juni 2021, en is de extra periode gedurende welke de toezending van persoonsgegevens van de EER naar het VK niet als een doorgifte wordt beschouwd.

[15] Zie WP254 rev.01, blz. 3.

[16] Met betrekking tot: artikel 48 AVG (voetnoot 78 van het ontwerpbesluit); verbeterde waarborgen en veiligheidsmaatregelen die door de verwerkingsverantwoordelijken worden toegepast bij de verwerking in verband met de nationale veiligheid (voetnoot 64 van het ontwerpbesluit); de verplichting voor de verwerkingsverantwoordelijke om per geval na te gaan of er een beroep op de vrijstelling moet worden gedaan, zelfs wanneer een nationaal veiligheidscertificaat is afgegeven (overweging 126 en voetnoot 172 van het ontwerpbesluit); het feit dat de beschermingsmaatregelen van de raamovereenkomst tussen de EU en de VS van toepassing zullen zijn op alle persoonsgegevens die in het kader van de overeenkomst VK-VS in het kader van de Amerikaanse CLOUD Act worden geproduceerd of bewaard, ongeacht de aard of het soort instantie die het verzoek doet, met betrekking tot de details van de daadwerkelijke uitvoering van de gegevensbeschermingswaarborgen die nog onderwerp zijn van besprekingen tussen het VK en de VS, de

44. Gelet op het bovenstaande en gezien de beperkte tijd (2 maanden) die de EDPB heeft om dit advies vast te stellen, heeft de EDPB ervoor gekozen zich te concentreren op enkele specifieke punten in het ontwerpbesluit en daarover zijn analyse en advies uit te brengen.

45. Bij de analyse van de wetgeving en praktijk van een derde land dat tot voor kort een EU-lidstaat was, is het duidelijk dat de EDPB veel aspecten als in grote lijnen overeenkomstig heeft aangemerkt. Gezien zijn rol in het vaststellen van een adequaatheidsbesluit en de hoeveelheid wetgeving en praktijken die moeten worden geanalyseerd, heeft de EDPB besloten zijn aandacht toe te spitsen op de aspecten waar hij een nadere bestudering het noodzakelijkst achtte. In overeenstemming met de HvJ-EU-jurisprudentie heeft een aanzienlijk deel van de analyse bovendien betrekking op de wettelijke regeling inzake de toegang van de nationale veiligheidsdiensten tot de aan het VK doorgegeven persoonsgegevens en op de praktijken van het nationale veiligheidsapparaat in het VK. Er moet echter rekening mee worden gehouden dat de nationale veiligheid klaarblijkelijk een gebied van wetgeving en praktijk is waarop de wetgevingen van de lidstaten niet op EU-niveau geharmoniseerd zijn en dus kunnen verschillen.

46. De EDPB is uitgegaan van het toepasselijke Europese gegevensbeschermingskader, waaronder de artikelen 7, 8 en 47 EU-Handvest, waarin respectievelijk het recht op de eerbiediging van het privé-leven en van het familie- en gezinsleven, het recht op de bescherming van persoonsgegevens, en het recht op een doeltreffende voorziening in rechte en op een onpartijdig gerecht worden beschermd; en artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens (hierna "EVRM" genoemd), waarin het recht op privé-, familie- en gezinsleven wordt beschermd. Daarnaast heeft de EDPB de vereisten van de AVG, alsook de desbetreffende jurisprudentie in aanmerking genomen.

47. Deze exercitie heeft tot doel de Europese Commissie te voorzien van een advies over de beoordeling van de adequaatheid van het beschermingsniveau in het Verenigd Koninkrijk. Het begrip "passend beschermingsniveau" werd al gehanteerd in Richtlijn 95/46/EG en is verder uitgewerkt door het HvJ-EU. Het is belangrijk te herinneren aan de norm die het HvJ-EU heeft gesteld in *Schrems I*, namelijk dat het "beschermingsniveau" in het derde land "in grote lijnen" moet overeenkomen met het in de EU gewaarborgde niveau, "*ook al kunnen de middelen waarmee dat derde land voor waarborgen voor een passend beschermingsniveau kan zorgen, anders zijn dan die welke binnen de Unie worden ingezet*"[17]. Het doel is dus niet de Europese wetgeving punt voor punt te kopiëren, maar de grote lijnen en de kernvereisten van de wetgeving in kwestie vast te stellen. Adequaatheid kan worden bereikt door een combinatie van rechten voor de betrokkenen, verplichtingen voor gegevensverwerkers of verwerkingsverantwoordelijken en toezicht door onafhankelijke instanties. Regelgeving voor gegevensverwerking is echter alleen doeltreffend als zij afdwingbaar is en in de praktijk wordt nageleefd. Daarom moet niet alleen worden gekeken naar de inhoud van de regels die van toepassing zijn op persoonsgegevens die naar een derde land of een internationale

bevestiging dat de autoriteiten van het VK deze overeenkomst pas in werking zullen laten treden wanneer zij ervan overtuigd zijn dat de uitvoering ervan voldoet aan de wettelijke verplichtingen waarin de overeenkomst voorziet, met inbegrip van helderheid ten aanzien van de naleving van de gegevensbeschermingsnormen voor alle gegevens die op grond van deze overeenkomst worden opgevraagd (overweging 153 van het ontwerpbesluit); situaties waarin gegevens van de EU naar het VK worden doorgegeven binnen de werkingssfeer van dit ontwerpbesluit, en het feit dat er altijd een "verbinding met de Britse eilanden" zou zijn en dat voor elke interferentie met apparatuur die betrekking heeft op dergelijke gegevens dus het verplichte bevelschrift van artikel 13, lid 1, IPA 2016 zou gelden (overweging 206 van het ontwerpbesluit); en de voorbeelden van operationele doeleinden die worden gegeven (overweging 216 en voetnoot 369 van het ontwerpbesluit).

[17] Zie het arrest van het HvJ-EU, C-362/14, *Maximilian Schrems/Data Protection Commissioner*, 6 oktober 2015, ECLI:EU:C:2015:650 (hierna "*Schrems I*" genoemd), punten 73-74.

organisatie worden doorgegeven, maar ook naar het bestaande systeem om de doeltreffendheid van dergelijke regels te waarborgen. Voor de doeltreffendheid van regelgeving voor gegevensbescherming zijn efficiënte handhavingsmechanismen van eminent belang[18].

2.3. Algemene opmerkingen en punten van zorg

2.3.1. Internationale toezeggingen van het VK

48. Overeenkomstig artikel 45, lid 2, punt c), AVG en de AVG-adequaatheidsreferentie[19] moet de Europese Commissie bij de beoordeling van de adequaatheid van het beschermingsniveau van een derde land onder meer rekening houden met de internationale toezeggingen die het derde land heeft gedaan, of andere verplichtingen die voortvloeien uit de deelname van dat derde land aan multilaterale of regionale regelingen, in het bijzonder met betrekking tot de bescherming van persoonsgegevens, alsook met de nakoming van deze verplichtingen. Verder moet rekening worden gehouden met de toetreding van het derde land tot het Verdrag van de Raad van Europa van 28 januari 1981 tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (hierna "Verdrag 108" genoemd)[20] en het bijbehorende Aanvullend Protocol[21].

49. **In dit verband neemt de EDPB er met voldoening kennis van dat het VK tot het EVRM is toegetreden en onder de rechtsmacht van het EHRM valt. Daarnaast is het VK ook toegetreden tot Verdrag 108 en het Aanvullend Protocol, heeft het in 2018 Verdrag 108+[22] ondertekend en werkt het momenteel aan de ratificatie ervan.**

2.3.2. Mogelijke toekomstige afwijking van het gegevensbeschermingskader van het Verenigd Koninkrijk

50. Zoals in overweging 281 van het ontwerpbesluit is vermeld, moet de Europese Commissie er rekening mee houden dat het Verenigd Koninkrijk na afloop van de overgangsperiode waarin het terugtrekkingsakkoord voorziet[23] zijn eigen gegevensbeschermingsregeling beheert, toepast en handhaaft, en zodra de overbruggingsbepaling uit hoofde van artikel FINPROV.10A van de handels- en samenwerkingsovereenkomst EU-VK[24] niet langer van toepassing is, kan dit met name wijzigingen of veranderingen met zich meebrengen in het gegevensbeschermingskader dat in het ontwerpbesluit wordt beoordeeld, alsook andere desbetreffende ontwikkelingen.

[18] Zie WP254 rev.01, blz. 2.
[19] Zie WP254 rev.01, blz. 2.
[20] Zie Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens; Verdrag 108, 28 januari 1981.
[21] Zie het Aanvullend Protocol bij het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens inzake toezichthoudende autoriteiten en grensoverschrijdend verkeer van gegevens, ter ondertekening opengesteld op 8 november 2001.
[22] Zie Protocol tot wijziging van het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens ("Verdrag 108+"), 18 mei 2018.
[23] Zie Akkoord inzake de terugtrekking van het Verenigd Koninkrijk van Groot-Brittannië en Noord-Ierland uit de Europese Unie en de Europese Gemeenschap voor Atoomenergie (PB L 029 van 31.1.2020, blz. 7).
[24] Zie Handels- en samenwerkingsovereenkomst tussen de Europese Unie en de Europese Gemeenschap voor Atoomenergie, enerzijds, en het Verenigd Koninkrijk van Groot-Brittannië en Noord-Ierland, anderzijds (PB L 444 van 31.12.2020, blz. 14).

51. De Europese Commissie heeft daarom besloten in haar ontwerpbesluit een vervalclausule op te nemen[25], waarbij de vervaldatum op vier jaar na de inwerkingtreding van het besluit wordt vastgesteld.

52. Het is van belang op te merken dat de mogelijkheid dat de Britse ministers en de Britse Secretary of State na afloop van de overbruggingsperiode secundaire wetgeving invoeren ertoe kan leiden dat het gegevensbeschermingskader van het Verenigd Koninkrijk in de toekomst aanzienlijk afwijkt van dat van de EU.

53. De Britse regering heeft namelijk te kennen gegeven dat zij voornemens is een afzonderlijk en onafhankelijk beleid inzake gegevensbescherming te ontwikkelen, hetgeen dan tot een afwijking van de EU-wetgeving inzake gegevensbescherming zou kunnen leiden[26]. Dit voornemen omvat het opnemen van aspecten van persoonsgegevens in handelsovereenkomsten[27], een praktijk die het risico in zich bergt dat het door het VK geboden beschermingsniveau voor persoonsgegevens wordt verlaagd[28].

54. Tot slot is het VK sinds het einde van de overgangsperiode niet alleen niet meer gebonden aan de jurisprudentie van het HvJ-EU, maar zouden ook de reeds vastgestelde arresten van het HvJ-EU, die in het Britse rechtskader als overgenomen jurisprudentie worden beschouwd, het VK niet meer

---

[25] Zie artikel 4 van het ontwerpbesluit. Zie ook overweging 282 van het ontwerpbesluit.

[26] In de National Data Strategy van het Verenigd Koninkrijk (laatstelijk bijgewerkt op 9 december 2020, https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy) is het volgende als een van de missies opgenomen: "*Bevordering van internationaal gegevensverkeer. Het grensoverschrijdend gegevensverkeer is de drijvende kracht achter wereldwijde bedrijfsoperaties, toeleveringsketens en handel, en stimuleert de groei in de hele wereld. Daarnaast speelt het ook een bredere maatschappelijke rol. Dankzij de doorgifte van persoonsgegevens kunnen salarissen worden betaald, en kunnen mensen van veraf in contact komen met hun dierbaren. Bovendien kan het uitwisselen van gezondheidsgegevens, zoals door de COVID-19-pandemie is aangetoond, essentieel wetenschappelijk onderzoek naar ziekten bevorderen en landen verenigen in hun reactie op noodsituaties in de wereldgezondheid.* ***Nu het VK de Europese Unie heeft verlaten, maakt het zich sterk voor de voordelen die gegevens kunnen opleveren.*** *Wij zullen binnenlandse beste praktijken bevorderen en samenwerken met internationale partners* ***om ervoor te zorgen dat gegevens niet ten onrechte worden beperkt door nationale grenzen en gefragmenteerde regelgevingsstelsels****, zodat zij ten volle kunnen worden benut*." (nadruk toegevoegd).

[27] Ibid.: "*Faciliteren van grensoverschrijdende gegevensstromen:* ***Wij zullen wereldwijd werken aan het opheffen van onnodige belemmeringen voor internationale gegevensstromen. Wij zullen in onze handelsbesprekingen ambitieuze bepalingen inzake gegevens overeenkomen*** *en onze nu onafhankelijke zetel in de Wereldhandelsorganisatie gebruiken om de handelsregels voor gegevens in positieve zin te beïnvloeden.* ***Voorts zullen wij belemmeringen wegnemen voor internationale doorgiften van gegevens*** *die groei en innovatie ondersteunen, onder meer door de ontwikkeling van een nieuwe Britse capaciteit die zorgt voor nieuwe en innovatieve mechanismen voor internationale doorgiften van gegevens. Ook zullen we samenwerken met onze G20-partners om interoperabiliteit tussen nationale gegevensregelingen tot stand te brengen, zodat er zo min mogelijk wrijving ontstaat bij de doorgifte van gegevens tussen verschillende landen"*. (nadruk toegevoegd).

[28] Zie de resolutie van het Europees Parlement van 12 december 2017 over "*Naar een digitale handelsstrategie*" (2017/2065(INI)), afdeling V, waarin wordt benadrukt dat "*bij de sluiting van [EU-]handelsovereenkomsten niet over de bescherming van persoonsgegevens mag worden onderhandeld*", beschikbaar op: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0488_NL.pdf Zie ook de resolutie van het Europees Parlement van 25 maart 2021 over het evaluatieverslag van de Commissie over de toepassing van de algemene verordening gegevensbescherming, twee jaar na de inwerkingtreding, punt 28, waarin wordt gesteld: *"steunt de praktijk van de Commissie om gegevensbescherming en persoonsgegevensstromen los van handelsovereenkomsten te behandelen"*, https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_NL.html

kunnen binden, aangezien het VK met name de mogelijkheid heeft om overgenomen EU-recht na het einde van de overbruggingsperiode te wijzigen en zijn Supreme Court niet gebonden is aan overgenomen EU-jurisprudentie[29].

55. **Met het oog op de risico's in verband met de mogelijke afwijking van het gegevensbeschermingskader van het Verenigd Koninkrijk van het EU-acquis na afloop van de overbruggingsperiode, is de EDPB ingenomen met het besluit van de Europese Commissie om voor het ontwerpbesluit een vervalclausule van vier jaar in te voeren. De EDPB wil hier echter wijzen op het belang van de toezichthoudende rol van de Europese Commissie[30]. De Europese Commissie moet namelijk alle relevante ontwikkelingen in het VK die van invloed kunnen zijn op de overeenkomst in grote lijnen van het beschermingsniveau voor persoonsgegevens die uit hoofde van het adequaatheidsbesluit voor het VK worden doorgegeven, vanaf de inwerkingtreding van dat besluit voortdurend en permanent in het oog houden. Bovendien moet de Europese Commissie de nodige maatregelen nemen door het adequaatheidsbesluit op te schorten, te wijzigen of in te trekken, afhankelijk van de omstandigheden, indien zij na de vaststelling van het adequaatheidsbesluit over aanwijzingen beschikt dat in het Verenigd Koninkrijk niet langer een passend beschermingsniveau wordt gewaarborgd.**

56. Van zijn kant zal de EDPB alles in het werk stellen om de Europese Commissie op de hoogte te brengen van alle desbetreffende maatregelen die de toezichthoudende autoriteiten voor gegevensbescherming van de lidstaten (hierna "TA's" genoemd) in de commerciële of de openbare sector hebben genomen, en met name met betrekking tot klachten van betrokkenen in de EER over de doorgifte van persoonsgegevens uit de EER naar het VK.

3. ALGEMENE ASPECTEN VAN GEGEVENSBESCHERMING

3.1. Inhoudelijke beginselen

57. Hoofdstuk 3 van de AVG-adequaatheidsreferentie is gewijd aan de "inhoudelijke beginselen". Het systeem van een derde land moet deze beginselen bevatten opdat zijn gegevensbeschermingsniveau kan worden beschouwd als in grote lijnen overeenstemmend met het niveau dat binnen de EU wordt gewaarborgd. De EDPB erkent dat het VK geen geschreven grondwet heeft, in die zin dat er niet één enkel document is waarin de fundamentele regels van het VK zijn vastgelegd. Het recht op eerbiediging van het privé-leven en het familie- en gezinsleven (en het recht op gegevensbescherming als onderdeel van dat recht) en het recht op een eerlijk proces[31] zijn echter opgenomen in de Human Rights Act 1998, en de grondwettelijke waarde van dit statuut is erkend door de Britse rechters. In de Human Rights Act 1998 zijn namelijk de in het EVRM vervatte rechten opgenomen[32]. Bovendien wordt in de Human Rights Act 1998 zeer nadrukkelijk bepaald dat elk optreden van overheidsinstanties verenigbaar moet zijn met het EVRM[33].

58. Afgezien van de structurele en formalistische verschillen tussen de Britse en de EU-wetgeving, merkt de EDPB op dat de aanpak van gegevensbescherming in het VK, zoals te verwachten valt, vergelijkbaar is met die in de EU, wat voortvloeit uit het feit dat het VK tot 31 januari 2020 een

[29] Zie artikel 6, leden 3 tot en met 6, wet van 2018 betreffende de terugtrekking uit de Europese Unie.
[30] Zie artikel 45, lid 4, AVG.
[31] Zie artikelen 6 en 8 EVRM (bijlage 1 bij de Human Rights Act 1998).
[32] Zie voor meer informatie overwegingen 8-10 van het ontwerpbesluit.
[33] Zie artikel 6 Human Rights Act 1998.

lidstaat van de EU was. Bijgevolg stemmen veel inhoudelijke beginselen overeen met die van de AVG en bieden deze derhalve een beschermingsniveau dat in grote lijnen overeenkomt met het door de EU geboden niveau. De EDPB heeft besloten de analyse van de inhoudelijke beginselen die overeenstemmen met de EU-wetgeving niet verder uit te werken en is tevreden met de analyse die de Europese Commissie in haar ontwerpbesluit heeft verstrekt. Dergelijke inhoudelijke beginselen zijn bijvoorbeeld de volgende: begrippen (d.w.z. "persoonsgegevens"; "verwerking van persoonsgegevens"; "verwerkingsverantwoordelijke"); gronden voor behoorlijke en rechtmatige verwerking voor legitieme doeleinden; doelbinding; kwaliteit en evenredigheid van de gegevens; bewaring van gegevens; beveiliging en vertrouwelijkheid; transparantie; bijzondere categorieën gegevens; direct marketing; geautomatiseerde besluitvorming en profilering. De EDPB constateert voorts dat de Britse AVG en de DPA 2018 inhoudelijke beginselen bevatten die verder gaan dan wat in de AVG-adequaatheidsreferentie wordt vereist en een afspiegeling zijn van de beginselen die in de AVG zijn opgenomen, waardoor het in het VK geboden beschermingsniveau wordt verhoogd. Zulke inhoudelijke beginselen betreffen bijvoorbeeld de kennisgevingen van inbreuken in verband met persoonsgegevens, de functionaris voor gegevensbescherming, gegevensbeschermingseffectbeoordelingen en gegevensbescherming door ontwerp en door standaardinstellingen.

59. Zoals vermeld in de inleiding wil de EDPB in dit advies echter specifiek ingaan op bepaalde punten waarover hij zich zorgen maakt en waarover hij de Europese Commissie om opheldering wil vragen.

3.1.1. Recht van inzage, rectificatie, wissing en bezwaar

60. De zogenaamde "afwijking op het gebied van immigratie", die is vastgelegd in punt 4, **deel 1, van bijlage 2 bij DPA 2018**, staat de verwerkingsverantwoordelijken die betrokken zijn bij "immigratiecontrole" toe om bepaalde rechten van betrokkenen waarin de DPA 2018 voorziet niet toe te passen indien dit "*de handhaving van doeltreffende immigratiecontrole zou kunnen schaden*" of voor "*het onderzoeken of opsporen van activiteiten die de handhaving van doeltreffende immigratiecontrole zou ondermijnen*".

61. Zoals de Europese Commissie in haar ontwerpbesluit erkent[34], en waarnaar wordt verwezen in het advies van de commissie LIBE van het Europees Parlement inzake de sluiting, namens de Unie, van de handels- en samenwerkingsovereenkomst tussen de EU en het VK[35], is deze afwijking **vrij "ruim" geformuleerd**. Zij is van toepassing op de volgende rechten: recht op informatie; recht op inzage; recht op gegevenswissing; recht op beperking van de verwerking; en recht van bezwaar.

[34] Zie overwegingen 62-65 van het ontwerpbesluit.

[35] Zie wat de **ruime formulering** van de afwijking op het gebied van immigratie betreft, het advies van de Commissie burgerlijke vrijheden, justitie en binnenlandse zaken inzake de sluiting, namens de Unie, van de handels- en samenwerkingsovereenkomst tussen de Europese Unie en de Europese Gemeenschap voor Atoomenergie, enerzijds, en het Verenigd Koninkrijk van Groot-Brittannië en Noord-Ierland, anderzijds, en van de overeenkomst tussen de Europese Unie en het Verenigd Koninkrijk van Groot-Brittannië en Noord-Ierland inzake beveiligingsprocedures voor de uitwisseling en bescherming van gerubriceerde gegevens (2020/0382(NLE)), 5 februari 2021, https://www.europarl.europa.eu/doceo/document/LIBE-AL-680848_NL.pdf, punt 10: *"herinnert in dit opzicht aan de resoluties van februari en juni 2020 van het Parlement, waarin wordt gewezen op de **algemene en brede vrijstelling** voor de verwerking van persoonsgegevens voor immigratiedoeleinden van de Britse gegevensbeschermingswet"*, en punt 11: *"is van mening dat de **algemene en brede** vrijstelling voor de verwerking van persoonsgegevens voor immigratiedoeleinden van de Britse gegevensbeschermingswet [...] moet worden gewijzigd voordat een geldig besluit waarbij het beschermingsniveau passend wordt verklaard, kan worden genomen;"* (nadruk toegevoegd).

62. Overigens is het van belang op te merken dat deze afwijking ook geldt wanneer persoonsgegevens niet worden verzameld met het oog op immigratiecontrole door een verwerkingsverantwoordelijke ("verwerkingsverantwoordelijke 1"), maar door deze laatste echter ter beschikking worden gesteld aan een andere verwerkingsverantwoordelijke ("verwerkingsverantwoordelijke 2") die deze persoonsgegevens verwerkt met het oog op immigratiecontrole (bv. het Britse ministerie van Binnenlandse Zaken)[36].

63. In *Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin) (3 oktober 2019),* betwistten verzoekers de rechtmatigheid van de afwijking op het gebied van immigratie op grond dat deze in strijd was met artikel 23 AVG en onverenigbaar met de door artikelen 7 en 8 EU-Handvest gewaarborgde rechten met betrekking tot het recht op de eerbiediging van het privé-leven en van het familie- en gezinsleven en het recht op de bescherming van persoonsgegevens. Het High Court of England and Wales (hierna "High Court" genoemd) heeft onderzocht of de afwijking op het gebied van immigratie in punt 4, deel 1 van bijlage 2 bij DPA 2018 rechtmatig is, en is tot de conclusie gekomen dat zij rechtmatig is.

64. Het High Court was met name van oordeel dat:

- *"[…] de afwijking op het gebied van immigratie duidelijk een zaak is van "zwaarwegend algemeen belang" en een legitiem doel nastreeft […]"*, punt 30;
- *"de afwijking op het gebied van immigratie voldoet aan de voorwaarden voor een maatregel opdat zij "in overeenstemming met de wet" is. […]"*, punt 38;
- *"de afwijking op het gebied van immigratie alleen kan worden ingeroepen indien en voor zover de naleving van "de genoemde AVG-bepalingen" **waarschijnlijk afbreuk zou doen aan** de handhaving van een doeltreffende immigratiecontrole of het onderzoeken of opsporen van activiteiten die de handhaving van een doeltreffende immigratiecontrole zouden ondermijnen. De woorden "waarschijnlijk afbreuk zou doen aan" werden in het kader van de Data Protection*

[36] Zie het voorbeeld in de "Guide to the General Data Protection Regulation (GDPR)" van het ICO, v 1 januari 2021, blz. 307 (nadruk toegevoegd): *"Een particuliere organisatie (verwerkingsverantwoordelijke 1) waarschuwt het ministerie van Binnenlandse Zaken (verwerkingsverantwoordelijke 2) dat een werknemer vermoedelijk valse documenten heeft voorgelegd als bewijs van zijn identiteit en kwalificaties om een baan te krijgen. De werkgever verstrekt de desbetreffende gegevens aan het ministerie van Binnenlandse Zaken. Het recht van de betrokkene om ervan in kennis te worden gesteld dat zijn persoonsgegevens aan het ministerie van Binnenlandse Zaken zijn doorgegeven, wordt beperkt voor zover de toepassing van dat recht het onderzoek zou kunnen schaden.*
*De **werkgever is dus niet verplicht om de betrokkene mee te delen dat zijn gegevens aan het ministerie van Binnenlandse Zaken zijn doorgegeven** en **het ministerie van Binnenlandse Zaken** is op zijn beurt niet verplicht om de betrokkene een privacyverklaring te verstrekken waarin wordt meegedeeld dat het nu zijn persoonsgegevens verwerkt. De vrijstelling geldt voor beide verwerkingsverantwoordelijken in dezelfde mate.*
*De werknemer vraagt het ministerie van Binnenlandse Zaken, dat nu een onderzoek instelt, echter om een kopie van zijn persoonsgegevens. Het **ministerie van Binnenlandse Zaken kan zich op de vrijstelling beroepen** om een deel van de gegevens achter te houden, indien de openbaarmaking het onderzoek zou kunnen schaden. Indien de werknemer een soortgelijk verzoek tot **zijn werkgever zou richten, zou deze de vrijstelling ook in dezelfde mate kunnen toepassen**."*
Met andere woorden, zoals verduidelijkt op blz. 300: *"In de meeste gevallen is het ministerie van Binnenlandse Zaken, of een van zijn instanties of contractanten, de verwerkingsverantwoordelijke die deze vrijstelling toepast. Het is echter van belang op te merken dat de toepassing van deze vrijstelling niet alleen beperkt is tot het ministerie van Binnenlandse Zaken. Ze kan ook betrekking hebben op andere verwerkingsverantwoordelijken, zoals werkgevers, universiteiten en de politie, die met het ministerie van Binnenlandse Zaken contact onderhouden over immigratiezaken."*

Act 1998 (die voorafging aan de DPA 2018) geïnterpreteerd als "een zeer aanzienlijke en zwaarwegende kans dat afbreuk wordt gedaan aan het specifieke openbaar belang. Het risico moet zo groot zijn dat er "heel goed" afbreuk aan die belangen kan worden gedaan, ook al is het risico verre van waarschijnlijk […].", punt 39 (nadruk toegevoegd).

65. Opgemerkt zij dat voor zover bekend bij de EDPB dit arrest nog niet definitief is en dat er beroep tegen is ingesteld.

66. Zoals is bepaald in de EDPB-richtsnoeren betreffende beperkingen uit hoofde van artikel 23 AVG ("de artikel 23-AVG-richtsnoeren")[37] *"[...] moeten beperkingen in een AVG-context worden* ***voorzien in een wetgevingsmaatregel****, betrekking hebben op een* ***beperkt aantal rechten van betrokkenen en/of verplichtingen van de verwerkingsverantwoordelijke*** *die zijn genoemd in artikel 23 AVG,* ***de wezenlijke inhoud onverlet laten*** *van de fundamentele rechten en vrijheden in kwestie, een* ***noodzakelijke en evenredige maatregel*** *zijn in een democratische samenleving en een van de in artikel 23, lid 1, AVG genoemde gronden waarborgen [...]"*[38]*.*

67. De EDPB wijst er ook op dat in overweging 41 AVG wordt gesteld: *"[w]anneer in deze verordening naar een* ***rechtsgrond of een wetgevingsmaatregel*** *wordt verwezen, vereist dit niet noodzakelijkerwijs dat een door een parlement vastgestelde wetgevingshandeling nodig is, onverminderd de vereisten overeenkomstig de grondwettelijke orde van de lidstaat in kwestie. Deze rechtsgrond of wetgevingsmaatregel moet evenwel* ***duidelijk en nauwkeurig zijn, en de toepassing daarvan moet voorspelbaar zijn voor degenen op wie deze van toepassing is****, zoals vereist door de rechtspraak van het Hof van Justitie van de Europese Unie [...] en het Europees Hof voor de Rechten van de Mens"* (nadruk toegevoegd).

68. Hoewel het EHRM heeft gesteld: "*[v]oorts, met betrekking tot de termen " bij de wet is voorzien" en "bij de wet zijn voorzien", die in de artikelen 8 tot en met 11 van het Verdrag voorkomen, merkt de [EDPB] op dat hij de term "wet" altijd in zijn "materiële" betekenis en niet in zijn "formele" betekenis heeft opgevat; het omvat zowel "geschreven recht", waaronder uitgevaardigde wetten van lagere rang en regelgevende maatregelen die door beroepsorden worden genomen op grond van onafhankelijke regelgevende bevoegdheden die door het Parlement aan hen zijn gedelegeerd, als ongeschreven recht. Onder "recht" moet zowel het geschreven recht* ***als "rechtersrecht"*** **worden verstaan"**[39], in de artikel 23 AVG-richtsnoeren wordt erop gewezen dat *"[v]olgens de rechtspraak van het HvJ-EU elke* ***wetgevende maatregel*** *die op grond van artikel 23, lid 1, [van de] AVG wordt vastgesteld, met name moet* ***voldoen aan de specifieke vereisten van artikel 23, lid 2, AVG****. In artikel 23, lid 2, [van de] AVG is bepaald dat de wetgevingsmaatregelen die beperkingen opleggen aan de rechten van de betrokkenen en de verplichtingen van de verwerkingsverantwoordelijken, in voorkomend geval,* ***specifieke bepalingen moeten bevatten over de verschillende hieronder***

[37] Zie EDPB-richtsnoeren 10/2020 inzake beperkingen op grond van artikel 23 AVG, versie 1.0, vastgesteld op 15 december 2020, waaraan momenteel de laatste hand wordt gelegd na openbare raadpleging, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-102020-restrictions-under-article-23_nl

[38] Zie artikel 23 AVG-richtsnoeren, punt 9, blz. 5.

[39] Zie EHRM, *Sanoma Uitgevers B.V./Nederland*, 14 september 2010, EC:ECHR:2010:0914JUD003822403, punt 83 (nadruk toegevoegd).

***uiteengezette criteria**. In de regel moeten alle hieronder beschreven vereisten **worden opgenomen in de wetgevingsmaatregel** die beperkingen oplegt krachtens artikel 23 [van de] AVG*"[40].

69. In dit verband kan worden opgemerkt dat in **de afwijking op het gebied van immigratie** zelf **de volgende elementen, waarnaar in artikel 23, lid 2, AVG wordt verwezen, niet worden gespecificeerd**:

- "de waarborgen ter voorkoming van misbruik of de onrechtmatige toegang of doorgifte" d);
- "de specificatie van de verwerkingsverantwoordelijke of de categorieën van verwerkingsverantwoordelijken" e)[41];
- "de risico's voor de rechten en vrijheden van de betrokkenen" g);
- "het recht van betrokkenen om van de beperking op de hoogte te worden gesteld, tenzij dit afbreuk kan doen aan het doel van de beperking" h).

70. In de "Guide to the General Data Protection Regulation (GDPR)" van het ICO[42], met onder meer een hoofdstuk over de "afwijking op het gebied van immigratie", worden wel verduidelijkingen gegeven over de afwijking op het gebied van immigratie, maar **kunnen niet** *per se* bindende regels worden gegeven ter aanvulling daarvan. Bovendien is de kwestie van de "kwaliteit van de wet" met name relevant met het oog op het belang van de beperkte rechten en de uitbreiding van de vrijstelling[43].

---

[40] Zie artikel 23-AVG-richtsnoeren, punten 45 en 46, blz. 11. In artikel 52, lid 3, EU-Handvest is bepaald: *"[v]oor zover dit Handvest rechten bevat die corresponderen met rechten welke zijn gegarandeerd door het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, zijn de inhoud en reikwijdte ervan dezelfde als die welke er door genoemd verdrag aan worden toegekend. Deze bepaling verhindert niet dat het recht van de Unie een ruimere bescherming biedt."* Wat betreft de uitdrukking "**bij wet gesteld**" in de zin van artikel 52, lid 1, EU-Handvest, moeten de door het EHRM ontwikkelde criteria worden gehanteerd, zoals voorgesteld in verschillende conclusies van de advocaat-generaal van het HvJ-EU, zie bijvoorbeeld de conclusies in de gevoegde zaken C-203/15 en C-698/15, *Tele2 Sverige AB*, ECLI:EU:C:2016:572, punten 137-154, en in zaak C-70/10, *Scarlet Extended*, ECLI:EU:C:2011:255, punten 88-114. Er kan dus onder meer worden verwezen naar het arrest van het EHRM in de zaak *Weber en Saravia/Duitsland*, punt 84: *"Het Hof herhaalt dat de uitdrukking "**bij de wet is voorzien**" in de zin van artikel 8, lid 2, [van het EVRM] in de eerste plaats vereist dat de aangevochten maatregel enige grondslag in het **nationaal recht** heeft; het verwijst ook naar de **kwaliteit van de desbetreffende wet**, dat wil zeggen dat ze toegankelijk moet zijn voor de betrokkene, die bovendien de gevolgen ervan voor hem moet kunnen voorzien, en dat ze verenigbaar moet zijn met de rechtsstaat."* (nadruk toegevoegd).
Zie ook overweging 41 AVG: *"Deze [rechtsgrond of] wetgevingsmaatregel moet evenwel **duidelijk** en **nauwkeurig** zijn, en de toepassing daarvan moet **voorspelbaar zijn voor degenen op wie deze van toepassing is**, zoals vereist door de rechtspraak van het Hof van Justitie van de Europese Unie (...) en het Europees Hof voor de Rechten van de Mens"* (nadruk toegevoegd).

[41] Zie de voornoemde zaak van het High Court, punt 54: *"Naar mijn mening is er niets onwettigs aan dat de afwijking op het gebied van immigratie beschikbaar is **voor alle verwerkingsverantwoordelijken** die gegevens voor de gespecificeerde doeleinden verwerken. Zoals verweerders opmerken, zou de afwijking op het gebied van immigratie zonder de leden 3 tot en met 4 van artikel 4 geen effect meer hebben in gevallen waarin gegevens van derden (zoals een plaatselijke autoriteit of HM Revenue and Customs) worden verkregen met het oog op de handhaving van een doeltreffende immigratiecontrole."* (nadruk toegevoegd), waarmee de **veralgemeende** toepassing van de beperkingen wordt bevestigd.

[42] "Guide to the General Data Protection Regulation (GDPR)" van het ICO, v 1 januari 2021, blz. 299-307.

[43] Zie punt 57 van de voornoemde zaak van het High Court: *"De heer Knight heeft mij meegedeeld dat de Commissioner de laatste hand legt aan richtsnoeren betreffende de vrijstelling, maar dat die alleen "wettelijk"*

71. *A fortiori* bevat de "**schadetoets**" geen waarborgen om misbruik of onwettige toegang of doorgifte te voorkomen, die bijvoorbeeld door het ministerie van Binnenlandse Zaken moeten worden toegepast.

---

zullen zijn in de zin dat zij uit hoofde van de bevoegdheden van de Commissioner op grond van artikel 57, lid 1, AVG zullen worden uitgevaardigd. Zij zullen geen wettelijke status hebben uit hoofde van DPA 2018."
De motivering voor de invoering van wettelijk bindende richtsnoeren zoals ondersteund door het ICO, wordt met name genoemd in de punten 56-60 van het arrest:
"56. Tot slot ga ik in op de stelling van de Commissioner dat de vrijstelling zonder begeleidende wettelijke richtsnoeren om waarborgen te bieden met betrekking tot de betekenis en de toepassing van de afwijking op het gebied van immigratie, geen evenredige uitvoering zou zijn van artikel 23, lid 1, AVG. De heer Knight zegt dat, mits aangevuld met dergelijke richtsnoeren, de bepaling evenredig is.
57. De heer Knight heeft mij meegedeeld dat de Commissioner de laatste hand legt aan richtsnoeren betreffende de vrijstelling, maar dat die alleen "wettelijk" zullen zijn in de zin dat zij uit hoofde van de bevoegdheden van de Commissioner op grond van artikel 57, lid 1, AVG zullen worden uitgevaardigd. Zij zullen geen wettelijke status hebben uit hoofde van DPA 2018. Verder heb ik begrepen dat het ministerie van Binnenlandse Zaken een ontwerp van interne richtsnoeren voor het personeel heeft opgesteld over de afwijking op het gebied van immigratie (zie [22] hierboven). In de praktijk zijn door de Commissioner uitgevaardigde richtsnoeren gezaghebbend, ongeacht de rechtsgrondslag. De Commissioner is echter niet bevoegd om "bindende" richtsnoeren uit te vaardigden van de aard die het Supreme Court voor ogen had in de zaak Christian Institute (onder [101] en [107]). Het lijkt erop dat er behoefte zou zijn aan formele wetgeving indien het nodig zou worden geacht dat er richtsnoeren over de afwijking op het gebied van immigratie komen met dezelfde status als de praktijkcodes die momenteel in artikelen 121–124 DPA 2018 zijn opgenomen.
58. In zijn pleidooi voor wettelijke richtsnoeren stelt de heer Knight dat de context waarin de afwijking op het gebied van immigratie wordt gebruikt noodzakelijkerwijs aanleiding geeft tot bezorgdheid over de noodzaak en de evenredigheid van het bestaan en het gebruik ervan. Hij vestigt in het bijzonder de aandacht op twee kwesties, met name in de juridische context. Ten eerste bestaat er bij persoonsgegevens waarop de afwijking op het gebied van immigratie wordt toegepast een inherente kans dat het gaat om gegevens van een bijzondere categorie in de zin van artikel 9, lid 1, AVG (d.w.z. gegevens "waaruit ras of etnische afkomst blijkt"). Dergelijke gegevens worden in de AVG genoemd omdat zij een hogere mate van bescherming vereisen (Advies 1/15 [2019] 3 C.M.L.R. 25 onder [141]). Ten tweede geldt als basisstelling van het gegevensbeschermingsrecht dat met name het recht van inzage van de betrokkene van groot belang is als toegangspoort tot het kunnen uitoefenen van de andere rechten die aan de betrokkenen worden verleend (zie YS/Minister voor Immigratie, Integratie en Asiel (C-141/12) EU:C:2014:2081; [2015] 1 C.M.L.R. 18 onder [44]).
59. De heer Knight noemt vier punten van praktische aard. Ten eerste, wanneer verwerkingsverantwoordelijken niet aan de betrokkenen uitleggen dat zij een beroep hebben gedaan op een wettelijke vrijstelling, en evenmin een brede samenvatting geven van de redenen waarom, zal de betrokkene niet weten dat de vrijstelling is toegepast, en zal hij deze bijgevolg niet doeltreffend kunnen aanvechten. Ten tweede zullen betrokkenen vooral op de verwerkingsverantwoordelijken aangewezen zijn om de vrijstelling zorgvuldig en alleen voor zover nodig toe te passen. Hoewel elke betrokkene het recht heeft bij de Commissioner een klacht in te dienen over de toepassing van de vrijstelling, of een gerechtelijke procedure in te leiden, is het waarschijnlijk dat de betrokkene niet op de hoogte is van zijn rechten en niet over de middelen beschikt om juridische stappen te ondernemen in omstandigheden waarin het noodzakelijk is dat de rechten inzake gegevensbescherming snel en nauwkeurig worden nageleefd. Ten derde verkeert de betrokkene als immigrant waarschijnlijk in een kwetsbare positie. Ten vierde gaat het hier niet om een abstracte kwestie ten aanzien van de bewijzen van verweerders over het gebruik van de afwijking op het gebied van immigratie (zie [4] hierboven).
60. De heer Knight stelt dat er sprake is van een nauwe parallel tussen het onderhavige bezwaar tegen de afwijking op het gebied van immigratie en de motivering van het Hof in de zaak Christian Institute [2016] UKSC 51. Hij stelt dat de afwijking op het gebied van immigratie, *net als in de zaak Christian Institute, ruim van opzet is, ongedefinieerde termen gebruikt, een lage drempel hanteert, onderworpen is aan controles die op het eerste gezicht niet uit de bepaling blijken en van toepassing is op een zeer breed scala van kaders en rechten. In tegenstelling tot in de zaak Christian Institute zijn er geen algemeen beschikbare richtsnoeren, laat staan een wettelijke status waarmee rekening moet worden gehouden, met betrekking tot de afwijking op het gebied van immigratie."*

72. Gezien al het bovenstaande merkt de EDPB op dat de toepassing van de afwijking op het gebied van immigratie verder moet worden verduidelijkt.

73. Voorts wijst de EDPB op het ontbreken van een juridisch bindend instrument dat de afwijking op het gebied van immigratie verduidelijkt met het oog op de vraag of deze in grote lijnen overeenkomt met artikel 23 AVG en artikelen 7 en 8 EU-Handvest. Tezelfdertijd is de EDPB van mening dat de noodzaak en de evenredigheid van de ruime werkingssfeer *ratione personae* van de afwijking op het gebied van immigratie door de Europese Commissie verder moet worden aangetoond en met bewijzen moet worden gestaafd.

74. **Tot besluit verzoekt de EDPB de Europese Commissie na te gaan wat de stand van zaken is in de bovengenoemde procedure *Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin)* en, aangezien dit arrest niet definitief is (*res judicata*), na te gaan of ze door het arrest in hoger beroep wordt bevestigd of herzien, rekening te houden met een eventuele actualisering op dit punt en deze nader te specificeren in het adequaatheidsbesluit. De EDPB verzoekt de Europese Commissie voorts nadere informatie te verstrekken over de noodzaak en de evenredigheid van de afwijking op het gebied van immigratie, met name gelet op het ruime toepassingsgebied *ratione personae*.**

75. **Tezelfdertijd verzoekt de EDPB de Europese Commissie nader te onderzoeken of er in het Britse rechtskader extra waarborgen bestaan of denkbaar zijn, bijvoorbeeld door middel van juridisch bindende instrumenten die de afwijking op het gebied van immigratie zouden aanvullen door de voorspelbaarheid ervan en de waarborgen voor de betrokkenen te versterken, en die ook een betere en snellere beoordeling van en toezicht op de vereisten inzake de noodzakelijkheid en de evenredigheid mogelijk zouden maken.**

3.1.2. Beperkingen op verdere doorgifte

76. In artikel 44, AVG is bepaald dat doorgiften en verdere doorgiften van persoonsgegevens alleen mogen plaatsvinden indien het door de AVG voor natuurlijke personen gewaarborgde beschermingsniveau niet wordt ondermijnd. Daarom zullen persoonsgegevens die uit de EER naar het VK worden doorgegeven op basis van het adequaatheidsbesluit een beschermingsniveau genieten dat in grote lijnen overeenkomt met het beschermingsniveau dat uit hoofde van het Europese gegevensbeschermingskader wordt geboden. **Dit betekent dat niet alleen de Britse wetgeving "in grote lijnen overeenkomt" met de EU-wetgeving wat betreft de verwerking van persoonsgegevens die in het kader van het ontwerpbesluit naar het VK worden doorgegeven, maar ook dat de in het VK geldende regels met betrekking tot de verdere doorgifte van die gegevens naar derde landen ervoor moeten zorgen dat een in grote lijnen overeenkomstig beschermingsniveau wordt gehandhaafd.**

77. Bijgevolg is het van belang dat elke verdere doorgifte van persoonsgegevens uit de EER van het VK naar een ander derde land naar behoren wordt beschermd met waarborgen of wordt uitgevoerd overeenkomstig de regels inzake afwijkingen[44] om de continuïteit van de door de EU-wetgeving geboden bescherming te waarborgen. **Indien een dergelijke bescherming niet kan worden geboden, mogen er namelijk geen verdere doorgiften van EER-persoonsgegevens plaatsvinden.**

78. De EDPB erkent dat hoofdstuk V AVG grotendeels is overgenomen in de Britse AVG (artikelen 44-49) en in de DPA 2018[45]. **De EDPB heeft echter bepaalde aspecten van het Britse rechtskader met**

[44] Zie artikel 49 Britse AVG.
[45] Zie artikelen 17A, 17B, 17C en 18 DPA 2018.

betrekking tot verdere doorgiften vastgesteld die het beschermingsniveau voor persoonsgegevens die vanuit de EER worden doorgegeven, zouden kunnen ondermijnen.

79. **De eerste uitdaging** die de EDPB heeft vastgesteld, heeft betrekking op de erkenning door het Verenigd Koninkrijk van derde landen, internationale organisaties of grondgebieden[46] als adequate ontvangers, volgens de procedure van de DPA 2018. Verdere doorgifte van EER-persoonsgegevens vanuit het VK naar andere derde landen kan immers plaatsvinden op basis van een eventuele toekomstige Britse verordening inzake adequaatheid[47].

80. Meer bepaald heeft de Britse Secretary of State, zoals uiteengezet in overweging 77 van het ontwerpbesluit, na raadpleging van het ICO de bevoegdheid om een derde land (of een grondgebied of een sector in een derde land), een internationale organisatie, of een beschrijving van een dergelijk land of grondgebied, of van een dergelijke sector of organisatie te erkennen als een land dat een passend beschermingsniveau voor persoonsgegevens waarborgt[48]. Bij de beoordeling van de adequaatheid van het beschermingsniveau moet de Britse Secretary of State rekening houden met dezelfde elementen die de Europese Commissie moet beoordelen op grond van artikel 45, lid 2, punten a) tot en met c), AVG, geïnterpreteerd in samenhang met overweging 104 AVG en de overgenomen EU-jurisprudentie. Dit betekent dat bij de beoordeling van het passende beschermingsniveau van een derde land de relevante norm zal zijn of dat derde land in kwestie een beschermingsniveau waarborgt dat "in grote lijnen overeenkomt" met het binnen het VK gewaarborgde niveau. De EDPB neemt er weliswaar kennis van dat het Verenigd Koninkrijk krachtens de Britse AVG gebieden kan erkennen als gebieden die een passend beschermingsniveau bieden in het licht van het gegevensbeschermingskader van het Verenigd Koninkrijk, maar wil er toch op wijzen dat deze laatste gebieden tot op heden wellicht niet in aanmerking komen voor een door de Europese Commissie uitgevaardigd adequaatheidsbesluit waarin een beschermingsniveau wordt erkend dat "in grote lijnen overeenkomt" met het in de EU gewaarborgde niveau. Dit kan ertoe leiden dat er risico's ontstaan voor de bescherming van persoonsgegevens die vanuit de EER worden doorgegeven, vooral als het gegevensbeschermingskader van het Verenigd Koninkrijk in de toekomst afwijkt van het EU-acquis. Er zij op gewezen dat de historische zaak *Schrems II* van het HvJ-EU[49] er in juli 2020 toe heeft geleid dat het EU-VS-privacyschildbesluit ongeldig werd verklaard, omdat volgens het HvJ-EU het rechtskader van de VS niet kon worden geacht een beschermingsniveau te bieden dat in grote lijnen overeenkomt met dat van de EU. De reeds vastgestelde arresten van het HvJ-EU, die in het Britse rechtskader als overgenomen jurisprudentie worden beschouwd, zouden het VK echter niet meer kunnen binden, aangezien het VK met name de mogelijkheid heeft om de overgenomen EU-wetgeving na afloop van de overbruggingsperiode te wijzigen, en zijn Supreme Court niet gebonden is aan overgenomen EU-jurisprudentie[50].

81. **De EDPB verzoekt de Europese Commissie om het proces van de beoordeling van de adequaatheid en de criteria van de Britse autoriteiten met betrekking tot andere derde landen nauwlettend te volgen, in het bijzonder met betrekking tot derde landen die door de EU niet als adequaat in het**

[46] Zie artikel 17A DPA 2018.
[47] Het Britse equivalent van een adequaatheidsbesluit volgens de AVG.
[48] Zie artikel 182, lid 2, DPA 2018. Zie ook het memorandum van overeenstemming over de rol van het ICO met betrekking tot nieuwe beoordelingen van de adequaatheid in het VK, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/03/secretary-of-state-for-the-department-for-dcms-and-the-information-commissioner-sign-memorandum-of-understanding/
[49] Zie *Schrems II*.
[50] Zie artikel 6, leden 3 tot en met 6, wet van 2018 betreffende de terugtrekking uit de Europese Unie.

kader van de AVG worden erkend. Wanneer de Europese Commissie vaststelt dat een derde land dat door het VK adequaat wordt bevonden geen beschermingsniveau waarborgt dat in grote lijnen overeenkomt met het binnen de EU gewaarborgde niveau, verzoekt de EDPB de Europese Commissie alle nodige stappen te ondernemen, zoals bijvoorbeeld een wijziging van het adequaatheidsbesluit voor het VK, om specifieke waarborgen voor uit de EER afkomstige persoonsgegevens in te voeren en/of de opschorting van het adequaatheidsbesluit voor het VK te overwegen wanneer persoonsgegevens die vanuit de EER naar het VK worden doorgegeven vervolgens aan het derde land in kwestie worden doorgegeven op basis van een Britse verordening inzake adequaatheid.

82. **De tweede uitdaging** heeft te maken met de komende herziening van de reeds bestaande adequaatheidsbesluiten die de Europese Commissie uit hoofde van Richtlijn 95/46/EG heeft genomen. Na deze herziening zou de Europese Commissie kunnen besluiten dat bepaalde landen die tot nu toe een adequaatheidsbesluit genoten, niet langer een in grote lijnen overeenkomstig beschermingsniveau bieden, rekening houdend met de huidige EU-wetgeving en de recente jurisprudentie. Zoals echter in punt 4 van bijlage 21 bij de DPA 2018 is bepaald, heeft het Verenigd Koninkrijk die landen reeds erkend als landen die een passend beschermingsniveau bieden. Hoewel de Britse Secretary of State deze adequaatheidsbesluiten binnen vier jaar moet herzien, merkt de Europese Commissie in haar ontwerpbesluit op dat deze adequaatheidsbesluiten niet automatisch zullen ophouden te bestaan indien de Britse minister de vereiste herziening niet binnen de gestelde termijn van vier jaar uitvoert[51].

83. **De EDPB verzoekt de Europese Commissie om na te gaan of een land dat geacht wordt niet langer een passend beschermingsniveau te bieden door het VK nog steeds als zodanig wordt beschouwd, wanneer de herziening door de EU van de reeds bestaande adequaatheidsbesluiten eenmaal is afgerond. Indien dit het geval is, verzoekt de EDPB de Europese Commissie op basis van de overwegingen 277-280 van het ontwerpbesluit alle passende maatregelen te nemen om de situatie te verhelpen, bijvoorbeeld door het adequaatheidsbesluit te wijzigen om er specifieke vereisten voor persoonsgegevens afkomstig uit de EER aan toe te voegen en/of door het adequaatheidsbesluit op te schorten indien persoonsgegevens die vanuit de EER naar het VK worden doorgegeven vervolgens verder worden doorgegeven naar het derde land in kwestie. De EDPB verzoekt de Europese Commissie deze controles voort te zetten zolang het adequaatheidsbesluit voor het VK van kracht is.**

84. **De derde uitdaging** betreft de verdere doorgifte van persoonsgegevens uit de EER naar niet-adequate landen op basis van de doorgifte-instrumenten waarin artikelen 46 en 47 Britse AVG voorzien. De EDPB benadrukt dat de Britse AVG weliswaar in dezelfde doorgifte-instrumenten voorziet als de AVG, maar dat ervoor moet worden gezorgd dat de daarin vervatte waarborgen een doeltreffende bescherming in het derde land bieden, vooral in het licht van het arrest *Schrems II*.

85. Naar aanleiding van het arrest *Schrems II*, waarin het HvJ-EU erop wijst dat de in de EU geboden bescherming van persoonsgegevens ook moet worden geboden als de gegevens naar elders worden doorgegeven, heeft de EDPB reeds eerste aanbevelingen vastgesteld voor aanvullende maatregelen[52] om de exporteurs zo nodig te helpen ervoor te zorgen dat de betrokkenen een

[51] Zie overweging 82 van het ontwerpbesluit.

[52] Zie de op 10 november 2020 vastgestelde EDPB-aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau voor persoonsgegevens in de Unie te waarborgen, waaraan momenteel de laatste hand wordt gelegd na openbare raadpleging,

beschermingsniveau wordt geboden dat in grote lijnen overeenkomt met het binnen de EU gewaarborgde niveau.

86. Volgens het HvJ-EU is het de taak van de gegevensexporteurs om van geval tot geval en, in voorkomend geval, in samenwerking met de gegevensimporteur in het derde land na te gaan of de wet of de praktijk van het derde land afbreuk doet aan de doeltreffendheid van de passende waarborgen die in de doorgifte-instrumenten van artikel 46 AVG zijn vervat[53]. Wanneer dit het geval is, moeten de gegevensexporteurs aanvullende maatregelen nemen om deze leemten in de bescherming op te vullen en ze op het door de EU-wetgeving vereiste niveau te brengen.

87. **De EDPB verzoekt de Europese Commissie om met het oog op de continuïteit van bescherming in het ontwerpbesluit de verzekering op te nemen dat wanneer de in de artikelen 46 en 47 Britse AVG bedoelde doorgifte-instrumenten door gegevensexporteurs in het Verenigd Koninkrijk worden gebruikt voor verdere doorgiften van door de EER doorgegeven gegevens naar andere derde landen, deze gegevensexporteurs per geval het gegevensbeschermingskader van het derde land beoordelen; en in voorkomend geval passende maatregelen nemen om ervoor te zorgen dat de waarborgen in het gekozen doorgifte-instrument daadwerkelijk in acht worden genomen om een beschermingsniveau te waarborgen dat in grote lijnen overeenkomt met het binnen de EU gewaarborgde niveau. De EDPB benadrukt dat zonder deze garanties het risico bestaat dat het beschermingsniveau dat in grote lijnen overeenkomt met het binnen de EU gewaarborgde niveau zal worden afgezwakt door verdere doorgiften vanuit het VK.**

88. **De vierde uitdaging** met betrekking tot verdere doorgiften betreft de internationale overeenkomsten die het VK heeft gesloten of in de toekomst zal sluiten en de mogelijke rechtstreekse toegang tot persoonsgegevens uit de EER voor de autoriteiten van derde landen die partij zijn bij dergelijke overeenkomsten. De EDPB maakt zich namelijk ernstige zorgen over de reeds gesloten overeenkomst VK-VS in het kader van de Amerikaanse CLOUD Act en de Europese Commissie onderkent deze uitdaging door te benadrukken dat "*een eventuele inwerkingtreding van de overeenkomst gevolgen kan hebben voor het in deze beschikking beoordeelde beschermingsniveau*"[54]. Zodra deze overeenkomst in werking treedt, zouden voor persoonsgegevens die op grond van het ontwerpbesluit van de EER naar het VK worden doorgegeven namelijk de bepalingen van deze overeenkomst gelden waarin de voorwaarden voor rechtstreekse toegang door de autoriteiten van de VS zijn vastgelegd, hetgeen gevolgen heeft voor het gegevensbeschermingskader van het Verenigd Koninkrijk, met inbegrip van de bepalingen betreffende verdere doorgiften. Dientengevolge kan het beschermingsniveau voor de gegevens die vanuit de EER worden doorgegeven aanzienlijk worden beïnvloed door de bepalingen van de met de VS gesloten overeenkomst, wat gevolgen kan hebben voor het beschermingsniveau voor die gegevens. De EDPB merkt in dit verband op dat de Europese Commissie in overweging 153 van haar ontwerpbesluit verwijst naar toelichtingen van de Britse autoriteiten, zonder concrete schriftelijke garanties of toezeggingen aan te halen of te verstrekken en zonder te verwijzen naar specifieke Britse wetgeving die uitvoering zou geven aan dergelijke toelichtingen.

https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_nl.pdf

[53] Zie *Schrems II*, punt 134.

[54] Zie overweging 153 van dit ontwerpbesluit.

89. De EDPB heeft deze bezorgdheid al eerder geuit in een brief aan het Europees Parlement van 15 juni 2020[55]. De EDPB had erop gewezen dat hij op basis van het "*EU-acquis op het gebied van gegevensbescherming, en met name de AVG en de Richtlijn gegevensbescherming bij rechtshandhaving*", voorbehoud maakt ten aanzien van de vraag of de waarborgen in de overeenkomst voor toegang tot persoonsgegevens in het VK van toepassing zouden zijn in bepaalde omstandigheden die openbaarmakingsverplichtingen aan de VS vereisen, en ook ten aanzien van de vraag of deze waarborgen toereikend zijn in het licht van de EU-normen, zodat zij het in de EU geboden beschermingsniveau niet ondermijnen.

90. Voorts kunnen de bepalingen van de overeenkomst VK-VS in het kader van de Amerikaanse CLOUD Act aanzienlijke gevolgen hebben voor de inhoudelijke en procedurele voorwaarden waaronder persoonsgegevens die in het bezit zijn van verwerkingsverantwoordelijken of verwerkers in het VK rechtstreeks toegankelijk zijn voor de autoriteiten van de VS, hetgeen gevolgen heeft voor het door de Britse wetgeving gewaarborgde beschermingsniveau. Om te zorgen voor een beschermingsniveau dat in grote lijnen overeenkomt met het door de EU-wetgeving gewaarborgde niveau, is het bijvoorbeeld "*van essentieel belang dat de waarborgen volgens een dergelijke overeenkomst een verplichte voorafgaande toestemming van de rechter omvatten, als een essentiële waarborg voor de toegang tot metadata en inhoudsgegevens. Op grond van zijn voorlopige beoordeling heeft de EDPB, die weliswaar opmerkt dat in de overeenkomst wordt verwezen naar de toepassing van het nationaal recht, geen duidelijke bepaling in die zin kunnen vinden in de tussen het VK en de VS gesloten overeenkomst*"[56].

91. Hoewel de Europese Commissie benadrukt dat gegevens die in het kader van deze overeenkomst zijn verkregen dezelfde bescherming zouden genieten als de specifieke waarborgen die in de zogenaamde "raamovereenkomst tussen de EU en de VS" zijn opgenomen, heeft de EDPB echter bedenkingen ten aanzien van de vraag of de opneming van deze waarborgen in de overeenkomst VK-VS in het kader van de Amerikaanse CLOUD Act door middel van een loutere verwijzing die *mutatis mutandis* van toepassing is, zou voldoen aan de criteria van duidelijke, precieze en toegankelijke regels wanneer het gaat om de toegang tot persoonsgegevens, of dergelijke waarborgen voldoende zou verankeren om doeltreffend en afdwingbaar te zijn krachtens de Britse wetgeving.

92. **De EDPB beveelt daarom aan dat de Europese Commissie verduidelijkt hoe en op basis van welk rechtsinstrument de beschermingsmaatregelen die gelijkwaardig zijn aan de specifieke waarborgen waarin de raamovereenkomst tussen de EU en de VS voorziet, van kracht zouden worden en een bindend karakter zouden krijgen onder de Britse wetgeving.**

93. De EDPB merkt voorts op dat de bepalingen van de overeenkomst VK-VS in het kader van de Amerikaanse CLOUD Act, gelezen in samenhang met artikel 3 van de Amerikaanse CLOUD Act[57], vragen oproept over de daadwerkelijke toepassing van de waarborgen die de overeenkomst biedt voor de toegang door rechtshandhavingsinstanties van de VS tot persoonsgegevens in het VK die worden verwerkt door aanbieders van elektronische communicatiediensten of afstandscomputerdiensten die onder de jurisdictie van de VS vallen. Mocht een in het VK gevestigde aanbieder van elektronische communicatiediensten of afstandscomputerdiensten namelijk onder de

[55] Zie het antwoord van de EDPB aan Europarlementariërs Sophie in 't Veld en Moritz Körner over de overeenkomst VK-VS in het kader van de Amerikaanse CLOUD Act, vastgesteld op 15 juni 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0054-uk-usagreement.pdf
[56] Zie de bovengenoemde brief van de EDPB.
[57] Zie de Amerikaanse CLOUD Act, https://www.congress.gov/bill/115th-congress/senate-bill/2383/text

wetgeving van de VS vallen (bijvoorbeeld omdat hij de dochtermaatschappij is van een onderneming uit de VS), dan moet nog worden nagegaan of de autoriteiten in de VS zich op de overeenkomst VK-VS in het kader van de Amerikaanse CLOUD Act zouden moeten beroepen om die gegevens te verkrijgen. Aangezien de Europese Commissie erop wijst dat *"[b]ijzondere aandacht zal worden besteed aan de toepassing en de aanpassing van de beschermingsmaatregelen van de raamovereenkomst aan het specifieke type doorgiften waarop de overeenkomst tussen het VK en de VS betrekking heeft",* benadrukt de EDPB dat het op basis van zijn voorlopige beoordeling onduidelijk is of de in de overeenkomst VK-VS in het kader van de Amerikaanse CLOUD Act vastgelegde waarborgen, en dus die van de raamovereenkomst tussen de EU en de VS, van toepassing zouden zijn op alle eventuele verzoeken om toegang tot gegevens in het VK die door de Amerikaanse autoriteiten op grond van de Amerikaanse CLOUD Act worden gedaan.

94. Het VK kan in de toekomst andere internationale overeenkomsten of verbintenissen met derde landen aangaan die van toepassing zouden zijn op persoonsgegevens die uit hoofde van het ontwerpbesluit van de EER naar het VK worden doorgegeven[58]. Afhankelijk van de bepalingen van deze overeenkomsten en de toepassing van specifieke waarborgclausules kunnen deze internationale overeenkomsten, doordat zij van invloed zijn op het gegevensbeschermingskader van het Verenigd Koninkrijk, ook aanzienlijke gevolgen hebben voor de inhoudelijke en procedurele voorwaarden voor de toegang tot persoonsgegevens in het VK door de autoriteiten van derde landen. Dit is met name het geval voor het ontwerp van een tweede aanvullend protocol bij het Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken van de Raad van Europa (hierna "Verdrag van Boedapest" genoemd), waarover momenteel wordt onderhandeld door de partijen bij dit Verdrag, waartoe verscheidene niet-EU-landen behoren. Het ontwerpprotocol bevat namelijk clausules die door de partijen naar eigen goeddunken kunnen worden geactiveerd, bijvoorbeeld betreffende de toestemming om al dan niet toegang te verlenen tot inhoudsgegevens. Hoewel alle lidstaten van de EU de clausules in overeenstemming met de EU-voorschriften inzake gegevensbescherming zouden activeren, is er geen garantie gegeven voor het VK, dat aanzienlijk zou kunnen afwijken van het beschermingsniveau dat dan binnen de EU zou worden geboden. Een ander voorbeeld van de hierboven geschetste problematiek is de overeenkomst tussen het VK en Japan voor een uitgebreid economisch partnerschap[59] (Comprehensive Economic Partnership, ("CEPA")), de eerste post-brexit-handelsovereenkomst van het VK die op 1 januari 2021[60] in werking is getreden en die bepalingen over persoonsgegevens bevat[61]. De EDPB wijst er voorts op dat het VK op 1 februari 2021 ook formeel zijn verzoek heeft aangekondigd om toe te treden tot het alomvattend en vooruitstrevend trans-Pacifisch partnerschap

[58] Zie punt 2.3.3 hierboven.

[59] Zie UK/Japan: Agreement for a Comprehensive Economic Partnership [CS Japan No.1/2020], https://www.gov.uk/government/publications/ukjapan-agreement-for-a-comprehensive-economic-partnership-cs-japan-no12020

[60] Zie de richtsnoeren van de Britse regering over de handelsovereenkomsten van het VK met niet-EU-landen, https://www.gov.uk/guidance/uk-trade-agreements-with-non-eu-countries

[61] Overeenkomstig artikel 8.80, lid 5, CEPA, verbinden de partijen zich ertoe de ontwikkeling aan te moedigen van mechanismen ter bevordering van de verenigbaarheid van hun verschillende juridische benaderingen van de bescherming van (persoons)gegevens. Overeenkomstig artikel 8.84 verbinden de partijen zich ertoe de grensoverschrijdende doorgifte van gegevens langs elektronische weg, met inbegrip van persoonsgegevens, niet te verbieden of te beperken wanneer deze activiteit geschiedt ten behoeve van de bedrijfsvoering van een onder de overeenkomst vallende persoon in de zin van de CEPA.

(Comprehensive and Progressive Trans-Pacific Partnership ("CPTPP")), waarin het trans-Pacifisch partnerschap (Trans-Pacific Partnership Agreement ("TPP")) is opgenomen[62].

95. De EDPB wijst erop dat de bovengenoemde internationale overeenkomsten , afgezien van de overeenkomst VK-VS in het kader van de Amerikaanse CLOUD Act, niet aan de orde komen in het ontwerpbesluit.

96. **De EDPB verzoekt de Europese Commissie om:**

- **onderzoek te doen naar de wisselwerking tussen het gegevensbeschermingskader van het Verenigd Koninkrijk en de internationale verbintenissen die het VK is aangegaan, buiten de overeenkomst VK-VS in het kader van de Amerikaanse CLOUD Act, met name om de continuïteit van het beschermingsniveau te waarborgen in geval van verdere doorgiften naar andere derde landen van persoonsgegevens die op grond van een adequaatheidsbesluit van het VK vanuit de EER naar het VK zijn doorgegeven; en om voortdurend zicht te houden op en zo nodig actie te ondernemen met betrekking tot de sluiting van andere internationale overeenkomsten tussen het Verenigd Koninkrijk en derde landen die het beschermingsniveau voor persoonsgegevens waarin de EU voorziet, dreigen te ondermijnen;**

- **aan de EDPB de schriftelijke toezeggingen van de Britse autoriteiten te verstrekken en specifieke bepalingen in de Britse wetgeving aan te wijzen met betrekking tot de uitleg in verband met de mogelijke toepassing en uitvoering van de overeenkomst VK-VS in het kader van de Amerikaanse CLOUD Act als bedoeld in overweging 153 van het ontwerpbesluit;**

- **in dit verband na te gaan of de overeenkomst VK-VS in het kader van de Amerikaanse CLOUD Act, naast de waarborgen die kunnen worden geboden door een passende uitvoering van de aanpassing van de raamovereenkomst tussen de EU en de VS, passende aanvullende waarborgen biedt om rekening te houden met de mate van gevoeligheid van de betrokken gegevenscategorieën en de unieke vereisten van de doorgifte van elektronisch bewijsmateriaal rechtstreeks door aanbieders van elektronische communicatiediensten of afstandscomputerdiensten in plaats van tussen instanties;**

- **te beoordelen wat de gevolgen en mogelijke risico's zijn van de bepalingen aangaande persoonsgegevens in internationale overeenkomsten die onlangs door het VK zijn ondertekend, zoals de CEPA.**

97. **De vijfde uitdaging** heeft betrekking op de toepassing van afwijkingen voor de doorgiften van persoonsgegevens naar een derde land. Hoewel de beschikbare afwijkingen uit hoofde van de Britse AVG dezelfde zijn als die uit hoofde van de AVG, is het van belang dat het ICO ten aanzien van het gebruik van deze afwijkingen een interpretatie toepast en zal blijven toepassen die overeenstemt met die van de EDPB. Indien dit niet het geval is of indien het VK in de toekomst van deze interpretatie afwijkt, ontstaat het risico dat het beschermingsniveau voor gegevens die via het VK van de EER naar derde landen worden overgebracht, wordt ondermijnd.

98. **De EDPB verzoekt de Europese Commissie om in het kader van haar toezichthoudende taak met name na te gaan of de Britse interpretatie van het gebruik van afwijkingen blijft overeenstemmen met de interpretatie van de EU. Indien het VK echter een andere interpretatie van het gebruik van de afwijkingen zou volgen, waardoor het beschermingsniveau zou worden ondermijnd, is het van**

[62] Overeenkomstig artikel 14.11, lid 2 TPP staat elke partij de grensoverschrijdende doorgifte van gegevens langs elektronische weg toe, met inbegrip van persoonsgegevens, wanneer deze activiteit geschiedt ten behoeve van de bedrijfsvoering van een onder de overeenkomst vallende persoon.

wezenlijk belang dat de Europese Commissie de nodige stappen onderneemt door het adequaatheidsbesluit te wijzigen om ervoor te zorgen dat het beschermingsniveau dat wordt geboden aan EER-persoonsgegevens die naar het VK worden doorgegeven dan niet wordt ondermijnd wanneer deze gegevens op basis van een andere interpretatie van de afwijkingen vanuit het VK verder worden doorgegeven naar derde landen.

99. **De zesde uitdaging,** die tevens de laatste is voor dit onderdeel, heeft betrekking op het ontbreken van bescherming op grond van artikel 48 AVG in het gegevensbeschermingskader van het Verenigd Koninkrijk.

100. De Europese Commissie heeft in haar ontwerpbesluit immers verduidelijkt dat een doorgifte bij gebrek aan adequaatheidsverordeningen of passende waarborgen alleen kan plaatsvinden op basis van afwijkingen die in artikel 49 Britse AVG zijn opgenomen, "*met uitzondering van artikel 48 van Verordening (EU) 2016/679, dat het Verenigd Koninkrijk niet in de Britse AVG heeft willen opnemen"*[63]*.* Het ontbreken van een bepaling in het gegevensbeschermingskader van het Verenigd Koninkrijk die in grote lijnen overeenstemt met artikel 48 AVG met betrekking tot doorgiften of verstrekkingen naar aanleiding van een rechterlijke uitspraak of een besluit van een administratieve autoriteit van een ander derde land, kan aanleiding geven tot rechtsonzekerheid omtrent de vraag of het beschermingsniveau voor persoonsgegevens die uit hoofde van het ontwerpbesluit van de EER naar het Verenigd Koninkrijk worden doorgegeven, wezenlijk zou worden aangetast.

101. De EDPB merkt in zijn AVG-adequaatheidsreferentie met betrekking tot verdere doorgiften op: "*verdere doorgifte van de persoonsgegevens door de eerste ontvanger van de oorspronkelijke gegevensdoorgifte mag alleen worden toegestaan wanneer de latere ontvanger eveneens is onderworpen aan voorschriften die een passend beschermingsniveau waarborgen en deze ontvanger de relevante instructies opvolgt wanneer hij/zij namens de verwerkingsverantwoordelijke gegevens verwerkt*"[64]. De EDPB benadrukt verder het volgende: "*de eerste ontvanger van de gegevens die vanuit de EU worden doorgegeven, heeft de verantwoordelijkheid om bij ontstentenis van een adequaatheidsbesluit toe te zien op passende waarborgen voor verdere doorgifte van gegevens. Verdere doorgiften van gegevens mogen alleen plaatsvinden voor beperkte en welbepaalde doeleinden en voor zover er een rechtsgrondslag voor de verwerking is*"[65]. Als onderdeel van hoofdstuk V AVG moet artikel 48 ten volle in aanmerking worden genomen bij de beoordeling van de vraag of door het Britse rechtskader in dit opzicht een in feite gelijkwaardig beschermingsniveau wordt gewaarborgd[66].

102. De EDPB benadrukt in dit verband de jurisprudentie van het HvJ-EU met betrekking tot het risico van misbruik of onrechtmatige toegang en onrechtmatig gebruik van gegevens, waarin met name het volgende staat: "*Wat het binnen de Unie gewaarborgde niveau van bescherming van de grondrechten en fundamentele vrijheden betreft, moet een regeling van de Unie die een inmenging in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten met zich brengt, volgens vaste rechtspraak van het Hof duidelijke en precieze regels betreffende de draagwijdte en de toepassing van een maatregel bevatten en minimale vereisten opleggen, zodat de personen van wie de persoonsgegevens aan de orde zijn, over voldoende garanties beschikken dat hun gegevens*

[63] Zie voetnoot 78 van het ontwerpbesluit.
[64] Zie WP254 rev.01, blz. 6.
[65] Zie WP254 rev.01, blz. 6.
[66] Zie met name de laatste zin van artikel 44 AVG: "*Alle bepalingen van dit hoofdstuk worden zodanig toegepast dat het door deze verordening voor natuurlijke personen gewaarborgde beschermingsniveau niet wordt ondermijnd.*"

doeltreffend worden beschermd tegen het risico van misbruik en tegen elke onrechtmatige raadpleging en elk onrechtmatig gebruik van deze gegevens. De noodzaak om over dergelijke garanties te beschikken is des te groter wanneer de persoonsgegevens automatisch worden verwerkt en er een aanzienlijk risico bestaat dat deze gegevens op onrechtmatige wijze zullen worden geraadpleegd"[67].

103. De EDPB merkt in dit verband op dat, op basis van de in het ontwerpbesluit beschikbare informatie, in het gegevensbeschermingskader van het Verenigd Koninkrijk niet duidelijk wordt bepaald dat een rechterlijke uitspraak en een besluit van een administratieve autoriteit van een derde land op grond waarvan een verwerkingsverantwoordelijke of een verwerker persoonsgegevens moet doorgeven of verstrekken, alleen op enigerlei wijze mag worden erkend of afdwingbaar zijn indien zij zijn gebaseerd op een internationale overeenkomst tussen het verzoekende derde land en het Verenigd Koninkrijk. Artikel 48 AVG is een wezenlijke bepaling in het kader van hoofdstuk V AVG, aangezien het voorschrijft dat een doorgifte of verstrekking van persoonsgegevens naar aanleiding van een rechterlijke uitspraak of een besluit van een administratieve autoriteit van een derde land alleen mag worden erkend of afdwingbaar mag zijn indien zij zijn gebaseerd op een internationale overeenkomst tussen het verzoekende derde land en de Unie of een lidstaat, onverminderd andere gronden voor doorgifte uit hoofde van hoofdstuk V AVG. De EDPB wijst er namelijk op dat "*een verzoek van een buitenlandse autoriteit op zichzelf geen rechtsgrond voor doorgifte vormt. Het bevel kan alleen worden erkend "als deze is gebaseerd op een internationale overeenkomst, zoals een verdrag inzake wederzijds rechtsbijstand, tussen het verzoekende derde land en de Unie of een lidstaat""*[68]. Het is derhalve van essentieel belang dat in de Britse wetgeving in grote lijnen overeenkomstige bepalingen kunnen worden vastgesteld.

104. In het ontwerpbesluit maakt de Europese Commissie melding van de uitleg van de Britse autoriteiten volgens welke een buitenlandse rechterlijke uitspraak waarbij om gegevens wordt verzocht volgens het gewoonterecht of het geschreven recht in het VK niet afdwingbaar is zonder een internationale overeenkomst, en elke doorgifte van gegevens op verzoek van een buitenlandse rechterlijke instantie of administratieve autoriteit een doorgifte-instrument vereist, zoals een adequaatheidsverordening of passende waarborgen, tenzij een afwijking krachtens artikel 49 Britse AVG van toepassing is. De EDPB heeft echter geen inzage gekregen in de uitwisselingen tussen de Europese Commissie en de Britse autoriteiten[69] ter zake en kan dus niet analyseren en onafhankelijk beoordelen of de door de Britse autoriteiten verstrekte garanties volstaan om een in grote lijnen overeenkomstig beschermingsniveau te garanderen met betrekking tot de waarborgen van artikel 48 AVG.

105. **De EDPB verzoekt de Europese Commissie om verdere garanties en specifieke verwijzingen naar Britse wetgeving die ervoor zorgen dat het beschermingsniveau in het Britse rechtskader in grote lijnen overeenkomt met het binnen de EER gewaarborgde niveau. Daarom verzoekt de EDPB de Europese Commissie om schriftelijke uitleg en toezeggingen van de Britse autoriteiten met betrekking tot de tenuitvoerlegging van beschermingsmaatregelen die in grote lijnen overeenkomen met die van artikel 48 AVG.**

[67] Zie *Schrems I*, punt 91.

[68] Zie de bijlage bij het gezamenlijke antwoord van de EDPB-EDPS aan de commissie LIBE over de gevolgen van de Amerikaanse Cloud Act voor het Europese rechtskader voor de bescherming van persoonsgegevens, vastgesteld op 10 juli 2019, https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en

[69] Zie voetnoot 78 van het ontwerpbesluit.

106. **De EDPB is van mening dat de vaststelling van bepalingen in de Britse wetgeving die een beschermingsniveau waarborgen dat in grote lijnen overeenkomt met de waarborgen van artikel 48 AVG, van des te groter belang is in het licht van de eerder geuite bedenkingen met betrekking tot verzoeken om toegang tot gegevens in het VK door autoriteiten van de VS of andere derde landen, en gezien het feit dat volgens het adequaatheidsbesluit persoonsgegevens van de EER naar het VK kunnen worden doorgegeven zonder enige verdere garantie of bindende toezegging van de ontvanger met betrekking tot verzoeken om toegang tot gegevens door autoriteiten van andere derde landen.**

3.2. Procedurele en handhavingsmechanismen

107. Op basis van de criteria in de AVG-adequaatheidsreferentie heeft de EDPB de volgende aspecten van het gegevensbeschermingskader van het Verenigd Koninkrijk geanalyseerd, zoals die onder het ontwerpbesluit vallen: het bestaan en het effectief functioneren van een onafhankelijke toezichthoudende autoriteit; het bestaan van een systeem dat een goed nalevingsniveau waarborgt; en een systeem van toegang tot passende verhaalmechanismen dat personen in de EU de middelen verschaft om hun rechten uit te oefenen en verhaal te zoeken zonder op omslachtige belemmeringen voor administratief en gerechtelijk beroep te stuiten.

3.2.1 Bevoegde onafhankelijke toezichthoudende autoriteit

108. De EDPB is ingenomen met de inspanningen van de Europese Commissie om in hoofdstuk 2.6. van het ontwerpbesluit de oprichting, werking en bevoegdheden van de Britse toezichthoudende autoriteit uitvoerig te onderzoeken. In het VK is de Information Commissioner (hierna "IC" genoemd) belast met het toezicht op en de handhaving van de naleving van de Britse AVG en de DPA 2018. Volgens bijlage 12 DPA 2018 is de IC een "Corporation Sole", d.w.z. een afzonderlijke juridische entiteit die bestaat uit één persoon en wordt ondersteund door een kantoor, het ICO.

109. Wat de onafhankelijkheid van de IC betreft, benadrukt de EDPB dat in artikel 51 Britse AVG niet uitdrukkelijk is bepaald dat de IC een onafhankelijke overheidsinstantie is, zoals in artikel 51 AVG wel is voorgeschreven met betrekking tot de TA's. De EDPB erkent niettemin dat artikel 52 Britse AVG soortgelijke regels inzake onafhankelijkheid bevat als artikel 52, leden 1 tot en met 3, AVG.

110. Voorts wijst de EDPB erop dat artikel 52 Britse AVG geen verplichtingen bevat die overeenstemmen met artikel 52, leden 4 tot en met 6, AVG, die uitdrukkelijk waarborgen dat de respectieve TA beschikt over de middelen die nodig zijn voor de effectieve uitvoering van haar taken en de uitoefening van haar bevoegdheden. De EDPB erkent echter dat in de DPA 2018 bepalingen zijn opgenomen die een passende financiering van het ICO beogen[70], alsook de omstandigheid dat in vergelijking met de TA's binnen de EU/EER het ICO momenteel een van de grootste TA's is. Aangezien een voortdurende toewijzing van passende middelen, met name wat personeel en begroting betreft[71], absoluut noodzakelijk is om ervoor te zorgen dat een TA al haar toegewezen taken naar behoren kan vervullen, en dit onlangs ook door het Europees Parlement als van groot belang is aangemerkt[72], acht de EDPB het van essentieel belang bijzondere aandacht te besteden aan de toekomstige ontwikkelingen op dit gebied.

[70] Zie artikelen 137, 138, 182 en punt 9 van bijlage 12 DPA 2018.
[71] Zie WP254 rev.01, blz. 7.
[72] Resolutie van het Europees Parlement van 25 maart 2021 over het evaluatieverslag van de Commissie over de toepassing van de algemene verordening gegevensbescherming, twee jaar na de inwerkingtreding, punt 15, https://www.europarl.europa.eu/doceo/document/B-9-2021-0211_NL.html

111. **Daarom verzoekt de EDPB de Europese Commissie toe te zien op alle ontwikkelingen met betrekking tot de toewijzing van middelen aan het ICO, die nadelig zouden zijn voor de goede vervulling van de taken van het ICO.**

3.2.2. Het bestaan van een systeem voor gegevensbescherming dat een goed nalevingsniveau waarborgt

112. In het ontwerpbesluit wordt uitvoerig ingegaan op de bevoegdheden waarmee het ICO krachtens artikel 58 Britse AVG en de DPA 2018 is toegerust om het toezicht op en de handhaving van de wetgeving te waarborgen. De EDPB erkent dat in artikel 58 Britse AVG de overeenkomstige regels met betrekking tot de bevoegdheden van de TA's van artikel 58, AVG op soortgelijke wijze zijn weergegeven. Wat betreft de bevoegdheid om administratieve geldboeten op te leggen, naargelang de omstandigheden van het concrete geval, bevat artikel 83 Britse AVG soortgelijke bepalingen en maximumbedragen als in artikel 83 AVG. De EDPB is dan ook van mening dat het Britse rechtskader op dit gebied momenteel in overeenstemming is met de normen die in de desbetreffende wetgeving van de EU zijn vastgesteld. In dat verband wijst de EDPB er niettemin op dat het bestaan van *doeltreffende* sancties een belangrijke rol speelt bij het doen naleven van de regels[73].

113. **Gezien het bovenstaande verzoekt de EDPB de Europese Commissie toe te zien op de doeltreffendheid van de sancties en de desbetreffende rechtsmiddelen in het gegevensbeschermingskader van het Verenigd Koninkrijk.**

3.2.3. Het gegevensbeschermingssysteem moet betrokkenen ondersteunen en bijstaan bij het uitoefenen van hun rechten en het toepassen van passende rechtsmiddelen

114. Een doeltreffend toezichtmechanisme, dat onafhankelijk onderzoek van klachten mogelijk maakt, zodat inbreuken op de rechten van de betrokkenen in de praktijk kunnen worden opgespoord en bestraft, alsmede een doeltreffend administratief en hoger beroep (met inbegrip van vergoeding van schade als gevolg van de onrechtmatige verwerking van persoonsgegevens van de betrokkene), zijn essentiële elementen voor de beoordeling van de vraag of een gegevensbeschermingssysteem een passend beschermingsniveau biedt.

115. De EDPB is ingenomen met het feit dat het ICO op zijn website uitgebreide informatie en richtsnoeren verstrekt, die bedoeld zijn om de verwerkingsverantwoordelijken en de verwerkers bewust te maken van hun verplichtingen en taken, en om de betrokkenen te ondersteunen zodat zij geïnformeerd zijn over hun rechten met betrekking tot persoonsgegevens en hun individuele rechten krachtens de Britse AVG en de DPA 2018 kunnen doen gelden.

116. **Onverminderd de huidige stand van zaken verzoekt de EDPB de Europese Commissie voortdurend toe te zien op het niveau van de steun die het ICO specifiek verleent aan personen wier persoonsgegevens in het kader van het adequaatheidsbesluit naar het VK zijn doorgegeven, om hen te helpen hun rechten uit hoofde van het Britse stelsel voor gegevensbescherming uit te oefenen.**

[73] Zie WP254 rev.01, blz. 7.

4. DE TOEGANG TOT EN HET GEBRUIK VAN PERSOONSGEGEVENS DIE VANUIT DE EU DOOR OVERHEIDSINSTANTIES IN HET VERENIGD KONINKRIJK ZIJN DOORGEGEVEN

4.1. De toegang van en het gebruik door de Britse overheidsdiensten met het oog op strafrechtelijke handhaving

4.1.1. Rechtsgrondslagen en toepasselijke beperkingen/waarborgen

117. Wat betreft de door de Europese Commissie uitgevoerde en in de overwegingen 132 en volgende van het ontwerpbesluit opgenomen beoordeling **van de toegang voor rechtshandhavingsdoeleinden**, verstrekt de Europese Commissie genuanceerde en gedetailleerde informatie, en komt zij in het algemeen tot duidelijke conclusies. De EDPB ziet er dan ook van af de meeste feitelijke bevindingen en beoordelingen in dit advies over te nemen. Er zijn echter bepaalde gevallen waarin de weergave van de feiten of de verklaring van de conclusies niet volstaan om door de EDPB te worden overgenomen.

4.1.1.1. Het gebruik van toestemming

118. De EDPB merkt op dat de Europese Commissie in voetnoot 184 van het ontwerpbesluit[74] stelt dat **het gebruik van toestemming** niet relevant is in een adequaatheidsscenario, aangezien de gegevens in doorgiftesituaties niet rechtstreeks door een Britse rechtshandhavingsautoriteit bij een betrokkene worden verzameld op basis van toestemming. Bijgevolg wordt het gebruik van toestemming als rechtsgrondslag bij politiewerk niet door de Europese Commissie beoordeeld.

119. In dit verband wijst de EDPB erop dat op grond van artikel 45, lid 2, punt a), AVG een uitgebreide reeks elementen moet worden beoordeeld, die niet beperkt is tot de doorgiftesituatie, waaronder "*de rechtsstatelijkheid, de eerbiediging van de mensenrechten en de fundamentele vrijheden, de toepasselijke algemene en sectorale wetgeving, onder meer [...] strafrecht*".

120. De EDPB merkt, mede op basis van de informatie die de Europese Commissie heeft verstrekt in overweging 38 van haar ontwerpuitvoeringsbesluit overeenkomstig Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad over de passende bescherming van persoonsgegevens door het Verenigd Koninkrijk (hierna "ontwerpadequaatheidsbesluit in het kader van de Richtlijn gegevensbescherming bij rechtshandhaving" genoemd), op dat voor het gebruik van toestemming, zoals dat in de regeling van het Verenigd Koninkrijk is ingekaderd in de context van rechtshandhaving, altijd een rechtsgrondslag nodig zou zijn waarop men zich kan beroepen. Dit betekent dat zelfs wanneer de politie over wettelijke bevoegdheden beschikt om de gegevens ten behoeve van een onderzoek te verwerken, zij het in bepaalde specifieke omstandigheden (bijvoorbeeld om een DNA-monster te verzamelen) passend kan achten om de toestemming van de betrokkene te vragen.

121. **De EDPB verzoekt de Europese Commissie om in het adequaatheidsbesluit haar analyse op te nemen van het mogelijke gebruik van toestemming in een rechtshandhavingscontext, waarin wordt voorzien in het ontwerpadequaatheidsbesluit in het kader van de Richtlijn gegevensbescherming bij rechtshandhaving**.

[74] Zie blz. 37 van het ontwerpbesluit.

4.1.1.2. Huiszoekingsbevelen en productiebevelen

122. Hoewel de EDPB geen opmerkingen maakt over het verkrijgen van bewijsmateriaal door de politie via huiszoekingsbevelen en productiebevelen in het algemeen, blijkt uit overweging 136 van het ontwerpbesluit dat de Europese Commissie haar overwegingen over de toegang tot rechtshandhaving heeft toegespitst op de politie, en dat de verwerking van persoonsgegevens door andere rechtshandhavingsinstanties in mindere mate is onderzocht.

123. Zo wordt in het Britse Explanatory Framework for Adequacy Decisions, Section F: Law Enforcement[75] op blz. 11 geopperd dat **het National Crime Agency** (hierna "NCA" genoemd) een rechtshandhavingsinstantie van bijzonder belang zou kunnen zijn, die *onder meer* een bredere criminele inlichtingenfunctie heeft. Het NCA omschrijft zijn missie als het samenbrengen van inlichtingen uit een reeks bronnen teneinde de analyse-, beoordelings- en tactische mogelijkheden te optimaliseren, onder meer via technische interceptie van communicatie, rechtshandhavingspartners in het VK en daarbuiten en veiligheids- en inlichtingendiensten[76]. Het NCA is ook een van de belangrijkste gesprekspartners voor internationale rechtshandhavingspartners en speelt een sleutelrol bij de uitwisseling van criminele inlichtingen[77].

124. De EDPB merkt voorts op dat Government Communications Headquarters (hierna "GCHQ" genoemd), waarvan de activiteiten gewoonlijk onder deel 4 DPA 2018 vallen, d.w.z. de nationale veiligheid, eveneens een actieve rol op zich neemt bij het beperken van de maatschappelijke en financiële schade die de zware en georganiseerde misdaad het Verenigd Koninkrijk berokkent, door nauw samen te werken met het ministerie van Binnenlandse Zaken, het NCA, HM Revenue and Customs (hierna "HMRC" genoemd) en andere overheidsdiensten[78]. Zijn activiteiten hebben betrekking op de bestrijding van seksueel misbruik van kinderen, fraude, andere vormen van economische criminaliteit, waaronder het witwassen van geld, crimineel gebruik van technologie, cybercriminaliteit, georganiseerde immigratiecriminaliteit, met inbegrip van mensenhandel, en drugs-, vuurwapen- en andere illegale smokkelactiviteiten.

---

[75] Zie Explanatory Framework for Adequacy Discussions, Section F: Law Enforcement van de Britse regering, 13 maart 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf

[76] Zie de website van het National Crime Agency, Intelligence: enhancing the picture of serious organised crime affecting the UK, https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work/intelligence-enhancing-the-picture-of-serious-organised-crime-affecting-the-uk

[77] Hoewel niet alle door het NCA verwerkte inlichtingen persoonsgegevens zijn, zou een aanzienlijk deel ervan dat wel kunnen zijn en de hier beschreven activiteiten verschillen van die van de reguliere politiediensten, zodat een beoordeling van de toegang tot persoonsgegevens door de rechtshandhavingsinstanties in het VK onvolledig zou zijn zonder een grondige beoordeling van de activiteiten van het NCA. Het ligt in de rede ervoor te zorgen dat aan de beginselen inzake gegevensbescherming bij alle betrokken rechtshandhavingsinstanties dezelfde betekenis wordt toegekend en zo licht te werpen op een bijzonder gegevensgestuurde instantie als het NCA. Daarnaast wordt in de toelichting bij de "Looking to the future" gezegd: *"Wij zoeken voortdurend naar nieuwe mogelijkheden om traditionele vermogens te verzamelen, te ontwikkelen en te verbeteren om de kwantiteit en de kwaliteit van de inlichtingen die zowel in het Verenigd Koninkrijk als daarbuiten beschikbaar zijn te vergroten." "In het kader daarvan ontwikkelen wij het nieuwe National Data Exploitation Capability, waarbij wij gebruikmaken van de bevoegdheden die het agentschap krachtens de Crime and Courts Act heeft gekregen om gegevens die bij de overheid worden bewaard aan elkaar te koppelen, te raadplegen en te exploiteren*." [...] "*Dit zal onze wendbaarheid en flexibiliteit vergroten om op nieuwe dreigingen te reageren en proactief te werk te gaan om informatie en inlichtingen over opkomende dreigingen te verzamelen en te analyseren, zodat wij maatregelen kunnen nemen voordat de dreigingen werkelijkheid worden*."

[78] Zie de website van GCHQ, Mission, Serious and Organised Crime, https://www.gchq.gov.uk/section/mission/serious-crime

125. **De EDPB verzoekt de Europese Commissie haar analyse aan te vullen met een analyse van de agentschappen die actief zijn op het gebied van de rechtshandhaving en die het verzamelen en analyseren van gegevens, waaronder persoonsgegevens, tot speerpunt van hun dagelijkse werkzaamheden lijken te hebben gemaakt, met name het NCA. Bovendien verzoekt de EDPB de Europese Commissie om nader onderzoek te doen naar agentschappen zoals GCHQ, waarvan de activiteiten zowel onder de rechtshandhaving als onder de nationale veiligheid vallen, en het rechtskader dat op hen van toepassing is voor de verwerking van persoonsgegevens.**

4.1.1.3. Onderzoeksbevoegdheden voor rechtshandhavingsdoeleinden

126. De EDPB merkt op dat onder hoofdstuk 4 van de AVG-adequaatheidsreferentie "Essentiële waarborgen in derde **landen voor de toegang van instanties voor wetshandhaving** en nationale veiligheid om aantasting van grondrechten te beperken" wordt vermeld: *"[i]n dit verband merkte het Hof ook kritisch op dat in de eerdere veiligehavenbeschikking "geen enkele vaststelling [is] gedaan ten aanzien van de vraag of er in de Verenigde Staten overheidsregels bestaan ter beperking van dergelijke inmengingen in de grondrechten van de personen van wie de gegevens vanuit de Unie naar de Verenigde Staten worden doorgegeven**, **waarbij geldt dat de overheidsinstanties van dat land tot een dergelijke inmenging mogen overgaan wanneer zij legitieme doelstellingen**, zoals de nationale veiligheid, nastreven*.""[79]. In dit referentiedocument stelt de EDPB dat de **vier Europese essentiële waarborgen**[80] **door alle derde landen, om als adequaat te kunnen worden aangemerkt, moeten worden geëerbiedigd voor de toegang tot gegevens, ongeacht of het gaat om** nationale veiligheid of **rechtshandhaving;** met name **moeten de noodzaak en de evenredigheid met betrekking tot de nagestreefde legitieme doelstellingen worden aangetoond.**

127. In dit deel van het ontwerpbesluit concludeert de Europese Commissie (overweging 139) "*aangezien de door de IPA 2016 verleende onderzoeksbevoegdheden dezelfde zijn als die waarover de nationale veiligheidsdiensten beschikken, worden de voorwaarden, beperkingen en waarborgen die voor die bevoegdheden gelden uitvoerig behandeld in het deel over de toegang tot en het gebruik van persoonsgegevens door de Britse overheidsinstanties voor nationale veiligheidsdoeleinden*". Het vloeit echter voort uit de rechtspraak van het HvJ-EU dat bij de toepassing van de toets van de noodzakelijkheid en de evenredigheid op de wetgeving van de lidstaten die bewaring van en toegang tot persoonsgegevens door overheidsinstanties toestaat, dat legitieme doelstellingen, zoals de nationale veiligheid of bestrijding van ernstige misdrijven, verschillend zijn en dat derhalve de ene wel en de andere niet een bepaald soort inmenging zou kunnen rechtvaardigen[81].

128. **De EDPB zou daarom prijs stellen op een specifieke beoordeling in het kader van het besluit van de noodzaak en de evenredigheid van de voorwaarden, beperkingen en waarborgen die worden beschreven in overweging 174 e.v. - een onderdeel dat is gewijd aan maatregelen waarmee nationale veiligheidsdoelstellingen worden nagestreefd - wanneer het gaat om de toepassing van deze voorwaarden, beperkingen en waarborgen in de context van een maatregel waarmee een rechtshandhavingsdoelstelling wordt nagestreefd. Hij verzoekt de Europese Commissie derhalve nader toe te lichten of de beschreven bewaring van persoonsgegevens en de toegang daartoe voor rechtshandhavingsdoeleinden voldoende beperkt zijn, zodat een beschermingsniveau wordt gewaarborgd dat in grote lijnen overeenkomt met het binnen de EU gewaarborgde niveau.**

---

[79] Zie WP254 rev.01, blz. 9.

[80] Zie Aanbevelingen 02/2020 van de EDPB over de Europese essentiële garanties voor surveillancemaatregelen.

[81] Zie het arrest van het HvJ-EU, gevoegde zaken C-511/18, C-512/18 en C-520/18, *La Quadrature du Net e.a.*, 6 oktober 2020, ECLI:EU:C:2020:791.

4.1.2. Verder gebruik van de verzamelde informatie voor rechtshandhavingsdoeleinden (overwegingen 140-154)

129. De EDPB merkt op dat het gegevensbeschermingskader van het Verenigd Koninkrijk voorziet in soortgelijke waarborgen en beperkingen als die waarin de EU-wetgeving voorziet met betrekking tot het verdere gebruik van de verzamelde informatie voor rechtshandhavingsdoeleinden.

4.1.2.1. Verder gebruik voor andere rechtshandhavingsdoeleinden

130. De DPA 2018 bepaalt in feite dat persoonsgegevens die door een bevoegde autoriteit voor een rechtshandhavingsdoel zijn verzameld verder mogen worden verwerkt (door de oorspronkelijke verwerkingsverantwoordelijke of door een andere verwerkingsverantwoordelijke) voor elk ander rechtshandhavingsdoel, op voorwaarde dat de verwerkingsverantwoordelijke bij wet gemachtigd is om gegevens voor dat andere doel te verwerken, en dat de verwerking noodzakelijk en evenredig is met dat doel. De Europese Commissie merkt op dat alle waarborgen van deel 3 DPA 2018 van toepassing zijn op de verwerking door de ontvangende autoriteit. De EDPB wijst er echter op dat artikel 44, lid 4, artikel 45, lid 4, artikel 48, lid 3, en artikel 68, lid 7, van deel 3 DPA 2018, voorzien in de mogelijkheid om de rechten van de betrokkene te beperken, en dat artikel 79 voorziet in de mogelijkheid om certificaten af te geven waarin wordt verklaard dat een beperking een noodzakelijke en evenredige maatregel is ter bescherming van de nationale veiligheid. **Derhalve beveelt de EDPB aan dat de Europese Commissie de mogelijke gevolgen van dergelijke beperkingen voor het niveau van bescherming van persoonsgegevens nader beoordeelt in verband met het verdere gebruik van de verzamelde informatie. Ook moet meer duidelijkheid worden verschaft met betrekking tot het Britse rechtskader dat een dergelijke doorgifte mogelijk maakt, met name de Digital Economy Act 2017, alsook de Crime and Courts Act 2013 die het delen van informatie met het NCA mogelijk maakt.**

4.1.2.2. Verder gebruik voor andere doeleinden dan rechtshandhaving binnen het Verenigd Koninkrijk

131. In de DPA 2018 is tevens bepaald dat persoonsgegevens die voor een rechtshandhavingsdoel zijn verzameld, mogen worden verwerkt voor een doel dat geen rechtshandhavingsdoel is, wanneer de verwerking bij de wet is toegestaan. In dit geval is artikel 19 van de Counter-Terrorism Act 2008 de rechtsgrondslag op grond waarvan een dergelijk delen is toegestaan. De EDPB merkt in dit verband op dat de werkingssfeer en de bepalingen van artikel 19 van de Counter-Terrorism Act niet volledig aan bod komen in de beoordeling van de Europese Commissie, en verder gebruik van ruimere aard kunnen impliceren, met name wat betreft artikel 19, lid 2, waarin is bepaald dat "[*i*]*nformatie die door een van de inlichtingendiensten is verkregen in verband met de uitoefening van een van zijn functies, door die dienst kan worden gebruikt in verband met de uitoefening van elk van zijn andere functies*."

132. De EDPB merkt voorts op dat de verwijzing van de Europese Commissie naar het feit dat de bevoegde autoriteiten overheidsinstanties zijn die moeten handelen in overeenstemming met het EVRM, met inbegrip van artikel 8, en er aldus voor moeten zorgen dat elke uitwisseling van gegevens tussen de rechtshandhavingsinstanties en de inlichtingendiensten in overeenstemming is met de wetgeving inzake gegevensbescherming en met het EVRM, nader zou kunnen worden onderbouwd door aan te geven in welke relevante besluiten en wetten van de Britse rechtsorde deze grenzen duidelijk en nauwkeurig zijn vastgelegd.

4.1.2.3. Verder gebruik in het kader van verdere doorgiften buiten het VK

133. De Europese Commissie heeft weliswaar verwezen naar het feit dat de overeenkomst VK-VS in het kader van de Amerikaanse CLOUD Act gevolgen kan hebben voor doorgiften van aanbieders van

elektronische communicatiediensten of afstandscomputerdiensten in het VK naar de VS, maar de EDPB wijst er tevens op dat de inwerkingtreding van deze overeenkomst ook gevolgen kan hebben voor het verdere gebruik van de via doorgiften verzamelde informatie van rechtshandhavingsinstanties in het VK, in het bijzonder met betrekking tot het uitvaardigen en doorgeven van bevelen overeenkomstig artikel 5 van de overeenkomst VK-VS in het kader van de Amerikaanse CLOUD Act.

134. In ruimere zin is de EDPB van mening dat het sluiten van toekomstige bilaterale overeenkomsten met derde landen met het oog op samenwerking bij de rechtshandhaving, die een rechtsgrondslag bieden voor de doorgifte van persoonsgegevens naar deze landen, ook van grote invloed kan zijn op de voorwaarden voor verder gebruik van de verzamelde informatie, aangezien dergelijke overeenkomsten van invloed kunnen zijn op het gegevensbeschermingskader van het Verenigd Koninkrijk zoals dat wordt beoordeeld. De EDPB beveelt de Europese Commissie dan ook aan dit punt nader te beoordelen, na te gaan of er internationale overeenkomsten bestaan en te verduidelijken of de bepalingen van deze overeenkomsten van invloed kunnen zijn op de toepassing van de Britse gegevensbeschermingswetgeving en kunnen voorzien in een verdere beperking of vrijstelling met betrekking tot het verdere gebruik en de verdere openbaarmaking overzee van voor rechtshandhavingsdoeleinden verzamelde informatie. De EDPB is van mening dat dergelijke informatie en beoordeling van essentieel belang zijn om een alomvattende beoordeling mogelijk te maken van het beschermingsniveau dat door het Britse rechtskader en de Britse praktijken wordt geboden met betrekking tot openbaarmaking overzee en verder gebruik.

4.1.3. Toezicht

135. De EDPB merkt op dat het toezicht op de strafrechtelijke handhavingsinstanties wordt uitgeoefend door verschillende Commissioners, naast het ICO. In de ontwerpadequaatheidsbesluiten worden de IPC, de Commissioner for the Retention and Use of Biometric Material en de Surveillance Camera Commissioner genoemd. In dit verband moet worden opgemerkt dat het HvJ-EU herhaaldelijk heeft gewezen op de noodzaak van onafhankelijk toezicht. De IPC is van bijzonder belang voor kwesties in verband met de toegang tot persoonsgegevens die naar het VK worden doorgegeven. De EDPB gaat ervan uit dat de IPC een zogenaamde “Judicial Commissioner” is, net als andere Judicial Commissioners, waarnaar in het kader van het hoofdstuk over de nationale veiligheid wordt verwezen, en dat die Judicial Commissioners de onafhankelijkheid van rechters genieten, ook wanneer zij als Commissioner optreden. Ten aanzien van het bureau van de IPC legt de Europese Commissie in overweging 245 van het ontwerpbesluit uit dat deze onafhankelijk functioneert als een zogenaamde onafhankelijke instantie, maar wel gefinancierd wordt door het ministerie van Binnenlandse Zaken.

136. De EDPB heeft in het ontwerpbesluit geen verdere indicaties gevonden om de onafhankelijkheid van de Commissioner for the Retention and Use of Biometric Material en de Surveillance Camera Commissioner te beoordelen.

137. **De Europese Commissie wordt verzocht de onafhankelijkheid van de Judicial Commissioners nader te beoordelen, ook in gevallen waarin de Commissioner niet (meer) als rechter optreedt, en de onafhankelijkheid van de Commissioner for the Retention and Use of Biometric Material en van de Surveillance Camera Commissioner te beoordelen.**

4.2. Algemeen rechtskader inzake gegevensbescherming op het gebied van de nationale veiligheid

4.2.1. Nationale veiligheidscertificaten

138. Overeenkomstig artikel 111 DPA 2018 kunnen verwerkingsverantwoordelijken nationale veiligheidscertificaten aanvragen die worden afgegeven door een minister, een lid van het kabinet, de procureur-generaal of de advocaat-generaal voor Schotland, en waarin wordt verklaard dat vrijstellingen van verplichtingen en rechten die zijn vastgelegd in delen 4 tot en met 6 DPA 2018 een noodzakelijke en evenredige maatregel zijn ter bescherming van de nationale veiligheid. Deze certificaten zijn bedoeld om verwerkingsverantwoordelijken meer rechtszekerheid te bieden en vormen een afdoende bewijs van het feit dat bij de verwerking van persoonsgegevens de nationale veiligheid van toepassing is. Er zij echter op gewezen dat deze certificaten niet vereist zijn om een beroep te kunnen doen op vrijstellingen ten behoeve van de nationale veiligheid, maar dat zij een maatregel van transparantie zijn[82].

139. De EDPB maakt op uit artikelen 17 en 18 van bijlage 20 DPA 2018 dat een nationaal veiligheidscertificaat dat is afgegeven op grond van de Data Protection Act 1998 (hierna "oud certificaat" genoemd) tot 25 mei 2019 geldig was voor de verwerking van persoonsgegevens op grond van de DPA 2018. Tot die datum werden de oude certificaten, tenzij ze vervangen of ingetrokken waren, behandeld alsof ze krachtens de DPA 2018 waren afgegeven.

140. Wanneer er echter geen uitdrukkelijke vervaldatum staat op een nationaal veiligheidscertificaat dat is afgegeven krachtens de Data Protection Act 1998, blijft een dergelijk certificaat volgens de EDPB van kracht met betrekking tot verwerking krachtens de Data Protection Act 1998, tenzij het certificaat wordt ingetrokken of ongeldig wordt verklaard[83]. Hoewel de door deze oude certificaten geboden bescherming beperkt is tot de verwerking van persoonsgegevens overeenkomstig de Data Protection Act 1998, merkt de EDPB op dat nieuwe nationale veiligheidscertificaten kunnen worden afgegeven overeenkomstig de Data Protection Act 1998 voor persoonsgegevens die overeenkomstig de Data Protection Act 1998 werden verwerkt[84].

141. **Omwille van de volledigheid verzoekt de EDPB de Europese Commissie in haar ontwerpbesluit te verduidelijken dat nationale veiligheidscertificaten nog steeds kunnen worden afgegeven op grond van de Data Protection Act 1998. De EDPB verzoekt de Europese Commissie voorts om in haar ontwerpbesluit de verhaal- en toezichtmechanismen te beschrijven met betrekking tot certificaten die zijn afgegeven op grond van de Data Protection Act 1998. Tot slot verzoekt de EDPB de Europese Commissie om in haar ontwerpbesluit ook het aantal bestaande certificaten op te nemen dat krachtens de Data Protection Act 1998 is afgegeven, en om dit aspect nauwlettend te volgen.**

4.2.2. Recht op rectificatie en wissing van gegevens

142. Wat het recht op rectificatie en wissing van gegevens betreft, merkt de EDPB op dat een betrokkene overeenkomstig artikel 100 en artikel 149 DPA 2018 de mogelijkheid heeft om een beroep te doen op het High Court (in Schotland, de "Court of Session") om een verwerkingsverantwoordelijke te gelasten zijn gegevens zonder onnodige vertraging te rectificeren of te wissen.

---

[82] Zie Home Office, The Data Protection Act 2018, National Security Certificates guidance, augustus 2020, punt 4, blz. 3, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf

[83] Zie Home Office, The Data Protection Act 2018, National Security Certificates guidance, augustus 2020, blz. 5.

[84] Zie Home Office, The Data Protection Act 2018, National Security Certificates guidance, augustus 2020, punt 8, blz. 5.

143. **De EDPB benadrukt dat de uitoefening van de rechten van de betrokkenen doeltreffend moet worden gewaarborgd; en verzoekt de Europese Commissie daarom in haar ontwerpbesluit te beschrijven hoe artikel 100 DPA 2018 in de praktijk functioneert, en de toepassing van dit artikel op de voet te volgen.**

4.2.3. Uitzondering ten behoeve van de nationale veiligheid

144. De EDPB vestigt de aandacht op artikel 110 DPA 2018, en in het bijzonder op bijlage 11, waarin de specifieke doeleinden worden genoemd waarvoor inlichtingendiensten kunnen afwijken van bepaalde gegevensbeschermingsbeginselen, onder meer met betrekking tot de rechten van de betrokkenen, en niet verplicht zijn inbreuken in verband met persoonsgegevens aan het ICO te melden[85].

145. De **EDPB verzoekt de Europese Commissie om de reikwijdte van de vrijstellingen verder te verduidelijken, aangezien hij zich afvraagt of alle vrijstellingen waarin bijlage 11 DPA 2018 voorziet relevant zijn voor het werk van de inlichtingendiensten en of zij de equivalentie met het beginsel van de noodzakelijkheid en de evenredigheid waarborgen**. De **EDPB verzoekt de Europese Commissie met name om meer verduidelijking te verschaffen over de omstandigheden waaronder een inlichtingendienst zich zou kunnen beroepen op artikel 10 van bijlage 11 DPA 2018, waarin staat dat "*[d]e opgesomde bepalingen niet van toepassing zijn op persoonsgegevens die bestaan uit aantekeningen van de intenties van de verwerkingsverantwoordelijke met betrekking tot onderhandelingen met de betrokkene, voor zover het waarschijnlijk is dat de toepassing van de opgesomde bepalingen de onderhandelingen zou schaden.*"**

4.3. Toegang van en gebruik door de Britse overheidsdiensten ten behoeve van de nationale veiligheid

146. De EDPB erkent in het algemeen dat de lidstaten een ruime beoordelingsmarge hebben in zaken van nationale veiligheid, hetgeen ook door het EHRM wordt erkend. De EDPB wijst er ook op dat, zoals hij in zijn bijgewerkte aanbevelingen over de Europese essentiële garanties voor surveillancemaatregelen heeft benadrukt[86], in artikel 6, lid 3, van het Verdrag betreffende de Europese Unie is bepaald dat de grondrechten die zijn vastgesteld in het EVRM als algemene beginselen deel uitmaken van de EU-wetgeving. Het HvJ-EU herinnert er in zijn jurisprudentie echter aan dat dit laatste, zolang de EU er niet toe is toegetreden, geen rechtsinstrument is dat formeel in de EU-wetgeving is opgenomen[87]. Bijgevolg moet het door artikel 45 AVG vereiste beschermingsniveau voor de grondrechten worden bepaald op basis van de bepalingen van die verordening, gelezen in het licht van de grondrechten die in het EU-Handvest zijn verankerd. Evenwel hebben volgens artikel 52, lid 3, EU-Handvest de daarin vervatte rechten die overeenkomen met door het EVRM gewaarborgde rechten, dezelfde inhoud en reikwijdte als die welke door het EVRM worden toegekend. Zoals het HvJ-EU heeft opgemerkt, moet bijgevolg rekening worden gehouden met de EHRM-jurisprudentie betreffende rechten die ook in het EU-Handvest zijn opgenomen, die

[85] Deze doeleinden omvatten het voorkomen en opsporen van "criminaliteit", "informatie die volgens de wet of in verband met gerechtelijke procedures openbaar moet worden gemaakt", "parlementaire onschendbaarheid", "gerechtelijke procedures", "onderscheidingen en waardigheden van de kroon", "krijgsmacht", "economisch welzijn", "professioneel verschoningsrecht", "onderhandelingen", "vertrouwelijke referenties van de verwerkingsverantwoordelijke", "examenteksten en examencijfers", "onderzoek en statistieken" en "archivering in het algemeen belang".

[86] Zie Aanbevelingen 02/2020 van de EDPB over de Europese essentiële garanties voor surveillancemaatregelen.

[87] Zie *Schrems II*, punt 98.

het minimale beschermingsniveau bepalen voor de uitlegging van de overeenkomstige rechten in het EU-Handvest[88]. De laatste zin van artikel 52, lid 3, EU-Handvest luidt echter: *"[d]eze bepaling verhindert niet dat het recht van de Unie een ruimere bescherming biedt*."

147. Daarom heeft de EDPB bij de volgende beoordeling rekening gehouden met de EHRM-jurisprudentie, voor zover het EU-Handvest, zoals uitgelegd door het HvJ-EU, niet voorziet in een hoger beschermingsniveau dat andere eisen stelt dan de EHRM-jurisprudentie.

4.3.1. Rechtsgrondslagen, beperkingen en waarborgen - onderzoeksbevoegdheden uitgeoefend in het kader van de nationale veiligheid

4.3.1.1. Algemene opmerkingen

148. De EDPB wijst erop dat de IPA 2016 een recente wet is waarbij verschillende bepalingen van de Intelligence Services Act 1994 zijn gewijzigd. Daarin wordt uiteengezet in hoeverre bepaalde onderzoeksbevoegdheden mogen worden gebruikt om de privacy te doorkruisen[89]. Ondanks twee verslagen van de IPC met nuttige informatie over de toepassing van dit nieuwe rechtskader is er nog steeds geen herziening van bepaalde aspecten, met name wat betreft de selecteurs en de gehanteerde zoekcriteria.

149. Bij wijze van algemene opmerking over de IPA 2016 en het toepassingsgebied benadrukt de EDPB voorts de volgende vier aandachtspunten:

150. Wat het **eerste aandachtspunt** betreft, wijst de EDPB met betrekking tot de kenmerken van de wet op twee aspecten:

151. Ten eerste merkt de EDPB op dat in de wetgeving wordt verwezen naar brede doeleinden voor het gebruik van procedures waarin de IPA 2016 voorziet, en niet naar de categorieën van personen die betrokken kunnen zijn bij het verzamelen van gegevens op grond van delen 2 tot en met 7 IPA 2016. In dit verband wijst de EDPB erop dat er een verband moet bestaan tussen de categorieën van personen die het voorwerp kunnen zijn van surveillancemaatregelen en de doeleinden die met de wetgeving worden nagestreefd om de personele werkingssfeer van de wet te bepalen.

152. Voorts vestigt de EDPB er de aandacht op dat ook de definities van "telecommunicatie-exploitanten", "telecommunicatiedienst" en "telecommunicatiesysteem", waarmee het toepassingsgebied van de wet wordt afgebakend, zeer ruim en tot op zekere hoogte onduidelijk zijn. De EDPB wijst er dan ook op dat deze begrippen in het kader van de IPA 2016 veel ruimer moeten worden opgevat dan in het kader van de telecommunicatiewetgeving, zoals die bijvoorbeeld is gedefinieerd in het Europees wetboek voor elektronische communicatie[90]. De EDPB merkt op dat de definities van "telecommunicatiedienst" en "telecommunicatiesysteem" in de wet naar verluidt doelbewust ruim zijn geformuleerd, zodat zij relevant zullen blijven voor nieuwe technologieën. Evenzo is de definitie

[88] Zie het arrest van het HvJ-EU, gevoegde zaken C-511/18, C-512/18 en C-520/18, *La Quadrature du Net e.a.*, 6 oktober 2020, ECLI:EU:C:2020:791, punt 124.
[89] Zie artikel 1 IPA 2016.
[90] Zie artikel 2, punt 5, van het Europees wetboek voor elektronische communicatie, waarin bijvoorbeeld een "interpersoonlijke communicatiedienst" wordt gedefinieerd als *"een gewoonlijk tegen vergoeding aangeboden dienst die directe persoonlijke en interactieve uitwisseling van informatie via elektronischecommunicatienetwerken tussen een eindig aantal personen mogelijk maakt, waarbij de personen die de communicatie starten of eraan deelnemen, bepalen welke de ontvangers zijn, en die geen diensten omvat die persoonlijke en interactieve communicatie mogelijk maken als een louter bijkomstig kenmerk dat onlosmakelijk verbonden is met een andere dienst*".

van een telecommunicatie-exploitant ook zeer ruim, en kan zij bijvoorbeeld online-videospelletjes met een chatfunctie omvatten, of andere websites die louter dergelijke chatvensters bevatten[91].

153. Daarnaast wordt weliswaar in het algemeen voorzien in procedures en toezicht betreffende de beoordeling van de noodzaak en de evenredigheid van het verzamelen van en de toegang tot gegevens, maar de criteria om tot een dergelijke beoordeling over te gaan, worden in de wet zelf niet omschreven. Aanvullende elementen zijn te vinden in andere documenten, zoals gedragscodes.

154. Zoals in de EDPB-aanbevelingen 02/2020 over de Europese essentiële garanties voor surveillancemaatregelen wordt opgemerkt, heeft het HvJ-EU echter aangegeven dat "*het vereiste volgens hetwelk elke beperking op de uitoefening van grondrechten bij wet wordt gesteld, inhoudt dat de rechtsgrond die de inmenging in die rechten toestaat zelf de reikwijdte van de beperking op de uitoefening van het betrokken recht moet bepalen*"[92]. Meer bepaald heeft het HvJ-EU verduidelijkt dat "*[o]m aan het evenredigheidsvereiste te voldoen, dient een regeling duidelijke en nauwkeurige regels te bevatten over de reikwijdte en de toepassing van de betrokken maatregel, zodat degenen van wie de persoonsgegevens aan de orde zijn, over voldoende waarborgen beschikken dat die gegevens doeltreffend worden beschermd tegen het risico van misbruik aan dit voorschrift te voldoen, moet de betrokken regeling niet alleen duidelijke en nauwkeurige regels over de reikwijdte en de toepassing van de maatregel bevatten, maar ook die minimale eisen opleggen, zodat degenen van wie de gegevens zijn doorgegeven over voldoende garanties beschikken dat hun persoonsgegevens doeltreffend worden beschermd tegen het risico van misbruik. Die regeling moet wettelijk verbindend zijn naar intern recht en in het bijzonder aangeven in welke omstandigheden en onder welke voorwaarden een maatregel die voorziet in de verwerking van dergelijke gegevens kan worden genomen, en aldus waarborgen dat de inmenging tot het strikt noodzakelijke wordt beperkt*"[93].

155. Het EHRM benadrukte ook dat het van belang is dat de wetgeving voldoende duidelijk is om personen "*een adequate indicatie te geven van de omstandigheden waarin en de voorwaarden waaronder de overheidsdiensten dergelijke maatregelen kunnen inzetten*"[94].

156. **De EDPB verzoekt de Europese Commissie derhalve deze aspecten betreffende de nauwkeurigheid, duidelijkheid en volledigheid van de desbetreffende wet nader te beoordelen, en verdere elementen aan te dragen om aan te tonen dat zij een beschermingsniveau biedt dat, wat de kenmerken van de wet betreft, in grote lijnen overeenkomt met het in de EU gewaarborgde niveau. De EDPB benadrukt voorts dat ruime definities ook moeten worden getoetst aan de evenredigheid van de interceptiemaatregelen.**

157. Hoewel sommige van deze elementen in verscheidene interne codes van de bevoegde autoriteiten van de inlichtingendiensten gedeeltelijk zijn uitgewerkt, bijvoorbeeld wat betreft de beoordeling van de noodzaak en de evenredigheid van het verzamelen van gegevens, benadrukt de EDPB dat de vereisten van het HvJ-EU met betrekking tot de aard van het recht impliceren dat de kernelementen, ook om ervoor te zorgen dat personen zich erop kunnen beroepen in het kader van de verhaalsmogelijkheden, moeten worden opgenomen in wetgeving die voorziet in voor beroep

[91] Zie Home Office, Code of practice on the interception of communications, maart 2018, punten 2.5 e.v., https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf

[92] Zie *Schrems II*, punt 175; en de aangehaalde rechtspraak, alsmede het arrest van het HvJ-EU, zaak C-623/17, *Privacy International/Secretary of State for Foreign and Commonwealth Affairs e.a.*, 6 oktober 2020, ECLI:EU:C:2020:790 (hierna "Privacy International" genoemd), punt 65.

[93] Zie *Privacy International*, punt 68.

[94] Zie EHRM, *Zakharov tegen Rusland*, 4 december 2015, CE:ECHR:2015:1204JUD004714306, punt 229.

vatbare rechten[95]. In artikel 6 van bijlage 7 IPA 2016 wordt immers vermeld dat rechtbanken (en toezichthoudende autoriteiten) "*bij het bepalen van een vraag in een dergelijke procedure rekening houden met het feit dat een persoon een code niet in acht heeft genomen*", zonder dat wordt verduidelijkt of individuele personen voor rechtbanken (of toezichthoudende autoriteiten) een schending van de codes kunnen aanvoeren. Bovendien wordt in de tot dusver in het ontwerpbesluit verstrekte elementen ofwel verwezen naar de erkenning door het EHRM van de voorzienbaarheid van de in die codes vervatte regels[96], en niet zozeer naar de "beroepsmogelijkheid" ervan voor de rechter, zoals het HvJ-EU vereist, ofwel naar het feit dat de Britse rechters in sommige gevallen naar codes hebben verwezen, terwijl geen van de genoemde gevallen de mogelijkheid illustreert voor individuen om aan de codes ontleende rechten te doen gelden. **Indien wordt geconcludeerd dat in de Britse wetgeving niet voldoende wordt aangegeven onder welke omstandigheden en voorwaarden een maatregel kan worden genomen en dat deze elementen in feite in interne codes van de autoriteiten van de inlichtingendiensten zijn vervat**, **verzoekt de EDPB de Europese Commissie derhalve verder te onderzoeken of de beperkingen en waarborgen die in de verschillende interne codes van de autoriteiten van de inlichtingendiensten zijn vervat, door particulieren voor de rechter kunnen worden ingeroepen en kunnen worden afgedwongen.**

158. **Het tweede aandachtspunt** betreft het feit dat de bepalingen betreffende enerzijds het gericht verwerven en bewaren van communicatiegegevens en anderzijds het in bulk verzamelen van gegevens, hetzij in de IPA 2016, hetzij in andere wetgeving zoals de Intelligence Services Act 1994 of de Regulation of Investigatory Powers Act 2000, ook van toepassing zullen zijn op gegevens die vanuit de EU naar het VK worden doorgegeven. Wat het in bulk verzamelen van gegevens betreft, benadrukt de EDPB dat de desbetreffende bepalingen van de Britse wetgeving het verzamelen van gegevens buiten het VK mogelijk maken; het kan dus ook gaan om gegevens die op grond van het adequaatheidsbesluit van de EER naar het VK worden doorgegeven[97]. De EDPB merkt voorts op dat de Europese Commissie aangeeft dat "*[er] op moet worden gewezen dat het bewaren en verkrijgen van communicatiegegevens normaliter geen betrekking heeft op persoonsgegevens van betrokkenen uit de EU die krachtens dit besluit aan het Verenigd Koninkrijk worden doorgegeven. De verplichting om communicatiegegevens te bewaren of openbaar te maken uit hoofde van deel 3 en 4 IPA 2016 heeft betrekking op gegevens die door telecommunicatie-exploitanten in het Verenigd Koninkrijk rechtstreeks worden verzameld bij de gebruikers van een telecommunicatiedienst*"[98]. Niettemin wijst de EDPB op het gebrek aan duidelijkheid over het feit dat alleen vestigingen van deze exploitanten die in het VK zijn gevestigd verzoeken van de bevoegde autoriteiten van het VK kunnen ontvangen, aangezien de definitie van telecommunicatie-exploitant in artikel 261, lid 10, IPA 2016 voorschrijft dat "een telecommunicatie-exploitant een persoon is die een telecommunicatiedienst aanbiedt of verstrekt aan personen in het VK *of die een telecommunicatiesysteem beheert of verstrekt dat (geheel of gedeeltelijk) in het VK is gevestigd of vanuit het VK wordt beheerd*". Bijgevolg zou het in feite kunnen gaan om persoonsgegevens van betrokkenen uit de EER, bijvoorbeeld in het geval van

[95] In dit verband heeft het HvJ-EU bijvoorbeeld geoordeeld dat PPD-28 in de VS niet in aanmerking kwam, hoewel het ook enkele beperkingen bevatte met betrekking tot bulkverzameling, zie punt 181 van *Schrems II*.

[96] Zie HvJ-EU, *Big Brother Watch e.a. tegen Verenigd Koninkrijk*, 13 september 2018, ECLI:CE:ECHR:2018:0913JUD005817013 (hierna "Big Brother Watch" genoemd), punt 325: "*Aangezien de IC-code een openbaar document is, dat door beide kamers van het Parlement moet worden goedgekeurd, en waarmee zowel degenen die interceptie-opdrachten uitvoeren als rechterlijke instanties rekening moeten houden, heeft het Hof uitdrukkelijk aanvaard dat de bepalingen ervan in aanmerking kunnen worden genomen bij de beoordeling van de voorzienbaarheid van de RIPA-regeling*."

[97] Zie punt 183 e.v. van *Schrems II* over de beoordeling van wetgeving die voorziet in toegang tot gegevens in doorvoer tussen de EU en een derde land in het kader van een adequaatheidsbesluit.

[98] Zie overweging 196 van het ontwerpbesluit.

gegevens die worden verzameld of gegenereerd door een binnen de EER gevestigde vestiging van een telecommunicatie-exploitant uit het VK, die op grond van het adequaatheidsbesluit worden doorgegeven aan een in het VK gevestigde vestiging van diezelfde exploitant (voor commerciële doeleinden), en vervolgens binnen het VK door de bevoegde overheidsinstanties worden verzameld.

159. **De EDPB is daarom van mening dat de beoordeling van deze bepalingen ook relevant is voor de beoordeling van de mate van adequaatheid van het Britse rechtskader en verzoekt de Europese Commissie dit aspect te verduidelijken en nader te beoordelen in hoeverre dit het geval is. De EDPB verzoekt de Europese Commissie met name haar interpretatie van de werkingssfeer van deze wetgeving te verduidelijken, met inbegrip van de vraag wat onder het begrip "gebruikers van telecommunicatiediensten" valt en of gegevens van vestigingen van telecommunicatie-exploitanten buiten het VK, voor zover het gegevens van betrokkenen uit de EER betreft, kunnen worden opgevraagd, gezien de zeer ruime definitie van telecommunicatie-exploitanten.**

160. **Het derde aandachtspunt** betreft de "dubbele-lockprocedure". De EDPB merkt op dat in de IPA 2016 een nieuwe "dubbele-lockprocedure" is ingevoerd. Niettemin begrijpt de EDPB ook dat, ook al kan het verzamelen van of de toegang tot gegevens voor nationale veiligheids- of inlichtingendoeleinden in beginsel alleen plaatsvinden met een door een Judicial Commissioner goedgekeurd bevelschrift, in de IPA 2016 is bepaald dat "*in welbepaalde beperkte gevallen rechtmatige interceptie zonder bevelschrift mogelijk is en alleen voorafgaande toestemming van de bevoegde IC-autoriteiten zelf vereist is [zie hieronder het artikel over Toezicht], ook voor intercepties overeenkomstig verzoeken uit het buitenland (artikel 52 IPA 2016)*". Zoals hierna wordt benadrukt, stemt dit ook overeen met de bedenkingen van de EDPB, met name wat de openbaarmaking overzee betreft. Bovendien merkt de EDPB op dat voor de interferentie met apparatuur, zij het gericht of in bulk, ook een afwijking van de dubbele-lockprocedure mogelijk is, en dat de Judicial Commissioner alleen de verlenging van bevelschriften in bulk mag goedkeuren, na een aanvankelijke maximumperiode van zes maanden. **De EDPB verzoekt de Europese Commissie verder te onderzoeken of en aan te tonen dat het Britse rechtskader zelfs in gevallen waarin de dubbele-lockprocedure niet van toepassing is, in passende waarborgen voorziet, onder meer door middel van de effectieve mogelijkheden voor toezicht *achteraf* en de verhaalsmogelijkheden die aan de betrokkenen worden geboden, om ervoor te zorgen dat het geboden beschermingsniveau in grote lijnen overeenkomt met het binnen de EU geboden niveau (zie ook hieronder artikel 4.3.3 over Toezicht).**

161. Hoewel de IPA 2016 weliswaar de "dubbele-lockprocedure" heeft ingevoerd, heeft de EDPB nog steeds bedenkingen over bepaalde aspecten van de nieuwe wetgeving. Na de presentatie van de overeenkomstige artikelen van het ontwerpbesluit heeft de EDPB de volgende soorten gegevensverzameling en toegang tot gegevens geanalyseerd, in dezelfde volgorde als door de Europese Commissie is gepresenteerd. De volgorde van de hierna beoordeelde elementen geeft dus geen hiërarchie weer wat betreft de mate van bezorgdheid van de EDPB.

4.3.1.2. Gericht verwerven en bewaren van communicatiegegevens

162. De EDPB merkt op dat er twee functionarissen zijn die gerichte machtigingen kunnen verlenen voor het verkrijgen van communicatiegegevens: de ordonnateur van het Office for Communications Data Authorisations (hierna "de IPC" genoemd), een aangewezen hoge functionaris (een persoon die een voorgeschreven functie of rang bij een relevante overheidsinstantie bekleedt), naast de goedkeuring door een Judicial Commissioner in bepaalde gevallen. Het is de EDPB echter nog steeds niet duidelijk welke functionaris volgens de wet en de desbetreffende code precies toestemming geeft voor welk

soort gerichte verwerving van communicatiegegevens, en in hoeverre een aangewezen functionaris voldoende onafhankelijk zou zijn[99].

163. **De EDPB verzoekt de Europese Commissie dan ook om dit aspect verder te onderzoeken en deze elementen nader toe te lichten.**

164. Wat betreft de kennisgeving waarin de bewaring van communicatiegegevens wordt vereist, merkt de EDPB ook op dat dergelijke kennisgevingen kunnen worden gericht aan een "beschrijving van exploitanten". Dit begrip lijkt te betekenen dat verschillende exploitanten tegelijk kunnen worden verzocht om allemaal gegevens te bewaren. De doelgerichte aard van de verwerving heeft in feite geen betrekking op het aantal exploitanten, maar op de naam of beschrijving van personen, organisaties, plaats of groep van personen die het "doelwit" vormen, een beschrijving van de aard van het onderzoek en een beschrijving van de activiteiten waarvoor de technische middelen worden ingezet. De EDPB wijst er daarom op dat de kennisgeving, afhankelijk van het aantal exploitanten waarop een dergelijke "beschrijving van exploitanten" betrekking heeft, ruimer kan zijn dan wat de procedure voor gerichte bewaring lijkt te impliceren. **De EDPB verzoekt de Europese Commissie dit aspect verder te onderzoeken en verdere garanties te geven dat deze, zelfs wanneer kennisgevingen aan meerdere exploitanten worden gericht, beperkt blijven tot wat strikt noodzakelijk en evenredig is.**

4.3.1.3. Interferentie met apparatuur

165. De EDPB merkt op dat de "interferentie met apparatuur" in geval van urgentie kan afwijken van de dubbele-lockprocedure[100]. De EDPB uit daarom zijn bedenkingen over de ruime formulering van de doeleinden waarvoor een dergelijke interferentie met apparatuur kan worden verzocht, en over het feit dat de criteria voor urgentie (in welk geval de Judicial Commissioner geen toestemming *vooraf* hoeft te geven na een beoordeling van de noodzaak en de evenredigheid van de interferentie met apparatuur) onduidelijk blijven. Aangezien in deze laatstgenoemde situatie "het bevelschrift ophoudt van kracht te zijn en niet kan worden verlengd" indien de Judicial Commissioner de interferentie met apparatuur *achteraf* niet goedkeurt, gaat de EDPB ervan uit dat de verzamelde gegevens ondertussen rechtmatig verzameld blijven. Om deze gegevens te wissen, kan een specifiek bevelschrift van de Judicial Commissioner worden afgegeven[101].

166. **De EDPB verzoekt de Europese Commissie nader te onderzoeken onder welke voorwaarden een beroep kan worden gedaan op urgentie en verduidelijking te geven over de mogelijke manieren waarop de betrokkenen hun rechten kunnen uitoefenen en de mogelijke rechtsmiddelen die hun worden aangereikt in het kader van de interferentie met apparatuur, met name wanneer deze plaatsvindt in het kader van urgentie die leidt tot een afwijking van de dubbele-lockprocedure.**

4.3.1.4. Bulkinterceptie van gegevens van dragers

167. Zoals beschreven in het verslag over de evaluatie van de bulkbevoegdheden[102] *"[b]ehelst bulkinterceptie gewoonlijk het verzamelen van communicatiegegevens wanneer deze via bepaalde dragers (communicatieverbindingen) worden doorgegeven*". In het officiële IPA 2016 informatieblad wordt "bulkinterceptie" omschreven als "*het proces voor het verzamelen van een hoeveelheid communicatie, gevolgd door de selectie van specifieke communicatie die moet worden gelezen,*

[99] Zie ook hieronder betreffende de beoordeling van de dubbele-lockprocedure en de onafhankelijkheid van de Judicial Commissioner.
[100] Zie artikel 109 IPA 2016.
[101] Zie artikel 110, lid 3, punt b), IPA 2016.
[102] Zie Report of the Bulk Powers Review van de Independent Reviewer of Terrorism Legislation, augustus 2016.

bekeken of beluisterd, wanneer dat noodzakelijk en evenredig is." De EDPB merkt op dat "bulkinterceptie" van gegevens in feite inhoudt dat gegevens worden verzameld nog vóór er sprake is van filtering door selecteurs (hetzij eenvoudig in de context van het volgen van personen waarvan reeds bekend is dat zij een bedreiging vormen, hetzij complex in de context van het opsporen van nieuwe bedreigingen en van voorheen onbekende personen die als belangwekkend zijn aangemerkt).

168. Het verzamelen van bulk-communicatiegegevens was ook een van de kwesties die door het HvJ-EU werden onderzocht in de zaak Privacy International, die heeft geleid tot een arrest van de Grote kamer van 6 oktober 2020 (naast de vraag of een dergelijke verzameling van gegevens in het kader van de EU-wetgeving werd verricht, zelfs voor nationale veiligheidsdoeleinden). De IPA 2016 is in de plaats gekomen van de wetgeving waarop dit arrest betrekking had.

169. De EDPB merkt op dat met de invoering van de IPA 2016 in de Britse wetgeving nu ook een bevelschrift vereist is voor de bulkinterceptie van gegevens. De procedure om dit bevelschrift uit te vaardigen berust op de vaststelling van "operationele doeleinden". De lijst van deze operationele doeleinden wordt opgesteld door de hoofden van de inlichtingendiensten en vervolgens goedgekeurd door de Secretary of State. Dit besluit wordt op zijn beurt goedgekeurd door een onafhankelijke Judicial Commissioner, die moet nagaan of het bevelschrift noodzakelijk is en in verhouding staat tot de operationele doeleinden. De EDPB begrijpt dat de Judicial Commissioner niet bevoegd is om de operationele doeleinden zelf te beoordelen, maar wel of het bevelschrift noodzakelijk is en in verhouding staat tot de operationele doeleinden die in het bevelschrift worden genoemd. Het Parliamentary Intelligence and Security Committee krijgt om de drie maanden een kopie van de lijst; de minister-president bekijkt de lijst van deze operationele doeleinden ten minste eenmaal per jaar.

170. Het lijkt echter moeilijk om op basis van de elementen die de Europese Commissie in het ontwerpbesluit verstrekt te beoordelen wat de reikwijdte is van deze operationele doeleinden in de lijst en of het toegestane verzamelen van gegevens voldoet aan de drempel die het HvJ-EU heeft vastgesteld (zo kan het verzamelen van gegevens worden afgebakend tot een geografisch gebied dat beperkt is tot enkele straten, maar kunnen er ook gegevens worden verzameld uit de EER als geheel).

171. Bovendien benadrukt de EDPB dat in bulk verzamelde gegevens gedurende lange perioden kunnen worden bewaard (om beschikbaar te zijn voor verdere toegang voor onderzoek). De EDPB merkt namelijk op dat artikel 150, leden 5 en 6, IPA 2016 alleen voorziet in de vernietiging van de kopieën van de verzamelde gegevens, en alleen als het bewaren ervan niet nodig is of waarschijnlijk niet nodig zal zijn, in het belang van de nationale veiligheid of andere gronden die onder de werkingssfeer van artikel 138, lid 2, IPA 2016 vallen, of als de bewaring niet nodig is voor verschillende andere doeleinden[103]. De EDPB benadrukt dat deze gronden wel erg ruim lijken en dat in elk geval alleen kopieën van de verkregen gegevens worden vermeld.

172. De EDPB merkt voorts op dat de IPA 2016 in dringende gevallen ook de mogelijkheid biedt om bevelschriften te wijzigen zonder voorafgaande goedkeuring van een Judicial Commissioner, en dat het bevelschrift in dat geval, indien de Judicial Commissioner die binnen drie werkdagen na de wijziging *achteraf* wordt geraadpleegd, weigert de wijziging goed te keuren, effect moet sorteren alsof de wijziging niet was doorgevoerd, maar dat de in de tussentijd verzamelde gegevens wel

[103] Zie artikel 150, leden 3 en 6, IPA 2016.

rechtmatig verzameld blijven[104]. Om deze gegevens te wissen, kan een specifiek bevelschrift van de Judicial Commissioner worden afgegeven[105].

173. **De EDPB verzoekt de Europese Commissie dan ook om verdere verduidelijkingen en beoordelingen van bulkintercepties, met name over de selectie en toepassing van selecteurs in het kader van deze bulkinterceptieprocedures, om te verduidelijken in hoeverre de toegang tot persoonsgegevens voldoet aan de door het HvJ-EU vastgestelde drempel (zie ook hieronder punt 4.3.1.7., met name over het toezicht op de selecteurs), en welke waarborgen er zijn ter bescherming van de grondrechten van personen wier gegevens in deze context worden onderschept, onder meer wat betreft de bewaartermijnen van de gegevens. Een onafhankelijke beoordeling door de bevoegde Britse toezichthoudende autoriteiten zou bijzonder nuttig zijn.**

174. **De EDPB benadrukt ook dat het des te hachelijker lijkt dat "communicatie overzee" binnen de werkingssfeer van bulkinterceptiepraktijken valt, hetgeen lijkt te impliceren dat het VK binnen de EER gegevens rechtstreeks zou kunnen onderscheppen en in bulk zou kunnen verzamelen, met inbegrip van gegevens tijdens de doorvoer tussen de EER en het VK die binnen de werkingssfeer van het ontwerpbesluit zouden vallen (zie punt 4.3.2. over het verdere gebruik van de verzamelde gegevens voor nationale veiligheidsdoeleinden en openbaarmaking overzee).**

4.3.1.5. Bescherming en waarborgen ten aanzien van secundaire gegevens

175. Daarnaast is de EDPB bezorgd over het feit dat de desbetreffende Britse wetgeving in verband met bulkinterceptie niet hetzelfde niveau van bescherming biedt voor alle communicatiegegevens. "Secundaire gegevens", die met een bulkbevelschrift kunnen worden verkregen, zijn volgens artikel 137 IPA 2016 zowel "systeemgegevens", "*die bestaan uit, opgenomen zijn in, gehecht zijn aan of logisch verbonden zijn met de communicatie (al dan niet door de afzender)*", als "identificerende gegevens", "*die bestaan uit, opgenomen zijn in, gehecht zijn aan of logisch verbonden zijn met de communicatie (al dan niet door de afzender), die logisch kunnen worden gescheiden van de overige communicatie en die, indien zij gescheiden zouden worden, niets zouden onthullen van wat redelijkerwijs als de (eventuele) betekenis van de communicatie zou kunnen worden beschouwd, ongeacht de betekenis die voortvloeit uit het feit van de communicatie of uit gegevens betreffende de transmissie van de communicatie*"[106].

176. De EDPB merkt op dat deze "secundaire gegevens", ook wel "metadata"[107] genoemd, die in bulk worden verzameld, niet dezelfde waarborgen lijken te genieten als gegevens die met een gericht bevelschrift worden verzameld, maar ook niet als inhoudsgegevens die in bulk worden verzameld. De EDPB constateert namelijk dat de selectie van een willekeurige onderschepte inhoud meer waarborgen[108] geniet dan de selectie van secundaire gegevens[109].

[104] Zie artikel 147 IPA 2016 (deel 6, hoofdstuk I).
[105] Zie artikel 181, lid 3, punt b), IPA 2016.
[106] "Systeemgegevens" en "identificerende gegevens" worden omschreven in artikel 263 IPA 2016.
[107] Zie Report of the Bulk Powers Review van de Independent Reviewer of Terrorism Legislation, augustus 2016.
[108] Zie artikel 152, lid 1, punt c), en leden 3 e.v., IPA 2016.
[108] Zie artikel 152, lid 1, punt c), en leden 3 e.v., IPA 2016.
[109] Zie artikel 152, lid 1, punten a) and b), IPA 2016.

177. Voorts benadrukt de EDPB dat zowel het EHRM[110] als het HvJ-EU[111] vraagtekens hebben geplaatst bij het feit dat dergelijke gegevens minder gevoelig zouden zijn dan andere gegevens, met name inhoudsgegevens. In de gedragscode voor interceptie staan namelijk als voorbeelden van "secundaire gegevens" (zowel "systeemgegevens", zoals routerconfiguraties, e-mailadressen of gebruikers-ID, als alternatieve accountidentificatoren, en "identificerende gegevens", zoals de plaats van een vergadering in een agenda-afspraak, informatie over foto's, zoals de tijd, datum en plaats waarop de foto genomen is). **De EDPB benadrukt dan ook de consequente beoordeling door het EHRM en het HvJ-EU, en herinnert aan de bedenkingen die zijn geuit met betrekking tot secundaire gegevens, die vanwege hun gevoeligheid specifieke waarborgen moeten genieten. De EDPB verzoekt de Europese Commissie daarom zorgvuldig na te gaan of de waarborgen die de Britse wetgeving voor een dergelijke categorie persoonsgegevens biedt, een beschermingsniveau waarborgen dat in grote lijnen overeenkomt met het binnen de EU gewaarborgde niveau.**

4.3.1.6. Geautomatiseerde verwerking van communicatiegegevens

178. De EDPB merkt op dat de autoriteiten van de inlichtingendiensten niet alleen eenvoudige of complexe selecteurs gebruiken om de door middel van bulkverwerving verkregen gegevens te filteren, maar dat zij ook een beroep kunnen doen op andere geautomatiseerde verwerkingsinstrumenten voor het analyseren van "*grote hoeveelheden informatie, waardoor de agentschappen ook verbanden, patronen, associaties of gedragingen kunnen vinden die zouden kunnen wijzen op een ernstige bedreiging die moet worden onderzocht*", aldus het verslag van het Intelligence and Security Committee van 2015[112]. **De EDPB is zich bewust van het feit dat dit openbaar verslag betrekking heeft op praktijken onder het vorige rechtskader, dat vervolgens vervangen werd door de IPA 2016. Niettemin ziet hij de noodzaak in van een verdere onafhankelijke beoordeling van en toezicht op het gebruik van geautomatiseerde verwerkingsinstrumenten door de bevoegde Britse toezichthoudende autoriteiten, en verzoekt hij de Europese Commissie een nadere beoordeling te maken van deze kwestie en de waarborgen die in dit verband aan de betrokkenen in de EER zouden en/of kunnen worden geboden.**

---

[110] Zie EHRM, *Big Brother Watch*, punt 357, onder verwijzing naar de Grote kamer: "*Bijgevolg betwijfelt het Hof weliswaar niet dat de betrokken communicatiegegevens een essentieel instrument zijn voor de inlichtingendiensten bij de bestrijding van terrorisme en zware criminaliteit, maar is het niet van oordeel dat de autoriteiten een redelijk evenwicht hebben gevonden tussen de concurrerende openbare en particuliere belangen door deze gegevens in hun geheel vrij te stellen van de waarborgen die van toepassing zijn op het zoeken en bestuderen van inhoud. Hoewel het Hof niet wil suggereren dat gerelateerde communicatiegegevens alleen toegankelijk zouden moeten zijn om te bepalen of een persoon zich al dan niet op de Britse eilanden bevindt, omdat dit zou betekenen dat voor gerelateerde communicatiegegevens strengere normen zouden moeten gelden dan voor inhoud, moeten er toch voldoende waarborgen zijn om ervoor te zorgen dat de vrijstelling van gerelateerde communicatiegegevens van de vereisten van artikel 16 RIPA beperkt blijft tot de mate die nodig is om te bepalen of een persoon zich op dat moment op de Britse eilanden bevindt.*"

[111] Zie het arrest van HvJ-EU, *Privacy International*, punt 71: "*De inmenging die de doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten vormt in het door artikel 7 van het Handvest gewaarborgde recht, moet als bijzonder ernstig worden beschouwd, met name gelet op het gevoelige karakter van de informatie die deze gegevens kunnen prijsgeven, en op de mogelijkheid om aan de hand van deze gegevens het profiel van de betrokken personen te bepalen, informatie die even gevoelig is als de inhoud zelf van de communicatie. Die inmenging kan bovendien bij de betrokken personen het gevoel opwekken dat hun privéleven constant in de gaten wordt gehouden (zie naar analogie arresten van 8 april 2014, Digital Rights Ireland e.a., C-293/12 en C-594/12, EU:C:2014:238, punten 27 en 37, en 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punten 99 en 100).*"

[112] Zie Intelligence and Security Committee of Parliament, Privacy and Security: A modern and transparent legal framework, 2015, punt 18, blz. 13, https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf

4.3.1.7. Nalevingsrisico's en onverenigbare praktijken van de bevoegde autoriteiten van de inlichtingendiensten

179. De EDPB neemt er nota van dat er gedetailleerde toezichtsverslagen beschikbaar zijn. Zij bieden waardevolle informatie over wat zij als positieve nalevingspraktijken beschouwen en over de vastgestelde nalevingsrisico's en niet-conforme praktijken.

180. Volgens de IPC in zijn verslag voor 2019 hebben verscheidene elementen betreffende de toepassing van het rechtskader door de diverse bevoegde autoriteiten in dit verband enkele (risico's op) niet-nalevingen aan het licht gebracht.

181. Ten eerste heeft de EDPB geconstateerd dat de criteria om een dataset als persoonsgegevens in een bulkdataset of als gerichte gegevens te classificeren niet altijd duidelijk lijken te zijn voor de MI5 en het SIS zelf, met name voor de MI5, hetgeen ertoe kan leiden dat er geen passende waarborgen op de gegevens worden toegepast[113]. In zijn verslag voor 2019 gaf de IPC in overweging dat "*deze kwestie met voorrang moet worden opgelost*"[114]. Ook in verband met persoonsgegevens in een bulkdataset merkt de EDPB op dat de interne nalevingsbeoordeling van bevelschriften door het speciale team voor GCHQ, hoewel de classificatie van persoonsgegevens in bulk bevredigend lijkt te zijn (maar nog door de IPC moet worden gecontroleerd), in maart 2019 ernstige bedenkingen opriep, waarbij 50 % van de motiveringen van bevelschriften voor verwerving in bulk die door het GCHQ-nalevingsteam werden beoordeeld, niet aan de vereiste norm voldeden. Volgens de IPC was het nalevingsteam begonnen met een onderzoek naar het probleem en met de herscholing van het personeel om deze norm te verbeteren. De bijgewerkte opleiding over de bepalingen van de IPA 2016 en de aanvullende training verzorgd door netwerken voor beleid en naleving hebben de naleving door GCHQ op dit gebied verbeterd. De IPC verwacht niet dat deze norm bij toekomstige inspecties zal worden overschreden, maar zal dit gebied nauwlettend blijven volgen[115]. **Daarom deelt de EDPB de mening dat verdere toetsing en monitoring van de genoemde elementen door de Europese Commissie nodig is als onderdeel van de beoordeling van het beschermingsniveau om ervoor te zorgen dat deze norm wordt verbeterd, zoals in het verslag van de IPC wordt benadrukt, en herinnert hij eraan dat bij de beoordeling van de overeenkomst in grote lijnen van een derde land ook rekening moet worden gehouden met de tenuitvoerlegging en concrete toepassing van het rechtskader, zoals bepaald in artikel 45 AVG.**

182. De EDPB wijst meer in het algemeen op de door de IPC gedeelde aandachtspunten betreffende de door de MI5-functionarissen geleide "taakgerichte zoekopdrachten" – waardoor een onderzoeker

[113] Zie het jaarverslag voor 2019 van de Investigatory Powers Commissioner, 15 december 2020, punt 8.39, https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPC-Annual-Report-2019_Web-Accessible-version_final.pdf: "*Wij hebben geconstateerd dat het [Bulk Oversight Panel (BOP)] een positieve ontwikkeling heeft doorgemaakt en merken de impact ervan bij het beheer van de interne naleving op. Wij blijven streven naar een grotere duidelijkheid over het proces dat MI5 gebruikt om nieuwe datasets aan een eerste onderzoek te onderwerpen, zodat wij een beter inzicht krijgen in de besluiten om een dataset te classificeren als BPD of bijvoorbeeld als gerichte gegevens. Wij waren bezorgd over één onopgeloste actie in de BOP-notulen, namelijk het oplossen van tegenstrijdigheden tussen de toewijzingen van BPD tussen MI5 en SIS. Vanwege het verschillende gebruik van de gegevens en de verschillende soorten gegevens die worden bewaard, is het mogelijk dat beide agentschappen dezelfde dataset, of versies daarvan, bewaren, en dat die door de ene agentschap rechtmatig als bulkgegevens en door de andere als gerichte gegevens wordt gecategoriseerd. Indien een van de agentschappen het bewaren van gegevens ten onrechte als gericht heeft aangemerkt, bestaat het risico dat die gegevens zonder passend mandaat zouden worden bewaard en dat er geen passende waarborgen voor zouden zijn*."

[114] Zie het jaarverslag voor 2019 van de Investigatory Powers Commissioner, punt 8.39.

[115] Zie het jaarverslag voor 2019 van de Investigatory Powers Commissioner, punt 10.48.

meer dan één zoekopdracht kan uitvoeren in de bulkverzamelingen van persoonsgegevens waarover hij beschikt, en de "*ernstige nalevingsrisico's in verband met bepaalde door de MI5 gebruikte technologie-omgevingen*", betreffende de plaats waar de gegevens in de omgeving werden opgeslagen, wie er toegang toe heeft gehad, de mate waarin zij werden gekopieerd of gedeeld, de verwijderingsprocedures die erop van toepassing waren, alsook betreffende de bewaartermijnen. Hoewel de IPC stelt dat er maatregelen zijn genomen en waarborgen zijn ingevoerd, zijn sommige daarvan nog steeds handmatig en worden zij op individuele, menselijke basis geleid, en benadrukt hij dat het van cruciaal belang is dat de *"MI5 deze nieuwe processen blijft handhaven en voldoende middelen verstrekt om ze doeltreffend te laten functioneren. Indien MI5 een toename van niet-conform gedrag constateert*"[116]. De IPC verwacht dat deze zo spoedig mogelijk onder zijn aandacht worden gebracht. **De EDPB verzoekt de Europese Commissie dan ook om deze aspecten in de toekomst nauwlettend in het oog te houden**.

183. De EDPB begrijpt ook uit het verslag van de IPC dat voor operaties die in het kader van de bevelschriften in bulk werden uitgevoerd, wat GCHQ betreft "*de kwaliteit van de aanvragen voor interne goedkeuring wisselend was en wij hebben vastgesteld dat de manier waarop dergelijke aanvragen werden geformuleerd voor verbetering vatbaar was*"[117], en dat de uitleg voor het gebruik van algemene descriptoren, voor de gerichte interferentie met apparatuur, in sommige gevallen te algemeen en te onnauwkeurig was[118]. De EDPB merkte ook op dat de IPC in het kader van de interferentie met apparatuur in bulk aanbeveelt dat "*in de aanvragen consequent en expliciet het verband tussen het doelwit en een wettelijk doel en de inlichtingenbehoeften moet worden vastgelegd*"[119], dat "*in alle aanvragen bij de beoordeling van de evenredigheid duidelijk moet worden ingegaan op de mogelijkheid van collaterale inbreuk en relevante verzachtende omstandigheden*"[120], en dat de IPC benadrukte dat ondanks de vooruitgang "*er nog ruimte voor verbetering is*"[121] en dat ook in de toekomst verdere aandacht nodig zal zijn.

184. Met betrekking tot de regeling voor bulkinterceptie op grond van de Regulation of Investigatory Powers Act 2000 (hierna "RIPA 2000" genoemd), die inmiddels is vervangen door bepalingen in de IPA 2016, wijst de EDPB erop dat het ontoereikende toezicht, zowel op het selecteren van internetdragers voor interceptie als op het filteren, doorzoeken en selecteren van onderschepte communicatie voor onderzoek, een van de kernaspecten was die het EHRM onverenigbaar met artikel 8 EVRM achtte ten aanzien van de vroegere wetgeving inzake de onderzoeksbevoegdheden van de Britse autoriteiten in het kader van de nationale veiligheid in de zaak *Big Brother Watch*, die nu naar de Grote kamer is verwezen. **De EDPB verzoekt de Europese Commissie de stand van zaken van de procedure na te gaan, rekening te houden met deze elementen, en ze te specificeren in het adequaatheidsbesluit, mocht de Europese Commissie het vaststellen.**

185. In deze zaak was het EHRM: "*er niet van overtuigd dat de waarborgen betreffende de selectie van de dragers voor interceptie en de selectie van het onderschepte materiaal voor onderzoek afdoende garanties tegen misbruik bieden. Wat echter de meeste zorgen baart, is het ontbreken van een degelijk onafhankelijk toezicht op de selecteurs en de zoekcriteria die gebruikt worden om onderschepte communicatie te filteren*"[122]. Zoals door de IPC wordt benadrukt*, "komt deze bevinding*

[116] Zie het jaarverslag voor 2019 van de Investigatory Powers Commissioner, punt 8.52.
[117] Zie het jaarverslag voor 2019 van de Investigatory Powers Commissioner, punt 10.2.
[118] Zie het jaarverslag voor 2019 van de Investigatory Powers Commissioner, punten 10.16 en 10.17.
[119] Zie het jaarverslag voor 2019 van de Investigatory Powers Commissioner, punt 10.23.
[120] Zie het jaarverslag voor 2019 van de Investigatory Powers Commissioner, punt 10.23.
[121] Zie het jaarverslag voor 2019 van de Investigatory Powers Commissioner, punt 10.23.
[122] Zie EHRM, *Big Brother Watch*, punt 347.

overeen met een soortgelijke aanbeveling in het verslag van het Intelligence and Security Committee, Privacy and Security: A modern and transparent legal framework" uit maart 2015[123]. **De EDPB is ingenomen met het feit dat de IPC bijgevolg in 2019 zijn aanpak van de inspecties van bulkinterceptie heeft herzien, "*waarbij onder meer zorgvuldig is gekeken naar de technisch complexe manieren waarop bulkinterceptie feitelijk wordt uitgevoerd*"**[124]**, en heeft toegezegd "*een grondig onderzoek van de selecteurs en de zoekcriteria waarop het EHRM hierboven heeft gezinspeeld*"**[125] **te zullen opnemen in de inspecties van bulkinterceptie vanaf 2020. Gezien het belang van dit aspect vindt de EDPB het zorgwekkend dat de IPC nog geen gedetailleerd onderzoek naar de selecteurs en de zoekcriteria heeft verricht, en verzoekt hij de Europese Commissie de ontwikkelingen op dit gebied van nabij te volgen, temeer daar de concrete vorm van een dergelijk toezicht nog moet worden verduidelijkt**[126]**.**

4.3.2. Verder gebruik van de verzamelde informatie voor nationale veiligheidsdoeleinden en openbaarmaking overzee

186. Wat het verdere gebruik van de voor de nationale veiligheid verzamelde gegevens betreft, verwijst de Europese Commissie in haar beoordeling naar artikel 87, lid 1, DPA 2018, waarin namelijk wordt bepaald dat "*de aldus verzamelde persoonsgegevens niet mogen worden verwerkt op een wijze die onverenigbaar is met het doel waarvoor zij worden verzameld*". De EDPB wijst er echter op dat voor deze bepaling uitzonderingen ten behoeve van de nationale veiligheid kunnen gelden, overeenkomstig artikel 110 DPA 2018. De EDPB merkt voorts op dat de wetgeving, of het nu gaat om gerichte interceptie en onderzoek, om gerichte verwerving en bewaring van communicatiegegevens, om gerichte interferentie met apparatuur of om bulkinterceptie en de interferentie met apparatuur in bulk, voorziet in de mogelijkheid van "openbaarmaking overzee".

4.3.2.1. Verder gebruik, openbaarmaking overzee en het toepasselijke Britse rechtskader

187. De Europese Commissie heeft deel 4 DPA 2018, en met name artikel 109, aangemerkt als toepasselijke bepalingen waarin specifieke eisen worden gesteld aan het verdere gebruik van de verzamelde informatie, en met name aan de internationale doorgifte van persoonsgegevens door inlichtingendiensten naar derde landen of internationale organisaties. De EDPB merkt echter op dat in artikel 110 DPA 2018 een vrijstelling ten behoeve van nationale veiligheid is opgenomen, waarin is bepaald dat sommige bepalingen van de DPA 2018 niet van toepassing zijn indien vrijstelling van deze bepalingen vereist is om de nationale veiligheid te waarborgen. Tot de betrokken bepalingen die mogelijk niet van toepassing zijn, behoren hoofdstuk 2 van deel 4 DPA 2018 met betrekking tot de beginselen van gegevensbescherming, waaronder doelbinding, en hoofdstuk 3 van deel 4 DPA 2018 met betrekking tot de rechten van de betrokkene. Artikel 109 DPA 2018 juncto artikel 110 DPA 2018 en de voorwaarden waaronder het van toepassing is, zouden kunnen leiden tot gevallen waarin een internationale doorgifte van persoonsgegevens door inlichtingendiensten naar derde landen plaatsvindt zonder toepassing van bepalingen in verband met de beginselen van gegevensbescherming en de rechten van de betrokkenen.

188. Zoals de Europese Commissie heeft geconstateerd, moet een dergelijke vrijstelling per geval worden beoordeeld, en kan er alleen een beroep op worden gedaan voor zover de toepassing van een specifieke bepaling negatieve gevolgen zou hebben voor de nationale veiligheid. De afgifte van een

[123] Zie het jaarverslag voor 2019 van de Investigatory Powers Commissioner, punt 10.28.
[124] Zie het jaarverslag voor 2019 van de Investigatory Powers Commissioner, punt 10.28.
[125] Zie het jaarverslag voor 2019 van de Investigatory Powers Commissioner, punt 10.28.
[126] Zie het jaarverslag voor 2019 van de Investigatory Powers Commissioner, punt 10.28: "over de precieze vorm van deze inspectie moet nog overeenstemming worden bereikt".

nationaal certificaat voor de Britse inlichtingendiensten heeft namelijk tot doel te bevestigen dat een vrijstelling vereist is voor bepaalde persoonsgegevens die worden verwerkt ten behoeve van de bescherming van de nationale veiligheid. De EDPB merkt echter op dat het Britse ministerie van Binnenlandse Zaken in zijn richtsnoeren voor het certificaat inzake nationale veiligheid krachtens de DPA 2018 verduidelijkt dat "*[h]et van meet af aan belangrijk is om op te merken dat een certificaat niet vereist is om een beroep te doen op de vrijstelling ten behoeve van nationale veiligheid; de controleurs zullen namelijk in de meeste gevallen zelf bepalen of de vrijstelling ten behoeve van de nationale veiligheid van toepassing is*" [127]. In de richtsnoeren van het Britse ministerie van Binnenlandse Zaken wordt voorts gesteld dat "*nationale veiligheidscertificaten van toepassing kunnen zijn op persoonsgegevens die specifiek kunnen worden geïdentificeerd, of op een ruimere categorie van persoonsgegevens. Zij kunnen zowel preëmptief als retrospectief zijn*" [128]. De vrijstelling ten behoeve van de nationale veiligheid kan dus van toepassing zijn op een internationale doorgifte van persoonsgegevens door inlichtingendiensten naar derde landen, bij gebreke van een nationaal veiligheidscertificaat.

189. De EDPB merkt verder op dat bijvoorbeeld op grond van het nationale veiligheidscertificaat DPA/S27/Security Service[129] tot 24 juli 2024 persoonsgegevens die worden verwerkt "*voor, namens, op verzoek van of met de hulp of bijstand van de veiligheidsdienst of*" en "*wanneer die verwerking noodzakelijk is om de goede uitvoering van de in artikel 1 van de Security Service Act 1989 beschreven taken van de veiligheidsdienst te vergemakkelijken*", zijn vrijgesteld van de overeenkomstige bepalingen in de Britse wetgeving bij hoofdstuk V AVG met betrekking tot de doorgifte van persoonsgegevens naar derde landen of internationale organisaties. Hoewel de andere nationale veiligheidscertificaten die openbaar beschikbaar zijn niet voorzien in een vrijstelling van de bepalingen van artikel 109 DPA 2018, wordt eraan herinnerd dat de tekst van een nationaal veiligheidscertificaat geheel of gedeeltelijk kan worden achtergehouden indien de publicatie ervan in strijd zou zijn met het belang van de nationale veiligheid, in strijd zou zijn met het openbaar belang, of de veiligheid van een persoon in gevaar zou kunnen brengen.

190. De EDPB constateert bij de beoordeling van het ontwerpbesluit met betrekking tot deze bepalingen in het algemeen dat de waarborgen voor deze openbaarmakingen uitsluitend bestaan uit het vereiste dat de ontvanger van de gegevens de vereisten inzake de beveiliging van de gegevens naleeft, dat de omvang van de openbaarmaking beperkt blijft tot hetgeen noodzakelijk is, dat de gegevens worden bewaard en dat de toegang tot de gegevens beperkt blijft tot een beperkt aantal personen. Met betrekking tot openbaarmaking overzee benadrukt de EDPB **dan ook dat de toepassing van de vrijstelling ten behoeve van de nationale veiligheid waarin de Britse wetgeving voorziet, kan leiden tot situaties waarin de waarborgen die ervoor moeten zorgen dat de beginselen van doelbinding, noodzakelijkheid en evenredigheid, alsook de rechten van de betrokkenen, toezicht en verhaal, in het derde land van bestemming niet volledig zouden worden geboden of in acht zouden worden genomen. De EDPB beveelt de Europese Commissie dan ook aan om de algemene waarborgen die de Britse wetgeving biedt als het gaat om openbaarmaking overzee nader te onderzoeken, met name in het licht van de toepassing van vrijstellingen ten behoeve van de nationale veiligheid.**

[127] Zie Home Office, The Data Protection Act 2018, National Security Certificates guidance, augustus 2020, punt 3, blz. 3.
[128] Zie Home Office, The Data Protection Act 2018, National Security Certificates guidance, augustus 2020, punt 5, blz. 4.
[129] Zie DPA/S27/Security Service, artikel 27 DPA 2018, Certificate of the Secretary of State, 24 juli 2019, https://ico.org.uk/media/about-the-ico/documents/nscs/2615660/nsc-part-2-mi5-201908.pdf

4.3.2.2. Openbaarmaking overzee en uitwisseling van inlichtingen in het kader van internationale samenwerking

191. De EDPB merkt verder op dat de Europese Commissie in het kader van haar beoordeling van de adequaatheid geen rekening heeft gehouden met bestaande internationale overeenkomsten tussen het Verenigd Koninkrijk en derde landen of internationale organisaties die kunnen voorzien in specifieke bepalingen voor de internationale doorgifte van persoonsgegevens door inlichtingendiensten naar derde landen.

192. De EDPB benadrukt voorts dat de beoordeling van de Europese Commissie voornamelijk berust op de beoordeling van deel 4 DPA 2018, en is met name bezorgd over het feit dat de IPA 2016 gericht is op "verzoeken" om het uitwisselen van inlichtingen met buitenlandse partners, maar niet ingaat op andere vormen van het delen van inlichtingen. De EDPB merkt in dit verband op dat in het ontwerpbesluit van de Europese Commissie niet wordt verwezen naar of een oordeel wordt gegeven over het verband tussen het Britse rechtskader en de "Brits-Amerikaanse overeenkomst inzake communicatie-inlichtingen" ("Brits-Amerikaanse CI-overeenkomst"). In een recente verklaring ter gelegenheid van de 75e verjaardag van deze overeenkomst vermeldde de US National Security Agency (hierna "NSA" genoemd) dat dit partnerschap het mogelijk maakt "*om zoveel mogelijk informatie tussen de twee agentschappen te delen, met minimale beperkingen*" en dat "*dit baanbrekende document de beleidslijnen en procedures vaststelde voor Britse en Amerikaanse inlichtingendiensten voor het delen van informatie over communicatie, vertalingen, analyses en het breken van codes*"[130]. Deze overeenkomst werd ook de grondslag voor andere partnerschappen op inlichtingengebied met Australië, Canada, en Nieuw-Zeeland.

193. De vertrouwelijke aard van deze overeenkomst en de bijzondere bepalingen ervan doen een ernstige vraag rijzen in verband met de duidelijkheid en de voorspelbaarheid van het recht in verband met het verdere gebruik en de openbaarmaking overzee van informatie die door de Britse autoriteiten voor nationale veiligheidsdoeleinden is verzameld. In dit verband brengt de EDPB in herinnering dat het HvJ-EU, wat het in de EU gewaarborgde beschermingsniveau betreft, heeft benadrukt dat een regeling die inmenging in het grondrecht op bescherming van persoonsgegevens met zich brengt, "*duidelijke en precieze regels betreffende de draagwijdte en de toepassing van een maatregel [moet] bevatten en minimale vereisten opleggen, zodat de personen van wie de persoonsgegevens aan de orde zijn, over voldoende garanties beschikken dat hun gegevens doeltreffend worden beschermd tegen het risico van misbruik en tegen elke onrechtmatige raadpleging en elk onrechtmatig gebruik van deze gegevens. De noodzaak om over dergelijke garanties te beschikken is des te groter wanneer de persoonsgegevens automatisch worden verwerkt en er een aanzienlijk risico bestaat dat deze gegevens op onrechtmatige wijze zullen worden geraadpleegd*"[131]. De EDPB is daarom van mening dat de Europese Commissie de gevolgen van de Brits-Amerikaanse CI-overeenkomst in aanmerking moet nemen als onderdeel van haar beoordeling van de adequaatheid.

194. Het EHRM heeft in het eerste deel van het arrest van 13 september 2018, in de zaak *Big Brother Watch*, de Britse regeling voor het delen van inlichtingen beoordeeld, en in het bijzonder de Brits-Amerikaanse CI-overeenkomst. Het EHRM heeft namelijk verklaard dat "*[h]et rechtskader op grond waarvan de inlichtingendiensten van het Verenigd Koninkrijk onderschept materiaal kunnen opvragen bij buitenlandse inlichtingendiensten, niet in de RIPA is vervat. Op grond van de Brits-Amerikaanse CI-overeenkomst van 5 maart 1946 is de uitwisseling van materiaal tussen de Verenigde*

[130] Zie het persbericht van de NSA: GCHQ and NSA Celebrate 75 Years of Partnership, 5 februari 2021, https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2494453/gchq-and-nsa-celebrate-75-years-of-partnership/
[131] Zie *Schrems I*, punt 91.

Staten en het Verenigd Koninkrijk uitdrukkelijk toegestaan"[132] en geoordeeld dat er *"een grondslag in de wet is voor het opvragen van inlichtingen aan buitenlandse inlichtingendiensten, en dat die wet voldoende toegankelijk is*"[133]. Hoewel het EHRM heeft geconcludeerd dat er geen schending van artikel 8[134] EVRM heeft plaatsgevonden met betrekking tot de regeling voor het delen van inlichtingen, merkt de EDPB op dat dit arrest nu is doorverwezen naar de Grote kamer, waarvan de uitspraak nog hangende is. De EDPB merkt ook op dat rechter Koskelo in een partly concurring opinion, partly dissenting opinion bij deze uitspraak, waarbij rechter Turković zich heeft aangesloten[135], heeft geconcludeerd dat er een schending is van artikel 8 EVRM met betrekking tot de regeling voor het delen van inlichtingen, door te stellen dat "*[h]et gemakkelijk is in te stemmen met het beginsel dat elke regeling waarbij inlichtingen uit de interceptie van communicatie worden verkregen via buitenlandse inlichtingendiensten, hetzij op basis van verzoeken om een dergelijke interceptie uit te voeren of om de resultaten ervan door te geven, niet mag leiden tot een omzeiling van de waarborgen die moeten gelden voor elke vorm van toezicht door binnenlandse autoriteiten (zie punten 216, 423 en 447). Elke andere benadering zou immers ongeloofwaardig zijn*".

195. Zoals in verscheidene verslagen van de media en van niet-gouvernementele organisaties wordt onderstreept[136][137], dateert de meest recente versie van de Brits-Amerikaanse CI-overeenkomst die openbaar is gemaakt van 1956, en sedertdien zijn de communicatietechnologie en de aard van de signaalinlichtingen ingrijpend veranderd. Uit mediaberichten is bijvoorbeeld gebleken dat gegevens die door onderzeese kabels lopen en in het VK aan land komen, door GCHQ worden onderschept en toegankelijk gemaakt voor de NSA[138].

196. De EDPB beschouwt de vraag of artikel 109 DPA 2018 en de bepalingen van de IPA 2016 van toepassing blijven wanneer de Britse inlichtingendiensten handelen overeenkomstig de Brits-Amerikaanse CI-overeenkomst als een belangrijke aangelegenheid in verband met het delen van inlichtingen. Een ander belangrijk element dat moet worden beoordeeld is of de bepalingen of de daadwerkelijke toepassing van deze overeenkomst gevolgen hebben voor het beschermingsniveau voor persoonsgegevens die vanuit de EER naar het VK worden doorgegeven, dan wel een rechtstreekse toegang tot en verwerving van persoonsgegevens door inlichtingendiensten van andere derde landen mogelijk maken.

197. De EDPB heeft bijgevolg niet alleen bedenkingen bij "openbaarmaking overzee" op basis van deel 4 DPA 2018 en de daarmee verband houdende vrijstelling ten behoeve van de nationale veiligheid, en op basis van verzoeken in het kader van de IPA 2016, **maar maakt zich ook zorgen over andere vormen van informatie-uitwisseling en openbaarmaking op basis van andere instrumenten, met name de verschillende internationale overeenkomsten die het VK met andere derde landen heeft gesloten, vooral wanneer deze instrumenten ontoegankelijk blijven voor het publiek, zoals de Brits-Amerikaanse CI-overeenkomst. Een dergelijke overeenkomst zou kunnen leiden tot een**

[132] Zie EHRM, *Big Brother Watch*, punt 425.
[133] Zie EHRM, *Big Brother Watch*, punt 427.
[134] Zie EHRM, *Big Brother Watch*, punt 448.
[135] Zie EHRM, *Big Brother Watch*, partly concurring, partly dissenting opinion van rechter Koskelo, waarbij rechter Turković zich heeft aangesloten.
[136] Zie BBC, Diary reveals birth of secret UK-US spy pact that grew into Five Eyes, 5 maart 2021, https://www.bbc.com/news/uk-56284453
[137] Zie Privacy International, Policy Briefing - UK Intelligence Sharing Arrangements, april 2018, https://privacyinternational.org/sites/default/files/2018-04/Privacy%20International%20Briefing%20-%20Intelligence%20Sharing%20%28UK%29%20FINAL.pdf
[138] Zie The Guardian, GCHQ taps fibre-optic cables for secret access to world's communications, 21 juni 2013, https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

omzeiling van de waarborgen die zijn vastgesteld met betrekking tot de toegang tot en het gebruik van persoonsgegevens voor nationale veiligheidsdoeleinden.

198. De EDPB deelt namelijk de mening van de speciale rapporteur van de Verenigde Naties, Joe Cannatacci, dat "*[h]et delen van inlichtingen er niet toe mag leiden dat een achterdeurtje wordt gebruikt om inlichtingen te verkrijgen of dat anderen gemakkelijker inlichtingen kunnen verkrijgen zonder binnenlandse waarborgen, noch dat buitenlandse regeringen met minder strenge normen inzake de bescherming van de persoonlijke levenssfeer (of andere mensenrechten) een achterpoortje krijgen om van de Britse inlichtingendiensten inlichtingen te verkrijgen die aanleiding kunnen geven tot schendingen van de mensenrechten*"[139].

199. Voorts is **de EDPB van mening dat het sluiten van bilaterale of multilaterale overeenkomsten met derde landen met het oog op samenwerking op inlichtingengebied, waarbij een rechtsgrondslag wordt verschaft voor de rechtstreekse interceptie en verwerving van persoonsgegevens of de doorgifte van persoonsgegevens naar deze landen, eveneens aanzienlijke gevolgen kan hebben voor de voorwaarden voor het verdere gebruik van de verzamelde informatie, aangezien dergelijke overeenkomsten waarschijnlijk gevolgen zullen hebben voor het gegevensbeschermingskader van het Verenigd Koninkrijk dat wordt beoordeeld.**

4.3.3. Toezicht

200. De EDPB benadrukt het belang van uitgebreid toezicht door onafhankelijke toezichthoudende autoriteiten voor een passend niveau van gegevensbescherming. De garantie van onafhankelijkheid van de toezichthoudende autoriteiten in de zin van artikel 8, lid 3, EU-Handvest is bedoeld om een doeltreffend en betrouwbaar toezicht op de naleving van de voorschriften inzake de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens te garanderen.

201. Wanneer persoonsgegevens worden geraadpleegd en gebruikt ten behoeve van de nationale veiligheid, wordt de toezichtfunctie voornamelijk vervuld door de IPC en de Judicial Commissioners (hierna de "Judicial Commissioners" genoemd).

202. **De EDPB erkent in het algemeen de introductie van Judicial Commissioners in de IPA 2016 als een aanzienlijke verbetering.** In overeenstemming met een verzoek hierboven wordt de Europese Commissie verzocht de onafhankelijkheid van de **Judicial Commissioners nader te beoordelen, en met name na te gaan in hoeverre de onafhankelijkheid van de IPC en het bureau van de IPC (hierna "IPCO" genoemd) wettelijk gewaarborgd is, aangezien die niet in de IPA 2016 is terug te vinden.** Dit is des te belangrijker omdat de IPC besluiten neemt over beroepen van de overheid, wanneer een verzoek om een surveillance**maatregel door** een Judicial Commissioner is afgewezen.

203. De IPC heeft zowel *ex-ante*- als *ex-post*-toezichtsfuncties. Wat het *ex-ante*-toezicht betreft, begrijpt de EDPB dat de functie van de Judicial Commissioners erin bestaat in individuele gevallen verschillende surveillancemaatregelen goed te keuren, waaronder gerichte interceptie en bulkverwerving van communicatiegegevens. De EDPB merkt voorts op dat de voorafgaande

[139] Zie End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion Of his Mission to the United Kingdom of Great Britain and Northern Ireland, Londen, 29 juni 2018, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E#:~:text=Intelligence%20sharing%20must%20not%20result,UK%20intelligence%20that%20could%20give

goedkeuring van surveillancemaatregelen niet uit de HvJ-EU-jurisprudentie kan worden afgeleid als een absoluut vereiste voor de evenredigheid van surveillancemaatregelen[140].

204. Met het oog op de beoordeling van de doeltreffendheid van dit niveau van toezicht acht de EDPB het niettemin nodig meer duidelijkheid te verkrijgen over de scenario's waarin een rechtmatige interceptie zonder voorafgaande goedkeuring van de Judicial Commissioners mogelijk is.

205. In haar ontwerpbesluit vermeldt de Europese Commissie in de voetnoten 201 en 266 "specifieke beperkte gevallen" waarin de IPA 2016 in de artikelen 44 tot en met 52 voorziet met betrekking tot gerichte intercepties. De EDPB merkt op dat de artikelen 45-51 IPA 2016 vrijstellingen zijn waarvan wordt beweerd dat ze niet regelmatig door inlichtingendiensten worden gebruikt. Voorts **begrijpt de EDPB** dat de voorafgaande goedkeuring door de Judicial Commissioners in de **gevallen waarin de vrijstellingen van toepassing zijn** (bv. aanbieders van telecommunicatie- en postdiensten), moet worden uitgevoerd ingeval rechtshandhavingsinstanties of inlichtingendiensten om toegang tot deze gegevens **verzoeken, en verzoekt hij de Europese Commissie om de juistheid hiervan in haar besluit te bevestigen**.

206. De EDPB erkent dat op grond van artikel 44, lid 2, IPA 2016 de interceptie van communicatie is toegestaan indien een van de partijen (verzender of ontvanger) daarmee heeft ingestemd en er sprake is van een machtiging op grond van de RIPA 2000 of de Regulation of Investigatory Powers (Scotland) Act 2000 (2000 asp 11), d.w.z. de vroegere juridische situatie vóór de instelling van de Judicial Commissioners. De EDPB **verzoekt** de Europese Commissie te verduidelijken of dit betekent dat de voorafgaande-goedkeuringsprocedure in gevallen waarin er sprake is van een unilaterale toestemming in het geheel niet van toepassing zou zijn.

207. Wat het *ex-post*-toezicht betreft, is het ook van belang na te gaan of een doeltreffend onafhankelijk toezicht zonder hiaten gewaarborgd is, met name wanneer dit *ex-ante* niet voorzien is.

208. De EDPB merkt op dat voor de artikelen 48-52 IPA 2016 een *ex-post*-beoordeling wordt uitgevoerd door de Judicial Commissioners en **verzoekt de Europese Commissie te verduidelijken volgens welke voorschriften en op wiens initiatief een dergelijke *ex-post*-beoordeling moet worden uitgevoerd**.

209. Volgens artikel 229, lid 4, IPA 2016 hoeft de IPC de uitoefening van bepaalde functies niet te controleren. In dit verband verzoekt de EDPB de Europese Commissie om de bepalingen van artikel 229, lid 4, punten d) en e), IPA 2016 te verduidelijken wat betreft de praktische gevolgen ervan voor de toetsingsbevoegdheid van de IPC. **De EDPB heeft begrepen dat het ICO de bevoegde toezichthoudende autoriteit is waarop de vrijstellingen van artikel 229, lid 4, IPA 2016 van toepassing zijn, en hij verzoekt de Europese Commissie in haar besluit de juistheid hiervan te bevestigen.**

210. **Het blijkt dat** de rol van **de IPC** bij het *ex-post*-toezicht beperkt is tot het doen van aanbevelingen in gevallen van niet-naleving en tot het in kennis stellen van de betrokkene indien de fout ernstig is en het in het algemeen belang is dat de betrokkene wordt ingelicht. **De EDPB verzoekt de Europese Commissie toe te lichten hoe het IPCO de naleving van de wet daadwerkelijk kan waarborgen.**

[140] Hij merkt echter ook op dat het HvJ-EU, toen het in de zaak *Schrems II* het privacyschild ongeldig verklaarde, kennis heeft genomen van het feit dat volgens het recht van de VS het zogeheten FISA-hof "*geen toestemming geeft voor individuele surveillancemaatregelen; in plaats daarvan toestemming geeft voor surveillanceprogramma's (zoals PRISM en Upstream) op basis van jaarlijkse certificeringen*"." (punt 179).

211. **Tot slot begrijpt de EDPB dat gedupeerde personen zich niet rechtstreeks tot het IPCO kunnen wenden, maar een klacht moeten indienen bij het ICO, dat echter beperkte bevoegdheden heeft op het gebied van de nationale veiligheid. De EDPB verzoekt de Europese Commissie dan ook om nader toe te lichten hoe juridisch gewaarborgd wordt dat in dergelijke gevallen klachten door het IPCO worden behandeld.**

4.3.4. Verhaal

212. In het licht van de arresten *Schrems I* en *Schrems II* van het HvJ-EU is het duidelijk dat doeltreffende rechterlijke bescherming in de zin van artikel 47 EU-Handvest van fundamenteel belang is voor de aanname van de adequaatheid van het recht van een derde land. Uit de arresten is ook gebleken dat in dit verband bijzondere aandacht moet worden besteed aan een doeltreffende rechterlijke bescherming op het gebied van de nationale veiligheid bij de toegang tot persoonsgegevens.

213. **De EDPB erkent dat het VK het IPT heeft opgericht. Het IPT is niet alleen bevoegd om zaken te behandelen inzake het gebruik van onderzoeksbevoegdheden door rechtshandhavingsinstanties, maar ook door inlichtingendiensten. De EDPB gaat ervan uit dat het IPT functioneert als een bevoegde rechterlijke instantie in de zin van artikel 47 EU-Handvest. De Europese Commissie wordt verzocht te bevestigen dat het IPT alle in overweging 262 van het ontwerpbesluit genoemde bevoegdheden heeft, ongeacht de rechtsgrondslag op basis waarvan de klacht is ingediend.**

214. Discrete surveillance door inlichtingendiensten betekent veelal dat het voorwerp van de surveillance, de betrokkene, niet op de hoogte is en zal zijn van de surveillance. In dit verband heeft de EDPB, wanneer hij het recht van de VS moest analyseren, vele malen zijn bezorgdheid geuit over het vereiste bij surveillancezaken van “standing”, zoals dat in het recht van de VS wordt geïnterpreteerd. Tegen deze achtergrond merkt de EDPB op dat voor het indienen van een klacht bij het IPT alleen een toets van “overtuiging” vereist is, volgens welke de klager moet aantonen dat hij of zij potentieel gevaar loopt om aan een maatregel te worden onderworpen.

215. Bij de analyse van het IPT besteedt de EDPB ook bijzondere aandacht aan het feit dat de werking van het IPT herhaaldelijk in overeenstemming is bevonden met het EVRM, zoals dat door het EHRM wordt geïnterpreteerd.