Publicatieblad van de Europese Unie

L 360

Uitgave in de Nederlandse taal

Wetgeving

64e jaargang

11 oktober 2021

Inhoud

[1] Voor de EER relevante tekst.

NL

Besluiten waarvan de titels mager zijn gedrukt, zijn besluiten van dagelijks beheer die in het kader van het landbouwbeleid zijn genomen en die in het algemeen een beperkte geldigheidsduur hebben.

Besluiten waarvan de titels vet zijn gedrukt en die worden voorafgegaan door een sterretje, zijn alle andere besluiten.

II

(Niet-wetgevingshandelingen)

BESLUITEN

UITVOERINGSVERORDENING (EU) 2021/1772 VAN DE COMMISSIE

van 28 juni 2021

overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad betreffende de passende bescherming van persoonsgegevens door het Verenigd Koninkrijk

(Kennisgeving geschied onder nummer C(2021) 4800)

(Voor de EER relevante tekst)

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) ([1]), en met name artikel 45, lid 3,

Overwegende hetgeen volgt:

1. INLEIDING

(1) Bij Verordening (EU) 2016/679 zijn de voorschriften vastgesteld voor de doorgifte van persoonsgegevens door verwerkingsverantwoordelijken of verwerkers in de Europese Unie aan derde landen en internationale organisaties, voor zover die doorgiften onder het toepassingsgebied ervan vallen. De voorschriften inzake internationale doorgiften van gegevens zijn vastgelegd in hoofdstuk V van die verordening, dat wil zeggen in de artikelen 44 tot en met 50. Hoewel het verkeer van persoonsgegevens van en naar landen buiten de Europese Unie noodzakelijk is voor de ontwikkeling van de internationale samenwerking en het grensoverschrijdende handelsverkeer, mogen doorgiften aan derde landen niet ten koste gaan van het niveau van de bescherming van de persoonsgegevens in de Europese Unie ([2]).

(2) Op grond van artikel 45, lid 3, van Verordening (EU) 2016/679 kan de Commissie door middel van een uitvoeringshandeling besluiten dat een derde land, een gebied of één of meerdere nader bepaalde sectoren in een derde land, of een internationale organisatie een passend beschermingsniveau waarborgt. Onder deze voorwaarde kan de doorgifte van persoonsgegevens aan een derde land plaatsvinden zonder dat verdere toestemming noodzakelijk is, zoals bepaald in artikel 45, lid 1, en overweging 103 van die verordening.

(3) Zoals bepaald in artikel 45, lid 2, van Verordening (EU) 2016/679 moet de vaststelling van een adequaatheidsbesluit berusten op een grondige analyse van de rechtsorde van het derde land, die zowel de voorschriften betreft die gelden voor de importeurs van gegevens en de beperkingen en waarborgen, als de toegang van overheidsinstanties tot persoonsgegevens. Bij haar beoordeling moet de Commissie nagaan of het betrokken derde land een beschermingsniveau waarborgt dat "in feite overeenkomend" is met het niveau dat in de Europese Unie wordt verzekerd (overweging 104 van Verordening (EU) 2016/679). De norm aan de hand waarvan wordt beoordeeld of het niveau "in feite overeenkomend" is, is de norm die in de Uniewetgeving, en met name in Verordening (EU) 2016/679, en de jurisprudentie van het Hof van Justitie van de Europese Unie is vastgesteld ([3]). In dit verband is ook de adequaatheidsreferentie van het Europees Comité voor gegevensbescherming (EDPB) van belang ([4]).

([1]) PB L 119 van 4.5.2016, blz. 1.
([2]) Zie overweging 101 van Verordening (EU) 2016/679.
([3]) Zie laatstelijke zaak van 16 juli 2020, Facebook Ireland en Schrems ("Schrems II"), C-311/18, ECLI:EU:C:2020:559.
([4]) Europees Comité voor gegevensbescherming, adequaatheidsreferentie, WP 254 rev. 01. beschikbaar op: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108

(4) Zoals het Hof van Justitie van de Europese Unie heeft verklaard, is hiervoor niet noodzakelijk dat hetzelfde beschermingsniveau wordt geboden ([5]). Met name mogen de middelen die het derde land in kwestie voor de bescherming van de persoonsgegevens tot zijn beschikking heeft, anders zijn dan de middelen die binnen de Europese Unie worden ingezet, zolang zij in de praktijk doeltreffend genoeg blijken om een passend beschermingsniveau te bieden ([6]). De adequaatheidsnorm vereist daarom niet dat de voorschriften van de Unie integraal worden overgenomen. Het gaat er veeleer om of het betreffende buitenlandse systeem als geheel het vereiste beschermingsniveau biedt, door de invulling van het recht op gegevensbescherming, de doeltreffende toepassing en afdwingbaarheid daarvan en het toezicht dat wordt uitgeoefend ([7]).

(5) De Commissie heeft het recht en de rechtspraktijk van het Verenigd Koninkrijk zorgvuldig geanalyseerd. Op basis van de bevindingen in de overwegingen (8) tot en met (270) concludeert de Commissie dat het Verenigd Koninkrijk een passend beschermingsniveau waarborgt voor persoonsgegevens die binnen het toepassingsgebied van Verordening (EU) 2016/679 worden doorgegeven van de Europese Unie aan het Verenigd Koninkrijk.

(6) Deze conclusie heeft geen betrekking op persoonsgegevens die worden doorgegeven voor controle van de immigratie door het Verenigd Koninkrijk of die anderszins vallen binnen de omvang van de vrijstelling van bepaalde rechten van de betrokkene met het oog op instandhouding van doeltreffende controle van de immigratie (de "uitzondering voor immigratie") overeenkomstig paragraaf 4, punt 1, van bijlage 2 bij de Data Protection Act (de Britse wet gegevensbescherming, hierna "DPA" genoemd). De geldigheid en interpretatie van de vrijstelling voor immigratie op grond van het Britse recht zijn niet vastgesteld na een besluit van de rechter in tweede aanleg in civiele zaken van Engeland en Wales van 26 mei 2021. Hoewel de rechter in tweede aanleg in civiele zaken erkent dat de rechten van de betrokkene met het oog op controle van de immigratie in beginsel kunnen worden beperkt tot "een belangrijk aspect van het algemeen belang", is hij tot de bevinding gekomen dat de uitzondering voor immigratie, in zijn huidige vorm, niet verenigbaar is met het Britse recht, aangezien de wettelijke maatregel geen specifieke bepalingen bevat waarin de in artikel 23, lid 2, van de United Kingdom General Data Protection Regulation (algemene verordening gegevensbescherming van het Verenigd Koninkrijk (UK GDPR)) ([8]) genoemde waarborgen uiteen worden gezet. Onder deze voorwaarden moet de doorgifte van persoonsgegevens uit de Unie naar het Verenigd Koninkrijk waarop de uitzondering voor immigratie kan worden toegepast worden uitgesloten van de reikwijdte van dit besluit ([9]). Wanneer de onverenigbaarheid met het Britse recht is opgelost, moet de uitzondering voor immigratie opnieuw worden beoordeeld, alsook de noodzaak om de beperking van de reikwijdte van dit besluit te handhaven.

(7) Dit besluit heeft geen gevolgen voor de rechtstreekse toepassing van Verordening (EU) 2016/679 op in het Verenigd Koninkrijk gevestigde organisaties in gevallen waarin is voldaan aan de voorwaarden inzake het territoriaal toepassingsgebied van die verordening, zoals vastgesteld in artikel 3 ervan.

2. VOORSCHRIFTEN DIE VAN TOEPASSING ZIJN OP DE VERWERKING VAN PERSOONSGEGEVENS

2.1. Het grondwettelijk kader

(8) Het Verenigd Koninkrijk is een parlementaire democratie met een constitutioneel vorst als staatshoofd. Het heeft een soeverein parlement, dat boven alle andere overheidsinstellingen staat, een uitvoerende macht die is samengesteld uit leden van het parlement en aan het parlement verantwoording moet afleggen, en een onafhankelijke rechterlijke macht. Het gezag van de uitvoerende macht berust op het vertrouwen dat zij kan afdwingen van het gekozen Lagerhuis en de uitvoerende macht moet verantwoording afleggen aan beide kamers van het parlement, die verantwoordelijk zijn voor het uitoefenen van toezicht op de regering en het bespreken en goedkeuren van wetten.

([5]) Zaak C-362/14, Schrems ("Schrems I"), ECLI:EU:C:2015:650, punt 73.

([6]) Schrems I, punt 74.

([7]) Zie Mededeling van de Commissie aan het Europees Parlement en de Raad, Uitwisseling en bescherming van persoonsgegevens in een geglobaliseerde wereld, COM(2017)7 van 10.1.2017, deel 3.1, blz. 6-7, beschikbaar op: https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52017DC0007&from=EN

([8]) Rechter in tweede aanleg (civiele zaken), *Open Rights Group v Secretary of State for the Home Department and Secretary of State for Digital, Culture, Media and Sport*, [2021] EWCA Civ 800, punten 53 tot en met 56. De rechter in tweede aanleg heeft het besluit van de High Court of Justice (hoogste Britse rechterlijke instantie) tenietgedaan, die de uitzondering eerder had beoordeeld in het licht van Verordening (EU) 2016/679 (met name artikel 23) en het Handvest van de grondrechten van de Europese Unie en de uitzondering wettig had bevonden (*Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor* [2019] EWHC 2562).

([9]) Mits aan de toepasselijke voorwaarden wordt voldaan, mogen doorgiften met het oog op controle van de immigratie door het Verenigd Koninkrijk worden uitgevoerd op basis van de doorgiftemechanismen in de artikelen 46 tot en met 49 van Verordening (EU) 2016/679.

(9) Het Verenigd Koninkrijk parlement heeft bevoegdheden gedelegeerd aan het Schotse parlement, het parlement van Wales (Senedd Cymru) en de Noord-Ierse Assemblee om wetgeving vast te stellen met betrekking tot interne kwesties in Schotland, Wales en Noord-Ierland, die het Britse parlement niet aan zichzelf heeft voorbehouden. Hoewel gegevensbescherming een voorbehouden kwestie is, wat betekent dat in het gehele land dezelfde wetgeving geldt, zijn andere beleidsgebieden die relevant zijn voor dit besluit gedelegeerd. Het strafrechtelijk systeem, met inbegrip van de politie, van Schotland en Noord-Ierland is bijvoorbeeld gedelegeerd aan respectievelijk het Schotse parlement en de Noord-Ierse Assemblee. Het Verenigd Koninkrijk heeft geen gecodificeerde grondwet in de zin van een vast constitutief document. De grondwettelijke beginselen zijn mettertijd ontstaan, met name op basis van de jurisprudentie en gebruiken. De grondwettelijke waarde van bepaalde statuten, zoals de Magna Carta, de Bill of Rights 1689 en de Human Rights Act 1998, is door de rechters erkend. De grondrechten van personen zijn, als onderdeel van de grondwet, ontwikkeld door middel van gewoonterecht, dit geschreven recht en internationale verdragen, en met name het Europees Verdrag voor de rechten van de mens, dat het Verenigd Koninkrijk in 1951 heeft geratificeerd. Het Verenigd Koninkrijk heeft in 1987 ook het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens van de Raad van Europa (Verdrag 108) geratificeerd ([10]).

(10) Bij de Human Rights Act 1998 worden de rechten van het Europees Verdrag voor de rechten van de mens opgenomen in het recht van het Verenigd Koninkrijk. De Human Rights Act verleent alle personen de grondrechten en fundamentele vrijheden van de artikelen 2 tot en met 12 en 14 van het Europees Verdrag voor de rechten van de mens, de artikelen 1, 2 en 3 van het eerste protocol en artikel 1 van het dertiende protocol bij dit verdrag, gelezen in samenhang met de artikelen 16, 17 en 18 van dat verdrag. Dit omvat het recht op eerbiediging van het privéleven en van het familie- en gezinsleven (en het recht op gegevensbescherming als onderdeel van dat recht) en het recht op een eerlijk proces ([11]). Overeenkomstig artikel 8 van dit verdrag is inmenging van een overheidsinstantie in het recht op privacy slechts toegestaan voor zover bij de wet bepaald en voor zover noodzakelijk in een democratische samenleving in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van ordeverstoring en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

(11) Krachtens de Human Rights Act 1998 moet elk optreden van overheidsinstanties verenigbaar zijn met de rechten van het verdrag ([12]). Daarnaast moet de primaire en afgeleide wetgeving op een wijze worden gelezen en uitgevoerd die verenigbaar is met de rechten van het verdrag ([13]).

2.2. **Het kader voor gegevensbescherming van het Verenigd Koninkrijk**

(12) Het Verenigd Koninkrijk heeft zich op 31 januari 2020 teruggetrokken uit de Europese Unie. Op basis van het Akkoord inzake de terugtrekking van het Verenigd Koninkrijk van Groot-Brittannië en Noord-Ierland uit de Europese Unie en de Europese Gemeenschap voor Atoomenergie ([14]) bleef het Unierecht tijdens de overgangsperiode tot 31 december 2020 van toepassing op en in het Verenigd Koninkrijk. Vóór de terugtrekking en tijdens de overgangsperiode bestond het wettelijk kader inzake de bescherming van de persoonsgegevens in het Verenigd Koninkrijk uit de desbetreffende EU-wetgeving (en met name Verordening (EU) 2016/679 en Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad ([15])) en interne wetgeving (en met name de Data Protection Act 2018 ([16]) (de Britse wet gegevensbescherming van 2018, hierna "DPA 2018" genoemd), waarin nationale regels waren vastgesteld, waar toegestaan op grond van Verordening (EU) 2016/679, om de toepassing van de regels van Verordening (EU) 2016/679 te specificeren en beperken, en waarbij Richtlijn (EU) 2016/680 werd omgezet.

([10]) De beginselen van Verdrag 108 werden in eerste instantie met de *Data Protection Act 1984* (de Britse wet gegevensbescherming van 1984, hierna "DPA 1984" genoemd), die werd vervangen door de DPA 1998 en vervolgens door de DPA 2018 (gelezen in samenhang met de AVG van het VK), omgezet in de wet van het Verenigd Koninkrijk. Het Verenigd Koninkrijk heeft in 2018 ook het Protocol tot wijziging van het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (ook wel Verdrag 108+) ondertekend en werkt momenteel aan de ratificering van het verdrag.

([11]) Artikelen 6 en 8 EVRM (zie ook bijlage 1 bij de Human Rights Act 1998).

([12]) Artikel 6 van de Human Rights Act 1998.

([13]) Artikel 3 van de Human Rights Act 1998.

([14]) Akkoord inzake de terugtrekking van het Verenigd Koninkrijk van Groot-Brittannië en Noord-Ierland uit de Europese Unie en de Europese Gemeenschap voor Atoomenergie 2019/C 384 I/01, XT/21054/2019/INIT, (PB C 384I van 12.11.2019, blz. 1), beschikbaar op: https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:12019W/TXT(02)

([15]) Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de uitvoering van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad (PB L 119 van 4.5.2016, blz. 89), beschikbaar op: https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016L0680

([16]) Data Protection Act 2018, beschikbaar op: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

(13) Ter voorbereiding van de terugtrekking uit de Europese Unie heeft de regering van het Verenigd Koninkrijk de European Union (Withdrawal) Act 2018 ([17]) (de Britse wet inzake de terugtrekking uit de Europese Unie van 2018) aangenomen, waarbij rechtstreeks toepasselijke Uniewetgeving wordt opgenomen in het recht van het Verenigd Koninkrijk ([18]). Dit "gehandhaafde" Unierecht omvat Verordening (EU) 2016/679 in haar geheel (met inbegrip van de overwegingen hiervan) ([19]). Overeenkomstig deze wet moet het ongewijzigde, gehandhaafde Unierecht door de rechters van het Verenigd Koninkrijk worden uitgelegd in overeenstemming met de desbetreffende jurisprudentie van het Europees Hof van Justitie en de algemene beginselen van het Unierecht, zoals deze wetgeving direct vóór het einde van de overgangsperiode van kracht is (respectievelijk de "gehandhaafde jurisprudentie van de EU" en de "gehandhaafde algemene beginselen van het Unierecht") ([20]).

(14) Op grond van de European Union (Withdrawal) Act 2018 hebben de ministers van het Verenigd Koninkrijk de bevoegdheid om door middel van wettelijke instrumenten secundaire wetgeving in te voeren teneinde in gehandhaafd Unierecht de noodzakelijke wijzigingen aan te brengen die voortvloeien uit de terugtrekking van het Verenigd Koninkrijk uit de Europese Unie. Zij oefenden die bevoegdheid uit door de Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (de Britse regelingen betreffende gegevensbescherming, privacy en elektronische communicatie (wijzigingen enz.) (terugtrekking EU) van 2019, hierna "DPPEC Regulations" genoemd) ([21]) aan te nemen. Bij de DPPEC Regulations wordt Verordening (EU) 2016/679, zoals ingevoerd in het Britse recht bij de European Union (Withdrawal) Act 2018, de DPA 2018 en overige wetgeving inzake gegevensbescherming, gewijzigd om aan te sluiten op de binnenlandse context ([22]).

(15) Dienovereenkomstig bestaat het rechtskader inzake de bescherming van persoonsgegevens in het Verenigd Koninkrijk na het einde van de overgangsperiode uit:

— De UK GDPR, zoals opgenomen in het recht van het Verenigd Koninkrijk bij de European Union (Withdrawal) Act 2018 en gewijzigd bij de DPPEC Regulations ([23]); en

— de DPA 2018 ([24]), zoals gewijzigd bij de DPPEC Regulations.

(16) Omdat de UK GDPR gebaseerd is op EU-wetgeving, sluiten veel aspecten van de voorschriften inzake gegevensbescherming in het Verenigd Koninkrijk nauw aan op de overeenkomstige voorschriften die in de Europese Unie van toepassing zijn.

(17) Naast de bevoegdheden die bij de European Union (Withdrawal) Act 2018 aan de Secretary of State werden toegekend, verlenen verschillende bepalingen van de DPA 2018 bevoegdheden aan de Secretary of State om secundaire wetgeving vast te stellen om sommige bepalingen van de Act te wijzigen of te voorzien in aanvullende voorschriften ([25]). De Secretary of State heeft tot dusverre van de bevoegdheid op grond van artikel 137 van de

([17]) European Union Withdrawal Act 2018, beschikbaar op: https://www.legislation.gov.uk/ukpga/2018/16/contents

([18]) Het doel en het gevolg van de European Union (Withdrawal) Act 2018 was dat alle Uniewetgeving met rechtstreekse werking aan het einde van de overgangsperiode in het recht van het Verenigd Koninkrijk werd opgenomen zoals deze onmiddellijk vóór het einde van de overgangsperiode in het EU-recht gold, zie artikel 3 van de European Union (Withdrawal) Act 2018.

([19]) In de toelichting bij de European Union (Withdrawal) Act 2018 wordt gespecificeerd dat wanneer wetgeving in het kader van dit artikel wordt omgezet, de tekst van de wetgeving zelf deel zal uitmaken van de interne wetgeving. Dit zal de volledige tekst van een EU-instrument omvatten (met inbegrip van de overwegingen hiervan). (Toelichting bij de European Union (Withdrawal) Act 2018, punt 83, beschikbaar op: https://www.legislation.gov.uk/ukpga/2018/16/pdfs/ukpgaen_20180016_en.pdf). Volgens informatie die door de Britse autoriteiten is verstrekt, was het niet noodzakelijk om de overwegingen op dezelfde manier te wijzigen als de artikelen van Verordening (EU) 2016/679 werden gewijzigd bij de DPPEC Regulations (de Britse regelingen betreffende gegevensbescherming, privacy en elektronische communicatie, hierna "DPPEC Regulations" genoemd), omdat de overwegingen niet de status van bindende rechtsregels hebben.

([20]) Artikel 6 van de European Union (Withdrawal) Act 2018.

([21]) De Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019, beschikbaar op: https://www.legislation.gov.uk/uksi/2019/419/contents/made, zoals gewijzigd bij de DPPEC Regulations van 2020, beschikbaar op: https://www.legislation.gov.uk/ukdsi/2020/9780348213522

([22]) Deze wijzigingen van de *United Kingdom General Data Protection Regulation* (algemene verordening gegevensbescherming van het Verenigd Koninkrijk, hierna de "UK GDPR" genoemd) en de DPA 2018 zijn hoofdzakelijk van technische aard, zoals de schrapping van verwijzingen naar "de lidstaten" of de aanpassing van de terminologie (bv. het vervangen van verwijzingen naar Verordening (EU) 2016/679 door verwijzingen naar de UK GDPR). In sommige gevallen waren wijzigingen noodzakelijk om de zuiver binnenlandse context van de bepalingen te weerspiegelen, zoals met betrekking tot "de instellingen" die "adequaatheidsbepalingen" vaststellen met het oog op het wettelijke kader voor gegevensbescherming van het VK (zie artikel 17A van de DPA 2018), d.w.z. de Secretary of State in plaats van de Europese Commissie.

([23]) UK GDPR, bijlage Keeling, beschikbaar op: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946117/20201102_-_GDPR_-__MASTER__Keeling_Schedule__with_changes_highlighted__V3.pdf

([24]) DPA 2018, bijlage Keeling, beschikbaar op: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946100/20201102_-_DPA_-__MASTER__Keeling_Schedule__with_changes_highlighted__V3.pdf

([25]) Deze bevoegdheden zijn bijvoorbeeld opgenomen in de artikelen 16 (de bevoegdheid om, in specifieke, nauw afgebakende situaties, te voorzien in aanvullende vrijstellingen van de specifieke bepalingen van de UK GDPR), 17A (de bevoegdheid om adequaatheidsbepalingen vast te stellen), 212 en 213 (de bevoegdheid om wetgeving in gang te zetten en te voorzien in overgangsbepalingen) en 211 (de bevoegdheid om minimale en voortvloeiende wijzigingen aan te brengen) van de DPA 2018.

DPA 2018 slechts gebruikgemaakt om de Data Protection (Charges and Information) (Amendment) Regulations 2019 vast te stellen, de Britse regelingen gegevensbescherming (bijdragen en informatie) (wijziging) van 2019, waarin de omstandigheden uiteen worden gezet waarin verwerkingsverantwoordelijken een jaarlijkse bijdrage moeten betalen aan de onafhankelijke autoriteit voor gegevensbescherming van het Verenigd Koninkrijk, de Information Commissioner (de Britse toezichthouder voor informatie).

(18) Tot slot wordt in de praktijkcodes en andere richtsnoeren die zijn vastgesteld door de Information Commissioner voorzien in verdere richtsnoeren met betrekking tot de wetgeving inzake gegevensbescherming van het Verenigd Koninkrijk. Hoewel zij formeel niet juridisch bindend zijn, zijn deze richtsnoeren van belang voor de uitlegging en tonen zij aan hoe de wetgeving inzake gegevensbescherming van toepassing is en door de Commissioner in de praktijk wordt gehandhaafd. De artikelen 121 tot en met 125 van de DPA 2018 in het bijzonder leggen aan de Commissioner de verplichting op om praktijkcodes op te stellen met betrekking tot het delen van gegevens, direct marketing, ontwerpen en gegevensbescherming die zijn aangepast aan de leeftijd en journalistiek.

(19) Het Britse rechtskader dat van toepassing is op gegevens die in het kader van dit besluit worden doorgegeven, is wat de structuur en belangrijkste onderdelen ervan betreft dus in grote mate hetzelfde als het kader dat in de Europese Unie van toepassing is. Dit omvat het feit dat dit kader niet alleen is gebaseerd op verplichtingen die in het nationale recht zijn vastgesteld, die zijn gevormd door het Unierecht, maar ook op verplichtingen die zijn verankerd in het internationaal recht, met name doordat het Verenigd Koninkrijk partij is bij het EVRM en Verdrag 108 en is onderworpen aan de bevoegdheid van het Europees Hof voor de Rechten van de Mens. Deze verplichtingen die voortvloeien uit juridisch bindende internationale instrumenten, met name met betrekking tot de bescherming van persoonsgegevens, vormen derhalve een bijzonder belangrijk element van het rechtskader dat in dit besluit wordt beoordeeld.

2.3. **Materieel en territoriaal toepassingsgebied**

(20) Net zoals Verordening (EU) 2016/679 is de UK GDPR van toepassing op geheel of gedeeltelijk geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen ([26]). De definities van "persoonsgegevens", "betrokkene" en "verwerking" van de UK GDPR zijn identiek aan de definities van Verordening (EU) 2016/679 ([27]). De UK GDPR is daarnaast van toepassing op de handmatige, ongestructureerde verwerking van persoonsgegevens ([28]) die in het bezit zijn van bepaalde overheidsinstanties van het Verenigd Koninkrijk ([29]), hoewel de beginselen en rechten van de UK GDPR die niet relevant zijn voor dergelijke persoonsgegevens hierop op grond van de artikelen 24 en 25 van de DPA 2018 niet worden toegepast. De UK GDPR is, net zoals Verordening (EU) 2016/679, niet van toepassing op de verwerking van persoonsgegevens door een natuurlijke persoon bij de uitoefening van een zuiver persoonlijke of huishoudelijke activiteit ([30]).

(21) De UK GDPR is ook van toepassing op de verwerking in het kader van een activiteit die, onmiddellijk vóór het einde van de overgangsperiode, niet onder het toepassingsgebied van het Unierecht viel (bv. nationale veiligheid) ([31]) of die onder titel 5, hoofdstuk 2, van het Verdrag betreffende de Europese Unie (activiteiten in het kader van het gemeenschappelijk buitenlands en veiligheidsbeleid) viel ([32]). Net als het systeem van de Europese Unie is de UK GDPR niet van toepassing op de verwerking van persoonsgegevens door een bevoegde autoriteit met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de uitvoering van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid (zogeheten

([26]) Artikel 2, leden 1 en 5, van de UK GDPR.
([27]) Artikel 4, leden 1 en 2, van de UK GDPR.
([28]) De handmatige, ongestructureerde verwerking van persoonsgegevens wordt in artikel 2, lid 5, punt b), gedefinieerd als een verwerking van persoonsgegevens die niet bestaat in de geautomatiseerde of gestructureerde verwerking van persoonsgegevens.
([29]) In artikel 2, lid 1A, van de UK GDPR is bepaald dat de UK GDPR ook van toepassing is op de handmatige, ongestructureerde verwerking van persoonsgegevens die in het bezit zijn van een FOI-overheidsinstantie. FOI-overheidsinstanties zijn overheidsinstanties zoals gedefinieerd in de Freedom of Information Act 2000 (de Britse wet op de vrijheid van informatie van 2000) of Schotse overheidsinstanties zoals gedefinieerd in de Freedom of Information (Scotland) Act 2002 (asp 13) (de Schotse wet op de vrijheid van informatie van 2002). Artikel 21, lid 5, van de DPA 2018.
([30]) Artikel 2, lid 2, punt a), van de UK GDPR.
([31]) Activiteiten in verband met de nationale veiligheid vallen alleen onder het toepassingsgebied van de UK GDPR voor zover zij niet worden uitgevoerd door een bevoegde autoriteit voor rechtshandhavingsdoeleinden (in dit geval is artikel 3 van de DPA 2018 van toepassing) of door of in opdracht van een inlichtingendienst, wier activiteiten zijn uitgesloten van het toepassingsgebied van de UK GDPR en die overeenkomstig artikel 2, lid 2, punt c), van de UK GDPR vallen onder artikel 4 van de DPA 2018. De politie mag bijvoorbeeld veiligheidscontroles bij een werknemer uitvoeren om te waarborgen dat hij te vertrouwen is met materiaal inzake de nationale veiligheid. Ondanks het feit dat de politie een bevoegde autoriteit is voor rechtshandhavingsdoeleinden, vindt de verwerking in kwestie niet voor rechtshandhavingsdoeleinden plaats en is de UK GDPR hierop van toepassing. Zie het UK Explanatory Framework for Adequacy Discussions (het Britse toelichtingskader voor de adequaatheidsdiscussie), section H: National Security Data Protection and Investigatory Powers Framework, blz. 8, beschikbaar op https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf
([32]) Artikel 2, lid 1, punten a) en b), van de UK GDPR.

"rechtshandhavingsdoeleinden") (een dergelijke verwerking valt in plaats daarvan onder artikel 3 van de DPA 2018, zoals het geval is voor Richtlijn (EU) 2016/680 in het kader van het Unierecht) of de verwerking van persoonsgegevens door inlichtingendiensten (de Security Service, de Secret Intelligence Service en de Government Communications Headquarters), die onder artikel 4 van de DPA 2018 valt ([33]).

(22) Het territoriale toepassingsgebied van de UK GDPR wordt beschreven in artikel 3 van de UK GDPR ([34]) en omvat de verwerking van persoonsgegevens (ongeacht waar deze plaatsvindt) in het kader van de activiteiten van een vestiging van een verwerkingsverantwoordelijke of een verwerker in het Verenigd Koninkrijk, evenals de verwerking van persoonsgegevens van betrokkenen die zich in het Verenigd Koninkrijk bevinden wanneer de verwerking verband houdt met het aanbieden van goederen of diensten aan deze betrokkenen of het monitoren van hun gedrag ([35]). Hiermee wordt de benadering van artikel 3 van Verordening (EU) 2016/679 gevolgd.

2.4. **Definities van persoonsgegevens en de concepten van verwerkingsverantwoordelijke en verwerker**

(23) De definities van persoonsgegevens, verwerking, verwerkingsverantwoordelijke, verwerker en pseudonimisering, zoals vastgesteld in Verordening (EU) 2016/679, zijn zonder materiële wijzigingen gehandhaafd in de UK GDPR ([36]). Bovendien zijn in artikel 9, lid 1, van de UK GDPR bijzondere categorieën gegevens gedefinieerd, op dezelfde wijze als in Verordening (EU) 2016/679 ("persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid"). In artikel 205 van de DPA 2018 is voorzien in de definitie van "biometrische gegevens" ([37]), "gegevens over gezondheid" ([38]) en "genetische gegevens" ([39]).

2.5. **Waarborgen, rechten en verplichtingen**

2.5.1. *Rechtmatigheid en behoorlijkheid van de verwerking*

(24) Persoonsgegevens moeten op rechtmatige en behoorlijke wijze worden verwerkt.

(25) De beginselen van rechtmatigheid, behoorlijkheid en transparantie en de gronden voor de rechtmatige verwerking worden gewaarborgd in het recht van het Verenigd Koninkrijk door middel van artikel 5, lid 1, en artikel 6, lid 1, van de UK GDPR, die identiek zijn aan de respectievelijke bepalingen van Verordening (EU) 2016/679 ([40]). Artikel 6,

([33]) Artikel 2, lid 2, punten b) en c), van de UK GDPR.

([34]) Hetzelfde territoriale toepassingsgebied geldt voor de verwerking van persoonsgegevens in het kader van artikel 2 van de DPA 2018, die de UK GDPR aanvult (artikel 207, lid 1A).

([35]) Dit houdt met name in dat de DPA 2018 en derhalve dit besluit niet van toepassing zijn op direct van de Britse Kroon afhankelijke gebieden (Jersey, Guernsey en Man), noch op de Britse overzeese gebieden, zoals de Falklandeilanden en het territorium Gibraltar.

([36]) Artikel 4, leden 1, 2, 5, 7 en 8, van de UK GDPR.

([37]) "Biometrische gegevens": persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een persoon op grond waarvan eenduidige identificatie van die persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens.

([38]) "Gegevens over gezondheid": persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven.

([39]) "Genetische gegevens": persoonsgegevens die verband houden met de overgeërfde of verworven genetische kenmerken van een persoon die unieke informatie verschaffen over de fysiologie of de gezondheid van die persoon en die met name voortkomen uit een analyse van een biologisch monster van die persoon.

([40]) Op grond van artikel 6, lid 1, van de UK GDPR is de verwerking slechts rechtmatig indien en voor zover aan een van de onderstaande voorwaarden is voldaan: a) de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden; b) de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen; c) de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust; d) de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen; e) de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen; of f) de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

lid 1, punt e), wordt aangevuld door artikel 8 van de DPA 2018, waarin is bepaald dat de verwerking van persoonsgegevens op grond van artikel 6, lid 1, punt e), van de UK GDPR (noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen) de verwerking van persoonsgegevens omvat die noodzakelijk is voor de rechtsbedeling, de vervulling van een taak van een van de kamers van het parlement, de uitoefening van een functie die door middel van de uitvoering van het recht of een rechtsregel aan een persoon is toegekend, de uitoefening van een functie van de kroon, een minister van de kroon of een ministerie of een activiteit aan de hand waarvan de betrokkenheid bij de democratie wordt gesteund of bevorderd.

(26) Wat betreft toestemming (een van de gronden voor rechtmatige verwerking), zijn in de UK GDPR ook de voorwaarden van artikel 7 van Verordening (EU) 2016/679 ongewijzigd gehandhaafd, dat wil zeggen dat de verwerkingsverantwoordelijke moet kunnen aantonen dat de betrokkene toestemming heeft gegeven, dat een schriftelijke verklaring in duidelijke en eenvoudige taal moet worden gepresenteerd, dat de betrokkene het recht heeft zijn toestemming te allen tijde in te trekken en dat bij de beoordeling van de vraag of de toestemming vrijelijk kan worden gegeven rekening moet worden gehouden met de vraag of voor de uitvoering van de overeenkomst toestemming vereist is voor een verwerking van persoonsgegevens die niet noodzakelijk is voor de uitvoering van die overeenkomst. Op grond van artikel 8 van de UK GDPR is de toestemming van een kind met betrekking tot diensten van de informatiemaatschappij bovendien slechts rechtmatig wanneer het kind ten minste 13 jaar is. Dit valt binnen de leeftijdsgroep die in artikel 8 van Verordening (EU) 2016/679 is vastgesteld.

2.5.2. *Verwerking van bijzondere categorieën van persoonsgegevens*

(27) Wanneer "bijzondere categorieën" gegevens worden verwerkt, moet worden voorzien in bijzondere waarborgen.

(28) De UK GDPR en de DPA 2018 bevatten specifieke regels met betrekking tot de verwerking van bijzondere categorieën persoonsgegevens, die in artikel 9, lid 1, van de UK GDPR op dezelfde wijze uiteen zijn gezet als in Verordening (EU) 2016/679 (zie overweging (23)). Overeenkomstig artikel 9 van de UK GDPR is de verwerking van bijzondere categorieën gegevens in principe verboden, tenzij een specifieke uitzondering van toepassing is.

(29) Deze uitzonderingen (die zijn opgenomen in artikel 9, leden 2 en 3, van de UK GDPR) verschillen inhoudelijk niet van de uitzonderingen van artikel 9, leden 2 en 3, van Verordening (EU) 2016/679. Tenzij de betrokkene uitdrukkelijke toestemming heeft gegeven voor de verwerking van die persoonsgegevens, is de verwerking van bijzondere categorieën persoonsgegevens slechts toegestaan in specifieke en beperkte omstandigheden. In de meeste gevallen moet de verwerking van gevoelige gegevens noodzakelijk zijn voor een specifiek doel dat in de desbetreffende bepaling (zie artikel 9, lid 2, punten b), c), f), g), h), i) en j)) is gedefinieerd.

(30) Voor gevallen waarin een uitzondering uit hoofde van artikel 9, lid 2, van de UK GDPR wettelijke toestemming vereist of naar het algemeen belang verwijst, worden in artikel 10 van de DPA 2018 en in bijlage 1 bij de DPA 2018 de voorwaarden verder uiteengezet waaraan moet worden voldaan om de uitzonderingen te mogen toepassen. Voor de verwerking van gevoelige gegevens voor de bescherming van de "volksgezondheid" (artikel 9, lid 2, punt i), van de UK GDPR) wordt in bijlage 1, deel 1, punt 3, b), naast de uitvoering van een noodzakelijkheidstoets bijvoorbeeld vereist dat een dergelijke verwerking wordt uitgevoerd door of onder de verantwoordelijkheid van een gezondheidswerker of door een andere persoon die op grond van de uitvoering van het recht of een rechtsregel een geheimhoudingsplicht heeft, waaronder in het kader van de gevestigde geheimhoudingsplicht volgens het gewoonterecht.

(31) Voor gevallen waarin gevoelige gegevens worden verwerkt om redenen van zwaarwegend algemeen belang (artikel 9, lid 2, punt g), van de UK GDPR), is in bijlage 1, deel 2, van de DPA 2018 voorzien in een uitputtende lijst van doeleinden die als zwaarwegend algemeen belang kunnen worden beschouwd, evenals, voor elk van deze doeleinden, specifieke aanvullende voorwaarden. De bevordering van raciale en etnische diversiteit op leidinggevende niveaus van organisaties wordt bijvoorbeeld erkend als zwaarwegend algemeen belang. Voor de verwerking van gevoelige gegevens voor dit specifieke doel gelden gedetailleerde vereisten, waaronder dat de verwerking moet worden uitgevoerd als onderdeel van een proces van het identificeren van geschikte personen voor leidinggevende functies, noodzakelijk moet zijn voor de bevordering van de raciale en etnische diversiteit en geen waarschijnlijke aanzienlijke schade of aanzienlijke nood voor de betrokkene mag veroorzaken.

(32) In artikel 11, lid 1, van de DPA 2018 worden de voorwaarden uiteengezet voor de verwerking van persoonsgegevens in de in artikel 9, lid 3, van de UK GDPR omschreven omstandigheden in verband met de geheimhoudingsplicht. Dit omvat omstandigheden waarin de verwerking wordt uitgevoerd door of onder de verantwoordelijkheid van een gezondheidswerker of sociaal werker of door een andere persoon die op grond van de uitvoering van het recht of een rechtsregel in deze omstandigheden een geheimhoudingsplicht heeft.

(33) Daarnaast vereist de toepassing van veel van de in artikel 9, lid 2, van de UK GDPR opgenomen uitzonderingen passende en specifieke waarborgen. Afhankelijk van de aard van de verwerking en het niveau van risico voor de rechten en vrijheden van betrokkenen zijn in de voorwaarden voor de verwerking van bijlage 1 bij de DPA 2018 verschillende waarborgen vastgesteld. In bijlage 1 zijn vervolgens de voorwaarden voor elke verwerkingssituatie vastgesteld.

(34) Voor sommige gevallen is het soort gevoelige gegevens dat mag worden verwerkt om te voldoen aan een specifieke wettelijke basis, in de DPA 2018 geregeld en beperkt. In bijlage 1, punt 8, wordt bijvoorbeeld de verwerking van gevoelige gegevens voor de bevordering van gelijke kansen en een gelijke behandeling toegestaan. Deze voorwaarde voor de verwerking kan alleen worden gebruikt als uit de gegevens de raciale of etnische afkomst, religieuze of levensbeschouwelijke overtuiging of seksuele gerichtheid blijkt of als de gegevens gezondheidsgegevens zijn.

(35) Voor sommige gevallen beperkt de DPA 2018 het type verwerkingsverantwoordelijke dat gebruik mag maken van de voorwaarde voor verwerking. In bijlage 1, punt 23, wordt bijvoorbeeld de verwerking van gevoelige gegevens geregeld in verband met de antwoorden van gekozen vertegenwoordigers aan het publiek. Deze voorwaarde voor de verwerking kan alleen worden gebruikt als de verwerkingsverantwoordelijke een gekozen vertegenwoordiger is of onder het gezag van een gekozen vertegenwoordiger handelt.

(36) Voor sommige andere gevallen zijn in de DPA 2018 beperkingen vastgesteld voor de categorieën betrokkenen ten aanzien waarvan gebruik kan worden gemaakt van de voorwaarde voor de verwerking. In bijlage 1, punt 21, wordt bijvoorbeeld de verwerking van gevoelige gegevens voor bedrijfspensioenregelingen geregeld. Deze voorwaarde kan slechts worden gebruikt wanneer de betrokkene in kwestie een broer of zus, ouder, grootouder of overgrootouder van de deelnemer aan de regeling is.

(37) Daarnaast moet de verwerkingsverantwoordelijke, wanneer hij gebruikmaakt van de uitzonderingen van artikel 9, lid 2, van de UK GDPR, die verder uiteengezet worden in artikel 10 van de DPA 2018 en in bijlage 1 bij de DPA 2018, in de meeste gevallen een document inzake passend beleid opstellen. Hierin moeten de procedures van de verwerkingsverantwoordelijke voor het waarborgen van de naleving van de beginselen van artikel 5 van de UK GDPR worden gespecificeerd. Daarnaast moet het beleid voor het bewaren en wissen, met een indicatie van de waarschijnlijke opslagtermijn, uiteengezet worden. Verwerkingsverantwoordelijken moeten dit document waar passend herzien en bijwerken. De verwerkingsverantwoordelijke moet het beleidsdocument voor een periode van zes maanden na afronding van de verwerking bewaren en het op verzoek ter beschikking stellen van de Information Commissioner ([41]).

(38) Overeenkomstig punt 41 van bijlage 1 bij de DPA 2018 moet het beleidsdocument altijd vergezeld gaan van een aangevuld verwerkingsdossier. In dit dossier moeten de toezeggingen van het beleidsdocument, dat wil zeggen of gegevens worden gewist of bewaard in overeenstemming met het beleid, worden gevolgd. Wanneer het beleid niet is gevolgd, moeten de redenen hiervoor in het dossier worden opgenomen. In het dossier moet bovendien worden beschreven hoe bij de verwerking wordt voldaan aan artikel 6 van de UK GDPR (rechtmatigheid van de verwerking) en aan de specifieke voorwaarde van bijlage 1 bij de DPA 2018 waarvan gebruik wordt gemaakt.

(39) Tot slot voorziet de UK GDPR, net zoals Verordening (EU) 2016/679, in algemene waarborgen voor bepaalde verwerkingsactiviteiten voor bijzondere categorieën gegevens. Artikel 35 van de UK GDPR vereist dat een gegevensbeschermingseffectbeoordeling wordt uitgevoerd wanneer bijzondere categorieën gegevens op grote schaal worden verwerkt. Overeenkomstig artikel 37 van de UK GDPR moet een verwerkingsverantwoordelijke of verwerker een functionaris voor gegevensbescherming aanwijzen wanneer hij hoofdzakelijk belast is met de grootschalige verwerking van bijzondere categorieën gegevens.

(40) Wat persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten betreft, is artikel 10 van de UK GDPR identiek aan artikel 10 van Verordening (EU) 2016/679. In dit artikel is bepaald dat de verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten alleen is toegestaan onder toezicht van de overheid of indien de verwerking is toegestaan bij nationaal recht dat passende waarborgen voor de rechten en vrijheden van de betrokkenen biedt.

(41) Voor gevallen waarin de verwerking van gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten niet onder toezicht van een overheid plaatsvindt, is in artikel 10, lid 5, van de DPA 2018 bepaald dat een dergelijke verwerking slechts mag plaatsvinden voor de specifieke doeleinden/in de specifieke situaties die zijn uiteengezet in de delen 1, 2 en 3, van bijlage 1 bij de DPA 2018 en dat hiervoor specifieke vereisten gelden die voor elk van deze doeleinden/situaties zijn vastgesteld. Gegevens betreffende strafrechtelijke veroordelingen mogen bijvoorbeeld worden verwerkt door non-profitorganisaties, mits de verwerking plaatsvindt a) in het kader van hun gerechtvaardigde activiteiten door een stichting, vereniging of andere non-profitorganisatie met een politiek, filosofisch, religieus of vakbondsdoel en b) op voorwaarde dat i) de verwerking uitsluitend verband houdt met de leden of voormalige leden van de organisatie of met personen die regelmatig contact met de organisatie hebben in verband met haar doeleinden en ii) de persoonsgegevens niet zonder toestemming van de betrokkenen buiten die organisatie worden meegedeeld.

([41]) Paragrafen 38-40 van bijlage 1 bij de DPA 2018.

(42) Daarnaast zijn in deel 3 van bijlage 1 bij de DPA 2018 aanvullende omstandigheden vastgesteld waarin gegevens betreffende strafrechtelijke veroordelingen mogen worden gebruikt, die overeenkomen met de wettelijke gronden voor de verwerking van gevoelige gegevens van artikel 9, lid 2, van Verordening (EU) 2016/679 en de UK GDPR (bv. toestemming van de betrokkene, vitale belangen van een persoon indien de betrokkene fysiek of juridisch niet in staat is zijn toestemming te geven, wanneer de gegevens kennelijk reeds door de betrokkene openbaar zijn gemaakt, wanneer de verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering enz.).

2.5.3. *Doelbinding, juistheid, minimale gegevensverwerking, opslagbeperking en gegevensbeveiliging*

(43) Persoonsgegevens moeten worden verwerkt voor een specifiek doel en mogen vervolgens uitsluitend worden gebruikt voor doeleinden die niet onverenigbaar zijn met het doel van de verwerking.

(44) Dit beginsel is opgenomen in artikel 5, lid 1, punt b), van Verordening (EU) 2016/679 en is onveranderd gehandhaafd in artikel 5, lid 1, punt b), van de UK GDPR. De voorwaarden voor een verdere verenigbare verwerking overeenkomstig artikel 6, lid 4, van Verordening (EU) 2016/679 zijn ook zonder materiële wijzigingen overgenomen in artikel 6, lid 4, punten a) tot en met e), van de UK GDPR.

(45) De gegevens moeten bovendien juist zijn en zo nodig worden geactualiseerd. Ze moeten ook toereikend en ter zake dienend zijn en beperkt blijven tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt en mogen in principe niet langer worden bewaard dan noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt.

(46) Deze beginselen van minimale gegevensverwerking, juistheid en opslagbeperking zijn uiteengezet in artikel 5, lid 1, punten c) tot en met e), van Verordening (EU) 2016/679 en zijn ongewijzigd gehandhaafd in artikel 5, lid 1, punten c) tot en met e), van de UK GDPR.

(47) Persoonsgegevens moeten ook op een dusdanige manier worden verwerkt dat de beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. Daartoe moeten bedrijfsexploitanten passende technische of organisatorische maatregelen treffen om de persoonsgegevens te beschermen tegen mogelijke bedreigingen. Bij de beoordeling van die maatregelen moet rekening worden gehouden met de stand van de techniek en de ermee gemoeide kosten.

(48) De gegevensbeveiliging is verankerd in de Britse wet in de vorm van het beginsel van integriteit en vertrouwelijkheid in artikel 5, lid 1, punt f), van de UK GDPR en in artikel 32 van de UK GDPR inzake de beveiliging van de verwerking. Deze bepalingen zijn identiek aan de respectievelijke bepalingen van Verordening (EU) 2016/679. De UK GDPR vereist bovendien onder dezelfde voorwaarden als die van de artikelen 33 en 34 van Verordening (EU) 2016/679 dat melding wordt gemaakt van een inbreuk in verband met persoonsgegevens bij de toezichthoudende autoriteit (artikel 33 UK GDPR) en dat een inbreuk in verband met de persoonsgegevens wordt meegedeeld aan de betrokkene (artikel 34 UK GDPR).

2.5.4 *Transparantie*

(49) Betrokkenen moeten worden ingelicht over de belangrijkste kenmerken van de verwerking van hun persoonsgegevens.

(50) Dit wordt gewaarborgd door de artikelen 13 en 14 van de UK GDPR, waarin naast het algemene beginsel van transparantie regels zijn opgenomen inzake de informatie die aan de betrokkene moet worden verstrekt ([42]). De regels van de overeenkomstige artikelen van Verordening (EU) 2016/679 zijn in de UK GDPR niet in wezenlijke mate gewijzigd. Net zoals het geval is voor Verordening (EU) 2016/679, gelden voor de transparantievereisten van deze artikelen verschillende uitzonderingen, die zijn vastgesteld in de DPA 2018 (zie de overwegingen (55) tot en met (72)).

([42]) In artikel 13, lid 1, punt f), en artikel 14, lid 1, punt f), zijn de verwijzingen naar adequaatheidsbesluiten van de Commissie vervangen door verwijzingen naar het gelijkwaardige Britse instrument, d.w.z. adequaatheidsbepalingen uit hoofde van de DPA 2018. Daarnaast zijn de verwijzingen naar het Unierecht of het recht van de lidstaten in artikel 14, lid 5, punten c) en d), vervangen door een verwijzing naar het nationale recht (als voorbeelden van dergelijk nationaal recht dat onder artikel 14, lid 5, punt c), kan vallen, heeft het Verenigd Koninkrijk artikel 7 van de Scrap Metal Dealers Act 2013 (de Britse wet inzake handelaren van metaalschroot van 2013) genoemd, waarin is voorzien in regels voor het registreren van vergunningen voor metaalschroot, evenals deel 35 van de Companies Act 2006 (de Britse vennootschapswet van 2006), waarin regels zijn vastgesteld voor het ondernemingsregister. Voorbeelden van nationaal recht dat onder artikel 14, lid 5, punt d), kan vallen, zijn onder meer wetgeving waarin regels zijn vastgesteld met betrekking tot het beroepsgeheim of verplichtingen in arbeidsovereenkomsten of de geheimhoudingsplicht volgens het gewoonterecht (zoals persoonsgegevens die worden verwerkt door gezondheidswerkers, personeelsafdelingen, maatschappelijk werkers enz.).

2.5.5 *Individuele rechten*

(51) Betrokkenen moeten bepaalde rechten hebben die kunnen worden afgedwongen ten opzichte van de verwerkingsverantwoordelijke of de verwerker, en met name het recht op inzage van de gegevens, het recht om bezwaar te maken tegen de verwerking en het recht op rectificatie of wissing van de gegevens. Voor deze rechten kunnen tegelijkertijd beperkingen gelden, mits deze noodzakelijk en evenredig zijn met het oog op de bescherming van de openbare veiligheid of andere belangrijke doelstellingen van algemeen belang.

2.5.5.1. De materiële rechten

(52) De UK GDPR biedt personen dezelfde afdwingbare rechten als Verordening (EU) 2016/679. De bepalingen die personen deze rechten verlenen, zijn in de UK GDPR zonder wezenlijke wijzigingen gehandhaafd.

(53) De rechten omvatten het recht op inzage van de betrokkene (artikel 15 UK GDPR), het recht op rectificatie (artikel 16 UK GDPR), het recht op wissing (artikel 17 UK GDPR), het recht op beperking van de verwerking (artikel 18 UK GDPR), een kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens of verwerkingsbeperking (artikel 19 UK GDPR), het recht op overdraagbaarheid van gegevens (artikel 20 UK GDPR) en het recht van bezwaar (artikel 21 UK GDPR) ([43]). Het laatstgenoemde recht omvat ook het recht van een betrokkene om bezwaar te maken tegen de verwerking van persoonsgegevens voor direct marketing, waarin is voorzien in artikel 21, leden 2 en 3, van Verordening (EU) 2016/679. Op grond van artikel 122 van de DPA 2018 moet de Information Commissioner bovendien een praktijkcode (Code of Practice) opstellen in verband met activiteiten voor direct marketing in overeenstemming met de vereisten van de wetgeving inzake gegevensbescherming (en de Privacy and Electronic Communications (EC Directive) Regulations 2003 (de Britse regelingen betreffende privacy en elektronische communicatie (EG-richtlijn) van 2003)) en dergelijke andere richtsnoeren ter bevordering van goede praktijken op het gebied van direct marketing die de Commissioner passend acht. Het bureau van de Information Commissioner (ICO) werkt momenteel aan de code voor direct marketing ([44]).

(54) Het recht van betrokkenen om niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit waaraan voor hen rechtsgevolgen zijn verbonden of dat hen anderszins in aanmerkelijke mate treft, waarin is voorzien in artikel 22 AVG,, is ook zonder belangrijke wijzigingen overgenomen in de UK GDPR. Hieraan is echter een nieuw lid 3A toegevoegd dat aangeeft dat in artikel 14 van de DPA 2018 waarborgen zijn vastgesteld voor de rechten, vrijheden en legitieme belangen van betrokkenen voor gevallen waarin de verwerking plaatsvindt in het kader van artikel 22, lid 2, punt b), van de UK GDPR. Dit geldt slechts wanneer de basis voor een dergelijk besluit een machtiging of vereiste op grond van het Britse recht is en niet wanneer het besluit noodzakelijk is op grond van een overeenkomst of is genomen met uitdrukkelijke toestemming van de betrokkene. Wanneer artikel 14 van de DPA 2018 van toepassing is, moet de verwerkingsverantwoordelijke de betrokkene zo snel als redelijkerwijs mogelijk schriftelijk meedelen dat een uitsluitend op geautomatiseerde verwerking gebaseerd besluit is genomen. De betrokkene heeft het recht de verwerkingsverantwoordelijke te verzoeken om — binnen één maand na ontvangst van de kennisgeving — het besluit te heroverwegen of een nieuw besluit te nemen dat niet uitsluitend op geautomatiseerde verwerking is gebaseerd. De Secretary of State is bevoegd om aanvullende waarborgen met betrekking tot de geautomatiseerde besluitvorming vast te stellen. Van deze bevoegdheid is nog geen gebruik gemaakt.

2.5.5.2. Beperkingen van de individuele rechten en overige bepalingen

(55) De DPA 2018 voorziet in verschillende beperkingen van de individuele rechten die passen binnen het kader van artikel 23 van de UK GDPR. Binnen dit kader zijn geen beperkingen ingevoerd met betrekking tot het recht om bezwaar te maken tegen direct marketing, als bedoeld in artikel 21, leden 2 en 3, van de UK GDPR, of van het recht om niet te worden onderworpen aan geautomatiseerde besluitvorming, als bedoeld in artikel 22 van de UK GDPR.

(56) De beperkingen zijn uitvoerig beschreven in de bijlagen 2 tot en met 4 bij de DPA 2018. De Britse autoriteiten hebben uitgelegd dat zij hierbij worden geleid door twee beginselen: het beginsel van specificiteit (waarbij een granulaire benadering wordt toegepast en brede beperkingen worden opgesplitst in meerdere specifiekere bepalingen) en het beginsel van voorwaardelijkheid (elke bepaling wordt aangevuld met waarborgen in de vorm van beperkingen of voorwaarden om misbruik te voorkomen) ([45]).

([43]) In artikel 17, lid 1, punt e), en artikel 17, lid 3, punt b), zijn de verwijzingen naar het Unierecht en het recht van de lidstaten vervangen door een verwijzing naar nationaal recht (als voorbeelden van dergelijk nationaal recht in het kader van artikel 17, lid 1, punt e), heeft het Verenigd Koninkrijk de *Education (Pupil Information) (England) Regulations 2006* (de Britse regelingen betreffende onderwijs (leerlinginformatie) (Engeland) van 2006) genoemd, waarin wordt vereist dat de namen van de leerlingen worden gewist uit de schoolregisters nadat zij de school hebben verlaten en artikel 34F van de *Medical Act 1983* (de Britse wet op de geneeskunde van 1983), waarin de regels uiteengezet zijn inzake het wissen van namen uit het huisartsenregister en het specialistenregister.

([44]) Het ontwerp van de praktijkcode is beschikbaar op: https://ico.org.uk/media/about-the-ico/consultations/2616882/direct-marketing-code-draft-guidance.pdf

([45]) UK Explanatory Framework for Adequacy Discussions, section E: Restrictions, blz. 1, beschikbaar op: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf

(57) De in artikel 23, lid 1, van de UK GDPR beschreven beperkingen zijn ontworpen om ervoor te zorgen dat zij uitsluitend van toepassing zijn in gespecificeerde omstandigheden waarin dat in een democratische samenleving noodzakelijk en evenredig is voor het legitieme belang dat hiermee wordt nagestreefd. Bovendien kan een uitzondering op de regels inzake gegevensbescherming in overeenstemming met de vaste jurisprudentie betreffende de uitlegging van beperkingen, slechts worden toegepast in een specifiek geval wanneer dit noodzakelijk en evenredig is ([46]). De noodzakelijkheidstoets moet streng zijn en vereisen dat een aantasting van de rechten van betrokkenen evenredig is aan de ernst van de bedreiging van het algemeen belang. Deze oefening omvat derhalve een klassieke evenredigheidsanalyse ([47]).

(58) De doelen die met deze beperkingen worden nagestreefd komen overeen met de doelen die zijn opgenomen in artikel 23 van Verordening (EU) 2016/679, met uitzondering van de beperkingen voor de nationale veiligheid en defensie, die in plaats daarvan zijn geregeld in artikel 26 van de DPA 2018, maar waarvoor dezelfde vereisten van noodzakelijkheid en evenredigheid gelden (zie de overwegingen (63) tot en met (66)).

(59) Sommige van de beperkingen, bijvoorbeeld die in verband met het voorkomen of opsporen van strafbare feiten, het aanhouden of vervolgen van misdadigers en de beoordeling of inning van belastingen of heffingen ([48]), staan de beperking van alle individuele rechten en transparantieverplichtingen toe (met uitzondering van de rechten uit hoofde van artikel 21, lid 2, en artikel 22). De omvang van de andere beperkingen is beperkt tot transparantieverplichtingen en het recht op inzage, zoals de beperkingen in verband met het professioneel verschoningsrecht ([49]), het recht op vrijstelling van een verplichting om informatie te verstrekken die zou leiden tot zelfbeschuldiging ([50]) en ondernemingsfinanciering, en met name het voorkomen van handel met voorkennis ([51]). Enkele van de beperkingen staan een beperking van de verplichting van de verwerkingsverantwoordelijke toe om een inbreuk aan een betrokkene te melden en van de beginselen van doelbinding en de rechtmatigheid, behoorlijkheid en transparantie van de verwerking ([52]).

(60) Enkele van de beperkingen zijn automatisch "volledig" van toepassing op een bepaald soort verwerking van persoonsgegevens (de toepassing van de transparantieverplichtingen en individuele rechten wordt bijvoorbeeld uitgesloten wanneer de persoonsgegevens worden verwerkt om de geschiktheid van een persoon voor een rechterlijk ambt te beoordelen of wanneer persoonsgegevens worden verwerkt door een rechter, administratieve rechtbank of persoon die optreedt in een rechterlijke hoedanigheid).

(61) In de meeste gevallen is in het desbetreffende punt van bijlage 2 bij de DPA 2018 echter bepaald dat de beperking slechts van toepassing is wanneer (en in die mate dat) de toepassing van de bepalingen het legitieme belang dat met die beperking wordt nagestreefd waarschijnlijk zal aantasten: de genoemde bepalingen van de UK GDPR zijn bijvoorbeeld niet van toepassing op persoonsgegevens die worden verwerkt met het oog op het voorkomen of opsporen van strafbare feiten, het aanhouden of vervolgen van misdadigers of de beoordeling of inning van belasting of heffingen voor zover de toepassing van die bepalingen waarschijnlijk nadelig zal zijn voor enige van deze zaken ([53]).

(62) De norm "waarschijnlijk nadelig zal zijn" is door de Britse rechter consequent uitgelegd als "een zeer aanzienlijke en zwaarwegende kans op aantasting van de vastgestelde algemene belangen" ([54]). Een aan de nadeligheidstoets onderhevige beperking kan derhalve alleen worden ingeroepen indien en voor zover er geen zeer aanzienlijke en zwaarwegende kans is dat de toekenning van een bepaald recht nadelig zou zijn voor het algemene belang in kwestie. De verwerkingsverantwoordelijke is verantwoordelijk voor de beoordeling per geval van de vraag of aan deze voorwaarden is voldaan ([55]).

(63) Naast de beperkingen die zijn opgenomen in bijlage 2 bij de DPA 2018, is in artikel 26 van de DPA 2018 een uitzondering opgenomen die op sommige bepalingen van de UK GDPR en de DPA 2018 kan worden toegepast indien deze uitzondering nodig is voor de waarborging van de nationale veiligheid of om redenen van defensie.

([46]) *Open Rights Group & Anor, R (On the Application Of)/Secretary of State for the Home Department & Anor* [2019] EWHC 2562 (Admin), punten 40 en 41.
([47]) *Guriev/Community Safety Development (United Kingdom) Ltd* [2016] EWHC 643 (QB), punt 43. Zie in dit verband ook Lin/Commissioner of Police for the Metropolis [2015] EWHC 2484 (QB), punt 80.
([48]) Paragraaf 2 van bijlage 2 bij de DPA 2018.
([49]) Paragraaf 19 van bijlage 2 bij de DPA 2018.
([50]) Paragraaf 20 van bijlage 2 bij de DPA 2018.
([51]) Paragraaf 21 van bijlage 2 bij de DPA 2018.
([52]) Beperkingen op het recht op melding van een inbreuk in verband met de gegevens zijn bijvoorbeeld alleen toegestaan in verband met strafbare feiten en belastingheffing (paragraaf 2 van bijlage 2 bij de DPA 2018), parlementaire voorrechten (paragraaf 13 van bijlage 2 bij de DPA 2018) en de verwerking voor journalistieke, academische, artistieke en literaire doeleinden (paragraaf 26 van bijlage 2 bij de DPA 2018).
([53]) Paragraaf 2 van bijlage 2 bij de DPA 2018.
([54]) *R (Lord)/Secretary of State for the Home Department* [2003] EWHC 2073 (Admin), punt 100, en *Guriev/Community Safety Development (United Kingdom) Ltd* [2016] EWHC 643 (QB), punt 43.
([55]) *Open Rights Group & Anor, R (On the Application Of)/Secretary of State for the Home Department & Anor,* punt 31.

Deze uitzondering is van toepassing op de beginselen van gegevensbescherming (met uitzondering van het beginsel van rechtmatigheid), de transparantieverplichtingen, de rechten van betrokkenen, de verplichting om een gegevensinbreuk te melden, regels inzake internationale doorgiften, enkele van de taken en bevoegdheden van de Information Commissioner en de regels inzake rechtsmiddelen, aansprakelijkheid en sancties, met uitzondering van de bepaling inzake de algemene voorwaarden voor het opleggen van administratieve geldboeten, zoals uiteengezet in artikel 83 van de UK GDPR, en de bepaling inzake sancties van artikel 84 van de UK GDPR. In artikel 28 van de DPA 2018 is bovendien de toepassing van artikel 9, lid 1, gewijzigd om de verwerking van bijzondere categorieën gegevens in artikel 9, lid 1, van de UK GDPR mogelijk te maken voor zover de verwerking wordt verricht om de nationale veiligheid te beschermen of voor defensiedoeleinden en met passende waarborgen voor de rechten en vrijheden van betrokkenen ([56]).

(64) De uitzondering kan slechts worden toegepast in de mate die noodzakelijk is om de nationale veiligheid of defensie te waarborgen. Zoals ook het geval is voor de andere uitzonderingen waarin in de DPA 2018 is voorzien, moet deze per geval door de verwerkingsverantwoordelijke worden overwogen en gebruikt. Een toepassing van de uitzondering moet bovendien in overeenstemming zijn met de mensenrechtennormen (geschraagd door de Human Rights Act 1998), volgens welke elke aantasting van het recht op privacy in een democratische samenleving noodzakelijk en evenredig moet zijn ([57]).

(65) Deze interpretatie van de uitzondering wordt bevestigd door de Information Commissioner, die gedetailleerde richtsnoeren heeft uitgegeven over de toepassing van de uitzondering inzake de nationale veiligheid en defensie, waarbij hij duidelijk heeft gemaakt dat de uitzondering per geval door de verwerkingsverantwoordelijke moet worden overwogen en toegepast ([58]). In de richtsnoeren wordt met name benadrukt dat „[d]it geen algemene vrijstelling is" en dat het, om hem in te roepen, "niet voldoende is dat de gegevens met het oog op de nationale veiligheid worden verwerkt". Daarentegen moet de verwerkingsverantwoordelijke die er gebruik van maakt "aantonen dat er een een reële kans van een nadelig effect op de nationale veiligheid bestaat" en wordt, indien nodig, van de verwerkingsverantwoordelijke verwacht dat hij „[de Information Commissioner] bewijs verstrekt over de reden waarom [hij] deze uitzondering heeft gebruikt". De richtsnoeren bevatten een controlelijst en een reeks voorbeelden om de voorwaarden onder welke deze uitzondering kan worden ingeroepen verder te verduidelijken.

(66) Het feit dat de gegevens worden verwerkt met het oog op de nationale veiligheid of defensie is op zich dus geen toereikende reden voor de toepassing van de uitzondering. Een verwerkingsverantwoordelijke moet de daadwerkelijke gevolgen voor de nationale veiligheid van de naleving van de specifieke bepaling inzake gegevensbescherming in aanmerking nemen. De uitzondering mag slechts worden toegepast voor die specifieke bepalingen waarvan is vastgesteld dat zij het risico veroorzaken en moet zo beperkt mogelijk worden toegepast ([59]).

(67) Deze benadering is bevestigd door het Information Tribunal ([60]) (de Britse administratieve rechtbank voor informatie). In de zaak Baker/Secretary of State for the Home Department (hierna: "Baker/Secretary of State" genoemd) oordeelde het Information Tribunal dat het onrechtmatig was om de uitzondering voor de nationale veiligheid als algemene uitzondering toe te passen op verzoeken om inzage die door de inlichtingendiensten werden ontvangen. De uitzondering moest in plaats daarvan per geval worden toegepast, door elk verzoek op zich te bekijken en het recht van personen op de eerbiediging van hun privéleven in overweging te nemen ([61]).

([56]) Volgens de informatie die de Britse autoriteiten hebben verstrekt, passen verwerkingsverantwoordelijken normaal gesproken versterkte waarborgen en beveiligingsmaatregelen toe bij de verwerking wanneer deze in het kader van de nationale veiligheid plaatsvindt, die aansluiten op de gevoelige aard van de verwerking. Welke waarborgen passend zijn, is afhankelijk van de risico's die de verwerking met zich meebrengt. Dit kan beperkingen van de inzage in de gegevens omvatten, zodat alleen geautoriseerde personen met passende veiligheidsmachtiging erin inzage krijgen, strenge beperkingen op het delen van de gegevens en de strenge beveiligingsnorm die wordt toegepast op de opslag- en behandelingsprocedures.

([57]) Zie ook *Guriev/Community Safety Development (United Kingdom) Ltd* [2016] EWHC 643 (QB), punt 45; Lin/Commissioner of the Police for the Metropolis [2015] EWHC 2484 (QB), punt 80.

([58]) Zie de richtsnoeren van de Information Commissioner over de uitzondering inzake de nationale veiligheid en defensie, beschikbaar op https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/national-security-and-defence/

([59]) Volgens een voorbeeld van de Britse autoriteiten zou het bij lopende onderzoeken door MI5, wanneer een persoon die verdacht wordt van terrorisme een verzoek om inzage indient bij het ministerie van Binnenlandse Zaken (bijvoorbeeld omdat hij een geschil heeft met het ministerie van Binnenlandse Zaken met betrekking tot immigratiekwesties), noodzakelijk zijn om te voorkomen dat de betrokkene op de hoogte wordt gesteld van het eventuele delen van gegevens door MI5 met het ministerie van Binnenlandse Zaken in verband met lopende onderzoeken, wat nadelig zou kunnen zijn voor gevoelige bronnen, methoden of technieken en/of kunnen leiden tot een verhoging van de dreiging die uitgaat van de persoon. In dergelijke omstandigheden is het waarschijnlijk dat zou zijn voldaan aan de drempel voor de toepassing van de uitzondering van artikel 26 en dat een uitzondering op het verstrekken van de informatie noodzakelijk zou zijn om de nationale veiligheid te waarborgen. Wanneer het ministerie van Binnenlandse Zaken echter ook beschikt over gegevens over de persoon die geen verband houden met het onderzoek van MI5 en die informatie zou kunnen worden verstrekt zonder dat de nationale veiligheid in gevaar komt, zou de uitzondering voor de nationale veiligheid niet van toepassing zijn wanneer de verstrekking van informatie aan de persoon wordt overwogen. De Information Commissioner stelt momenteel richtsnoeren op voor de wijze waarop verwerkingsverantwoordelijken het gebruik van de uitzondering van artikel 26 moeten benaderen. De richtsnoeren zullen naar verwachting eind maart 2021 worden gepubliceerd.

([60]) Het Information Tribunal werd opgericht om beroepen inzake de gegevensbescherming in het kader van de Data Protection Act 1984 te behandelen. In 2010 werd het Information Tribunal onderdeel van de General Regulatory Chamber (de algemene kamer voor regelgeving) van het First Tier Tribunal (de Britse administratieve rechtbank van eerste aanleg), in het kader van de hervorming van de structuur van het Britse stelsel van administratieve rechtbanken.

([61]) Zie Baker/Secretary of State for the Home Department [2001] UKIT NSA2 (hierna: "Baker/Secretary of State" genoemd).

2.5.6 *Beperkingen inzake persoonsgegevens die worden verwerkt voor journalistieke, artistieke, academische en literaire doeleinden, evenals voor archivering en onderzoek*

(68) Artikel 85, lid 2, van de UK GDPR staat toe dat voor persoonsgegevens die worden verwerkt voor journalistieke, artistieke, academische en literaire doeleinden, wordt voorzien in een uitzondering op verschillende bepalingen van de UK GDPR. In deel 5 van bijlage 2 bij de DPA 2018 zijn de uitzonderingen met betrekking tot verwerking voor deze doeleinden uiteengezet. Er wordt voorzien in uitzonderingen op de beginselen van de gegevensbescherming (met uitzondering van het beginsel van integriteit en vertrouwelijkheid), de wettelijke gronden voor de verwerking (met inbegrip van bijzondere categorieën gegevens en gegevens betreffende strafrechtelijke veroordelingen enz.), de voorwaarden voor toestemming, de transparantieverplichtingen, de rechten van betrokkenen, de verplichting om inbreuken op gegevens te melden, en de vereiste om de Information Commissioner te raadplegen voorafgaande aan een verwerking met een hoog risico en de regels inzake internationale doorgiften ([62]). De UK GDPR wijkt in dit opzicht niet in wezenlijke mate af van Verordening (EU) 2016/679, waarin in artikel 85 ook is voorzien in de mogelijkheid om met het oog op de verwerking voor journalistieke doeleinden of ten behoeve van academische, artistieke of literaire uitdrukkingsvormen uitzonderingen vast te stellen op een aantal vereisten van Verordening (EU) 2016/679. De bepalingen van de DPA 2018, en met name van bijlage 2, deel 5, zijn verenigbaar met de UK GDPR.

(69) De kernafweging die in het kader van artikel 85 van de UK GDPR moet worden gemaakt, houdt verband met de vraag of een uitzondering op de regels betreffende gegevensbescherming als genoemd in overweging (68) noodzakelijk is om het recht op de bescherming van de persoonsgegevens te verenigen met de vrijheid van meningsuiting en informatie ([63]). Volgens bijlage 2, paragraaf 26, punten 2 en 3, bij de DPA 2018 past het Verenigd Koninkrijk een toets van "redelijke overtuiging" toe om deze afweging te maken. Een uitzondering is gerechtvaardigd wanneer de verwerkingsverantwoordelijke er redelijkerwijs van overtuigd is dat i) de bekendmaking in het algemeen belang is; en ii) de toepassing van de desbetreffende GDPR-bepaling onverenigbaar zou zijn met de journalistieke, academische, artistieke of literaire doeleinden. Zoals bevestigd in de jurisprudentie ([64]) heeft de toets van redelijke overtuiging zowel een subjectieve als een objectieve component: het is niet toereikend wanneer de verwerkingsverantwoordelijke aantoont dat hij zelf van mening was dat de naleving onverenigbaar was. Zijn overtuiging moet redelijk zijn, dat wil zeggen moet kunnen worden gedeeld door een redelijke persoon die op de hoogte is van de desbetreffende feiten. De verwerkingsverantwoordelijke moet zijn overtuiging derhalve zorgvuldig onderbouwen teneinde de redelijkheid ervan te kunnen aantonen. Volgens de uitleg die door de Britse autoriteiten is verstrekt, moet de toets van redelijke overtuiging bij elke uitzondering worden uitgevoerd ([65]). Wanneer aan de voorwaarden is voldaan, wordt de uitzondering noodzakelijk en evenredig geacht uit hoofde van de Britse wetgeving.

(70) De Information Commissioner moet overeenkomstig artikel 124 van de DPA 2018 een praktijkcode opstellen inzake gegevensbescherming en journalistiek. Hieraan wordt momenteel gewerkt. In het kader van de Data Protection Act 1998 zijn richtsnoeren gegeven over de kwestie, waarin met name wordt benadrukt dat het voor het gebruik van deze uitzondering niet voldoende is om slechts te verklaren dat de naleving journalistieke activiteiten zou belemmeren, maar er een duidelijk argument moet zijn dat de bepaling in

([62]) Zie artikel 85 van de UK GDPR en bijlage 2, deel 5, paragraaf 26, punt 9, bij de DPA 2018.

([63]) Overeenkomstig bijlage 2, deel 5, paragraaf 26, punt 2, bij de DPA 2018 is de uitzondering van toepassing op de verwerking van persoonsgegevens voor bijzondere doeleinden (journalistieke, academische, artistieke en literaire doeleinden) wanneer de verwerking plaatsvindt met het oog op de publicatie door een persoon van journalistiek, academisch, artistiek of literair materiaal en de verwerkingsverantwoordelijke redelijkerwijs van mening is dat de publicatie van dat materiaal in het algemeen belang zou zijn. Om te bepalen of een publicatie in het algemeen belang zou zijn, moet de verwerkingsverantwoordelijke rekening houden met het speciale algemene belang bij de vrijheid van meningsuiting en informatie. De verwerkingsverantwoordelijke moet bovendien praktijkcodes of richtsnoeren in aanmerking nemen die relevant zijn voor de publicatie in kwestie (de redactionele richtsnoeren van de BBC, de Ofcom Broadcasting Code en de praktijkcode van redacteuren). Om een uitzondering toe te passen, moet de verwerkingsverantwoordelijke daarnaast redelijkerwijs van mening zijn dat de naleving van de desbetreffende bepaling onverenigbaar zou zijn met de bijzondere doeleinden (punt 26(3) van bijlage 2 bij de DPA 2018).

([64]) In het arrest in NT1/Google [2018] EWHC 799 (QB), punt 102, werd de vraag besproken of de verwerkingsverantwoordelijke er redelijkerwijs van overtuigd was dat de publicatie in het algemeen belang was en dat de naleving van de desbetreffende bepalingen onverenigbaar was met de bijzondere doeleinden. De rechter merkte op dat artikel 32, lid 1, punten b) en c), van de Data Protection Act 1998 een subjectief en een objectief element had: de verwerkingsverantwoordelijke moest aantonen dat hij de overtuiging had dat de publicatie in het algemeen belang zou zijn en dat deze overtuiging objectief gezien redelijk was; hij moest daarnaast de subjectieve overtuiging hebben dat de naleving van de bepaling waarop de uitzondering zou worden toegepast, onverenigbaar zou zijn met de bijzondere doeleinden in kwestie.

([65]) Een voorbeeld van de toepassing van de toets van redelijke overtuiging is opgenomen in het besluit van het ICO om een sanctie op te leggen aan *True Visions Productions*, dat in het kader van de Data Protection Act 1998 werd genomen. De Information Commissioner aanvaardde dat de verwerkingsverantwoordelijke voor de media de subjectieve overtuiging had dat de naleving van het eerste beginsel betreffende gegevensbescherming (behoorlijkheid en rechtmatigheid) onverenigbaar was met journalistieke doeleinden. De Information Commissioner was echter van mening dat deze overtuiging objectief gezien niet redelijk was. Het besluit van de Information Commissioner is beschikbaar op: https://ico.org.uk/media/action-weve-taken/mpns/2614746/true-visions-productions-20190408.pdf

kwestie een obstakel vormt voor verantwoorde journalistiek ([66]). De regelgevende instantie voor telecommunicatie van het Verenigd Koninkrijk, OFCOM, en de BBC (in haar redactionele leidraad) hebben ook richtsnoeren gepubliceerd voor de uitvoering van de toets van het algemeen belang en de afweging van het algemeen belang tegen het belang van een persoon bij privacy ([67]). In deze richtsnoeren worden met name voorbeelden van informatie gegeven die in het algemeen belang is en wordt de noodzaak uitgelegd om te kunnen aantonen dat het algemeen belang in de specifieke omstandigheden van het geval zwaarder weegt dan het recht op privacy.

(71) Net zoals in artikel 89 AVG is bepaald, kan de verwerking van persoonsgegevens met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden vrijgesteld van een aantal genoemde bepalingen van de UK GDPR ([68]). Wat onderzoek en statistiek betreft, zijn uitzonderingen op de UK GDPR mogelijk in verband met de bevestiging van de verwerking, en de inzage in gegevens en waarborgen voor doorgiften aan derde landen; het recht op rectificatie; de beperking van de verwerking en het maken van bezwaar tegen de verwerking. Wat de archivering in het algemeen belang betreft, zijn ook uitzonderingen mogelijk op de kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens of beperking van de verwerking en op het recht op overdraagbaarheid van gegevens.

(72) Overeenkomstig punt 27(1) en punt 28(1) van bijlage 2 bij de DPA 2018 zijn de uitzonderingen op de genoemde bepalingen van de UK GDPR mogelijk wanneer de toepassing van de bepalingen het behalen van de doeleinden in kwestie zou verhinderen of ernstig zou schaden ([69]).

(73) Gezien het belang daarvan voor een doeltreffende uitoefening van individuele rechten, worden relevante ontwikkelingen met betrekking tot de interpretatie en toepassing in de praktijk van de bovengenoemde uitzonderingen (naast die in verband met de instandhouding van een doeltreffende controle van de immigratie, zoals uitgelegd in overweging (6), met inbegrip van eventuele verdere ontwikkelingen in de jurisprudentie en in de richtsnoeren en handhavingsmaatregelen van de Information Commissioner, naar behoren in aanmerking genomen in de context van de voortdurende monitoring van dit besluit ([70]).

2.5.7 *Beperkingen ten aanzien van verdere doorgifte*

(74) Het beschermingsniveau dat wordt geboden aan persoonsgegevens die worden doorgegeven vanuit de Europese Unie naar verwerkingsverantwoordelijken of verwerkers in het Verenigd Koninkrijk mag niet worden ondermijnd door verdere doorgifte van dergelijke gegevens aan ontvangers in een derde land. Dergelijke "verdere doorgiften", die uit het oogpunt van de Britse verwerkingsverantwoordelijke of verwerker internationale doorgiften vanuit het Verenigd Koninkrijk vormen, mogen slechts worden toegestaan wanneer de verdere ontvanger buiten het Verenigd Koninkrijk zelf is onderworpen aan voorschriften die zorgen voor een beschermingsniveau dat vergelijkbaar is met het beschermingsniveau dat wordt gegarandeerd binnen de Britse rechtsorde. De toepassing van de regels van de UK GDPR en de DPA 2018 inzake internationale doorgiften van persoonsgegevens is derhalve een belangrijke factor om de continuïteit van de bescherming te waarborgen in gevallen waarin persoonsgegevens vanuit de Europese Unie naar het Verenigd Koninkrijk worden doorgegeven uit hoofde van dit besluit.

([66]) Volgens de richtsnoeren moeten organisaties kunnen uitleggen waarom de naleving van de desbetreffende bepaling van de Data Protection Act 1998 onverenigbaar is met de journalistieke doeleinden. Verwerkingsverantwoordelijken moeten met name het nadelige effect van de naleving op de journalistiek afwegen tegen het nadelige effect van de niet-naleving op de rechten van betrokkenen. Als journalisten hun redactionele doelen kunnen behalen op een wijze die in overeenstemming is met de standaardbepalingen van de DPA, moeten zij dit doen. Organisaties moeten hun gebruik van de beperking voor elke bepaling die zij niet hebben nageleefd, kunnen rechtvaardigen. "Data protection and journalism: a guide for the media", beschikbaar op: https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf

([67]) Voorbeelden van algemeen belang zijn onder andere het onthullen of opsporen van strafbare feiten, het beschermen van de volksgezondheid of openbare veiligheid, het onthullen van misleidende beweringen van personen of organisaties of het onthullen van onbekwaamheid die gevolgen heeft voor het publiek. Zie de richtsnoeren van OFCOM op: https://www.ofcom.org.uk/__data/assets/pdf_file/0017/132083/Broadcast-Code-Section-8.pdf en de redactionele richtsnoeren van de BBC op: https://www.bbc.com/editorialguidelines/guidelines/privacy

([68]) Zie artikel 89 van de UK GDPR en bijlage 2, deel 6, paragraaf 27, punt 2, en paragraaf 28, punt 2, bij de DPA 2018.

([69]) Dit is onder voorwaarde van de vereiste dat de persoonsgegevens worden verwerkt in overeenstemming met artikel 89, lid 1, van de UK GDPR, zoals aangevuld door artikel 19 van de DPA 2018.

([70]) Zie de overwegingen (281) tot en met (287).

(75) De regeling inzake internationale doorgiften van persoonsgegevens vanuit het Verenigd Koninkrijk is vervat in de artikelen 44 tot en met 49 van de UK GDPR, aangevuld door de DPA 2018, en is in wezen identiek aan de voorschriften van hoofdstuk V van Verordening (EU) 2016/679 ([71]). Doorgiften van persoonsgegevens aan een derde land of internationale organisatie mogen slechts plaatsvinden op basis van een adequaatheidsbepaling (de Britse versie van een adequaatheidsbesluit in het kader van Verordening (EU) 2016/679), of, bij het ontbreken van een adequaatheidsbepaling,, wanneer de verwerkingsverantwoordelijke of verwerker heeft voorzien in passende waarborgen in overeenstemming met artikel 46 van de UK GDPR. Indien adequaatheidsbepalingen of passende waarborgen ontbreken, kan een doorgifte slechts plaatsvinden op basis van afwijkingen zoals vastgesteld in artikel 49 van de UK GDPR.

(76) In de adequaatheidsbepalingen van de Secretary of State kan worden bepaald dat een derde land (of een gebied of sector in een derde land), een internationale organisatie, of een beschrijving ([72]) van een dergelijk land of gebied of dergelijke sector of organisatie een toereikend niveau van bescherming van persoonsgegevens waarborgt. Bij de beoordeling van de adequaatheid van het beschermingsniveau moet de Secretary of State rekening houden met precies dezelfde elementen als die welke de Commissie moet beoordelen uit hoofde van artikel 45, lid 2, punten a) tot en met c), van Verordening (EU) 2016/679, uitgelegd in combinatie met overweging 104 van Verordening (EU) 2016/679 en de gehandhaafde jurisprudentie van de EU. Dit betekent dat de relevante norm bij de beoordeling van het adequate beschermingsniveau van een derde land de vraag is of dat derde land in kwestie een niveau van bescherming waarborgt dat "in feite overeenkomend" is met het niveau dat in het Verenigd Koninkrijk wordt verzekerd.

(77) Wat de procedure betreft, vallen adequaatheidsbepalingen onder de "algemene" procedurele vereisten van artikel 182 van de DPA 2018. In het kader van deze procedure moet de Secretary of State de Information Commissioner raadplegen wanneer hij voorstelt om Britse adequaatheidsbepalingen vast te stellen ([73]). Zodra deze bepalingen zijn vastgesteld door de Secretary of State, worden zij voorgelegd aan het parlement volgens de zogeheten negative resolution procedure, waarbij beide kamers van het parlement de bepalingen kunnen bestuderen en binnen veertig dagen een motie kunnen aannemen om de bepalingen nietig te verklaren ([74]).

(78) Volgens artikel 17B, lid 1, van de DPA 2018 moeten de adequaatheidsbepalingen met tussenpozen van maximaal vier jaar worden herzien en moet de Secretary of State doorlopend toezicht houden op ontwikkelingen in derde landen en binnen internationale organisaties die mogelijk gevolgen hebben voor besluiten om adequaatheidsbepalingen op te stellen, te wijzigen of in te trekken. Wanneer de Secretary of State vaststelt dat een bepaald land of een bepaalde organisatie niet langer een passend niveau van bescherming van persoonsgegevens waarborgt, moet hij, voor zover noodzakelijk, de bepalingen wijzigen of intrekken en in overleg gaan met het betrokken derde land of de betrokken internationale organisatie om het gebrek aan een passend beschermingsniveau te verhelpen. Deze procedurele aspecten weerspiegelen ook de dienovereenkomstige vereisten van Verordening (EU) 2016/679.

([71]) Met uitzondering van artikel 48 van Verordening (EU) 2016/679, dat het Verenigd Koninkrijk niet heeft overgenomen in de UK GDPR. In dat opzicht moet er allereerst op worden gewezen dat de norm die moet worden beschouwd als een norm die een adequaat beschermingsniveau biedt een norm is waarvan het niveau "in feite overeenkomend" is in plaats van identiek, zoals uitgelegd door het Hof van Justitie (Schrems I, punten 73 en74) en erkend wordt door het EDPB (adequaatheidsreferentie, bladzijde 3). Zoals door het EDPB wordt uitgelegd in zijn adequaatheidsreferentie, is het doel derhalve niet om "de Europese wetgeving punt voor punt te weerspiegelen, maar om de essentiële — belangrijkste vereisten van die wetgeving vast te stellen". In dat opzicht is het belangrijk om erop te wijzen dat, hoewel de Britse rechtsorde formeel gezien geen aan artikel 48 identieke bepaling bevat, hetzelfde effect wordt gewaarborgd door andere wettelijke bepalingen en beginselen, d.w.z. dat naar aanleiding van een verzoek om persoonsgegevens van een rechterlijke instantie of administratieve autoriteit in een derde land, persoonsgegevens alleen naar dat derde land kunnen worden doorgegeven indien er sprake is van een internationale overeenkomst — op basis waarvan de gerechtelijke uitspraak of het administratieve besluit in kwestie van het derde land wordt erkend of gehandhaafd in het Verenigd Koninkrijk — of indien die doorgifte is gebaseerd op een van de doorgiftemechanismen van hoofdstuk V van de UK GDPR. Om een buitenlands arrest uit te voeren, moeten rechters in het Verenigd Koninkrijk meer specifiek kunnen verwijzen naar gewoonterecht of geschreven recht dat de afdwingbaarheid hiervan mogelijk maakt. Noch in het gewoonterecht (zie Adams and Others v Cape Industries Plc., [1990] 2 W.L.R. 657), noch in het geschreven recht is echter voorzien in de uitvoering van buitenlandse arresten die de doorgifte van gegevens vereisen zonder dat sprake is van een internationale overeenkomst. Als gevolg hiervan zijn verzoeken om gegevens bij het ontbreken van een internationale overeenkomst niet afdwingbaar op grond van het Britse recht. Bovendien blijft de doorgifte van persoonsgegevens naar derde landen — ook op verzoek van een buitenlandse rechter of administratieve autoriteit — vallen onder de beperkingen van hoofdstuk V van de UK GDPR, die identiek zijn aan de overeenkomstige bepalingen van Verordening (EU) 2016/679 en derhalve vereisen om zich te baseren op een van de gronden voor doorgifte van hoofdstuk V in overeenstemming met de specifieke voorwaarden die uit hoofde van dat hoofdstuk op de doorgifte van toepassing zijn.

([72]) De Britse autoriteiten hebben uitgelegd dat de beschrijving van een land of internationale organisatie verwijst naar een situatie waarin het noodzakelijk zou zijn om een specifieke en gedeeltelijke bepaling van adequaatheid te verrichten met gerichte beperkingen (bijvoorbeeld adequaatheidsbepalingen in verband met uitsluitend bepaalde soorten doorgiften van gegevens).

([73]) Zie het memorandum van overeenstemming tussen de Secretary of State van het Ministerie van Digitale Zaken, Cultuur, Media en Sport en het bureau van de Information Commissioner over de rol van de Information Commissioner in verband met de nieuwe adequaatheidsbepalingen van het Verenigd Koninkrijk, beschikbaar op https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments

([74]) Wanneer dit gebeurt, hebben de bepalingen uiteindelijk geen verdere rechtsgevolgen meer.

(79) Zijn er geen adequaatheidsbepalingen vastgesteld, dan kunnen internationale doorgiften plaatsvinden wanneer de verwerkingsverantwoordelijke of verwerker heeft voorzien in passende waarborgen in overeenstemming met artikel 46 van de UK GDPR. Deze waarborgen zijn vergelijkbaar met de waarborgen van artikel 46 van Verordening (EU) 2016/679. Zij omvatten juridisch bindende en afdwingbare instrumenten tussen overheidsinstanties of -organen, bindende bedrijfsvoorschriften ([75]), standaardbepalingen inzake gegevensbescherming, goedgekeurde gedragscodes, goedgekeurde certificeringsmechanismen en, onder voorbehoud van toestemming van de Information Commissioner, contractbepalingen tussen verwerkingsverantwoordelijken (of verwerkers) of administratieve regelingen tussen overheidsinstanties. De regels zijn, wat de procedurele aspecten betreft, echter gewijzigd om ze aan te passen aan het kader van het Verenigd Koninkrijk: de standaardbepalingen inzake gegevensbescherming kunnen in overeenstemming met de DPA 2018 worden vastgesteld door de Secretary of State (artikel 17C) of de Information Commissioner (artikel 119A).

(80) Indien adequaatheidsbepalingen of passende waarborgen ontbreken, kan een doorgifte slechts plaatsvinden op basis van afwijkingen zoals vastgesteld in artikel 49 van de UK GDPR ([76]). De afwijkingen zijn in vergelijking met de regels van de desbetreffende artikelen van Verordening (EU) 2016/679 niet in wezenlijke mate gewijzigd in de UK GDPR. Op grond van de UK GDPR kunnen bepaalde afwijkingen, net zoals op grond van Verordening (EU) 2016/679, slechts worden gebruikt wanneer de doorgifte incidenteel is ([77]). Het ICO heeft in zijn richtsnoeren over internationale doorgiften bovendien verduidelijkt dat: deze afwijkingen alleen mogen worden gebruikt als echte uitzonderingen op de algemene regel dat een beperkte doorgifte niet dient te worden verricht, tenzij deze onder een adequaatheidsbesluit valt of in passende waarborgen is voorzien ([78]). Met betrekking tot doorgiften die wegens gewichtige redenen van algemeen belang (artikel 49, lid 1, punt d)) noodzakelijk zijn, kan de Secretary of State regelingen vaststellen om de omstandigheden te specificeren waarin een doorgifte van persoonsgegevens aan een derde land of internationale organisatie niet noodzakelijk is wegens gewichtige redenen van algemeen belang. De Secretary of State kan de doorgifte van een categorie persoonsgegevens aan een derde land of internationale organisatie bovendien door middel van een regeling beperken wanneer de doorgifte niet op basis van een adequaatheidsbepaling kan plaatsvinden en de Secretary of State van oordeel is dat de beperking noodzakelijk is wegens gewichtige redenen van algemeen belang. Dergelijke regelingen zijn tot nu toe niet vastgesteld.

(81) Dit kader voor internationale doorgiften is aan het einde van de overgangsperiode van toepassing geworden ([79]). In punt 4 van bijlage 21 bij de DPA van 2018 (ingevoerd bij de DPPEC Regulations) is echter bepaald dat bepaalde doorgiften van persoonsgegevens vanaf het einde van de overgangsperiode worden behandeld alsof zij zouden zijn gebaseerd op adequaatheidsbepalingen. Deze doorgiften omvatten doorgiften aan EER-landen, het territorium Gibraltar, een instelling, orgaan of instantie van de Unie, opgericht bij of krachtens het VEU, en derde landen die aan het einde van de overgangsperiode onder een adequaatheidsbesluit van de EU vielen. Doorgiften aan deze landen kunnen blijven plaatsvinden zoals vóór de terugtrekking van het Verenigd Koninkrijk uit de EU. Na de overgangsperiode moet de Secretary of State een evaluatie van deze adequaatheidsbevindingen uitvoeren gedurende een periode van vier jaar, dat wil zeggen vóór eind december 2024. Hoewel de Secretary of State vóór eind

([75]) In de UK GDPR zijn de regels van artikel 47 van Verordening (EU) 2016/679 overgenomen, waarbij slechts wijzigingen zijn aangebracht om ervoor te zorgen dat de regels in de binnenlandse context passen, bijvoorbeeld door de verwijzingen naar de bevoegde toezichthoudende autoriteit te vervangen door verwijzingen naar de Information Commissioner en de verwijzingen naar het coherentiemechanisme van lid 1 en het volledige lid 3 te schrappen.

([76]) Op grond van artikel 49 van de UK GDPR kunnen doorgiften slechts plaatsvinden mits aan één van de volgende voorwaarden is voldaan: a) de betrokkene heeft uitdrukkelijk met de voorgestelde doorgifte ingestemd, na te zijn ingelicht over de risico's die dergelijke doorgiften voor hem kunnen inhouden bij ontstentenis van een adequaatheidsbesluit en van passende waarborgen; b) de doorgifte is noodzakelijk voor de uitvoering van een overeenkomst tussen de betrokkene en de verwerkingsverantwoordelijke of voor de uitvoering van op verzoek van de betrokkene genomen precontractuele maatregelen; c) de doorgifte is noodzakelijk voor de sluiting of de uitvoering van een in het belang van de betrokkene tussen de verwerkingsverantwoordelijke en een andere natuurlijke persoon of rechtspersoon gesloten overeenkomst; d) de doorgifte is noodzakelijk wegens gewichtige redenen van algemeen belang; e) de doorgifte is noodzakelijk voor de instelling, uitoefening of onderbouwing van een rechtsvordering; f) de doorgifte is noodzakelijk voor de bescherming van de vitale belangen van de betrokkene of van andere personen, indien de betrokkene lichamelijk of juridisch niet in staat is zijn toestemming te geven; g) de doorgifte geschiedt vanuit een register dat krachtens het nationale recht is bedoeld om het publiek voor te lichten en dat door het publiek in het algemeen of door eenieder die zich op een rechtmatig belang kan beroepen, kan worden geraadpleegd, maar alleen voor zover in het gegeven geval aan de in het nationale recht neergelegde voorwaarden voor raadpleging wordt voldaan. Wanneer geen van de bovenstaande voorwaarden van toepassing is, mag een doorgifte bovendien alleen plaatsvinden mits deze niet repetitief is, een beperkt aantal betrokkenen betreft, noodzakelijk is voor dwingende gerechtvaardigde belangen van de verwerkingsverantwoordelijke die niet ondergeschikt zijn aan de belangen of rechten en vrijheden van de betrokkene, en de verwerkingsverantwoordelijke alle omstandigheden in verband met de gegevensdoorgifte heeft beoordeeld en op basis van die beoordeling passende waarborgen voor de bescherming van persoonsgegevens heeft geboden.

([77]) In overweging 111 van de UK GDPR is gespecificeerd dat doorgiften in verband met een overeenkomst of rechtsvordering alleen mogen plaatsvinden wanneer deze incidenteel zijn.

([78]) Richtsnoeren van de Information Commissioner inzake internationale doorgiften, beschikbaar op: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/#ib7

([79]) Gedurende een periode van ten hoogste zes maanden die uiterlijk op 30 juni 2021 eindigt, moet de toepasselijkheid van dit nieuwe kader worden beoordeeld in het licht van artikel 782 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 (PB L 444 van 31.12.2020, blz. 14) (hierna "de handels- en samenwerkingsovereenkomst EU-VK" genoemd), beschikbaar op: https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:22020A1231(01)

december 2024 een evaluatie moet uitvoeren, bevatten de overgangsbepalingen volgens de uitleg van de Britse autoriteiten geen beëindigingsbepaling en zal de geldigheid van de desbetreffende overgangsbepalingen niet eindigen wanneer er geen evaluatie is verricht vóór eind december 2024.

(82) Tot slot zal de Commissie met betrekking tot de toekomstige ontwikkeling van de Britse regeling inzake internationale doorgiften — door nieuwe adequaatheidsbepalingen aan te nemen, internationale overeenkomsten te sluiten of andere doorgiftemechanismen te ontwikkelen — de situatie van dichtbij volgen, beoordelen of de verschillende doorgiftemechanismen worden gebruikt op een manier die de continuïteit van de bescherming waarborgt, en, indien noodzakelijk, passende maatregelen nemen om mogelijke nadelige effecten op die continuïteit aan te pakken (zie de overwegingen (278) tot en met (287)). Aangezien de EU en het Verenigd Koninkrijk gelijksoortige voorschriften voor internationale doorgiften hanteren, zouden problematische verschillen naar verwachting ook kunnen worden vermeden door middel van samenwerking en de uitwisseling van informatie en ervaringen, onder andere tussen de Information Commissioner en het EDPB.

2.5.8 *Verantwoordingsplicht*

(83) Volgens het verantwoordingsbeginsel moeten entiteiten die gegevens verwerken passende technische en organisatorische maatregelen nemen om doeltreffend hun verplichtingen inzake gegevensbescherming te kunnen naleven, en moeten zij de naleving daarvan kunnen aantonen, in het bijzonder ten overstaan van de bevoegde toezichthoudende autoriteit.

(84) Het verantwoordingsbeginsel waarin is voorzien in Verordening (EU) 2016/679 is in artikel 5, lid 2, van de UK GDPR zonder wezenlijke wijzigingen gehandhaafd. Hetzelfde geldt voor artikel 24 inzake de verantwoordelijkheid van de verwerkingsverantwoordelijke, artikel 25 inzake gegevensbescherming door ontwerp en door standaardinstellingen en artikel 30 inzake het register van de verwerkingsactiviteiten. Ook de artikelen 35 en 36 inzake de gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging van de toezichthoudende autoriteit zijn gehandhaafd. De artikelen 37 tot en met 39 van Verordening (EU) 2016/679 inzake de aanwijzing en de taken van de functionaris voor gegevensbescherming zijn ook zonder wezenlijke wijzigingen overgenomen in de UK GDPR. De bepalingen van de artikelen 40 en 42 van Verordening (EU) 2016/679 inzake gedragscodes en certificering zijn tevens gehandhaafd in de UK GDPR ([80]).

2.6 **Toezicht en handhaving**

2.6.1 *Onafhankelijk toezicht*

(85) Om ervoor te zorgen dat in de praktijk een passend niveau van bescherming van persoonsgegevens wordt gewaarborgd, moet er worden voorzien in een onafhankelijke toezichthoudende autoriteit met bevoegdheden tot monitoring en handhaving van de naleving van de gegevensbeschermingsvoorschriften. Deze autoriteit moet bij de uitvoering van haar taken en de uitoefening van haar bevoegdheden volledig onafhankelijk en onpartijdig handelen.

(86) In het Verenigd Koninkrijk worden het toezicht op en de handhaving van de naleving van de UK GDPR en de DPA 2018 uitgevoerd door de Information Commissioner. De Information Commissioner is een "enkele instantie": een afzonderlijke rechtspersoon die wordt gevormd door één natuurlijke persoon. De werkzaamheden van de Information Commissioner worden ondersteund door een bureau. Op 31 maart 2020 had het bureau van de Information Commissioner 768 vaste personeelsleden ([81]). De Information Commissioner wordt gefinancierd door het Ministerie voor Digitale Zaken, Cultuur, Media en Sport ([82]).

(87) De onafhankelijkheid van de Commissioner is uitdrukkelijk vastgesteld in artikel 52 van de UK GDPR, dat niet wezenlijk is gewijzigd in vergelijking met artikel 52, leden 1 tot en met 3 van de AVG. De Commissioner moet bij de uitvoering van zijn taken en de uitoefening van zijn bevoegdheden overeenkomstig de UK GDPR volledig onafhankelijk optreden en vrij blijven van al dan niet rechtstreekse externe invloed in verband met deze taken en

([80]) Waar nodig zijn deze verwijzingen vervangen door verwijzingen naar de Britse autoriteiten. Op grond van artikel 17 van de DPA 2018 kan de Information Commissioner of een nationale accreditatie-instantie van het Verenigd Koninkrijk bijvoorbeeld een persoon die voldoet aan de vereisten van artikel 43 van de UK GDPR accrediteren om de naleving van een certificering te controleren.

([81]) Het jaarverslag en de jaarrekening 2019-2020 van de Information Commissioner, beschikbaar op: https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf

([82]) De relatie tussen de Information Commissioner en het ministerie is geregeld in een beheersovereenkomst. De belangrijkste taken van het Ministerie van Digitale Zaken, Cultuur, Media en Sport als financierder zijn onder meer: zorgen dat de Information Commissioner beschikt over voldoende middelen; de belangen van de Information Commissioner behartigen bij het parlement en andere ministeries; waarborgen dat er een robuust nationaal kader voor gegevensbescherming bestaat; en voorzien in richtsnoeren voor en ondersteuning van het bureau van de Information Commissioner met betrekking tot zakelijke kwesties zoals vastgoedvraagstukken, leases en aanbesteding (de Management Agreement 2018-2021, beschikbaar op: https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf).

bevoegdheden en mag van niemand instructies vragen of aanvaarden. De Commissioner dient zich te onthouden van handelingen die onverenigbaar zijn met zijn taken en mag gedurende zijn ambtstermijn geen al dan niet bezoldigde beroepswerkzaamheden verrichten die onverenigbaar zijn met zijn taken.

(88) De voorwaarden voor de benoeming en het ontslag van de Information Commissioner zijn vervat in bijlage 12 bij de DPA 2018. De Information Commissioner wordt benoemd door Hare Majesteit op voordracht van de regering aan de hand van een eerlijke en open concurrentieprocedure. De kandidaat moet beschikken over passende kwalificaties, vaardigheden en competenties. In overeenstemming met de Governance Code on Public Appointments ([83]) (de Britse governancecode voor benoemingen in overheidsfuncties) stelt een adviespanel een lijst van geschikte kandidaten op. Voordat de Secretary of State van het Ministerie van Digitale Zaken, Cultuur, Media en Sport een definitief besluit neemt, moet de desbetreffende beperkte commissie van het parlement voorafgaand aan de benoeming een onderzoek uitvoeren. Het standpunt van de commissie wordt openbaar gemaakt ([84]).

(89) De Information Commissioner wordt voor een termijn van zeven jaar benoemd. Een persoon kan slechts éénmaal tot Information Commissioner worden benoemd. De Information Commissioner kan door Hare Majesteit naar aanleiding van een address van beide kamers van het parlement worden ontslagen ([85]). Een verzoek om ontslag van de Information Commissioner kan slechts worden voorgelegd aan een kamer van het parlement wanneer een minister een verslag heeft gepresenteerd waarin hij verklaart dat hij het bewezen acht dat de Information Commissioner zich schuldig heeft gemaakt aan ernstig wangedrag en/of niet langer voldoet aan de voorwaarden die vereist zijn voor de uitoefening van diens taken ([86]).

(90) De financiering van de Information Commissioner is afkomstig uit drie bronnen: i) bijdragen voor gegevensbescherming die door verwerkingsverantwoordelijken worden betaald en die zijn vastgesteld in de regelingen van de Secretary of State ([87]) (de *Data Protection (Charges and Information) Regulations 2018* (de Britse regelingen gegevensbescherming (bijdragen en informatie) van 2018)), en die goed zijn voor 85 tot 90 % van de jaarlijkse begroting van het bureau ([88]); ii) subsidies die door de regering worden betaald aan de Information Commissioner. Subsidies worden voornamelijk gebruikt om de bedrijfskosten van de Information Commissioner te financieren met betrekking tot taken die geen verband houden met gegevensbescherming ([89]); en iii) vergoedingen die voor diensten in rekening worden gebracht ([90]). Dergelijke vergoedingen worden momenteel niet in rekening gebracht.

(91) De algemene taken van de Information Commissioner in verband met de verwerking van persoonsgegevens die vallen onder de UK GDPR zijn vastgesteld in artikel 57 van de UK GDPR en zijn bijna gelijk aan de dienovereenkomstige regels van Verordening (EU) 2016/679. Tot zijn taken behoren de monitoring en handhaving van de UK GDPR, de bevordering van de bekendheid bij het brede publiek, de behandeling van klachten van betrokkenen, de verrichting van onderzoeken enz. Daarnaast zijn in artikel 115 van de DPA 2018 andere algemene taken van de Commissioner uiteengezet, waaronder een verplichting om advies te verlenen aan het parlement, de regering en andere instellingen en organen over wetgevingsinitiatieven en bestuursmaatregelen in verband met de bescherming van de rechten en vrijheden van personen op het gebied van de verwerking van persoonsgegevens, en een bevoegdheid om op eigen initiatief of op verzoek advies uit te brengen aan het parlement, de regering of andere instellingen en organen, alsmede het publiek, over kwesties in verband met de bescherming van persoonsgegevens. Om de onafhankelijkheid van de rechterlijke macht te handhaven, mag de Information Commissioner zijn taken

([83]) Governance Code on Public Appointments, beschikbaar op: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/578498/governance_code_on_public_appointments_16_12_2016.pdf

([84]) Tweede verslag van sessie 2015-2016 van de commissie voor Cultuur, Media en Sport van het Lagerhuis, beschikbaar op: https://publications.parliament.uk/pa/cm201516/cmselect/cmcumeds/990/990.pdf

([85]) Een "address" is een motie die wordt voorgelegd aan het parlement, waarmee ernaar wordt gestreefd de vorst op de hoogte te stellen van de standpunten van het parlement over een bepaalde kwestie.

([86]) Paragraaf 3, punt 3, van bijlage 12 bij de DPA 2018.

([87]) Artikel 137 van de DPA 2018, zie overweging (17).

([88]) In de artikelen 137 en 138 van de DPA 2018 is een aantal waarborgen opgenomen om te garanderen dat de vergoedingen op een passend niveau worden vastgesteld. Met name in artikel 137, lid 4, worden de zaken genoemd die de Secretary of State in aanmerking moet nemen bij het vaststellen van regelingen waarin het bedrag wordt gespecificeerd dat verschillende organisaties moeten betalen. Artikel 138, lid 1, en artikel 182 van de DPA 2018 bevatten daarnaast een wettelijk vereiste voor de Secretary of State om de Information Commissioner en andere vertegenwoordigers of personen voor wie de regelingen waarschijnlijk gevolgen zullen hebben, te raadplegen alvorens deze regelingen vast te stellen, zodat rekening kan worden gehouden met hun standpunten. Op grond van artikel 138, lid 2, van de DPA 2018 moet de Information Commissioner bovendien de werking van de Charges Regulations blijven evalueren en kan hij bij de Secretary of State voorstellen indienen tot wijziging van de Regulations. Wanneer regelingen enkel worden vastgesteld om rekening te houden met een stijging van de index van kleinhandelsprijzen (waarbij deze vallen onder de negatieve procedure) moet hiervoor de bevestigende procedure worden gevolgd en mogen zij niet worden vastgesteld voordat zij per resolutie zijn goedgekeurd door beide kamers van het parlement.

([89]) In de beheersovereenkomst is verduidelijkt dat de Secretary of State betalingen aan de Information Commissioner mag verrichten met geld dat door het parlement ter beschikking wordt gesteld op grond van paragraaf 9 van bijlage 12 bij de DPA 2018. Na raadpleging van de Information Commisioner betaalt het Ministerie van Digitale Zaken, Cultuur, Media en Sport de Information Commissioner passende bedragen (de subsidies) voor administratieve kosten van het ICO en voor de uitoefening van de taken van de Information Commissioner in verband met een aantal specifieke taken, waaronder de vrijheid van informatie (Management Agreement 2018-2021, paragraaf 1.12, zie voetnoot 82).

([90]) Zie artikel 134 van de DPA 2018.

niet uitoefenen in verband met de verwerking van persoonsgegevens van een persoon die optreedt in een rechterlijke hoedanigheid of een rechter of administratieve rechtbank die optreedt in zijn rechterlijke hoedanigheid. Het toezicht op de rechterlijke macht wordt echter gewaarborgd door gespecialiseerde organen (zie de overwegingen (99) tot en met (103)).

2.6.2 *Handhaving, met inbegrip van sancties*

(92) De bevoegdheden van de Information Commissioner zijn uiteengezet in artikel 58 van de UK GDPR, waarin geen wezenlijke wijzigingen zijn aangebracht ten opzichte van het overeenkomstige artikel van Verordening (EU) 2016/679. In de DPA 2018 zijn aanvullende regels vastgesteld over de manier waarop deze bevoegdheden kunnen worden uitgeoefend. De Commissioner heeft met name de bevoegdheid om: a) de verwerkingsverantwoordelijke en de verwerker (en, in bepaalde omstandigheden, een andere persoon) te gelasten de vereiste informatie te verstrekken door middel van een aanzegging tot informatie ("aanzegging tot informatie") ([91]); b) onderzoeken en controles te verrichten in de vorm van een aanzegging tot beoordeling, waarin de verwerkingsverantwoordelijke of verwerker kan worden gelast de Commissioner toegang te verlenen tot gespecificeerde bedrijfsruimten om documenten of uitrusting te inspecteren of onderzoeken, personen te interviewen die namens de verwerkingsverantwoordelijke persoonsgegevens verwerken enz. ("aanzegging tot beoordeling") ([92]); c) anderszins toegang te verkrijgen tot documenten enz. van verwerkingsverantwoordelijken en verwerkers, evenals toegang tot hun bedrijfsruimten in overeenstemming met artikel 154 van de DPA 2018 ("toegangs- en inspectiebevoegdheden"); d) zijn corrigerende bevoegdheden uit te oefenen, onder meer door middel van waarschuwingen en berispingen, of opdrachten te geven aan de hand van een sommatie tot nakoming, waarmee verwerkingsverantwoordelijken/verwerkers worden gelast genoemde stappen te nemen of hiervan af te zien, waaronder het gelasten van de verwerkingsverantwoordelijke of verwerker om handelingen uit te voeren die zijn gespecificeerd in artikel 58, lid 2, punten c) tot en met g) en j), van de UK GDPR ("sommatie tot nakoming") ([93]); en e) administratieve sancties op de leggen in de vorm van een sanctiebeschikking ("sanctiebeschikking") ([94]). Deze laatste kan ook worden opgelegd indien een overheidsinstantie de UK GDPR niet heeft nageleefd ([95]).

(93) In het Regulatory Action Policy (beleid voor regelgevend optreden) van de Information Commissioner zijn de omstandigheden uiteengezet waarin deze een aanzegging tot informatie, beoordeling, sommatie tot nakoming of sanctiebeschikking vaststelt ([96]). Met een sommatie tot nakoming die wordt gedaan als reactie op nalaten van een verwerkingsverantwoordelijke of verwerker mogen alleen vereisten worden opgelegd die de Commissioner passend acht om het nalaten te verhelpen. Sommaties tot nakoming en sanctiebeschikkingen mogen aan een verwerkingsverantwoordelijke of verwerker worden afgegeven in verband met inbreuken op hoofdstuk II van de UK GDPR (beginselen inzake verwerking), de artikelen 12 tot en met 22 (rechten van de betrokkene), de artikelen 25 tot en met 39 (verplichtingen van verwerkingsverantwoordelijken en verwerkers) en de artikelen 44 tot en met 49 (internationale doorgiften) van de UK GDPR. Een sommatie tot nakoming kan ook worden afgegeven wanneer een verwerkingsverantwoordelijke de vereiste niet naleeft om een bijdrage te betalen zoals neergelegd in regelingen die op grond van artikel 137 van de DPA 2018 zijn vastgesteld. Er kan daarnaast een sommatie tot nakoming worden afgegeven aan een toezichthoudende autoriteit, zoals bedoeld in artikel 41, of een verlener van certificeringen indien zij hun verplichtingen uit hoofde van de UK GDPR niet nakomen. Een sanctiebeschikking kan ook worden afgegeven aan een persoon die niet heeft voldaan aan een aanzegging tot informatie of beoordeling of een sommatie tot nakoming.

(94) In het geval van een sanctiebeschikking wordt vereist dat de persoon de Information Commissioner een in de beschikking gespecificeerd bedrag betaalt. Bij het bepalen of een sanctiebeschikking aan een persoon moet worden afgegeven en bij het bepalen van de hoogte van de sanctie, moet de Information Commissioner rekening houden met de kwesties die zijn opgenomen in artikel 83, leden 1 en 2, van de UK GDPR, die identiek zijn aan de overeenkomstige regels van Verordening (EU) nr. 2016/679 ([97]). Overeenkomstig artikel 83, leden 4 en 5, zijn de maximumbedragen van administratieve geldboeten wegens niet-nakoming van de in die bepalingen bedoelde verplichtingen respectievelijk 8 700 000 GBP en 17 500 000 GBP. Betreft het een onderneming, dan kan de Information Commissioner ook geldboeten opleggen als percentage van de wereldwijde jaaromzet, indien deze hoger is. Net zoals in de gelijkwaardige bepalingen van Verordening (EU) 2016/679 zijn deze bedragen vastgesteld

([91]) Artikel 142 van de DPA 2018 (behoudens de in artikel 143 van de DPA 2018 vastgestelde beperkingen).
([92]) Artikel 146 van de DPA 2018 (behoudens de in artikel 147 van de DPA 2018 vastgestelde beperkingen).
([93]) Artikelen 149 tot en met 151 van de DPA 2018 (behoudens de in artikel 152 van de DPA 2018 vastgestelde beperkingen).
([94]) Artikel 155 van de DPA 2018 en artikel 83 van de UK GDPR.
([95]) Dit volgt uit artikel 155, lid 1, van de DPA 2018, gelezen in samenhang met artikel 149, leden 2 en 5, van de DPA 2018, en uit artikel 156, lid 4, van de DPA 2018, waarin het opleggen van sanctiebeschikkingen alleen wordt beperkt met betrekking tot de commissarissen staatsdomeinen en verwerkingsverantwoordelijken voor de koninklijke familie overeenkomstig artikel 209, lid 4, van de DPA 2018.
([96]) Regulatory Action Policy, beschikbaar op: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf
([97]) Waaronder de aard en ernst van de inbreuk (rekening houdend met de aard, de omvang of het doel van de verwerking in kwestie, alsmede het aantal getroffen betrokkenen en de omvang van de door hen geleden schade), de opzettelijke of nalatige aard van de inbreuk, de door de verwerkingsverantwoordelijke genomen maatregelen om de door betrokkenen geleden schade te beperken, de mate waarin de verwerkingsverantwoordelijke of de verwerker verantwoordelijk is (rekening houdend met de technische en organisatorische maatregelen die hij heeft uitgevoerd), eerdere relevante inbreuken door de verwerkingsverantwoordelijke of de verwerker; de mate waarin met de Commissioner is samengewerkt, de categorieën persoonsgegevens waarop de inbreuk betrekking heeft, elke andere op de omstandigheden van de zaak toepasselijke verzwarende of verzachtende omstandigheid, zoals behaalde financiële winsten, of vermeden verliezen, die al dan niet rechtstreeks uit de inbreuk voortvloeien.

op 2 en 4 % in artikel 83, leden 4 en 5. Bij niet-naleving van een aanzegging tot informatie of beoordeling of een sommatie tot nakoming is het maximumbedrag van de sanctie die kan worden opgelegd 17 500 000 GBP of, in het geval van een onderneming, 4 % van de wereldwijde jaaromzet, indien dit cijfer hoger is.

(95) De UK GDPR en de DPA 2018 versterken ook de overige bevoegdheden van de Information Commissioner. De Commissioner kan nu bijvoorbeeld verplichte controles uitvoeren in verband met alle verwerkingsverantwoordelijken en verwerkers aan de hand van aanzeggingen tot beoordeling, terwijl de Commissioner op grond van de eerdere wetgeving, de Data Protection Act 1998, deze bevoegdheid slechts had met betrekking tot organisaties van de centrale overheid en op het gebied van gezondheid en overige organisaties moesten instemmen met een controle.

(96) Sinds de invoering van Verordening (EU) 2016/679 behandelt het ICO jaarlijks ongeveer 40 000 klachten van betrokkenen ([98]) en voert het daarnaast ambtshalve ongeveer 2 000 onderzoeken ([99]) uit. De meeste klachten hebben betrekking op het recht van inzage en het recht op mededeling van gegevens. Naar aanleiding van zijn onderzoeken neemt de Commissioner handhavingsmaatregelen in een brede reeks sectoren. Meer specifiek heeft de Information Commissioner volgens zijn meest recente jaarverslag (2019-2020) ([100]) tijdens de verslagperiode 54 aanzeggingen tot informatie, 8 aanzeggingen tot beoordeling, 7 sommaties tot nakoming, 4 waarschuwingen, 8 vervolgingen en 15 geldboetes opgelegd ([101]).

(97) Dit omvatte enkele aanzienlijke financiële sancties die op grond van Verordening (EU) 2016/679 en de DPA 2018 werden opgelegd. De Information Commissioner legde in het bijzonder in oktober 2020 een boete van 20 miljoen GBP op aan een Britse luchtvaartmaatschappij voor een inbreuk op gegevens die gevolgen had voor meer dan 400 000 klanten. Eind oktober 2020 werd een geldboete van 18,4 miljoen GBP opgelegd aan een internationale hotelketen omdat deze de persoonsgegevens van miljoenen klanten niet had beveiligd en in november 2020 werd een geldboete van 1,25 miljoen GBP opgelegd aan een Britse dienstverlener die online tickets voor evenementen verkocht omdat deze de betalingsgegevens van klanten niet had beschermd ([102]).

(98) Naast de in overweging (92) beschreven handhavingsbevoegdheden van de Information Commissioner, vormen bepaalde schendingen van de wetgeving betreffende gegevensbescherming strafbare feiten en kunnen hiervoor derhalve strafrechtelijke sancties worden opgelegd (artikel 196 van de DPA 2018). Dit geldt bijvoorbeeld voor het opzettelijk of door onachtzaamheid verkrijgen of meedelen van persoonsgegevens zonder de toestemming van de verwerkingsverantwoordelijke ([103]), het bewerkstelligen van de bekendmaking van persoonsgegevens aan een andere persoon zonder toestemming van de verwerkingsverantwoordelijke, het ongedaan maken van de anonimisering van persoonsgegevens ([104]) zonder toestemming van de verwerkingsverantwoordelijke die hiervoor verantwoordelijk is, het opzettelijk belemmeren van de bevoegdheid van de Commissioner om zijn bevoegdheden uit te oefenen in verband met de inspectie van persoonsgegevens in overeenstemming met internationale verplichtingen ([105]), het afleggen van valse verklaringen in reactie op een aanzegging tot informatie of het vernietigen van informatie in verband met aanzeggingen tot informatie en beoordeling ([106]).

([98]) Volgens de door de Britse autoriteiten verstrekte informatie werd in de periode die het jaarverslag 2019-2020 van de Information Commissioner beslaat in ongeveer 25 % van de gevallen een inbreuk geconstateerd, werd de betrokkene in ongeveer 29 % van de gevallen verzocht de kwestie eerst bij de verwerkingsverantwoordelijke onder de aandacht te brengen, te wachten op het antwoord van de verwerkingsverantwoordelijke of de lopende dialoog met de verwerkingsverantwoordelijke voort te zetten, werd in ongeveer 17 % van de gevallen geen inbreuk vastgesteld, maar advies verleend aan de verwerkingsverantwoordelijke, werd in ongeveer 25 % van de gevallen een inbreuk vastgesteld door de Information Commissioner en werd advies verleend aan de verwerkingsverantwoordelijke of werd hij gelast bepaalde maatregelen te nemen, werd in ongeveer 3 % van de gevallen vastgesteld dat de klacht niet viel onder Verordening (EU) 2016/679 en werd ongeveer 1 % van de gevallen doorgestuurd naar een andere autoriteit voor gegevensbescherming in het kader van het Europees Comité voor gegevensbescherming.

([99]) Het ICO kan deze onderzoeken starten op basis van informatie die van verschillende bronnen wordt verkregen, waaronder meldingen van inbreuken in verband met persoonsgegevens, doorverwijzingen van andere Britse overheidsinstanties of buitenlandse autoriteiten voor gegevensbescherming en klachten van personen of maatschappelijke organisaties.

([100]) Het jaarverslag en de jaarrekening 2019-2020 van de Information Commissioner (zie voetnoot 81).

([101]) Volgens het voorgaande jaarverslag voor de periode 2018-2019 vaardigde de Information Commissioner in de verslagperiode 22 sanctiebeschikkingen op grond van de DPA 1998 uit, met geldboetes van in totaal 3 010 610 GBP, waaronder twee geldboetes van 500 000 GBP (het maximum dat uit hoofde van de DPA 1998 was toegestaan). In 2018 voerde de Information Commissioner met name een onderzoek uit naar het gebruik van data-analyse voor politieke doeleinden naar aanleiding van de onthullingen omtrent Cambridge Analytica. Het onderzoek resulteerde in een beleidsrapport, een reeks aanbevelingen, een boete van 500 000 GBP voor Facebook en een sommatie tot nakoming voor Aggregate IQ, een Canadese gegevensmakelaar, waarbij het bedrijf werd gelast persoonsgegevens van Britse onderdanen en inwoners van het Verenigd Koninkrijk te wissen (zie het jaarverslag en de jaarrekening 2018-2019 van de Information Commissioner, beschikbaar op: https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf)

([102]) Zie de website van het ICO voor een samenvatting van de getroffen handhavingsmaatregelen, beschikbaar op: https://ico.org.uk/action-weve-taken/enforcement/

([103]) Artikel 170 van de DPA 2018.

([104]) Artikel 171 van de DPA 2018.

([105]) Artikel 119 van de DPA 2018.

([106]) Artikelen 144 en 148 van de DPA 2018.

2.6.3 *Toezicht op de rechterlijke macht*

(99) Het toezicht op de verwerking van persoonsgegevens door rechters en de rechtelijke macht is tweeledig. Wanneer gerechtsambtenaren of rechters niet optreden in een rechterlijke hoedanigheid, wordt het toezicht verricht door het ICO. Wanneer de verwerkingsverantwoordelijke optreedt in een rechterlijke hoedanigheid, kan het ICO zijn toezichtstaken ([107]) niet uitoefenen en wordt het toezicht verricht door speciale organen. Hiermee wordt de benadering van Verordening (EU) 2016/679 (artikel 55, lid 3) gevolgd.

(100) In het tweede scenario wordt dit toezicht op de rechters van Engeland en Wales en de First-tier en Upper Tribunals (administratieve rechtbanken van eerste aanleg en hogere administratieve rechtbanken) van Engeland en Wales uitgeoefend door het Judicial Data Protection Panel (gerechtelijk panel voor gegevensbescherming) ([108]). Daarnaast hebben de Lord Chief Justice (hoogste rechter) en de Senior President of Tribunals (eerste voorzitter van de administratieve rechtbanken) een privacyverklaring ([109]) bekendgemaakt, waarin uiteen is gezet hoe de rechters in Engeland en Wales persoonsgegevens verwerken voor de uitoefening van gerechtelijke taken. De Noord-Ierse ([110]) en Schotse rechterlijke macht ([111]) hebben een vergelijkbare verklaring afgegeven.

(101) In Noord-Ierland heeft de Lord Chief Justice van Noord-Ierland bovendien een rechter van de High Court aangewezen als Data Supervisory Judge (rechter voor gegevenstoezicht, hierna "DSJ" genoemd) ([112]). Hij heeft voor de Noord-Ierse rechterlijke macht ook richtsnoeren uitgevaardigd voor wat er moet worden gedaan in het geval dat gegevens verloren gaan of mogelijk verloren gaan en voor het omgaan met problemen die hieruit voortvloeien ([113]).

(102) In Schotland heeft de Lord President een DSJ aangewezen voor het onderzoeken van klachten op grond van de gegevensbescherming. Dit is uiteengezet in de regels betreffende gerechtelijke klachten, die overeenkomen met de regels die voor Engeland en Wales zijn vastgesteld ([114]).

(103) Tot slot wordt binnen de Supreme Court (hoogste Britse rechterlijke instantie) een van de rechters van de Supreme Court aangewezen om toezicht te houden op de gegevensbescherming.

2.6.4 *Verhaalmogelijkheden*

(104) Om een passende bescherming en vooral handhaving van individuele rechten te waarborgen, moeten aan de betrokkene doeltreffende administratieve en gerechtelijke rechtsmiddelen worden toegekend, met inbegrip van een recht op schadeloosstelling.

([107]) Artikel 117 van de DPA 2018.

([108]) Het panel is verantwoordelijk voor het verstrekken van richtsnoeren en opleidingen aan de rechterlijke macht. Het behandelt daarnaast klachten van betrokkenen in verband met de verwerking van persoonsgegevens door rechters, administratieve rechtbanken en personen die optreden in een rechterlijke hoedanigheid. Het panel moet de middelen verstrekken om alle klachten te kunnen oplossen. Indien een klager ontevreden is met een beslissing van het panel en aanvullend bewijs overlegt, kan het panel zijn beslissing heroverwegen. Hoewel het panel zelf geen financiële sancties oplegt, kan het, wanneer het van mening is dat sprake is van een voldoende ernstige inbreuk op de DPA 2018, de zaak doorverwijzen naar het Judicial Conduct Investigation Office (het Britse Onderzoeksbureau Gerechtelijk Optreden, hierna "JCIO" genoemd), dat de klacht zal onderzoeken. Als de klacht gegrond wordt verklaard, moeten de Lord Chancellor (grootkanselier) en de Lord Chief Justice (of een hoge rechter aan wie hij deze taak delegeert) besluiten welke maatregelen tegen de ambtsdrager moeten worden genomen. Dit kan het volgende omvatten, in volgorde van ernst: een formeel advies, een formele waarschuwing, een berisping en, uiteindelijk, de ontzetting uit het ambt. Als een persoon ontevreden is met de wijze waarop de klacht door het JCIO is onderzocht, kan hij een verdere klacht indienen bij de Judicial Appointments and Conduct Ombudsman (ombudsman voor gerechtelijke benoemingen en gerechtelijk optreden) (zie https://www.gov.uk/government/organisations/judicial-appointments-and-conduct-ombudsman). De ombudsman is bevoegd om het JCIO te verzoeken een klacht opnieuw te onderzoeken en kan voorstellen om een vergoeding te betalen aan de klager wanneer hij van mening is dat deze schade heeft geleden als gevolg van wanbeheer.

([109]) De privacyverklaring van de Lord Chief Justice en de Senior President of Tribunals is beschikbaar op: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice

([110]) De privacyverklaring van de Lord Chief Justice van Noord-Ierland is beschikbaar op: https://judiciaryni.uk/data-privacy

([111]) De privacyverklaring voor de Schotse rechters en administratieve rechtbanken is beschikbaar op: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice

([112]) De DSJ verstrekt richtsnoeren aan de rechterlijke macht en onderzoekt inbreuken en/of klachten met betrekking tot de verwerking van persoonsgegevens door rechters of personen die optreden in een rechterlijke hoedanigheid.

([113]) Wanneer de klacht of inbreuk ernstig wordt geacht, wordt deze doorgestuurd naar de *Judicial Complaints Officer* (functionaris voor gerechtelijke klachten) voor een verder onderzoek in overeenstemming met de praktijkcode voor klachten van de Lord Chief Justice van Noord-Ierland. De uitkomst van een dergelijke klacht kan zijn: geen verdere maatregelen, advies, opleiding of begeleiding, een informele waarschuwing, een formele waarschuwing, een laatste waarschuwing, beperking van de praktijk of doorverwijzing naar een statutaire administratieve rechtbank. De privacyverklaring van de Lord Chief Justice van Noord-Ierland is beschikbaar op: https://judiciaryni.uk/sites/judiciary/files/media-files/14G.%20CODE%20OF%20PRACTICE%20Judicial%20~%2028%20Feb%2013%20%28Final%29%20updated%20with%20new%20comp..__1.pdf

([114]) Gegronde klachten worden onderzocht door de DSJ en doorverwezen naar de Lord President, die bevoegd is om advies, een formele waarschuwing of een berisping vast te stellen indien hij dit nodig acht (voor leden van administratieve rechtbanken bestaan gelijkwaardige regels, die beschikbaar zijn op: https://www.judiciary.scot/docs/librariesprovider3/judiciarydocuments/complaints/complaintsaboutthejudiciaryscotlandrules2017_1d392ab6e14f6425aa0c7f48d062f5cc5.pdf?sfvrsn=5d3eb9a1_2).

(105) Ten eerste hebben betrokkenen het recht om een klacht in te dienen bij de Information Commissioner wanneer zij van mening zijn dat sprake is van een inbreuk op de UK GDPR ([115]) in verband met persoonsgegevens die hen betreffen. In de UK GDPR zijn de regels van artikel 77 van Verordening (EU) 2016/679 inzake dat recht zonder wezenlijke wijzigingen overgenomen. Hetzelfde geldt voor artikel 57, lid 1, punt f), en artikel 57, lid 2, waarin de taken van de Commissioner in verband met de behandeling van klachten zijn vastgesteld. Zoals beschreven in de overwegingen (92) tot en met (98), is de Information Commissioner bevoegd om de naleving van de UK GDPR en de DPA 2018 door de verwerkingsverantwoordelijke en de verwerker te beoordelen, om hen te gelasten in het geval van niet-naleving de noodzakelijke stappen te nemen of hiervan af te zien en om geldboetes op te leggen.

(106) Ten tweede bieden de UK GDPR en de DPA 2018 het recht om een voorziening in rechte in te stellen tegen de Information Commissioner. Overeenkomstig artikel 78, lid 1, van de UK GDPR hebben personen het recht om een doeltreffende voorziening in rechte in te stellen tegen een hen betreffend juridisch bindend besluit van de Commissioner. In het kader van de rechterlijke toetsing onderzoekt de rechter het besluit dat in de vordering wordt aangevochten en stelt hij vast of de Information Commissioner rechtmatig heeft gehandeld. De klager heeft op grond van artikel 78, lid 2, van de UK GDPR bovendien recht om een voorziening in rechte in te stellen wanneer de Commissioner een klacht van de betrokkene niet naar behoren behandelt ([116]). De klager kan een procedure instellen bij een First Tier Tribunal om de Commissioner te gelasten de passende maatregelen te nemen om op de klacht te reageren of de klager te informeren over de voortgang ten aanzien van de ingediende klacht ([117]). Daarnaast kan een persoon die een van de bovengenoemde kennisgevingen (aanzegging tot informatie, beoordeling, sommatie tot nakoming of sanctiebeschikking) van de Commissioner ontvangt, beroep aantekenen bij een First Tier Tribunal ([118]). Als het Tribunal oordeelt dat het besluit van de Commissioner niet in overeenstemming is met de wet of dat de Information Commissioner zijn bevoegdheid op een andere wijze had moeten uitoefenen, moet het Tribunal het ingestelde beroep toestaan of de aanzegging/sommatie/beschikking of het besluit vervangen door een andere aanzegging/sommatie/beschikking of een ander besluit die/dat door de Information Commissioner had kunnen worden afgegeven of genomen.

(107) Ten derde kunnen personen op grond van artikel 79 van de UK GDPR en artikel 167 van de DPA 2018 rechtstreeks voor de rechter een voorziening in rechte instellen tegen verwerkingsverantwoordelijken en verwerkers. Als een rechter het met betrekking tot een verzoek van een betrokkene bewezen acht dat er sprake is geweest van een inbreuk op de rechten van de betrokkene op grond van de wetgeving betreffende gegevensbescherming, kan de rechter de verwerkingsverantwoordelijke, of een verwerker die namens die verwerkingsverantwoordelijke optreedt, met betrekking tot de verwerking gelasten de in het bevel genoemde stappen te nemen of af te zien van de in het bevel genoemde stappen.

(108) Een persoon die materiële of immateriële schade heeft geleden als gevolg van een inbreuk op de UK GDPR, heeft bovendien op grond van artikel 82 UK GDPR en artikel 168 van de DPA 2018 recht op een vergoeding van de verwerkingsverantwoordelijke of de verwerker voor de geleden schade. De regels inzake de vergoeding en aansprakelijkheid van artikel 82, leden 1 tot en met 5, van de UK GDPR zijn identiek aan de overeenkomstige regels van Verordening (EU) 2016/679. Op grond van artikel 168 van de DPA 2018 valt nood ook onder immateriële schade. Op grond van artikel 80 van de UK GDPR heeft de betrokkene ook een recht om een vertegenwoordigend orgaan of vertegenwoordigende organisatie opdracht te geven de klacht namens hem in te dienen bij de Commissioner (op grond van artikel 77 van de UK GDPR) en om de in de artikelen 78 (recht om een doeltreffende voorziening in rechte in te stellen tegen de Commissioner), 79 (recht om een doeltreffende voorziening in rechte in te stellen tegen een verwerkingsverantwoordelijke of verwerker) en 82 (recht op schadevergoeding en aansprakelijkheid) van de UK GDPR namens hem uit te oefenen.

(109) Ten vierde kunnen personen die van mening zijn dat hun rechten, met inbegrip van het recht op privacy en gegevensbescherming, door overheidsinstanties zijn geschonden niet alleen middels een hierboven genoemde voorziening in rechte, maar ook voor de Britse rechter op grond van de Human Right Act 1998 ([119]) een schadeloosstelling verkrijgen. Een persoon die stelt dat een overheidsinstantie op een wijze heeft gehandeld (of voorstelt te handelen) die onverenigbaar is met een verdragsrecht en die dienovereenkomstig onrechtmatig is op grond van artikel 6, lid 1, van de Human Rights Act 1998, kan een procedure tegen de instantie instellen bij de passende rechter of administratieve rechtbank of de desbetreffende rechten in een juridische procedure inroepen wanneer hij het slachtoffer is (of zou zijn) van de onrechtmatige handeling.

(110) Indien de rechter oordeelt dat een handeling van een overheidsinstantie onrechtmatig is, kent hij, binnen zijn bevoegdheden en zoals hij billijk en passend acht, een dergelijke schadeloosstelling of voorziening toe of geeft hij hiertoe opdracht ([120]). De rechter kan ook een bepaling van de primaire wetgeving onverenigbaar verklaren met een verdragsrecht.

([115]) Artikel 77 van de UK GDPR.

([116]) In artikel 166 van de DPA 2018 wordt specifiek verwezen naar de volgende situaties: a) de Commissioner heeft niet de passende stappen genomen om op de klacht te reageren, b) de Commissioner heeft voor het einde van de periode van drie maanden vanaf de ontvangst van de klacht door de Commissioner geen informatie verstrekt aan de klager over de voortgang of het resultaat van de klacht of c) de Commissioner heeft, indien de behandeling van de klacht door de Commissioner niet binnen de bovengenoemde periode wordt afgerond, de klager hiervan niet binnen een daaropvolgende periode van drie maanden op de hoogte gesteld.

([117]) Artikel 78, lid 2, van de UK GDPR en artikel 166 van de DPA 2018.

([118]) Artikel 78, lid 1, van de UK GDPR en artikel 162 van de DPA 2018.

([119]) Artikel 7, lid 1, van de Human Rights Act 1998. Overeenkomstig artikel 7, lid 7, is een persoon alleen het slachtoffer van een onrechtmatige handeling als hij een slachtoffer zou zijn in de zin van artikel 34 van het Europees Verdrag voor de rechten van de mens wanneer in verband met die handeling een procedure zou worden ingesteld voor het Europees Hof voor de Rechten van de Mens.

([120]) Artikel 8, lid 1, van de Human Rights Act 1998.

(111) Tot slot kan een persoon, nadat alle nationale rechtsmiddelen zijn uitgeput, een voorziening instellen bij het Europees Hof voor de Rechten van de Mens in verband met schendingen van de rechten die door het Europees Verdrag voor de rechten van de mens worden gewaarborgd.

3. TOEGANG TOT EN GEBRUIK VAN UIT DE EUROPESE UNIE DOORGEGEVEN PERSOONSGEGEVENS DOOR OVERHEIDSINSTANTIES IN HET VERENIGD KONINKRIJK

(112) De Commissie heeft ook het rechtskader van het Verenigd Koninkrijk beoordeeld inzake de verzameling en het daaropvolgende gebruik van persoonsgegevens die door Britse overheidsinstanties in het algemeen belang, met name de handhaving van het strafrecht en nationale veiligheid, worden doorgegeven aan bedrijfsexploitanten in het Verenigd Koninkrijk (hierna "overheidstoegang" genoemd). Bij de beoordeling van de vraag of de voorwaarden waaronder overheidstoegang tot gegevens die op grond van dit besluit aan het Verenigd Koninkrijk worden doorgegeven "in feite overeenkomend" zijn met artikel 45, lid 1, van Verordening (EU) 2016/679 (de "AVG"), zoals uitgelegd door het Hof van Justitie van de Europese Unie (het "HvJ-EU") in het licht van het Handvest van de grondrechten, heeft de Commissie met name rekening gehouden met de volgende criteria.

(113) Ten eerste moet elke beperking van het recht op bescherming van persoonsgegevens bij wet worden geregeld en moet de rechtsgrondslag die de aantasting van een dergelijk recht mogelijk maakt, zelf de reikwijdte van de beperking op de uitoefening van het betrokken recht bepalen ([121]).

(114) Ten tweede moet, om te voldoen aan het evenredigheidsvereiste, dat inhoudt dat afwijkingen en beperkingen van de bescherming van persoonsgegevens slechts van toepassing mogen zijn voor zover zulks in een democratische samenleving strikt noodzakelijk is om specifieke doelstellingen van algemeen belang te verwezenlijken die gelijkwaardig zijn aan die welke door de Unie worden erkend, de wetgeving van het betrokken derde land die de inmenging toestaat, duidelijke en nauwkeurige regels betreffende de werkingssfeer en de toepassing van de betrokken maatregelen vaststellen en minimumwaarborgen opleggen, opdat de personen wier gegevens zijn doorgegeven, over voldoende waarborgen beschikken om hun persoonsgegevens doeltreffend te beschermen tegen het risico van misbruik ([122]) De wetgeving moet met name aangeven in welke omstandigheden en onder welke voorwaarden een maatregel kan worden genomen ([123]) die voorziet in de verwerking van dergelijke gegevens, en moet de naleving van dergelijke vereisten aan onafhankelijk toezicht onderwerpen ([124]).

(115) Ten derde moet die wetgeving volgens het nationale recht juridisch bindend zijn en moeten die wettelijke voorschriften niet alleen bindend zijn voor de autoriteiten, maar ook voor de rechterlijke instantie afdwingbaar zijn tegenover de autoriteiten van het betrokken derde land ([125]). Betrokkenen moeten met name de mogelijkheid hebben een rechtsvordering in te stellen bij een onafhankelijke en onpartijdige rechterlijke instantie om inzage te krijgen in hun persoonsgegevens of om deze gegevens te laten corrigeren of wissen ([126]).

3.1 **Algemeen rechtskader**

(116) Als bevoegdheidsuitoefening door een overheidsinstantie moet overheidstoegang in het Verenigd Koninkrijk plaatsvinden met volledige inachtneming van de wet. Het Verenigd Koninkrijk heeft het Europees Verdrag tot bescherming van de rechten van de mens geratificeerd (zie overweging (9)) en alle Britse overheidsinstanties zijn verplicht te handelen in overeenstemming met dat verdrag ([127]). Artikel 8 van het verdrag bepaalt dat inmenging in de persoonlijke levenssfeer in overeenstemming moet zijn met de wet, in het belang van een van de in artikel 8, lid 2, genoemde doelstellingen, en evenredig moet zijn in het licht van die doelstelling. Artikel 8 vereist ook dat de inmenging "voorzienbaar" is, d.w.z. een duidelijke, toegankelijke grondslag in de wet heeft, en dat de wet passende waarborgen bevat om misbruik te voorkomen.

(117) Bovendien heeft het Europees Hof voor de Rechten van de Mens in zijn rechtspraak gespecificeerd dat elke aantasting van het recht op privacy en gegevensbescherming onderworpen moet zijn aan een doeltreffend, onafhankelijk en onpartijdig toezichtsysteem, dat ofwel door een rechter, ofwel door een ander onafhankelijk orgaan ([128]) (bijvoorbeeld een administratieve autoriteit of een parlementair orgaan) moet worden ingesteld.

([121]) Zie *Schrems II*, punten 174–175, en de aangehaalde rechtspraak. Zie ook, wat de toegang van overheidsinstanties van de lidstaten betreft, het arrest van het Hof (grote kamer) van 6 oktober 2020, Privacy International, Zaak C-623/17, ECLI:EU:C:2020:790, punt 65; en het arrest van het Hof (grote kamer) van 6 oktober 2020, La Quadrature du Net e.a., gevoegde zaken C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791, punt 175.

([122]) Zie Schrems II, punten 176 en 181, en de aangehaalde rechtspraak. Zie ook, wat de toegang van overheidsinstanties van de lidstaten betreft, Privacy International, punt 68, en La Quadrature du Net e.a., punt 132.

([123]) Zie Schrems II, punt 176. Zie ook, wat de toegang van overheidsinstanties van de lidstaten betreft, Privacy International, punt 68, en La Quadrature du Net e.a., punt 132.

([124]) Zie Schrems II, punt 179.

([125]) Zie Schrems II, punten 181–182.

([126]) Zie Schrems I, punt 95 en Schrems II, punt 194. In dat verband heeft het HvJ-EU met name benadrukt dat artikel 47 van het Handvest van de grondrechten (dat het recht op een doeltreffende voorziening in rechte bij een onafhankelijk en onpartijdig gerecht waarborgt), deel uitmaakt van "het binnen de Unie vereiste beschermingsniveau en [dat] de Commissie de naleving [ervan] moet vaststellen alvorens een adequaatheidsbesluit op grond van artikel 45, lid 1, AVG vast te stellen" (Schrems II, punt 186).

([127]) Artikel 6 van de Human Rights Act 1998.

([128]) Arrest van het Europees Hof voor de Rechten van de Mens, Klass e.a./Duitsland, verzoekschrift nr. 5029/71, punten 17–51.

(118) Bovendien moeten personen over een doeltreffend rechtsmiddel beschikken, en het Europees Hof voor de Rechten van de Mens heeft verduidelijkt dat dit rechtsmiddel moet worden geboden door een onafhankelijk en onpartijdig orgaan dat zijn eigen reglement van orde heeft vastgesteld, dat bestaat uit leden die een hoge rechterlijke functie bekleden of hebben bekleed of ervaren advocaten zijn, en dat er geen bewijslast mag zijn die moet worden overwonnen om een verzoek bij het Europees Hof voor de Rechten van de Mens in te dienen. Bij het onderzoek van klachten van individuen moet het onafhankelijke en onpartijdige orgaan toegang hebben tot alle relevante informatie, met inbegrip van vertrouwelijk materiaal. Ten slotte moet het de bevoegdheid hebben om niet-naleving te corrigeren ([129]).

(119) Het Verenigd Koninkrijk heeft ook het Verdrag van de Raad van Europa tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (ETS nr. 108, "Verdrag 108") geratificeerd, en heeft in 2018 het Protocol tot wijziging van het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (bekend als ETS nr. 108+, "Verdrag 108+") ondertekend ([130]). Artikel 9 van Verdrag 108 bepaalt dat afwijkingen van de algemene beginselen inzake gegevensbescherming (artikel 5, Hoedanigheid van de gegevens), van de voorschriften betreffende bijzondere categorieën gegevens (artikel 6, Bijzondere categorieën gegevens) en van de rechten van de betrokkene (artikel 8, Bijkomende waarborgen voor de betrokkene) alleen zijn toegestaan wanneer de wetgeving van de partij in een dergelijke afwijking voorziet en het gaat om een maatregel die in een democratische samenleving noodzakelijk is ter bescherming van de staatsveiligheid, de openbare veiligheid of de monetaire belangen van de staat, ter bestrijding van strafbare feiten, of ter bescherming van de betrokkene of van de rechten en vrijheden van anderen ([131]).

(120) Door zijn lidmaatschap van de Raad van Europa, zijn toetreding tot het Europees Verdrag tot bescherming van de rechten van de mens en zijn onderwerping aan de jurisdictie van het EHRM, is het Verenigd Koninkrijk derhalve onderworpen aan een aantal in het internationaal recht verankerde verplichtingen, die zijn systeem van overheidstoegang inkaderen op basis van beginselen, waarborgen en individuele rechten die vergelijkbaar zijn met die welke door het EU-recht worden gewaarborgd en op de lidstaten van toepassing zijn. Zoals in overweging (19) wordt benadrukt, is de blijvende naleving van dergelijke instrumenten dan ook een bijzonder belangrijk element van de beoordeling waarop dit besluit is gebaseerd.

(121) Bovendien worden in de DPA 2018 specifieke waarborgen en rechten inzake gegevensbescherming gegarandeerd wanneer gegevens worden verwerkt door overheidsinstanties, met inbegrip van rechtshandhavingsinstanties en nationale veiligheidsdiensten.

(122) Met name is de regeling voor de verwerking van persoonsgegevens in het kader van de strafrechtelijke wetshandhaving opgenomen in deel 3 van de DPA 2018, die is vastgesteld ter omzetting van Richtlijn (EU) 2016/680. Deel 3 van de DPA 2018 is van toepassing op de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de uitvoering van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid ([132]).

(123) Het concept „bevoegde autoriteit"wordt in artikel 30 van de DPA gedefinieerd als een in bijlage 7 bij de DPA 2018 vermelde persoon alsook elke andere persoon, voor zover de persoon wettelijke taken uitoefent voor een van de rechtshandhavingsdoeleinden ([133]). Zoals hierboven uitgelegd (zie overweging (139)), mogen bepaalde bevoegde autoriteiten (zoals het National Crime Agency (Nationaal agentschap voor criminaliteitsbestrijding)) onder bepaalde voorwaarden gebruikmaken van de bevoegdheden uit hoofde van de Investigatory Powers Act 2016 (Wet op de onderzoeksbevoegdheden, IPA 2016). In dit geval zijn de waarborgen uit hoofde van de IPA 2016 van toepassing, naast de waarborgen van deel 3 van de DPA 2018. De inlichtingendiensten (Secret Intelligence Service, Security Service en de Government Communications Headquarters) zijn geen onder deel 3 van de DPA 2018 vallende "bevoegde autoriteiten" ([134]) en derhalve zijn de daarin vervatten voorschriften niet op hun activiteiten van toepassing. Een specifiek deel van de DPA 2018 (deel 4) behelst de verwerking van persoonsgegevens door inlichtingendiensten (zie voor meer details overweging (125)).

([129]) Arrest van het Europees Hof voor de Rechten van de Mens, Kennedy/Verenigd Koninkrijk, verzoekschrift nr. 26839/05, ("Kennedy"), punten 167 en 190.

([130]) Voor meer informatie over het Europees Verdrag tot bescherming van de rechten van de mens en de opneming daarvan in de wetgeving van het Verenigd Koninkrijk via de Human Rights Act 1998, alsmede over Verdrag 108, zie overweging (9).

([131]) Evenzo zijn, uit hoofde van artikel 11 van Verdrag 108+, beperkingen van bepaalde specifieke rechten en verplichtingen van het Verdrag ten behoeve van de nationale veiligheid of het voorkomen, onderzoeken en vervolgen van strafbare feiten en de uitvoering van straffen alleen toegestaan indien zij bij wet zijn voorzien, zij de wezenlijke inhoud van de fundamentele rechten en vrijheden eerbiedigen, en zij in een democratische samenleving noodzakelijk en evenredig zijn. Verwerkingsactiviteiten voor nationale veiligheids- en defensiedoeleinden moeten ook onderworpen zijn aan onafhankelijke en doeltreffende toetsing en toezicht uit hoofde van de nationale wetgeving van de respectieve partij bij het verdrag.

([132]) Artikel 31 van de DPA 2018.

([133]) De in bijlage 7 vermelde bevoegde autoriteiten omvatten niet alleen de politiemacht, maar ook alle Britse ministeriële overheidsdiensten alsook alle overige autoriteiten met opsporingstaken (bv. de Commissioner for Her Majesty's Revenue and Customs (de Britse toezichthouder voor douane en accijnzen, the National Crime Agency, the Welsh Revenue Authority (de belastingdienst voor Wales), de Competition and Markets Authority (de Autoriteit concurrentie en markten) of Her Majesty's Land Register (het Britse kadaster)), vervolgingsinstanties, andere strafrechtelijke instanties en andere houders of organisaties die rechtshandhavingsactiviteiten verrichten (daarvan worden in bijlage 7 bij de DPA 2018 de directeurs van de officieren van justitie, de directeur van de officieren van justitie voor Noord-Ierland of de Information Commissioner vermeld).

([134]) Artikel 30, lid 2, van de DPA 2018.

(124) Net als in Richtlijn (EU) 2016/680 worden in deel 3 van de DPA 2018 de beginselen van rechtmatigheid en behoorlijkheid ([135]), doelbinding ([136]), minimale gegevensverwerking ([137]), nauwkeurigheid ([138]), opslagbeperking ([139]) en gegevensbeveiliging ([140]) uiteengezet. De wetgeving legt specifieke transparantieverplichtingen ([141]) op en verleent personen het recht op inzage ([142]), rectificatie en wissing ([143]) en het recht om niet aan geautomatiseerde besluitvorming ([144]) te worden onderworpen. De bevoegde autoriteiten zijn ook verplicht gegevensbescherming door ontwerp en door standaardinstellingen toe te passen, een register van verwerkingsactiviteiten bij te houden en voor bepaalde verwerkingsactiviteiten een privacyeffectbeoordeling uit te voeren en de Information Commissioner vooraf te raadplegen ([145]). Krachtens artikel 56 van de DPA 2018 moeten zij de naleving aantonen. Bovendien moeten zij passende maatregelen nemen om de beveiliging van de verwerking ([146]) te waarborgen en gelden voor hen specifieke verplichtingen in geval van een inbreuk in verband met gegevens, waaronder kennisgeving van dergelijke inbreuken aan de Information Commissioner en de betrokkenen ([147]). Zoals tevens het geval is in Richtlijn (EU) 2016/680, is een verwerkingsverantwoordelijke (tenzij het gaat om een rechter of een andere rechterlijke instantie die in een justitiële hoedanigheid optreedt) verplicht om een functionaris voor gegevensbescherming ([148]) aan te wijzen, die de verwerkingsverantwoordelijke bijstaat bij het nakomen van zijn verplichtingen en bij het toezicht op die nakoming ([149]). Bovendien stelt de wetgeving specifieke eisen aan de internationale doorgifte van persoonsgegevens voor rechtshandhavingsdoeleinden aan derde landen of internationale organisaties, teneinde de continuïteit van de bescherming te waarborgen ([150]). Op dezelfde datum als dit besluit heeft de Commissie een adequaatheidsbesluit [vastgesteld] op grond van artikel 36, lid 3, van Richtlijn (EU) 2016/680, waarin wordt bepaald dat de gegevensbeschermingsregeling die van toepassing is op de verwerking door de Britse strafrechtelijke wetshandhavingsinstanties een beschermingsniveau waarborgt dat in feite overeenkomend is met het niveau dat door Richtlijn (EU) 2016/680 wordt gewaarborgd.

(125) Deel 4 van de DPA 2018 is van toepassing op alle verwerking door of namens de inlichtingendiensten. Het beschrijft met name de belangrijkste beginselen inzake gegevensbescherming (rechtmatigheid, behoorlijkheid en transparantie ([151]); doelbinding ([152]); minimale gegevensverwerking ([153]); nauwkeurigheid ([154]); opslagbeperking ([155]) en gegevensbeveiliging ([156])), stelt voorwaarden aan de verwerking van bijzondere categorieën persoonsgegevens ([157]), voorziet in de rechten van betrokkenen ([158]), vereist gegevensbescherming

([135]) Artikel 35 van de DPA 2018.
([136]) Artikel 36 van de DPA 2018.
([137]) Artikel 37 van de DPA 2018.
([138]) Artikel 38 van de DPA 2018.
([139]) Artikel 39 van de DPA 2018.
([140]) Artikel 40 van de DPA 2018.
([141]) Artikel 44 van de DPA 2018.
([142]) Artikel 45 van de DPA 2018.
([143]) Artikelen 46 en 47 van de DPA 2018.
([144]) Artikelen 49 en 50 van de DPA 2018.
([145]) Artikelen 56 tot en met 65 van de DPA 2018.
([146]) Artikel 66 van de DPA 2018.
([147]) Artikelen 67 en 68 van de DPA 2018.
([148]) Artikel 69 tot en met 71 van de DPA 2018.
([149]) Artikelen 67 en 68 van de DPA 2018.
([150]) Hoofdstuk 5 van deel 3 van de DPA 2018.
([151]) Uit hoofde van artikel 86, lid 6, van de DPA 2018 moet, om de behoorlijkheid en transparantie van de verwerking te bepalen, worden gekeken naar de methode waarmee deze gegevens zijn verkregen. In die zin wordt aan het vereiste van behoorlijkheid en transparantie voldaan indien de gegevens worden verkregen van een persoon die wettelijk gemachtigd of verplicht is ze te verstrekken.
([152]) Uit hoofde van artikel 87 van de DPA 2018 moeten de doeleinden van de verwerking welbepaald, uitdrukkelijk en rechtmatig zijn. De gegevens mogen niet worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor zij worden verzameld. Uit hoofde van artikel 87, lid 3, van de DPA 2018 kan verdere verenigbare verwerking van persoonsgegevens alleen worden toegestaan indien de verwerkingsverantwoordelijke bij wet gemachtigd is om de gegevens voor dat doel te verwerken en de verwerking noodzakelijk en evenredig is met dat andere doel. De verwerking moet als verenigbaar worden beschouwd indien de verwerking bestaat uit verwerking voor archiveringsdoeleinden in het algemeen belang, voor wetenschappelijk of historisch onderzoek of voor statistische doeleinden, en deze verwerking met passende waarborgen is omgeven (artikel 87, lid 4, van de DPA 2018).
([153]) Persoonsgegevens moeten toereikend, ter zake dienend en niet bovenmatig zijn (artikel 88 van de DPA 2018).
([154]) Persoonsgegevens moeten juist en actueel zijn (artikel 89 van de DPA 2018).
([155]) Persoonsgegevens mogen niet langer worden bewaard dan nodig is (artikel 90 van de DPA 2018).
([156]) Het zesde gegevensbeschermingsbeginsel houdt in dat persoonsgegevens op zodanige wijze moeten worden verwerkt dat onder meer passende beveiligingsmaatregelen worden genomen ten aanzien van de risico's die voortvloeien uit de verwerking van persoonsgegevens. De risico's omvatten (maar zijn niet beperkt tot) toevallige of ongeoorloofde toegang tot, of vernietiging, verlies, gebruik, wijziging of openbaarmaking van persoonsgegevens (artikel 91 van de DPA 2018). Artikel 107 vereist ook dat 1) elke verwerkingsverantwoordelijke passende beveiligingsmaatregelen neemt die zijn afgestemd op de risico's die voortvloeien uit de verwerking van persoonsgegevens, en 2) in het geval van geautomatiseerde verwerking, elke verwerkingsverantwoordelijke en elke verwerker preventieve of beschermende maatregelen neemt op basis van een risicobeoordeling.
([157]) Artikel 86, lid 2, punt b), en bijlage 10 bij de DPA 2018.
([158]) Hoofdstuk 3 van deel 4 van de DPA 2018, met name het recht: op inzage, rectificatie en wissing, het recht op bezwaar tegen de verwerking en het recht om niet te worden onderworpen aan geautomatiseerde besluitvorming, om in te grijpen in geautomatiseerde besluitvorming en om te worden geïnformeerd over de besluitvorming. Bovendien moet de verwerkingsverantwoordelijke de betrokkene informatie verstrekken over de verwerking van zijn persoonsgegevens. Zoals uitgelegd in de richtsnoeren van de Information Commissioner over de verwerking door inlichtingendiensten, kunnen personen al hun rechten (met inbegrip van een verzoek om rectificatie) uitoefenen door een klacht in te dienen bij de Information Commissioner of naar de rechter te stappen (zie de richtsnoeren van de Information Commissioner over verwerking door inlichtingendiensten, beschikbaar op https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-intelligence-services-processing/).

door ontwerp ([159]) en regelt de internationale doorgifte van persoonsgegevens ([160]). De Information Commissioner heeft onlangs richtsnoeren uitgegeven over de verwerking door inlichtingendiensten op grond van deel 4 van de DPA 2018 ([161]).

(126) Tegelijkertijd voorziet artikel 110 van de DPA 2018 in een vrijstelling van gespecificeerde bepalingen van deel 4 van de DPA 2018 ([162]), wanneer een dergelijke vrijstelling nodig is om de nationale veiligheid te waarborgen. Op deze vrijstelling kan een beroep worden gedaan op basis van een analyse per geval ([163]). Zoals de Britse autoriteiten hebben uitgelegd en door de rechtspraak is bevestigd, moet een verwerkingsverantwoordelijke "nagaan wat de feitelijke gevolgen voor de nationale veiligheid of defensie zijn indien zij de specifieke gegevensbeschermingsbepaling moeten naleven, en of zij redelijkerwijs de gebruikelijke regel kunnen naleven zonder de nationale veiligheid of defensie in gevaar te brengen" ([164]). Of de vrijstelling al dan niet correct is gebruikt, is onderworpen aan het toezicht van het ICO ([165]).

(127) Bovendien kan een verwerkingsverantwoordelijke met betrekking tot de mogelijkheid om ter waarborging van de "nationale veiligheid" de toepassing van de bovengenoemde gespecificeerde bepalingen overeenkomstig artikel 111 van de DPA 2018 te beperken, een door een minister van het kabinet of de procureur-generaal ondertekend certificaat aanvragen waarin wordt verklaard dat een beperking van dergelijke rechten een noodzakelijke en evenredige maatregel is ter waarborging van de nationale veiligheid ([166]).

(128) De Britse regering heeft richtsnoeren uitgevaardigd om verwerkingsverantwoordelijken te helpen wanneer zij overwegen of zij een nationaleveiligheidscertificaat uit hoofde van de DPA 2018 moeten aanvragen, waarin met name wordt benadrukt dat elke beperking van de rechten van betrokkenen ter bescherming van de nationale veiligheid evenredig en noodzakelijk moet zijn ([167]). Alle nationaleveiligheidscertificaten moet op de website van de Information Commissioner worden gepubliceerd ([168]).

([159]) Artikel 103 van de DPA 2018.

([160]) Artikel 109 van de DPA 2018. Doorgifte van persoonsgegevens aan internationale organisaties of landen buiten het Verenigd Koninkrijk is mogelijk indien de doorgifte een noodzakelijke en evenredige maatregel is die wordt uitgevoerd ten behoeve van de wettelijke taken van de verwerkingsverantwoordelijke, of voor andere doeleinden waarin is voorzien in specifieke artikelen van de Security Service Act 1989 (de Britse wet inzake de veiligheidsdiensten van 1989) en de Intelligence Services Act 1994 (de Britse wet inzake de inlichtingendiensten van 1994).

([161]) Richtsnoeren van de Information Commissioner, zie voetnoot 158.
Artikel 30 van de DPA 2018 en bijlage 7 bij de DPA 2018.

([162]) Artikel 110, lid 2, van de DPA 2018 somt de bepalingen op waarvan vrijstelling is toegestaan. Het omvat de beginselen inzake gegevensbescherming (met uitzondering van het beginsel van rechtmatigheid), de rechten van de betrokkene, de verplichting om de Information Commissioner in kennis te stellen van een inbreuk in verband met persoonsgegevens, de bevoegdheden van de Information Commissioner inzake inzage overeenkomstig internationale verplichtingen, bepaalde handhavingsbevoegdheden van de Information Commissioner, de bepalingen die bepaalde inbreuken op de gegevensbescherming strafbaar stellen, en de bepalingen betreffende bijzondere doeleinden van verwerking, zoals journalistieke, academische of artistieke doeleinden.

([163]) Zie Baker/Secretary of State, zie voetnoot 61.

([164]) Het UK Explanatory Framework for Adequacy Discussions (het Britse toelichtingskader voor de adequaatheidsdiscussie), section H: National Security Data Protection and Investigatory Powers Framework, blz. 15–16 (zie voetnoot 31). Zie ook Baker/Secretary of State (zie voetnoot 61), waarin het Hof een door de minister van Binnenlandse Zaken afgegeven nationaleveiligheidscertificaat nietig verklaarde en de toepassing van de uitzondering ten behoeve van de nationale veiligheid bevestigde, omdat het van oordeel was dat er geen reden was om te voorzien in een algemene uitzondering op de verplichting om verzoeken om inzage te beantwoorden en dat het toestaan van een dergelijke uitzondering in alle omstandigheden, zonder een analyse per geval, verder ging dan wat noodzakelijk en evenredig was voor het waarborgen van de nationale veiligheid.

([165]) Zie het memorandum van overeenstemming tussen het ICO en het UKIC: "Wanneer het ICO een klacht ontvangt van een betrokkene, zal zij zich ervan willen vergewissen dat de zaak correct is afgehandeld en, in voorkomend geval, dat op passende wijze gebruik is gemaakt van een eventuele vrijstelling." Memorandum van overeenstemming tussen de Information Commission's Office (ICO) en de Britse inlichtingengemeenschap (UKIC), punt 16, te raadplegen via de volgende link: https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf

([166]) Met de DPA 2018 is de mogelijkheid om op grond van artikel 28, lid 2, van de Data Protection Act 1998 certificaten af te geven ingetrokken. De mogelijkheid om "oude certificaten" af te geven bestaat echter nog voor zover er sprake is van een historische uitdaging op grond van de wet van 1998 (zie paragraaf 17 van deel 5 van bijlage 20 bij de DPA 2018). Deze mogelijkheid lijkt echter zeer zeldzaam te zijn en is slechts in een beperkt aantal gevallen van toepassing, zoals wanneer een betrokkene protest aantekent tegen het gebruik van de nationaleveiligheidsvrijstelling in verband met een verwerking door een overheidsinstantie die zijn verwerking heeft uitgevoerd op grond van de wet van 1998. Er zij opgemerkt dat in die gevallen artikel 28 van de DPA 1998 in zijn geheel van toepassing zal zijn, derhalve met inbegrip van de mogelijkheid voor de betrokkene om het certificaat voor de rechter aan te vechten.

([167]) Richtsnoeren van de Britse regering inzake nationaleveiligheidscertificaten in het kader van de Data Protection Act 2018, te raadplegen via de volgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf. Volgens de toelichting van de Britse autoriteiten is een certificaat weliswaar een afdoend bewijs dat de vrijstelling van toepassing is op de in het certificaat beschreven gegevens of verwerking, maar neemt het niet weg dat de verwerkingsverantwoordelijke per geval moet nagaan of een beroep op de vrijstelling nodig is.

([168]) Volgens artikel 130 van de DPA 2018, kan de Information Commissioner besluiten de tekst of een deel van de tekst van het certificaat niet te publiceren indien dit zou indruisen tegen het belang van de nationale veiligheid of in strijd met het algemeen belang zou zijn of de veiligheid van personen in gevaar zou kunnen brengen. In die gevallen publiceert de Information Commissioner echter wel het feit dat het certificaat is afgegeven.

(129) Het certificaat moet een vaste geldigheidsduur hebben van ten hoogste vijf jaar, en moet dus regelmatig door het uitvoerende orgaan worden herzien ([169]). Een certificaat identificeert de persoonsgegevens of de categorieën persoonsgegevens waarvoor de vrijstelling geldt, alsook de bepalingen van de DPA 2018 waarop de vrijstelling van toepassing is ([170]).

(130) Het is belangrijk erop te wijzen dat de nationaleveiligheidscertificaten geen bijkomende grond biedt voor het beperken van het recht op gegevensbescherming met het oog op de nationale veiligheid. De verwerkingsverantwoordelijke of de verwerker kan zich met andere woorden alleen op een certificaat beroepen wanneer hij heeft geconcludeerd dat het noodzakelijk is een beroep te doen op de nationaleveiligheidsvrijstelling, die, zoals hierboven is uitgelegd, per geval moet worden toegepast ([171]). Zelfs indien een nationaleveiligheidscertificaat van toepassing is op de betreffende kwestie, kan het ICO onderzoeken of het in een specifiek geval al dan niet gerechtvaardigd was een beroep te doen op de nationaleveiligheidsvrijstelling ([172]).

(131) Eenieder die rechtstreeks wordt geraakt door de afgifte van het certificaat kan bij het Upper Tribunal ([173]) (beroepsrechter) beroep instellen tegen het certificaat ([174]) of, wanneer het certificaat gegevens aanduidt door middel van een algemene beschrijving, de toepassing van het certificaat op specifieke gegevens aanvechten ([175]). Het Upper Tribunal toetst het besluit tot afgifte van een certificaat en beslist of er redelijke gronden waren voor de afgifte van het certificaat ([176]). Het kan een groot aantal kwesties in overweging nemen, waaronder de noodzaak, de evenredigheid en de rechtmatigheid, rekening houdend met het effect op de rechten van de betrokkenen en een afweging van de noodzaak om de nationale veiligheid te waarborgen. Als gevolg daarvan kan het Upper Tribunal bepalen dat het certificaat niet van toepassing is op specifieke persoonsgegevens waartegen het beroep is ingesteld ([177]).

(132) Een andere reeks mogelijke beperkingen betreft de beperkingen die uit hoofde van bijlage 11 bij de DPA 2018 van toepassing zijn op bepaalde bepalingen van deel 4 van de DPA 2018 ([178]) ter bescherming van andere belangrijke doelstellingen van algemeen openbaar belang of beschermde belangen, zoals bijvoorbeeld parlementaire onschendbaarheid, de wettelijke geheimhoudingsplicht, het voeren van gerechtelijke procedures of de gevechtseffectiviteit van de strijdkrachten ([179]). De toepassing van deze bepalingen is ofwel vrijgesteld voor bepaalde categorieën gegevens ("specifieke categorie"), ofwel vrijgesteld voor zover de toepassing van deze bepalingen het beschermde belang zou kunnen schaden ("specifiek belang") ([180]). Er kan slechts een beroep worden gedaan op een vrijstelling op

([169]) Richtsnoeren van de Britse regering inzake nationaleveiligheidscertificaten, punt 15, zie voetnoot 167.
([170]) Richtsnoeren van de Britse regering inzake nationaleveiligheidscertificaten, punt 5, zie voetnoot 167.
([171]) Zie voetnoot 164.
([172]) Artikel 102 van de DPA 2018 vereist dat de verwerkingsverantwoordelijke in staat is aan te tonen dat hij de DPA 2018 heeft nageleefd. Dit houdt in dat een inlichtingendienst aan het ICO moet aantonen dat hij, wanneer hij zich op de vrijstelling beroept, de specifieke omstandigheden van het geval in aanmerking heeft genomen. Het ICO publiceert ook een overzicht van de nationaleveiligheidscertificaten, dat te raadplegen is via de volgende link: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/
([173]) Het Upper Tribunal is de rechterlijke instantie die bevoegd is om kennis te nemen van beroepen tegen beslissingen van lagere administratieve rechtbanken en heeft een specifieke bevoegdheid voor rechtstreekse beroepen tegen beslissingen van bepaalde overheidsinstanties.
([174]) Artikel 111, lid 3, van de DPA 2018.
([175]) Artikel 111, lid 5, van de DPA 2018.
([176]) In de zaak Baker/Secretary of State (zie voetnoot 61) heeft het Information Tribunal een door de minister van Binnenlandse Zaken afgegeven nationaleveiligheidscertificaat nietig verklaard, omdat het van oordeel was dat er geen reden was om te voorzien in een algemene uitzondering op de verplichting om verzoeken om inzage te beantwoorden, en dat het toestaan van een dergelijke uitzondering in alle omstandigheden zonder een analyse per geval verder ging dan wat noodzakelijk en evenredig was voor de bescherming van de nationale veiligheid.
([177]) Richtsnoeren van de Britse regering inzake nationaleveiligheidscertificaten, punt 25, zie voetnoot 167.
([178]) Daarbij gaat het onder meer om: i) de gegevensbeschermingsbeginselen van deel 4, met uitzondering van het vereiste van rechtmatigheid van de verwerking uit hoofde van het eerste beginsel en het feit dat de verwerking moet voldoen aan een van de relevante voorwaarden die zijn opgenomen in de bijlagen 9 en 10; ii) de rechten van betrokkenen; en iii) de verplichtingen in verband met het melden van inbreuken aan het ICO.
([179]) Deel 4 van de DPA 2018 voorziet in het rechtskader dat van toepassing is op alle soorten verwerkingen van persoonsgegevens die door inlichtingendiensten worden uitgevoerd (en niet alleen voor het verrichten van hun taken op het gebied van de nationale veiligheid). Derhalve is deel 4 ook van toepassing wanneer inlichtingendiensten bijvoorbeeld gegevens verwerken met het oog op het beheer van personele middelen, in de context van geschillen of in de context van overheidsopdrachten. De in bijlage 11 vermelde beperkingen zijn voornamelijk bedoeld om in deze andere contexten van toepassing te zijn. In de context van een geschil met een werknemer, kan bijvoorbeeld de beperking met het oog op een "juridische procedure" worden ingeroepen, of in de context van overheidsopdrachten kan de beperking voor "onderhandelingen" worden ingeroepen, enz. Dit komt tot uiting in de richtsnoeren van de Information Commissioner over verwerking door inlichtingendiensten, waarin melding wordt gemaakt van onderhandelingen over een schikking tussen een inlichtingendienst en een voormalig werknemer die een uit de arbeidsverhouding voortvloeiende aanspraak gebruikt als een voorbeeld voor de toepassing van de beperkingen van bijlage 11 (zie voetnoot 161). Er zij tevens opgemerkt dat dezelfde beperkingen voor andere overheidsinstanties beschikbaar zijn overeenkomstig bijlage 2 bij deel 2 van de DPA 2018.
([180]) Volgens het UK Explanatory Framework zijn de uitzonderingen die op een "specifieke categorie" zijn gebaseerd: i) informatie over de toekenning van koninklijke onderscheidingen en waardigheden; ii) de wettelijke geheimhoudingsplicht; iii) vertrouwelijke referenties inzake werk, opleiding of onderwijs; en iv) examenteksten en cijfers. De op een "specifiek belang" gebaseerde uitzonderingen hebben betrekking op de volgende gevallen: i) preventie of opsporing van strafbare feiten; aanhouding en vervolging van overtreders; ii) parlementaire onschendbaarheid; iii) gerechtelijke procedures; iv) de gevechtseffectiviteit van de Britse strijdkrachten; v) het economisch welzijn van het Verenigd Koninkrijk; vi) onderhandelingen met de betrokkene; vii) wetenschappelijk of historisch onderzoek, of statistische doeleinden; viii) archivering in het algemeen belang. Het UK Explanatory Framework for Adequacy Discussions (het Britse toelichtingskader voor de adequaatheidsdiscussie), section H: National Security, blz. 13, zie voetnoot 31.

basis van een specifiek belang voor zover de toepassing van de in de lijst opgenomen gegevensbeschermingsbepaling het betrokken specifieke belang zou kunnen schaden. Het gebruik van een vrijstelling moet derhalve altijd worden gerechtvaardigd door te verwijzen naar de relevante schade die zich in het afzonderlijke geval zou kunnen voordoen. Op vrijstellingen op basis van specifieke categorieën kan alleen een beroep worden gedaan met betrekking tot de specifieke, nauw omschreven categorie gegevens waarvoor de vrijstelling is verleend. Deze zijn qua doel en effect vergelijkbaar met diverse uitzonderingen op de UK GDPR (uit hoofde van bijlage 2 bij de DPA 2018), die op hun beurt een afspiegeling zijn van de uitzonderingen in artikel 23 van de UK GDPR.

(133) Uit het bovenstaande volgt dat er uit hoofde van de toepasselijke wettelijke bepalingen van het Verenigd Koninkrijk, zoals die ook door de rechterlijke instanties en de Information Commissioner worden geïnterpreteerd, beperkingen en voorwaarden gelden om ervoor te zorgen dat deze vrijstellingen en beperkingen binnen de grenzen blijven van wat noodzakelijk en evenredig is om de nationale veiligheid te beschermen.

3.2 **Toegang van en gebruik door de Britse overheidsdiensten met het oog op rechtshandhaving**

(134) De Britse wet legt een aantal beperkingen op aan de toegang tot en het gebruik van persoonsgegevens voor rechtshandhaving, en voorziet in toezichts- en verhaalsmechanismen op dit gebied die in overeenstemming zijn met de in de overwegingen (113) tot en met (115) van dit besluit bedoelde vereisten. De voorwaarden waaronder deze toegang kan plaatsvinden en de waarborgen die van toepassing zijn op het gebruik van deze bevoegdheden worden in de volgende punten in detail beoordeeld.

3.2.1 *Rechtsgrondslag en toepasselijke beperkingen/waarborgen*

(135) Overeenkomstig het in artikel 35 van de DPA 2018 gewaarborgde rechtmatigheidsbeginsel is de verwerking van persoonsgegevens voor een van de rechtshandhavingsdoeleinden alleen rechtmatig indien zij op de wet is gebaseerd en ofwel de betrokkene toestemming heeft gegeven voor de verwerking voor dat doel ([181]), ofwel de verwerking noodzakelijk is voor de uitvoering van een taak die voor dat doel door een bevoegde autoriteit wordt uitgevoerd.

3.2.1.1. Bevelen tot doorzoeking en bevelen tot overlegging

(136) In het Britse rechtskader is het verzamelen van persoonsgegevens van bedrijfsexploitanten, met inbegrip van die welke uit hoofde van het onderhavige adequaatheidsbesluit uit de EU doorgegeven gegevens zouden verwerken, met het oog op de strafrechtelijke wetshandhaving toegestaan op basis van bevelen tot doorzoeking ([182]) en bevelen tot overlegging ([183]).

(137) Bevelen tot doorzoeking worden uitgevaardigd door een rechter, gewoonlijk op verzoek van de opsporingsambtenaar. Zij staan een politieambtenaar toe een pand te betreden om te zoeken naar materiaal of personen die relevant zijn voor zijn onderzoek en om alles waarvoor een huiszoeking is toegestaan, met inbegrip van relevante documenten of materiaal dat persoonsgegevens bevat, in bewaring te nemen ([184]). Een bevel tot overlegging, dat ook door een rechter moet worden uitgevaardigd, verplicht de daarin genoemde persoon ertoe materiaal dat hij in bezit of onder zijn controle heeft, over te

([181]) Het gebruik van toestemming lijkt niet relevant in een adequaatheidsscenario, aangezien de gegevens in een doorgiftesituatie niet rechtstreeks door een Britse rechtshandhavingsinstantie bij een EU-betrokkene zullen zijn verzameld op basis van toestemming.

([182]) Zie voor de relevante rechtsgrondslag artikel 8 e.v. van de Police and Criminal Evidence Act 1984 (Wet inzake politie en strafrechtelijk bewijs, PACE 1984) (voor Engeland en Wales), artikel 10 e.v. van de Police and Criminal Evidence (Northern Ireland) Order 1989 (Besluit inzake politie en strafrechtelijk bewijs, Noord-Ierland) en voor Schotland wordt deze verkregen op grond van het gewoonterecht (zie artikel 46 van de Criminal Justice (Scotland) Act 2016) (Wet strafrechtspleging, Schotland) en artikel 23B van de Criminal Law (Consolidation) (Scotland) Act (Geconsolideerde wet strafrechtspleging, Schotland). Voor bevelen tot doorzoeking die na de aanhouding worden uitgevaardigd, is de rechtsgrondslag artikel 18 van de PACE 1984 (voor Engeland en Wales), artikel 20 e.v. van de Police and Criminal Evidence (Northern Ireland) Order 1989 en voor Schotland wordt deze verkregen op grond van het gewoonterecht (zie artikel 46 van de Criminal Justice (Scotland) Act 2016). De Britse autoriteiten hebben verduidelijkt dat bevelen tot doorzoeking worden uitgevaardigd door een rechter, op verzoek van de opsporingsambtenaar. Zij staan een politieambtenaar toe een pand te betreden om te zoeken naar zaken of personen die relevant zijn voor zijn onderzoek; voor de uitvoering van het arrestatiebevel zal vaak de bijstand van een politieagent nodig zijn.

([183]) Wanneer het onderzoek betrekking heeft op het witwassen van geld (met inbegrip van confiscatie- en civiele terugvorderingsprocedures), zijn de relevante rechtsgrondslagen voor een verzoek om een bevel tot overlegging artikel 345 e.v. voor Engeland, Wales en Noord-Ierland en artikel 380 e.v. van de *Proceeds of Crime Act 2002* (Wet op de opbrengsten uit misdrijven) voor Schotland. Wanneer het onderzoek betrekking heeft op andere zaken dan het witwassen van geld, kan een verzoek om een bevel tot overlegging worden ingediend op grond van artikel 9 van en bijlage 1 bij de PACE 1984 voor Engeland en Wales, en artikel 10 e.v. van de Police and Criminal Evidence (Northern Ireland) Order 1989 voor Noord-Ierland. Voor Schotland wordt deze verkregen op grond van het gewoonterecht (zie artikel 46 van de Criminal Justice (Scotland) Act 2016) en artikel 23B van de Criminal Law (Consolidation) (Scotland) Act. De Britse autoriteiten hebben verduidelijkt dat een bevel tot overlegging de daarin genoemde persoon ertoe verplicht het materiaal waarover hij beschikt of dat hij onder zijn controle heeft, over te leggen of er toegang toe te verlenen (zie punt 4 van bijlage 1 bij de PACE 1984).

([184]) Zo bevat de PACE 1984 in de artikelen 8 en 18 bevoegdheden om alles waarvoor een huiszoeking is toegestaan in beslag te nemen en te bewaren.

leggen of er toegang toe te verlenen. De verzoeker moet voor de rechter onderbouwen waarom het bevel of de beschikking noodzakelijk is, en waarom het in het algemeen belang is. Er zijn verschillende wettelijke bevoegdheden die de uitvaardiging van bevelen tot doorzoeking en bevelen tot overlegging mogelijk maken. Elke bepaling heeft haar eigen reeks wettelijke voorwaarden waaraan moet zijn voldaan voor de uitvaardiging van een bevel tot doorzoeking ([185]) of een bevel tot overlegging ([186]).

(138) Bevelen tot overlegging en bevelen tot doorzoeking kunnen worden aangevochten door middel van rechterlijke toetsing ([187]). Wat de waarborgen betreft, mogen alle strafrechtelijke wetshandhavingsinstanties die onder het toepassingsgebied van deel 3 van de DPA 2018 vallen slechts toegang krijgen tot persoonsgegevens – hetgeen een vorm van verwerking is – overeenkomstig de beginselen en vereisten die

([185]) Zo regelen bijvoorbeeld de artikelen 8 en 18 van de PACE respectievelijk de bevoegdheid van een vrederechter om een bevel tot doorzoeking af te geven en die van een politieambtenaar om een pand te doorzoeken. In het eerste geval (artikel 8) moet de vrederechter, alvorens een bevel tot doorzoeking uit te vaardigen, ervan overtuigd zijn dat er redelijke gronden zijn om aan te nemen dat: i) een strafbaar feit is gepleegd; ii) zich op het adres materiaal bevindt dat (alleen of samen met ander materiaal) van aanzienlijke waarde kan zijn voor het onderzoek naar het strafbare feit; iii) het materiaal waarschijnlijk relevant bewijsmateriaal is; iv) het niet bestaat uit zaken die onder de wettelijke geheimhoudingsplicht vallen of die uitgesloten materiaal of materiaal voor bijzondere procedures bevatten; en v) het niet mogelijk zou zijn om het pand te betreden zonder een bevel tot doorzoeking. In het tweede geval staat artikel 18 een politieambtenaar toe om in het pand van een persoon die is aangehouden voor een strafbaar feit ander materiaal te zoeken dan materiaal dat onder de wettelijke geheimhoudingsplicht valt, indien hij redelijke gronden heeft om te vermoeden dat zich in het pand bewijsmateriaal bevindt dat betrekking heeft op dat strafbare feit of een ander vergelijkbaar of daarmee samenhangend strafbaar feit. Een dergelijke doorzoeking moet beperkt blijven tot het vinden van dat materiaal en er moet schriftelijk toestemming voor worden gegeven door een politieambtenaar met ten minste de rang van inspecteur, tenzij zij noodzakelijk is voor het onderzoek van het strafbare feit. In dat geval moet een politieambtenaar met ten minste de rang van inspecteur daarvan zo spoedig mogelijk na de uitvoering in kennis worden gesteld. De redenen voor de doorzoeking en de aard van het gezochte bewijsmateriaal moeten worden vastgelegd. Bovendien bevatten de artikelen 15 en 16 van de PACE 1984 wettelijke waarborgen die in acht moeten worden genomen bij een verzoek om een bevel tot doorzoeking. In artikel 15 worden de vereisten vastgesteld waaraan moet worden voldaan om een bevel tot doorzoeking te verkrijgen (met inbegrip van de inhoud van het door de politieambtenaar ingediende verzoek en het feit dat in het bevel onder meer moet worden vermeld op grond van welke wet het wordt uitgevaardigd en, voor zover mogelijk, de voorwerpen en personen die moeten worden gezocht en het te doorzoeken pand). Artikel 16 regelt hoe een doorzoeking krachtens een bevel moet worden uitgevoerd (bijvoorbeeld: in artikel 16, lid 5, is bepaald dat de politieambtenaar die het bevel ten uitvoer legt, aan de bewoner een afschrift van het bevel tot doorzoeking verstrekt; in artikel 16, lid 11, is bepaald dat het bevel tot doorzoeking, zodra het is uitgevoerd, gedurende twaalf maanden moet worden bewaard; Artikel 16, lid 12, geeft de bewoner het recht om het bevel tot doorzoeking gedurende die periode in te zien, indien hij dat wenst. Deze artikelen dragen bij tot de naleving van art. 8 EVRM (zie bijvoorbeeld Kent Pharmaceuticals/Director of the Serious Fraud Office [2002] EWHC 3023 (QB) bij [30] van Lord Woolf CJ). Het niet in acht nemen van deze waarborgen kan ertoe leiden dat de doorzoeking onrechtmatig wordt verklaard (zie bijvoorbeeld R (Brook)/Preston Crown Court [2018] EWHC 2024 (Admin), [2018] ACD 95; R (Superior Import/Export Ltd)/Revenue and Customs Commissioners [2017] EWHC 3172 (Admin), [2018] Lloyd's Rep FC 115; en R (F)/Blackfriars Crown Court [2014] EWHC 1541 (Admin)). Artikelen 15 en 16 van de PACE 1984 worden aangevuld met Code B van de PACE, een praktijkcode die de uitoefening van de politiebevoegdheid tot doorzoeking regelt.

([186]) Bij het uitvaardigen van een bevel tot overlegging op grond van de Proceeds of Crime Act 2002 bijvoorbeeld, moeten er niet alleen redelijke aanwijzingen zijn dat is voldaan aan de voorwaarden van artikel 346, lid 2, van de Proceeds of Crime Act, maar moeten er ook redelijke gronden zijn om aan te nemen dat de persoon in het bezit is van of de controle heeft over het gespecificeerde materiaal en dat het materiaal waarschijnlijk van aanzienlijke waarde is. Bovendien geldt voor het uitvaardigen van een bevel tot overlegging ook de voorwaarde dat er redelijke gronden moeten zijn om aan te nemen dat het in het openbaar belang is dat het materiaal wordt overgelegd of dat er toegang toe wordt verleend, gelet op a) het voordeel dat het voor het onderzoek kan opleveren indien het materiaal wordt verkregen; en b) de omstandigheden waaronder de persoon die volgens het verzoek in het bezit lijkt te zijn van of de controle lijkt te hebben over het materiaal, dit materiaal onder zich heeft. Evenzo moet een rechter die een verzoek om een bevel tot overlegging op grond van bijlage 1 bij de PACE 1984 in behandeling neemt, ervan overtuigd zijn dat aan specifieke voorwaarden is voldaan. Bijlage 1 bij de PACE bevat met name twee afzonderlijke, alternatieve reeksen voorwaarden, aan één waarvan moet zijn voldaan voordat een rechter een bevel tot overlegging kan uitvaardigen. De eerste reeks vereist dat de rechter redelijke gronden heeft om aan te nemen dat i) er een strafbaar feit is gepleegd; ii) het op het adres gezochte materiaal bestaat uit materiaal voor bijzondere procedures of dit omvat, maar niet bestaat uit uitgesloten materiaal of dit omvat; iii) het waarschijnlijk is dat het, op zichzelf of samen met ander materiaal, van aanzienlijke waarde is voor het onderzoek; iv) en dat het waarschijnlijk relevant bewijsmateriaal zal zijn; v) andere methoden om het materiaal te verkrijgen zijn geprobeerd of niet zijn geprobeerd omdat zij gedoemd zijn te mislukken; en vi) na afweging van het nut voor het onderzoek en de omstandigheden waarin de betrokkene verkeert, het in het openbaar belang is dat het materiaal wordt overgelegd of dat toegang daartoe wordt verleend. De tweede reeks voorwaarden vereist dat: i) er zich materiaal op het adres bevindt dat bestaat uit materiaal dat onder een bijzondere procedure valt of is uitgesloten; ii) ware het niet dat op basis van vóór de PACE aangenomen wetgeving geen huiszoeking mag worden verricht inzake materiaal dat onder een bijzondere procedure valt, is uitgesloten of onder een wettelijke geheimhoudingsplicht valt, een huiszoekingsbevel voor het materiaal had kunnen worden uitgevaardigd; en iii) het passend zou zijn geweest om een dergelijk bevel tot doorzoeking uit te vaardigen.

([187]) Rechterlijke toetsing is de juridische procedure waarmee de besluiten van een overheidsinstantie kunnen worden aangevochten bij de High Court (hoogste rechterlijke instantie). De High Court "toetst" de aangevochten beslissing en bepaalt of het aannemelijk is dat de beslissing juridisch ondeugdelijk is, rekening houdend met publiekrechtelijke begrippen/beginselen. De belangrijkste gronden voor rechterlijke toetsing zijn: onwettigheid, onredelijkheid, procedurele onregelmatigheid, gewettigd vertrouwen en mensenrechten. Na een geslaagde rechterlijke toetsing kan de High Court een aantal verschillende maatregelen gelasten; waarvan de meest gebruikelijke een bevel tot nietigverklaring is (waarbij het oorspronkelijke besluit – d.w.z. het besluit om een bevel tot doorzoeking uit te vaardigen – wordt vernietigd of ingetrokken); in sommige omstandigheden kan dit ook de toekenning van een financiële vergoeding omvatten. Meer informatie over rechterlijke toetsing in het Verenigd Koninkrijk is te vinden in de publicatie "Judge Over Your Shoulder – a guide to good decision-making" van het Government Legal Department , die via de volgende link kan worden geraadpleegd: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746170/JOYS-OCT-2018.pdf

in de DPA 2018 zijn vastgesteld (zie de overwegingen (122) en (124)). Daarom moet een verzoek van een rechtshandhavingsinstantie in overeenstemming zijn met het beginsel dat de doeleinden van de verwerking welbepaald, uitdrukkelijk en rechtmatig ([188]) moeten zijn en dat de persoonsgegevens die door een bevoegde instantie worden verwerkt, voor dat doel relevant en niet buitensporig ([189]) moeten zijn.

3.2.1.2. Onderzoeksbevoegdheden voor rechtshandhavingsdoeleinden

(139) Met het oog op het voorkomen of opsporen van alleen ernstige strafbare feiten ([190]), kunnen bepaalde rechtshandhavingsinstanties, zoals de National Crime Agency of de korpschef ([191]), gebruikmaken van gerichte onderzoeksbevoegdheden uit hoofde van de IPA 2016. In dit geval zijn de waarborgen uit hoofde van de IPA 2016 van toepassing, naast de waarborgen van deel 3 van de DPA 2018. De specifieke onderzoeksbevoegdheden waarvan die rechtshandhavingsinstanties gebruik kunnen maken, zijn: gerichte intercepties (deel 2 van de IPA 2016), verkrijging van communicatiegegevens (deel 3 van de IPA 2016), bewaring van communicatiegegevens (deel 4 van de IPA 2016) en gerichte materiële interferentie (deel 5 van de IPA 2016). Interceptie heeft betrekking op het verkrijgen van de inhoud van communicatie ([192]), terwijl het verkrijgen en bewaren van communicatiegegevens niet gericht is op het verkrijgen van de inhoud van de communicatie, maar op het "wie", "wanneer", "waar" en "hoe" van de communicatie. Het gaat bijvoorbeeld om het tijdstip en de duur van de communicatie, het telefoonnummer of e-mailadres van de afzender en de ontvanger van de communicatie, en soms de locatie van de apparaten van waaruit de communicatie plaatsvond, de abonnee van een telefoondienst of een gespecificeerde rekening ([193]). Onder materiële interferentie wordt een reeks technieken verstaan die worden gebruikt om allerlei gegevens te verkrijgen uit apparatuur, waaronder computers, tablets en smartphones, maar ook kabels, snoeren en opslagapparaten ([194]).

(140) Gerichte interceptiebevoegdheden kunnen ook worden gebruikt wanneer dat "noodzakelijk is om uitvoering te geven aan de bepalingen van een EU-instrument voor wederzijdse bijstand of een internationale overeenkomst voor wederzijdse bijstand" (het zogeheten "bevel tot wederzijdse bijstand") ([195]). Bevelen tot wederzijdse bijstand worden alleen uitgevaardigd met betrekking tot interceptie, niet met betrekking tot het verkrijgen van communicatiegegevens of materiële interferentie. Deze gerichte bevoegdheden zijn geregeld in de Investigatory Powers Act 2016 ([196]) (Wet op de onderzoeksbevoegdheden, IPA 2016), die samen met de Regulation of Investigatory Powers Act 2000 (RIPA) voor Engeland, Wales en Noord-Ierland en de Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) voor Schotland, voorziet in de rechtsgrondslag en de toepasselijke beperkingen en waarborgen voor het gebruik van dergelijke bevoegdheden vastlegt. De IPA 2016 voorziet ook in de regeling voor het gebruik van onderzoeksbevoegdheden voor bulksgewijze verzameling, hoewel die niet beschikbaar zijn voor rechtshandhavingsinstanties (alleen inlichtingendiensten kunnen er gebruik van maken) ([197]).

([188]) Artikel 36, lid 1, van de DPA 2018.

([189]) Artikel 37 van de DPA 2018.

([190]) Artikel 263, lid 1, van de IPA 2016 bepaalt dat onder een "ernstig misdrijf" wordt verstaan een misdrijf waarvoor van een volwassene, die niet eerder is veroordeeld, redelijkerwijs kan worden verwacht dat hij wordt veroordeeld tot een gevangenisstraf van drie jaar of meer, of waarbij de gedraging gepaard gaat met het gebruik van geweld, aanzienlijk financieel gewin oplevert of het misdrijf door een groot aantal personen wordt gepleegd. Voor de doeleinden van de verkrijging van communicatiegegevens op grond van deel 4 van de IPA 2016 bepaalt artikel 87, lid 10B, bovendien dat onder een "ernstig misdrijf" wordt verstaan een misdrijf waarvoor een gevangenisstraf van twaalf maanden of meer kan worden opgelegd, of een misdrijf dat is gepleegd door een persoon die geen natuurlijke persoon is of waarvan de verzending van een communicatie of een inbreuk op de persoonlijke levenssfeer van een persoon onderdeel is.

([191]) Met name de volgende rechtshandhavingsinstanties kunnen een verzoek om een gericht interceptiebevel indienen: de directeur-generaal van het National Crime Agency (Nationaal agentschap voor criminaliteitsbestrijding), de Commissioner of Police of the Metropolis (politiecommissaris van Londen), de korpschef van de politiedienst van Noord-Ierland, de korpschef van de politiedienst van Schotland, de Commissioner for Her Majesty's Revenue and Customs, het hoofd van Defence Intelligence (Inlichtingendienst van het ministerie van Defensie) en een persoon die een bevoegde instantie is van een land of gebied buiten het Verenigd Koninkrijk voor de toepassing van een EU-instrument voor wederzijdse bijstand of een internationale overeenkomst voor wederzijdse bijstand (artikel 18, lid 1, van de IPA 2016).

([192]) Zie artikel 4 van de IPA 2016.

([193]) Zie artikel 261, lid 5, van de IPA 2016 en de Code of Practice on Bulk Acquisition of Communications Data (Praktijkcode inzake de bulksgewijze verkrijging van communicatiegegevens), te raadplegen via de volgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf, punt 2.9.

([194]) *Code of Practice on Equipment Interference* (Praktijkcode inzake materiële interferentie), te raadplegen via de volgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf, punt 2.2.

([195]) Een bijstandsbevel machtigt een Britse autoriteit om bijstand te verlenen aan een autoriteit buiten het Britse grondgebied met het oog op het onderscheppen en het vrijgeven van het onderschepte materiaal aan die autoriteit, overeenkomstig een internationaal bijstandsinstrument (artikel 15, lid 4, van de IPA 2016).

([196]) De Investigatory Powers Act 2016 (zie: https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted) heeft een aantal wetten betreffende de interceptie van communicatie, materiële interferentie en de verkrijging van communicatiegegevens vervangen, met name deel I van de RIPA 2000, dat het vroegere algemene wetgevingskader vormde voor het gebruik van onderzoeksbevoegdheden door rechtshandhavingsinstanties en nationale veiligheidsdiensten.

([197]) Artikel 138, lid 1, artikel 158, lid 1, artikel 178, lid 1, artikel 199, lid 1, van de IPA 2016.

(141) Om deze bevoegdheden te kunnen uitoefenen, moeten de autoriteiten beschikken over een bevel ([198]) dat is uitgevaardigd door een bevoegde autoriteit ([199]) en is bevestigd door een onafhankelijke Judicial Commissioner ([200]) (rechterlijke toezichthouder) (de zogenaamde "double-lockprocedure"). De verkrijging van een dergelijk bevel is onderworpen aan een noodzakelijkheids- en evenredigheidstoets ([201]). Aangezien deze gerichte onderzoeksbevoegdheden waarin de IPA 2016 voorziet, dezelfde zijn als die waarover de nationale veiligheidsdiensten beschikken, worden de voorwaarden, beperkingen en waarborgen die op dergelijke bevoegdheden van toepassing zijn, uitvoerig behandeld in het artikel over inzage in en gebruik van persoonsgegevens door Britse overheidsinstanties voor nationale veiligheidsdoeleinden (zie overweging (177) e.v.).

3.2.2 *Verder gebruik van de verzamelde informatie*

(142) Het delen van gegevens door een rechtshandhavingsinstantie met een andere autoriteit voor andere doeleinden dan die waarvoor zij oorspronkelijk zijn verzameld (de zogenoemde "verdere doorgifte"), is onderworpen aan bepaalde voorwaarden.

(143) Vergelijkbaar met wat is bepaald in artikel 4, lid 2, van Richtlijn (EU) 2016/680, biedt artikel 36, lid 3, van de DPA 2018 de mogelijkheid dat persoonsgegevens die door een bevoegde instantie voor een rechtshandhavingsdoel zijn verzameld, verder worden verwerkt (door de oorspronkelijke verwerkingsverantwoordelijke of door een andere verwerkingsverantwoordelijke) voor elk ander rechtshandhavingsdoel, mits de verwerkingsverantwoordelijke bij wet gemachtigd is om gegevens voor het andere doel te verwerken en de verwerking noodzakelijk is en in verhouding staat tot dat doel ([202]). In dat geval zijn alle waarborgen van deel 3 van de DPA 2018, waarnaar in de overwegingen (122) en (124) wordt verwezen, van toepassing op de door de ontvangende autoriteit uitgevoerde verwerking.

(144) In de Britse rechtsorde staan verschillende wetten een dergelijke verdere doorgifte uitdrukkelijk toe. Met name i) staat de Digital Economy Act 2017 (Wet inzake de digitale economie) uitwisseling tussen overheidsinstanties voor verschillende doeleinden toe, bijvoorbeeld in geval van fraude tegen de publieke sector die verlies of een risico van verlies voor overheidsinstanties ([203]) met zich meebrengt, of in geval van een schuld aan een overheidsinstantie of aan de Britse Kroon ([204]); ii) de *Crime and Courts Act 2013* (Wet inzake het strafrecht en de gerechten), op grond waarvan gegevens kunnen worden uitgewisseld met het National Crime Agency (NCA) ([205]), voor de bestrijding, het onderzoek en de vervolging van zware en georganiseerde criminaliteit; iii) de *Serious Crime Act 2007* (Wet zware criminaliteit), die overheidsinstanties toestaat informatie te verstrekken aan fraudebestrijdingsorganisaties met het oog op fraudepreventie ([206]).

(145) In deze wetten is uitdrukkelijk bepaald dat de gegevensuitwisseling in overeenstemming moet zijn met de in de DPA 2018 vastgestelde beginselen. Bovendien heeft het College of Policing (College van Politiezaken) een Authorised Professional Practice on Information Sharing ([207]) (Toegestane beroepspraktijken in verband met de gegevensuitwisseling) uitgebracht om de politie te helpen bij het nakomen van haar verplichtingen inzake gegevensbescherming uit hoofde van de UK GDPR, de

([198]) Deel 2, hoofdstuk 2, van de IPA 2016 voorziet in een beperkt aantal gevallen waarin interceptie zonder bevelschrift kan worden uitgevoerd. Daarbij gaat het onder meer om: interceptie met toestemming van de verzender of de ontvanger, interceptie voor administratieve of handhavingsdoeleinden, interceptie in bepaalde instellingen (gevangenissen, psychiatrische ziekenhuizen en inrichtingen voor vreemdelingenbewaring), alsmede interceptie op grond van een internationale overeenkomst ter zake.

([199]) In de meeste gevallen is de Secretary of State de autoriteit die de bevelen uitvaardigt op grond van de IPA 2016, terwijl de Schotse ministers bevoegd zijn om gerichte interceptiebevelen, bevelen tot wederzijdse bijstand en beleven tot gerichte materiële interferentie uit te vaardigen wanneer de te onderscheppen personen of adressen en de te onderscheppen apparatuur zich in Schotland bevinden (zie de artikelen 22 en 103 van de IPA 2016). In geval van gerichte materiële interferentie kan een hoge rechtshandhavingsfunctionaris (als beschreven in deel 1 en deel 2 van bijlage 6 bij de IPA 2016) het bevel uitvaardigen onder de voorwaarden van artikel 106 van de IPA 2016.

([200]) De Judicial Commissioners staan de *Investigatory Powers Commissioner* (toezichthouder voor onderzoeksbevoegdheden, IPC) bij, een onafhankelijk orgaan dat toezicht houdt op het gebruik van onderzoeksbevoegdheden door inlichtingendiensten (zie voor meer details overweging (162) e.v.).

([201]) Zie met name de artikelen 19 en 23 van de IPA 2016.

([202]) Artikel 36, lid 3, van de DPA 2018.

([203]) Artikel 56 van de Digital Economy Act 2017, te raadplegen via de volgende link: https://www.legislation.gov.uk/ukpga/2017/30/section/56

([204]) Artikel 48 van de Digital Economy Act 2017.

([205]) Artikel 7 van de Crime and Courts Act 2013, te raadplegen via de volgende link: https://www.legislation.gov.uk/ukpga/2013/22/section/7

([206]) Artikel 68 van de Serious Crime Act 2007, te raadplegen via de volgende link: https://www.legislation.gov.uk/ukpga/2007/27/contents

([207]) Authorised Professional Practice on information sharing, te raadplegen via de volgende link: https://www.app.college.police.uk/app-content/information-management/sharing-police-information

DPA en de Human Rights Act 1998. Of gegevensuitwisseling in overeenstemming is met het toepasselijke rechtskader voor gegevensbescherming is uiteraard onderworpen aan rechterlijke toetsing ([208]).

(146) Bovendien bepaalt de DPA 2018, naar analogie van wat is bepaald in artikel 9 van Richtlijn (EU) 2016/680, dat persoonsgegevens die voor een rechtshandhavingsdoel zijn verzameld, mogen worden verwerkt voor een doel dat geen rechtshandhavingsdoel is, wanneer de verwerking bij wet is toegestaan ([209]).

(147) Deze vorm van uitwisseling omvat twee scenario's: 1) wanneer een strafrechtelijke wetshandhavingsinstantie gegevens uitwisselt met een civiele wetshandhavingsinstantie anders dan een inlichtingendienst (zoals bijvoorbeeld een financiële of fiscale autoriteit, een mededingingsautoriteit, een bureau voor jeugdzorg enz.); en 2) wanneer een strafrechtelijke wetshandhavingsinstantie gegevens uitwisselt met een inlichtingendienst. In het eerste scenario valt de verwerking van persoonsgegevens zowel onder de werkingssfeer van de UK GDPR als onder deel 2 van de DPA 2018. De Commissie heeft in de overwegingen (12) tot en met (111) de door de UK GDPR en deel 2 van de DPA 2018 geboden waarborgen beoordeeld en is tot de conclusie gekomen dat het Verenigd Koninkrijk een passend beschermingsniveau waarborgt voor persoonsgegevens die binnen de werkingssfeer van de AVG van de Europese Unie naar het Verenigd Koninkrijk worden doorgegeven.

(148) In het tweede scenario, met betrekking tot de uitwisseling van door een strafrechtelijke wetshandhavingsinstantie verzamelde gegevens met een inlichtingendienst ten behoeve van de nationale veiligheid, is artikel 19 van de Counter Terrorism Act 2008 (Wet ter bestrijding van terrorisme, CTA 2008) de rechtsgrondslag die een dergelijke uitwisseling toestaat ([210]). Uit hoofde van deze wet kan eenieder informatie verstrekken aan een van de inlichtingendiensten met het oog op de uitvoering van één van de taken van die dienst, met inbegrip van de "nationale veiligheid".

(149) Wat betreft de voorwaarden waaronder gegevens voor nationale veiligheidsdoeleinden kunnen worden uitgewisseld, beperken de Intelligence Services Act ([211]) en de Security Service Act ([212]) de mogelijkheid van de inlichtingendiensten om gegevens te verkrijgen tot hetgeen noodzakelijk is om hun wettelijke taken te vervullen. Rechtshandhavingsinstanties die gegevens met de inlichtingendiensten willen uitwisselen, moeten rekening houden met een aantal factoren/beperkingen, naast de statutaire taken van de instanties die in de Intelligence Services Act en Security Service Act ([213]) zijn vastgelegd. Artikel 20 van de CTA 2008 maakt duidelijk dat de uitwisseling van gegevens op grond van artikel 19 nog steeds in overeenstemming moet zijn met de wetgeving inzake gegevensbescherming; hetgeen betekent dat alle beperkingen en voorschriften van deel 3 van de DPA 2018 van toepassing zijn. Aangezien de bevoegde autoriteiten voorts overheidsinstanties zijn in de zin van de Human Rights Act 1998, moeten zij ervoor zorgen dat zij handelen in overeenstemming met de verdragsrechten, met inbegrip van artikel 8 van het EVRM. Deze beperkingen zorgen ervoor dat elke uitwisseling van gegevens tussen de rechtshandhavingsinstanties en de inlichtingendiensten in overeenstemming is met de wetgeving inzake gegevensbescherming en het EVRM.

([208]) Zie bijvoorbeeld de zaak M, R/Chief Constable of Sussex Police [2019] EWHC 975 (Admin), waarin de High Court werd gevraagd zich te buigen over de uitwisseling van gegevens tussen de politie en een Business Crime Reduction Partnership (Zakelijk partnerschap voor de bestrijding van criminaliteit, BCRP), een organisatie die bevoegd is om regelingen voor aanzeggingen tot uitsluiting te beheren, waarbij personen de toegang wordt ontzegd tot de bedrijfsruimten van haar leden. De High Court onderzocht de gegevensuitwisseling die plaatsvond op basis van een overeenkomst die tot doel had het publiek te beschermen en criminaliteit te voorkomen, en concludeerde uiteindelijk dat de meeste aspecten van de gegevensuitwisseling rechtmatig waren, behalve met betrekking tot enkele gevoelige gegevens die tussen de politie en de BCRP werden uitgewisseld. Een ander voorbeeld is de zaak Cooper/NCA [2019] EWCA Civ 16, waarin het Court of Appeal (hof van beroep) de gegevensuitwisseling tussen de politie en het Serious Organised Crime Agency (Agentschap ter bestrijding van zware georganiseerde criminaliteit, SOCA), een rechtshandhavingsinstantie die momenteel deel uitmaakt van het NCA, heeft bekrachtigd.

([209]) Artikel 36, lid 4, van de DPA 2018.

([210]) Counter Terrorism Act 2008, te raadplegen via de volgende link: https://www.legislation.gov.uk/ukpga/2008/28/section/19

([211]) Intelligence Services Act 1994, te raadplegen via de volgende link: https://www.legislation.gov.uk/ukpga/1994/13/contents

([212]) Security Service Act 1989, te raadplegen via de volgende link: https://www.legislation.gov.uk/ukpga/1989/5/contents

([213]) Artikel 2, lid 2, van de Intelligence Services Act 1994 bepaalt dat "het hoofd van de inlichtingendienst verantwoordelijk is voor de doeltreffendheid van die dienst en het zijn plicht is ervoor te zorgen: dat er regelingen zijn om te waarborgen dat door de inlichtingendienst geen informatie wordt verkregen behalve voor zover noodzakelijk voor de juiste uitvoering van zijn taken en dat door de inlichtingendienst geen informatie wordt verstrekt, tenzij voor zover noodzakelijk i) voor dat doel; ii) in het belang van de nationale veiligheid; iii) met het oog op het voorkomen of opsporen van ernstige misdrijven; of iv) ten behoeve van een strafrechtelijke procedure; en b) dat de inlichtingendienst geen actie onderneemt om de belangen van een politieke partij in het Verenigd Koninkrijk te bevorderen", terwijl in artikel 2, lid 2, van de Security Service Act van 1989 is bepaald dat "de directeur-generaal verantwoordelijk is voor de doeltreffendheid van de dienst en het zijn taak is ervoor te zorgen a) dat er regelingen zijn om te waarborgen dat de dienst geen informatie verkrijgt, behalve voor zover noodzakelijk voor de goede uitvoering van zijn taken, of verstrekt, behalve voor zover noodzakelijk voor dat doel of met het oog op de preventie of opsporing van ernstige misdrijven of in het kader van strafrechtelijke procedures; dat de dienst geen acties onderneemt om de belangen van een politieke partij te bevorderen; en c) dat er regelingen zijn getroffen, overeengekomen met de directeur-generaal van het National Crime Agency, voor de coördinatie van de activiteiten van de dienst overeenkomstig artikel 1, lid 4, van deze wet met de activiteiten van de politiediensten, het National Crime Agency en andere rechtshandhavingsinstanties".

(150) Wanneer een bevoegde autoriteit voornemens is persoonsgegevens die op grond van deel 3 van de DPA 2018 zijn verwerkt, uit te wisselen met rechtshandhavingsinstanties van een derde land, gelden specifieke vereisten ([214]). Dergelijke doorgiften kunnen met name plaatsvinden wanneer zij gebaseerd zijn op door de Secretary of State vastgestelde adequaatheidsregelingen of, bij gebreke van dergelijke regelingen, wanneer passende waarborgen worden geboden. Artikel 75 van de DPA 2018 bepaalt dat er sprake is van passende waarborgen wanneer deze zijn vastgesteld bij een rechtsinstrument dat de beoogde ontvanger bindt, of wanneer de verwerkingsverantwoordelijke, na alle omstandigheden rond de doorgifte van dat soort persoonsgegevens naar het derde land of de internationale organisatie te hebben beoordeeld, tot de conclusie komt dat er passende waarborgen bestaan om de gegevens te beschermen.

(151) Indien een doorgifte niet is gebaseerd op een adequaatheidsregeling of passende waarborgen, kan deze alleen plaatsvinden in bepaalde, gespecificeerde omstandigheden die "bijzondere omstandigheden" ([215]) worden genoemd. Dit is het geval wanneer de doorgifte noodzakelijk is: a) om de vitale belangen van de betrokkene of van een andere persoon te beschermen; b) om de legitieme belangen van de betrokkene te beschermen; c) ter voorkoming van een onmiddellijk en ernstig gevaar voor de openbare veiligheid van een lidstaat of een derde land; d) in individuele gevallen voor een van de rechtshandhavingsdoeleinden; of e) in individuele gevallen voor een juridisch doeleinde (zoals in verband met een gerechtelijke procedure of om juridisch advies in te winnen). Er zij op gewezen dat de punten d) en e) niet van toepassing zijn indien de rechten en vrijheden van de betrokkene zwaarder wegen dan het openbaar belang van de doorgifte. Deze reeks omstandigheden komt overeen met de specifieke situaties en voorwaarden die in aanmerking komen als "afwijkingen" uit hoofde van artikel 38 van Richtlijn (EU) 2016/680.

(152) Bovendien legt, wanneer het materiaal dat rechtshandhavingsinstanties hebben verkregen in het kader van een bevel tot machtiging tot het gebruik van interceptie of materiële interferentie, aan een derde land wordt overhandigd, de IPA 2016 extra waarborgen op. Met name is een dergelijke verstrekking, die wordt omschreven als "overzeese verstrekking", alleen toegestaan indien de autoriteit van afgifte van oordeel is dat er specifieke passende regelingen zijn getroffen ter beperking van het aantal personen aan wie de gegevens worden verstrekt, de mate waarin materiaal wordt verstrekt of beschikbaar wordt gesteld, alsmede de mate waarin materiaal wordt gekopieerd en het aantal kopieën dat wordt gemaakt. Bovendien kan de autoriteit van afgifte van oordeel zijn dat passende regelingen nodig zijn om ervoor te zorgen dat elke kopie die van enig deel van dat materiaal is gemaakt, wordt vernietigd zodra er geen relevante redenen meer zijn om deze te bewaren (indien deze niet al eerder is vernietigd) ([216]).

(153) Ten slotte zouden in de toekomst specifieke vormen van verdere doorgifte van het Verenigd Koninkrijk naar de Verenigde Staten kunnen plaatsvinden op basis van de "Overeenkomst tussen de regering van het Verenigd Koninkrijk van Groot-Brittannië en Noord-Ierland en de regering van de Verenigde Staten van Amerika inzake de toegang tot elektronische gegevens ten behoeve van de bestrijding van zware criminaliteit" (de "UK–US Agreement" of de "Agreement") ([217]), die in oktober 2019 is gesloten ([218]). Hoewel de UK–US Agreement nog niet in werking is getreden [ten tijde van de vaststelling van dit besluit], kan de te verwachten inwerkingtreding ervan gevolgen hebben voor de verdere doorgifte aan de Verenigde Staten van gegevens die voor het eerst op basis van het besluit aan het Verenigd Koninkrijk zijn doorgegeven. Meer in het bijzonder kunnen gegevens die vanuit de EU aan dienstverleners in het Verenigd Koninkrijk worden doorgegeven, worden onderworpen aan bevelen tot overlegging van elektronisch bewijsmateriaal die door bevoegde rechtshandhavingsinstanties in de Verenigde Staten worden uitgevaardigd en uit hoofde van deze overeenkomst in het Verenigd Koninkrijk van toepassing worden verklaard zodra zij in werking treedt. Om deze redenen is de beoordeling van de voorwaarden en waarborgen waaronder dergelijke bevelen kunnen worden uitgevaardigd en uitgevoerd, relevant voor dit besluit.

([214]) Zie hoofdstuk 5 van deel 3 van de DPA 2018.

([215]) Artikel 76 van de DPA 2018.

([216]) Artikel 54 en artikel 130 van de IPA 2016. De autoriteiten van afgifte moeten nagaan of het nodig is specifieke waarborgen op te leggen voor het materiaal dat aan buitenlandse autoriteiten wordt verstrekt, om ervoor te zorgen dat de gegevens onderworpen zijn aan vergelijkbare waarborgen ten aanzien van bewaring, vernietiging en verstrekking als die welke in artikel 53 en artikel 129 van de IPA 2016 worden opgelegd.

([217]) Overeenkomst tussen de regering van het Verenigd Koninkrijk van Groot-Brittannië en Noord-Ierland en de regering van de Verenigde Staten van Amerika inzake de toegang tot elektronische gegevens met het oog op de bestrijding van zware criminaliteit, te raadplegen via de volgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf

([218]) Dit is de eerste overeenkomst die is bereikt in het kader van de US Clarifying Lawful Overseas Use of Data (CLOUD) Act (Wet ter verduidelijking van wettig overzees gebruik van gegevens). De CLOUD Act is een Amerikaanse federale wet die op 23 maart 2018 is aangenomen en die door middel van een wijziging van de Stored Communications Act (Wet op de opgeslagen communicatie) van 1986 verduidelijkt dat Amerikaanse dienstverleners verplicht zijn gehoor te geven aan Amerikaanse bevelen om inhoud en niet-inhoudelijke gegevens te verstrekken, ongeacht waar die gegevens zijn opgeslagen. De CLOUD Act maakt het ook mogelijk uitvoeringsovereenkomsten te sluiten met buitenlandse overheden, op basis waarvan Amerikaanse dienstverleners inhoudsgegevens rechtstreeks aan deze buitenlandse overheden zouden kunnen verstrekken (de tekst van de CLOUD Act is te raadplegen via de volgende link: https://www.congress.gov/115/bills/s2383/BILLS-115s2383is.pdf).

(154) In dit verband zij er in de eerste plaats op gewezen dat de Agreement, wat de materiële werkingssfeer betreft, alleen van toepassing is op misdrijven waarop een maximumgevangenisstraf van ten minste drie jaar staat (omschreven als een "ernstig misdrijf") ([219]), met inbegrip van "terroristische activiteiten". In de tweede plaats kunnen in het andere rechtsgebied verwerkte gegevens alleen op grond van deze Agreement worden verkregen na een "bevel […] dat volgens het nationale recht van de partij van afgifte door een rechterlijke instantie, een rechter, een vrederechter of een andere onafhankelijke autoriteit voorafgaand aan of in het kader van een procedure betreffende de uitvoering van het bevel wordt getoetst of gecontroleerd" ([220]). Ten derde moet elk bevel "gebaseerd zijn op eisen inzake een redelijke rechtvaardiging op basis van duidelijke en geloofwaardige feiten, bijzonderheid, wettigheid en ernst met betrekking tot het onderzochte gedrag" ([221]) en "gericht zijn op specifieke accounts en een specifieke persoon, account, adres of persoonlijk toestel, of een ander specifiek identificatiekenmerk" ([222]). Ten vierde genieten gegevens die in het kader van deze Agreement zijn verkregen, een bescherming die gelijkwaardig is aan de specifieke waarborgen die worden geboden door de zogenoemde "Overeenkomst tussen de VS en de EU" ([223]) — een uitgebreide gegevensbeschermingsovereenkomst die in december 2016 door de EU en de VS is gesloten en waarin de waarborgen en rechten zijn vastgelegd die van toepassing zijn op gegevensdoorgiften op het gebied van samenwerking bij rechtshandhaving — en die alle door middel van verwijzing in deze Agreement overeenkomstig zijn opgenomen, met name om rekening te houden met de specifieke aard van de doorgiften (d.w.z. doorgiften van particuliere partijen aan een rechtshandhavingsinstantie, in plaats van doorgiften tussen rechtshandhavingsinstanties) ([224]). De UK–US Agreement bepaalt uitdrukkelijk dat gelijkwaardige bescherming als die waarin de Overeenkomst tussen de VS en de EU voorziet, zal worden toegepast "op alle persoonsgegevens die worden geproduceerd bij de uitvoering van bevelen die onder de Agreement vallen, om gelijkwaardige bescherming te bieden" ([225]).

(155) Gegevens die op grond van de UK–US Agreement aan de Amerikaanse autoriteiten worden doorgegeven, moeten derhalve beschermd worden door een EU-wetgevingsinstrument, met de nodige aanpassingen om rekening te houden met de aard van de doorgifte in kwestie. De Britse autoriteiten hebben voorts bevestigd dat de beschermingsmaatregelen van de Overeenkomst tussen de VS en de EU van toepassing zullen zijn op alle in het kader van de Agreement geproduceerde of bewaarde persoonsgegevens, ongeacht de aard of het type van de instantie die het verzoek indient (bv. zowel de Amerikaanse federale rechtshandhavingsinstanties als die van de afzonderlijke staten), zodat in alle gevallen een gelijkwaardige bescherming moet worden geboden. De Britse autoriteiten hebben echter ook uitgelegd dat de details van de concrete uitvoering van de gegevensbeschermingswaarborgen nog onderwerp van gesprek zijn tussen het Verenigd Koninkrijk en de Verenigde Staten. In het kader van de besprekingen met de diensten van de Europese Commissie over dit besluit hebben de Britse autoriteiten bevestigd dat zij de Agreement pas in werking zullen laten treden wanneer zij ervan overtuigd zijn dat de uitvoering ervan in overeenstemming is met de daarin vervatte wettelijke verplichtingen, met inbegrip van duidelijkheid met betrekking tot de naleving van de gegevensbeschermingsnormen voor alle gegevens die op grond van deze Agreement worden opgevraagd. Aangezien een eventuele inwerkingtreding van de Agreement gevolgen kan hebben voor het in dit besluit beoordeelde beschermingsniveau, moeten alle informatie over en elke toekomstige verduidelijking van de wijze waarop de Verenigde Staten aan hun verplichtingen uit hoofde van de Agreement zullen voldoen, door het Verenigd Koninkrijk aan de Europese Commissie worden meegedeeld zodra deze beschikbaar komen en in elk geval voordat de Agreement in werking treedt, teneinde te zorgen voor een passend toezicht op dit besluit in overeenstemming met artikel 45, lid 4, AVG. Bijzondere aandacht zal worden besteed aan de toepassing en aanpassing van de beschermingsmaatregelen van de Overeenkomst tussen de VS en de EU aan het specifieke type doorgiften waarop de UK–US Agreement betrekking heeft.

(156) Meer in het algemeen zal in het kader van de voortdurende toetsing van dit besluit terdege rekening worden gehouden met alle relevante ontwikkelingen met betrekking tot de inwerkingtreding en de toepassing van de Agreement, ook wat betreft de consequenties die moeten worden getrokken indien er aanwijzingen zijn dat een in feite overeenkomend beschermingsniveau niet langer gewaarborgd is.

3.2.3 *Toezicht*

(157) Afhankelijk van de bevoegdheden die de bevoegde autoriteiten gebruiken bij de verwerking van persoonsgegevens voor rechtshandhavingsdoeleinden (op grond van de DPA 2018 of de IPA 2016), zorgen verschillende organen voor het toezicht op het gebruik van deze bevoegdheden. De Information Commissioner houdt met name toezicht op de verwerking van persoonsgegevens wanneer deze onder de werkingssfeer van deel 3 van de DPA 2018

([219]) Artikel 1, lid 14, van de Agreement.
([220]) Artikel 5, lid 2, van de Agreement.
([221]) Artikel 5, lid 1, van de Agreement.
([222]) Artikel 4, lid 5, van de Agreement. Een bijkomende en strengere norm is van toepassing met betrekking tot realtime-interceptie: bevelen moeten van beperkte duur zijn, die niet langer mag zijn dan redelijkerwijs nodig is om het doel van het bevel te verwezenlijken, en mogen alleen worden uitgevaardigd indien dezelfde informatie redelijkerwijs niet met een minder ingrijpende methode kan worden verkregen (artikel 5, lid 3, van de overeenkomst).
([223]) 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, PB L 336 van 10.12.2016, blz. 3, te raadplegen via de volgende link: https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:22016A1210(01)&from=NL
([224]) Artikel 9, lid 1, van de Agreement.
([225]) Artikel 9, lid 1, van de Agreement.

valt ([226]). Onafhankelijk en gerechtelijk toezicht op het gebruik van onderzoeksbevoegdheden uit hoofde van de IPA 2016 wordt gewaarborgd door het *Investigatory Powers Commissioner's Office* (Bureau van de toezichthouder voor onderzoeksbevoegdheden, IPCO) ([227]) (dit onderdeel wordt behandeld in de overwegingen (250) tot en met (255)). Bovendien wordt aanvullend toezicht gewaarborgd door het Britse parlement en door andere organen.

3.2.3.1. Toezicht op deel 3 van de DPA 2018

(158) De algemene functies van het ICO — wier onafhankelijkheid en organisatie in overweging (87) zijn toegelicht — met betrekking tot de verwerking van persoonsgegevens die onder de werkingssfeer van deel 3 van de DPA 2018 vallen, zijn uiteengezet in bijlage 13 van de DPA 2018. De belangrijkste taak van de Information Commissioner is toezicht te houden op deel 3 van de DPA 2018 en de naleving ervan af te dwingen, alsook de bewustmaking van het publiek te bevorderen, het Britse parlement, de regering en andere instellingen en instanties te adviseren. Om de onafhankelijkheid van de rechterlijke macht te handhaven, is de Information Commissioner niet gemachtigd zijn taken uit te oefenen in verband met de verwerking van persoonsgegevens door een individu die in een rechterlijke hoedanigheid optreedt, of door een rechter of rechterlijke instantie in zijn justitiële hoedanigheid. In deze omstandigheden zouden andere organen de toezichtsfuncties uitoefenen, zoals uiteengezet in de overwegingen (99) tot en met (103).

(159) De Information Commissioner heeft algemene bevoegdheden tot onderzoek, correctie, autorisatie en advies met betrekking tot de verwerking van persoonsgegevens waarop deel 3 van toepassing is. De Information Commissioner heeft met name de bevoegdheid om de verwerkingsverantwoordelijke of de verwerker in kennis te stellen van een vermeende inbreuk op deel 3 van de DPA 2018, om waarschuwingen of berispingen te geven aan een verwerkingsverantwoordelijke of een verwerker die bepalingen van deel 3 van de wet heeft geschonden, alsook om op eigen initiatief of op verzoek adviezen uit te brengen aan het Britse parlement, de regering of andere instellingen en instanties, alsook aan het publiek, over elke kwestie in verband met de bescherming van persoonsgegevens ([228]).

(160) Bovendien heeft de Information Commissioner de bevoegdheid om aanzeggingen tot informatie ([229]), aanzeggingen tot beoordeling ([230]) en sommaties tot nakoming ([231]) uit te vaardigen, alsook de bevoegdheid om documenten van verwerkingsverantwoordelijken en verwerkers in te zien, hun gebouwen te betreden ([232]) en administratieve boetes op te leggen in de vorm van sanctiebeschikkingen ([233]). In het *Regulatory Action Policy* (Beleid inzake regelgevende maatregelen) van het ICO wordt uiteengezet onder welke omstandigheden zij respectievelijk aanzeggingen tot informatie, beoordeling, sommaties tot nakoming en sanctiebeschikkingen uitvaardigt ([234]) (zie ook overweging (93) en Richtlijn (EU) 2016/680 adequaatheidsbesluit overwegingen 101–102).

(161) Volgens zijn laatste jaarverslagen (2018–2019 ([235]), 2019–2020 ([236])) heeft de Information Commissioner een aantal onderzoeken verricht en handhavingsmaatregelen genomen met betrekking tot de verwerking van gegevens door rechtshandhavingsinstanties. Zo heeft de Commissioner in oktober 2019 een onderzoek uitgevoerd en een advies gepubliceerd over het gebruik door rechtshandhavingsinstanties van gezichtsherkenningstechnologie in openbare ruimten. Het onderzoek richtte zich met name op het gebruik van live gezichtsherkenning door de politie van Zuid-Wales en de Metropolitan Police Service (Londense Politie, MPS). De Information Commissioner heeft ook de "gangs matrix" ([237]) van de MPS onderzocht en een reeks ernstige inbreuken op de wetgeving inzake gegevensbescherming vastgesteld die het vertrouwen van het publiek in de matrix en in het gebruik van de gegevens waarschijnlijk zullen ondermijnen. In november 2018 heeft de Information Commissioner een sommatie tot nakoming uitgevaardigd en de MPS heeft vervolgens de nodige stappen ondernomen om de beveiliging en de verantwoording te vergroten en ervoor te zorgen dat de gegevens proportioneel werden gebruikt. Een ander voorbeeld van een handhavingsactie op dit gebied is de boete van 325 000 GBP die het ICO in mei 2018 heeft opgelegd aan de Crown Prosecution Service (het Britse openbare

([226]) Artikel 116 van de DPA 2018.
([227]) Zie de IPA 2016 en met name hoofdstuk 1, deel 8.
([228]) Lid 2 van bijlage 13 bij de DPA 2018.
([229]) De verwerkingsverantwoordelijke en de verwerker (en in bepaalde omstandigheden iedere andere persoon) worden gelast de nodige gegevens te verstrekken (artikel 142 van de DPA 2018).
([230]) Staat het uitvoeren van onderzoeken en audits toe, waarbij het nodig kan zijn dat de verwerkingsverantwoordelijke of de verwerker het ICO toestaat om gespecificeerde gebouwen te betreden, documenten of apparatuur te inspecteren of te onderzoeken, mensen te ondervragen die namens de verwerkingsverantwoordelijke persoonsgegevens verwerken (artikel 146 van de DPA 2018).
([231]) Staat de uitoefening toe van corrigerende bevoegdheden, op grond waarvan verwerkingsverantwoordelijken/verwerkers gespecificeerde stappen moeten nemen of nalaten (artikel 149 van de DPA 2018).
([232]) Artikel 154 van de DPA 2018.
([233]) Artikel 155 van de DPA 2018.
([234]) Regulatory Action Policy, zie voetnoot 96.
([235]) Information Commissioner's Annual Report and Financial Statements 2018-19, zie voetnoot 101.
([236]) Information Commissioner's Annual Report and Financial Statements 2019-20, zie voetnoot 82.
([237]) Een gegevensbank waarin inlichtingen werden opgeslagen over vermeende bendeleden en slachtoffers van bendegerelateerde misdrijven.

ministerie), voor het kwijtraken van niet-versleutelde dvd's met opnames van politieverhoren. De Information Commissioner heeft ook onderzoek gedaan naar bredere onderwerpen, bijvoorbeeld in de eerste helft van 2020 naar het gebruik van mobiele telefoon-extractie voor politiedoeleinden en de verwerking van gegevens van slachtoffers door de politie. Bovendien onderzoekt het ICO momenteel een zaak die betrekking heeft op de inzage van rechtshandhavingsinstanties in gegevens die in het bezit zijn van een entiteit uit de particuliere sector, Clearview AI Inc ([238]).

(162) Naast de in de overwegingen (160) en (161) genoemde handhavingsbevoegdheden van de Information Commissioner vormen bepaalde schendingen van de gegevensbeschermingswetgeving strafbare feiten en kunnen derhalve strafmaatregelen worden opgelegd (artikel 196 van de DPA 2018). Dit geldt bijvoorbeeld voor het verkrijgen, verstrekken of bewaren van persoonsgegevens zonder toestemming van de verwerkingsverantwoordelijke en het bewerkstelligen van de verstrekking van persoonsgegevens aan een andere persoon zonder toestemming van de verwerkingsverantwoordelijke ([239]); het heridentificeren van geanonimiseerde persoonsgegevens, zonder de toestemming van de verwerkingsverantwoordelijke die verantwoordelijk is voor het anonimiseren van de persoonsgegevens ([240]); het opzettelijk belemmeren van de uitoefening van de bevoegdheden van het ICO met betrekking tot de inzage in persoonsgegevens overeenkomstig internationale verplichtingen ([241]), het afleggen van valse verklaringen in antwoord op een aanzegging tot informatie, of het vernietigen van gegevens in verband met aanzeggingen tot informatie en sommaties tot nakoming ([242]).

3.2.3.2. Andere toezichthoudende instanties op het gebied van strafrechtelijke wetshandhaving

(163) Naast de Information Commissioner zijn er diverse toezichthoudende instanties op het gebied van strafrechtelijke wetshandhaving met specifieke mandaten die relevant zijn voor gegevensbeschermingsvraagstukken. Hiertoe behoren bijvoorbeeld de Commissioner for the Retention and Use of Biometrical Material (Toezichthouder voor de bewaring en het gebruik van biometrisch materiaal, de "Commissioner for Biometrics") ([243]) en de Surveillance Camera Commissioner (Toezichthouder voor bewakingscamera's) ([244]).

3.2.3.3. Parlementair toezicht op het gebied van strafrechtelijke wetshandhaving

(164) De Home Affairs Select Committee (Beperkte commissie voor binnenlandse zaken, HASC) oefent parlementair toezicht uit op het gebied van de rechtshandhaving. Deze commissie bestaat uit elf parlementsleden, afkomstig uit de drie grootste politieke partijen. De commissie heeft tot taak de uitgaven, het beheer en het beleid van het ministerie van Binnenlandse Zaken en aanverwante overheidsinstanties te onderzoeken, met inbegrip van de politie en het National Crime Agency (NCA), waarvan de commissie de werkzaamheden specifiek kan controleren ([245]).

([238]) Zie de verklaring van het ICO, te raadplegen via de volgende link: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/oaic-and-ico-open-joint-investigation-into-clearview-ai-inc/

([239]) Artikel 170 van de DPA 2018.

([240]) Artikel 171 van de DPA 2018.

([241]) Artikel 119, lid 6, van de DPA 2018.

([242]) In het begrotingsjaar dat de periode van 1 april 2019 tot en met 31 maart 2020 bestrijkt, hebben de onderzoeken van het ICO geleid tot vier waarschuwingen en acht vervolgingen. Deze zaken werden vervolgd op grond van artikel 55 van de Data Protection Act 1998, artikel 77 van de Freedom of Information Act 2000 en artikel 170 van de Data Protection Act 2018. In 75 % van de gevallen pleitten de verdachten schuldig, waardoor langdurige processen met de bijbehorende kosten niet nodig waren. (Information Commissioner's Annual Report and Financial Statements 2019/2020, zie voetnoot 87, blz. 40).

([243]) De Commissioner for Biometrics is aangesteld bij de *Protection of Freedoms Act 2012* (Wet op de bescherming van de vrijheden, PoFa) (zie: https://www.legislation.gov.uk/ukpga/2012/9/contents). De Commissioner for Biometrics beslist, naast andere functies, of de politie al dan niet registers van DNA-profielen en vingerafdrukken mag bewaren die zijn verkregen van personen die zijn aangehouden, maar aan wie geen *qualifying offence* (zwaar misdrijf) ten laste is gelegd (artikel 63G van de PACE 1984). Bovendien heeft de Biometrics Commissioner een algemene verantwoordelijkheid om de bewaring en het gebruik van DNA en vingerafdrukken, en bewaring om redenen van nationale veiligheid, te blijven volgen (artikel 20, lid 2, van de POFA 2012). De Biometric Commissioner wordt genoemd op grond van de Code for Public Appointments (de Britse code voor benoemingen in overheidsfuncties) (de wet is te raadplegen is via de volgende link: https://www.gov.uk/government/publications/governance-code-for-public-appointments) en uit de voorwaarden voor zijn benoeming blijkt duidelijk dat hij alleen onder enkele nauwkeurig omschreven omstandigheden door de minister van Binnenlandse Zaken mag worden afgezet; deze omstandigheden omvatten het niet uitvoeren van zijn taken gedurende een periode van drie maanden, veroordeling voor een strafbaar feit of niet-naleving van de voorwaarden van zijn benoeming.

([244]) De Surveillance Camera Commissioner is ingesteld bij de Protection of Freedoms Act 2012 en heeft als taak de naleving van de *Surveillance Camera Code of Practice* (Praktijkcode voor bewakingscamera's) te bevorderen; de werking van deze praktijkcode te toetsen; en advies uit te brengen aan ministers over de mogelijke noodzaak tot wijziging van deze praktijkcode. De Commissioner wordt benoemd volgens dezelfde regels als de the Biometrics Commissioners en beschikt over soortgelijke bevoegdheden, middelen en bescherming tegen afzetting.

([245]) Zie https://committees.parliament.uk/committee/83/home-affairs-committee/news/100537/work-of-the-national-crime-agency-scrutinised/

(165) De commissie kan, binnen de grenzen van haar mandaat, haar eigen enquêteonderwerpen kiezen, met inbegrip van specifieke gevallen, zolang de zaak niet onder de rechter is. De commissie kan ook schriftelijke en mondelinge informatie inwinnen bij een breed scala van relevante groepen en personen. Zij brengt verslag uit over haar bevindingen en doet aanbevelingen aan de regering ([246]). De regering moet binnen 60 dagen reageren op elk van de aanbevelingen in het verslag ([247]).

(166) Op het gebied van bewaking heeft de commissie ook een verslag opgesteld over de Regulation of Investigatory Powers Act 2000 ([248]) (Wet op de regulering van onderzoeksbevoegdheden, RIPA 2000), waarin werd vastgesteld dat de RIPA 2000 niet geschikt was voor het beoogde doel. Het verslag is in aanmerking genomen bij de vervanging van belangrijke delen van de RIPA 2000 door de IPA 2016. Een volledige lijst van enquêtes is te vinden op de website van de commissie ([249]).

(167) De taken van de HASC worden in Schotland uitgeoefend door de Justice Subcommittee on Policing (subcommissie Justitie inzake politie) en in Noord-Ierland door de Committee for Justice ([250]) (commissie voor Justitie).

3.2.4 *Verhaalmogelijkheden*

(168) Wat de verwerking van gegevens door rechtshandhavingsinstanties betreft, zijn er verhaalsmechanismen beschikbaar uit hoofde van deel 3 van de DPA 2018 en uit hoofde van de IPA 2016, alsook uit hoofde van de Human Rights Act 1998.

(169) Deze reeks mechanismen biedt betrokkenen doeltreffende administratieve en justitiële verhaalsmogelijkheden, waardoor zij met name hun rechten kunnen doen gelden, waaronder het recht op inzage in hun persoonsgegevens of op rectificatie of wissing van die gegevens.

(170) Ten eerste heeft een betrokkene uit hoofde van artikel 165 van de DPA 2018 het recht om een klacht in te dienen bij de Information Commissioner indien de betrokkene van mening is dat er in verband met persoonsgegevens met betrekking tot de betrokkene sprake is van een inbreuk op deel 3 van de DPA 2018 ([251]). De Information Commissioner heeft de bevoegdheid om te beoordelen of de verwerkingsverantwoordelijke en de verwerker de DPA 2018 naleven, hen te verplichten de nodige stappen te ondernemen in geval van niet-naleving en boetes op te leggen.

([246]) Beperkte commissies, met inbegrip van de HASC, zijn onderworpen aan de standing orders (het reglement van orde) van het Britse Lagerhuis. Standing orders zijn de door het Lagerhuis overeengekomen regels voor de manier waarop het parlement zaken afhandelt. De opdracht van de beperkte commissies is ruim, want in lid 1 van Standing Order 152 is bepaald dat "beperkte commissies worden ingesteld om de uitgaven, het beheer en het beleid te onderzoeken van de voornaamste regeringsdepartementen als vermeld in lid 2 van deze Standing Order en de daarmee verbonden openbare organen". Hierdoor kan de HASC elk beleid van het ministerie van Binnenlandse Zaken bekijken, met inbegrip van het beleid (en de daarmee samenhangende wetgeving) inzake onderzoeksbevoegdheden. Bovendien wordt in lid 4 van Standing Order 152 duidelijk gemaakt dat de commissies diverse bevoegdheden hebben, waaronder de mogelijkheid om personen te verzoeken bewijsstukken of documenten over een bepaalde kwestie te verstrekken, en om verslagen op te stellen. De huidige en eerder uitgevoerde onderzoeken van de commissie zijn te raadplegen via de volgende link: https://committees.parliament.uk/committee/83/home-affairs-committee/

([247]) De bevoegdheden van de HASC in Engeland en Wales zijn uiteengezet in de standing orders van het Britse Lagerhuis, die via de volgende link kunnen worden geraadpleegd: https://www.parliament.uk/business/publications/commons/standing-orders-public11/

([248]) Zij zijn via de volgende link te raadplegen: https://publications.parliament.uk/pa/cm201415/cmselect/cmhaff/711/71103.htm

([249]) Zij zijn via de volgende link te raadplegen: https://committees.parliament.uk/committee/83/home-affairs-committee

([250]) Het reglement van het Justice Subcommittee on Policing in Schotland is via de volgende link te raadplegen: https://www.parliament.scot/parliamentarybusiness/CurrentCommittees/justice-committee.aspx, en het reglement van het Committee for Justice in Noord-Ierland is te raadplegen via de volgende link: http://www.niassembly.gov.uk/assembly-business/standing-orders/

([251]) Het laatste jaarverslag van het ICO bevat een uitsplitsing van de aard van de ontvangen en afgehandelde klachten. In het bijzonder bedraagt het aantal ontvangen klachten over "politie en strafregisters" 6 % van het totale aantal ontvangen klachten (een stijging van 1 % ten opzichte van het vorige begrotingsjaar). Uit het jaarverslag blijkt ook dat klachten over inzageverzoeken van betrokkenen het hoogste aantal vertegenwoordigen (46 % van het totale aantal klachten, een stijging van 8 % ten opzichte van het vorige begrotingsjaar) (jaarverslag 2019–2020 van de Information Commissioner, blz. 55; zie voetnoot 88).

(171) Ten tweede voorziet de DPA 2018 in het recht op een rechtsmiddel tegen de Information Commissioner indien deze een klacht van de betrokkene niet naar behoren afhandelt. Meer in het bijzonder heeft de klager, indien de Information Commissioner geen "vooruitgang" ([252]) boekt met een door de betrokkene ingediende klacht, toegang tot een rechtsmiddel, aangezien hij een beroep kan doen op een First Tier Tribunal ([253]) (rechter in eerste aanleg) om het ICO te gelasten passende stappen te ondernemen om op de klacht te reageren, of om de klager te informeren over de vooruitgang met betrekking tot de klacht ([254]). Bovendien kan eenieder die een van de genoemde kennisgevingen (aanzeggingen tot informatie, beoordeling, sommaties tot nakoming of sanctiebeschikkingen) van de Information Commissioner heeft gekregen, in beroep gaan bij een First Tier Tribunal. Als het Tribunal oordeelt dat het besluit van de Commissioner niet in overeenstemming is met de wet of dat de Information Commissioner zijn bevoegdheid op een andere wijze had moeten uitoefenen, moet het Tribunal het ingestelde beroep toestaan of de aanzegging/sommatie/beschikking of het besluit vervangen door een andere aanzegging/sommatie/beschikking of een ander besluit die/dat door de Information Commissioner had kunnen worden afgegeven of genomen ([255]).

(172) Ten derde kunnen personen rechtstreeks bij de rechterlijke instanties rechtsvorderingen instellen tegen verwerkingsverantwoordelijken en verwerkers. Met name kan een betrokkene uit hoofde van artikel 167 van de DPA 2018 bij een rechter een verzoek indienen wegens een inbreuk op zijn recht uit hoofde van de gegevensbeschermingswetgeving en kan de rechter door middel van een bevel de verwerkingsverantwoordelijke verzoeken met betrekking tot de verwerking elke maatregel te nemen (of zich daarvan te onthouden) om te voldoen aan de DPA 2018. Bovendien heeft uit hoofde van artikel 169 van de DPA 2018 eenieder die schade heeft geleden als gevolg van een schending van een voorschrift van de gegevensbeschermingswetgeving (met inbegrip van deel 3 van de DPA 2018), anders dan de UK GDPR, recht op vergoeding van die schade door de verwerkingsverantwoordelijke of de verwerker, tenzij de verwerkingsverantwoordelijke of de verwerker bewijst dat de verwerkingsverantwoordelijke of de verwerker op geen enkele wijze verantwoordelijk is voor de gebeurtenis die de schade heeft doen ontstaan. Schade omvat zowel financiële verliezen als schade zonder financiële verliezen, zoals smart.

(173) Ten slotte kan eenieder die van oordeel is dat zijn rechten, met inbegrip van het recht op bescherming van de persoonlijke levenssfeer en gegevensbescherming, door overheidsinstanties zijn geschonden, uit hoofde van de Human Rights Act 1998 ([256]) verhaal halen bij de Britse rechter, en kunnen personen, niet-gouvernementele organisaties en groepen personen, nadat de nationale rechtsmiddelen zijn uitgeput, bij het Europees Hof voor de Rechten van de Mens verhaal halen wegens schendingen van de rechten die door het Europees Verdrag tot bescherming van de rechten van de mens ([257]) worden gewaarborgd (zie overweging (111)).

3.2.4.1. Beschikbare verhaalmogelijkheden uit hoofde van de IPA 2016

(174) Personen kunnen bij het Investigatory Powers Tribunal (gerecht dat toezicht uitoefent op de onderzoeksbevoegdheden) beroep instellen tegen schendingen van de IPA 2016. De verhaalsmogelijkheden die in het kader van de IPA 2016 beschikbaar zijn, worden beschreven in de overwegingen (263) tot en met (269).

([252]) Artikel 166 van de DPA 2018 verwijst specifiek naar de volgende situaties: a) het ICO nalaat de nodige stappen te ondernemen om op de klacht te antwoorden, b) het ICO nalaat de klager te informeren over de vooruitgang in verband met de klacht of over het resultaat van de klacht vóór het einde van de periode van 3 maanden die begon op het moment dat het ICO de klacht ontving, of c) als de behandeling van de klacht door het ICO niet binnen die periode wordt afgesloten, nalaat de klager dergelijke informatie gedurende een daaropvolgende periode van 3 maanden te verstrekken.

([253]) De First Tier Tribunal is de rechterlijke instantie die bevoegd is beroepen tegen besluiten van regelgevende overheidsinstanties te behandelen. In het geval van een beslissing van de Information Commissioner is de bevoegde kamer de General Regulatory Chamber (Algemene regelgevende kamer), die bevoegd is voor het gehele Verenigd Koninkrijk.

([254]) Artikel 166 van de DPA 2018. Voorbeelden van acties tegen de Information Commissioner die door het Tribunal zijn toegewezen omvatten een zaak waarin de Information Commissioner de ontvangst van een klacht van een betrokkene bevestigde, maar niet aangaf welke actie zij van plan was te ondernemen, en daarom werd gelast binnen 21 kalenderdagen te bevestigen of zij de klachten zou onderzoeken en, zo ja, de klager vervolgens ten minste om de 21 kalenderdagen op de hoogte te houden van de voortgang van het onderzoek (het arrest is nog niet gepubliceerd), en een zaak waarin het First Tier Tribunal van oordeel was dat het onduidelijk was of het antwoord van de Information Commissioner aan een klager het "resultaat" van de klacht vormde (zie Susan Milne/Information Commissioner [2020], arrest te raadplegen via de volgende link: https://informationrights.decisions.tribunals.gov.uk/DBFiles/Decision/i2730/Milne,%20S%20-%20QJ2020-0296-GDPR-V,%20051220%20Section%20166%20DPA%20-DECISION.pdf).

([255]) Artikelen 162 en 163 van de DPA 2018.

([256]) Zie bijvoorbeeld Brown/Commissioner of Police of the Metropolis & Anor [2019] EWCA Civ 1724, waar een schadevergoeding van 9 000 GBP werd toegekend op grond van de DPA 1998 en de Human Rights Act 1998 wegens het onrechtmatig verkrijgen en misbruiken van persoonsgegevens, en R (op verzoek van Bridges)/Chief Constable of South Wales [2020] EWCA Civ 1058, waarbij het hof van beroep de inzet van een gezichtsherkenningssysteem door de politie van Wales onwettig heeft verklaard, aangezien dit in strijd was met artikel 8 EVRM en de door de verwerkingsverantwoordelijke opgestelde prviacyeffectbeoordeling niet in overeenstemming was met de DPA 2018.

([257]) Artikel 34 van het Europees Verdrag tot bescherming van de rechten van de mens bepaalt: "Het Hof kan verzoekschriften ontvangen van ieder natuurlijk persoon, iedere niet-gouvernementele organisatie of iedere groep personen die beweert slachtoffer te zijn van een schending door een van de Hoge Verdragsluitende Partijen van de rechten die in het Verdrag of de Protocollen daarbij zijn vervat. De Hoge Verdragsluitende Partijen verplichten zich ertoe de doeltreffende uitoefening van dit recht op generlei wijze te belemmeren."

3.3 **Toegang van en gebruik door de Britse overheidsdiensten ten behoeve van de nationale veiligheid**

(175) De inlichtingendiensten die, om redenen van nationale veiligheid, gemachtigd zijn om in situaties die relevant zijn voor een adequaatheidsscenario elektronische informatie te verzamelen die in het bezit is van verwerkingsverantwoordelijken of verwerkers, zijn in de Britse rechtsorde de Security Service ([258]) (Britse veiligheidsdienst) (MI5), de Secret Intelligence Service ([259]) (Britse geheime dienst, MI6) (SIS) en de Government Communication Headquarters ([260]) (GCHQ, het communicatiehoofdkwartier van de Britse regering) ([261]).

3.3.1 *Rechtsgrondslagen, beperkingen en waarborgen*

(176) In het Verenigd Koninkrijk zijn de bevoegdheden van de inlichtingendiensten vastgelegd in de IPA 2016 en de RIPA 2000, waarin, net als in de DPA 2018, het materiële en persoonlijke toepassingsgebied van deze bevoegdheden alsook de beperkingen en waarborgen voor het gebruik ervan wordt vastgesteld. Deze bevoegdheden, alsmede de beperkingen en waarborgen die erop van toepassing zijn, worden in de volgende punten in detail beoordeeld.

3.3.1.1. Onderzoeksbevoegdheden die worden uitgeoefend in het kader van de nationale veiligheid

(177) De IPA 2016 biedt het rechtskader voor het gebruik van onderzoeksbevoegdheden, d.w.z. de bevoegdheid om communicatiegegevens te onderscheppen, inzage daarin te verkrijgen en apparatuur te verstoren. De IPA 2016 voert een algemeen verbod in en stelt het strafbaar om zonder wettig gezag technieken te gebruiken waarmee toegang tot de inhoud van communicatie, toegang tot communicatiegegevens of materiële interferentie mogelijk is ([262]). Dit komt tot uiting in het feit dat het gebruik van deze onderzoeksbevoegdheden alleen rechtmatig is wanneer het wordt uitgevoerd op basis van een bevel of een machtiging ([263]).

(178) In de IPA 2016 zijn gedetailleerde voorschriften betreffende de draagwijdte en de toepassing van elke onderzoeksbevoegdheid alsook de specifieke beperkingen en waarborgen ervan neergelegd. Er gelden verschillende regels naar gelang van het soort onderzoeksbevoegdheid (interceptie van communicatie,

([258]) De MI5 staat onder het gezag van de minister van Binnenlandse Zaken. In de Security Service Act van 1989 worden de taken van de MI5 als volgt omschreven: bescherming van de nationale veiligheid (waaronder bescherming tegen bedreigingen door spionage, terrorisme en sabotage, tegen activiteiten van agenten van buitenlandse mogendheden en tegen acties die erop gericht zijn de parlementaire democratie met politieke, industriële of gewelddadige middelen omver te werpen of te ondermijnen), bescherming van het economisch welzijn van het Verenigd Koninkrijk tegen bedreigingen van buitenaf en ondersteuning van de activiteiten van de politiediensten en andere rechtshandhavingsinstanties op het gebied van preventie en opsporing van ernstige misdrijven.

([259]) De SIS staat onder het gezag van de minister van Buitenlandse Zaken. De taken van deze dienst zijn omschreven in de Intelligence Services Act van 1994. Hij heeft tot taak informatie te verkrijgen en te verstrekken over de handelingen of bedoelingen van personen buiten de Britse eilanden en andere taken te verrichten met betrekking tot de handelingen of bedoelingen van deze personen. Deze functies kunnen alleen worden uitgeoefend in het belang van de nationale veiligheid, in het belang van het economisch welzijn van het Verenigd Koninkrijk of ter ondersteuning van de preventie of opsporing van ernstige misdrijven.

([260]) Het GCHQ staat onder het gezag van de minister van Buitenlandse Zaken. De functies zijn vastgelegd in de Intelligence Services Act van 1994. Deze functies zijn a) het monitoren van, het gebruikmaken van of verstoren van elektromagnetische en andere emissies en apparatuur die dergelijke emissies voortbrengt, het verkrijgen en verstrekken van informatie die is afgeleid van of verband houdt met dergelijke emissies of apparatuur en van versleuteld materiaal; b) het verstrekken van advies en bijstand inzake talen, met inbegrip van terminologie voor technische aangelegenheden en cryptografie en andere aangelegenheden in verband met de bescherming van informatie aan de strijdkrachten, aan de regering of aan andere organisaties of personen die geschikt worden geacht. Deze functies kunnen alleen worden uitgeoefend in het belang van de nationale veiligheid, in het belang van het economisch welzijn van het Verenigd Koninkrijk in verband met de handelingen of bedoelingen van personen buiten de Britse eilanden of ter ondersteuning van de preventie of opsporing van ernstige misdrijven.

([261]) Andere overheidsinstanties die functies uitoefenen die van belang zijn voor de nationale veiligheid zijn de Defence Intelligence (Inlichtingendienst van Defensie, DI), de National Security Council and Secretariat (Nationale Veiligheidsraad en het Secretariaat), de Joint Intelligence Organisation (Gemeenschappelijke Inlichtingenorganisatie, JIO) en de Joint Intelligence Committee (Gemeenschappelijke Inlichtingencommissie, JIC). Noch de JIC, noch de JIO kunnen echter gebruikmaken van onderzoeksbevoegdheden uit hoofde van de IPA 2016, terwijl de DI beperkte mogelijkheden heeft om zijn bevoegdheden te gebruiken.

([262]) Het verbod geldt zowel voor openbare als voor particuliere communicatienetwerken, alsmede voor de openbare posterijen wanneer de interceptie in het Verenigd Koninkrijk wordt uitgevoerd. Het verbod geldt niet voor de beheerder van het privénetwerk indien de verwerkingsverantwoordelijke uitdrukkelijk of stilzwijgend toestemming heeft gegeven om de interceptie uit te voeren (deel 3 van de IPA 2016).

([263]) In specifieke beperkte gevallen is wettige interceptie zonder bevel mogelijk, namelijk bij interceptie met toestemming van de verzender of de ontvanger (artikel 44 van de IPA 2016), in geval van beperkte administratieve of handhavingsdoeleinden (artikelen 45–48 van de IPA), in bepaalde bijzondere instellingen (artikelen 49–51 van de IPA 2016) en in overeenstemming met verzoeken van overzeese gebieden (artikel 52 van de IPA 2016).

verkrijgen en bewaren van communicatiegegevens en materiële interferentie) ([264]), en naar gelang van de vraag of de bevoegdheid wordt uitgeoefend ten aanzien van een specifiek doelwit of bulksgewijze verzameling. Details over het toepassingsgebied, de waarborgen en de beperkingen van elke maatregel uit hoogde van de IPA 2016 worden in het specifieke deel hieronder beschreven.

(179) De IPA 2016 wordt bovendien aangevuld met een aantal door de minister uitgevaardigde, door beide kamers van het Britse parlement ([265]) goedgekeurde en in het gehele land toepasselijke praktijkcodes, die verdere richtsnoeren bevatten voor het gebruik van deze bevoegdheden ([266]). Hoewel betrokkenen voor de uitoefening van hun rechten rechtstreeks een beroep kunnen doen op de bepalingen die in de IPA 2016 zijn neergelegd, is in bijlage 7, punt 5, van de IPA 2016 bepaald dat de praktijkcodes toelaatbaar zijn als bewijs in civiele en strafrechtelijke procedures, en dat de rechterlijke instantie, het gerecht of de toezichthoudende autoriteit bij de vaststelling van een relevante kwestie in een gerechtelijke procedure rekening mag houden met niet-naleving van de praktijkcodes ([267]). De Grote Kamer van het Europees Hof voor de Rechten van de Mens heeft in de context van zijn beoordeling van de "kwaliteit van het recht" van de eerdere Britse wetgeving op het gebied van bewaking, de RIPA 2000, uitdrukkelijk de relevantie van de Britse praktijkcodes erkend en aanvaard dat de bepalingen ervan in aanmerking kunnen worden genomen bij de beoordeling van de voorzienbaarheid van de wetgeving die bewaking toestaat ([268]).

(180) Voorts zij opgemerkt dat gerichte bevoegdheden (gerichte interceptie ([269]), verkrijging van communicatiegegevens ([270]), bewaring van communicatiegegevens ([271]) en gerichte materiële interferentie ([272])) ter beschikking staan van nationale veiligheidsdiensten en bepaalde rechtshandhavingsinstanties ([273]), terwijl alleen inlichtingendiensten gebruik kunnen maken van bevoegdheden voor bulksgewijze verzameling (d.w.z. bulksgewijze interceptie ([274]), bulksgewijze verkrijging van communicatiegegevens ([275]), bulksgewijze materiële interferentie ([276]) en bulkdatasets met persoonsgegevens ([277])).

(181) Om te bepalen welke onderzoeksbevoegdheid moet worden gebruikt, moet de inlichtingendienst voldoen aan de "algemene plichten met betrekking tot de persoonlijke levenssfeer" die zijn opgesomd in artikel 2, lid 2, punt a), van de IPA 2016, waaronder een noodzakelijkheids- en evenredigheidstoets. Meer in het bijzonder moet volgens deze bepaling een overheidsinstantie die voornemens is een onderzoeksbevoegdheid te gebruiken i) nagaan of hetgeen

([264]) Met betrekking tot het voorbeeld van het toepassingsgebied van die maatregelen, op grond van deel 3 en deel 4 (bewaring en verkrijging van communicatiegegevens), houdt het toepassingsgebied van de maatregel nauw verband met de definitie van "telecommunicatie-exploitanten" van wie de gebruikersgegevens onder de maatregel vallen. Een ander voorbeeld kan worden gegeven in verband met het gebruik van bevoegdheden "voor bulksgewijze verzameling". In dit geval is het toepassingsgebied van deze bevoegdheden beperkt tot "berichten die worden verzonden of ontvangen door personen die zich buiten de Britse eilanden bevinden".

([265]) In bijlage 7 bij de IPA 2016 zijn de werkingssfeer van de praktijkcodes, de te volgen procedure bij de uitvaardiging ervan, de regels voor de herziening ervan en de gevolgen van de praktijkcodes vastgesteld.

([266]) De praktijkcodes uit hoofde van de IPA 2016 zijn te raadplegen via de volgende link: https://www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice

([267]) De rechters en gerechten gebruiken de praktijkcodes om de rechtmatigheid van het gedrag van de autoriteiten te beoordelen. Zie bijvoorbeeld: Dias/Cleveland Police, [2017] UKIPTrib15_586-CH, waarbij het Investigatory Powers Tribunal verwees naar specifieke passages van de Code of Practice on Communication Data (Praktijkcode inzake communicatiegegevens) om de definitie te begrijpen van de grond "voorkoming of opsporing van strafbare feiten dan wel voorkoming van ordeverstoring" die wordt gebruikt voor het verzoek om de verkrijging van communicatiegegevens. De praktijkcode werd opgenomen in de motivering om na te gaan of die grond onjuist was gebruikt. De rechter concludeerde vervolgens dat de litigieuze gedragingen onrechtmatig waren. Rechters hebben ook een beoordeling gemaakt van het niveau van de in de praktijkcodes beschikbare waarborgen, zie bijvoorbeeld Just for Law Kids/Secretary of State for the Home Department [2019] EWHC 1772 (Admin), waarin de High Court oordeelde dat de primaire en secundaire wetgeving samen met de interne richtsnoeren voldoende waarborgen boden; of R (National Council for Civil Liberties)/Secretary of State for the Home Department e.a. [2019] EWHC 2057 (Admin), waarin de rechter oordeelde dat zowel de IPA 2016 als de Code of Practice on Equipment Interference voldoende bepalingen bevatten met betrekking tot de noodzaak van specificiteit van bevelen.

([268]) In de zaak Big Brother Watch merkte de Grote Kamer van het Europees Hof voor de Rechten van de Mens op dat "De IC-code een door beide kamers van het parlement goedgekeurd openbaar document is dat online en op papier door de regering wordt gepubliceerd en dat in aanmerking moet worden genomen door personen die interceptietaken uitoefenen en door rechterlijke instanties (zie de punten 93 en 94). Bijgevolg heeft dit Hof aanvaard dat de bepalingen ervan in aanmerkingen kunnen worden genomen bij het beoordelen van de voorzienbaarheid van RIPA (zie Kennedy, reeds aangehaald, punt 157). Dienovereenkomstig zou het Hof aanvaarden dat het nationale recht voldoende 'toegankelijk' was." (zie Europees Hof voor de Rechten van de Mens (Grote Kamer), Big Brother Watch e.a./Verenigd Koninkrijk, verzoekschriften nrs. 58170/13, 62322/14 en 24960/15 van 25 mei 2021, punt 366).

([269]) Deel 2 van de IPA 2016.

([270]) Deel 3 van de IPA 2016.

([271]) Deel 4 van de IPA 2016.

([272]) Deel 5 van de IPA 2016.

([273]) Voor de lijst van relevante rechtshandhavingsinstanties die op grond van de IPA 2016 gerichte onderzoeksbevoegdheden kunnen toepassen, zie voetnoot (139).

([274]) Artikel 136 van de IPA 2016.

([275]) Artikel 158 van de IPA 2016.

([276]) Artikel 176 van de IPA 2016.

([277]) Artikel 199 van de IPA 2016.

met het bevel, de machtiging of de aanzegging/sommatie/beschikking wordt beoogd redelijkerwijs met andere, minder ingrijpende middelen kan worden bereikt; ii) of het niveau van bescherming dat moet worden toegepast met betrekking tot het verkrijgen van informatie op grond van het bevel, de machtiging of de aanzegging/sommatie/beschikking hoger is wegens de bijzondere gevoeligheid van die informatie; iii) het algemeen belang van de integriteit en de veiligheid van telecommunicatiesystemen en posterijen, en iv) alle andere aspecten van het algemeen belang van de bescherming van de persoonlijke levenssfeer ([278]).

(182) De wijze waarop deze criteria moeten worden toegepast – en de wijze waarop de naleving ervan wordt beoordeeld in het kader van de toestemming voor het gebruik van dergelijke bevoegdheden door de Secretary of State en de onafhankelijke Judicial Commissioners – wordt nader gespecificeerd in de desbetreffende praktijkcodes. In het bijzonder moet het gebruik van een van deze onderzoeksbevoegdheden altijd "in verhouding staan tot hetgeen ermee wordt beoogd, [hetgeen] inhoudt dat de ernst van de inbreuk op de persoonlijke levenssfeer (en andere overwegingen als uiteengezet in artikel 2, lid 2) moet worden afgewogen tegen de noodzaak van de activiteit uit het oogpunt van onderzoek, operationele taken of capaciteiten". Dit betekent met name dat het "een realistisch vooruitzicht moet bieden op het verwezenlijken van het verwachte voordeel en niet onevenredig of willekeurig mag zijn" en dat "inmenging in de persoonlijke levenssfeer niet als evenredig mag worden beschouwd indien de gevraagde informatie redelijkerwijs met andere, minder indringende middelen had kunnen kan worden verkregen" ([279]). Meer in het bijzonder moet de naleving van het evenredigheidsbeginsel worden beoordeeld aan de hand van de volgende criteria: "i) de omvang van de voorgestelde inmenging in de persoonlijke levenssfeer, afgezet tegen hetgeen daarmee wordt beoogd; ii) hoe en waarom de toe te passen methoden zo weinig mogelijk hinder voor de betrokkene en anderen zullen opleveren; iii) of de activiteit een passend gebruik van de wet vormt en een redelijke manier is om, na afweging van alle redelijke alternatieven, te bereiken wat wordt nagestreefd; iv) welke andere methoden, naar gelang van het geval, hetzij niet zijn toegepast, hetzij zijn gebruikt, maar als ontoereikend worden beschouwd om de operationele doelstellingen te bereiken zonder gebruikmaking van de voorgestelde onderzoeksbevoegdheid" ([280]).

(183) In de praktijk zorgt dit ervoor, zoals de Britse autoriteiten hebben uitgelegd, dat een inlichtingendienst eerst de operationele doelstelling bepaalt (en zo de verzameling afbakent, bv. tot een internationaal terrorismebestrijdingsdoel in een specifiek geografisch gebied) en vervolgens, op basis van die operationele doelstelling, moet overwegen welke technische optie (bv. gerichte of bulksgewijze interceptie, materiële interferentie, verkrijging van communicatiegegevens) het meest evenredig is (d.w.z. het minst inbreuk maakt op de persoonlijke levenssfeer, zie artikel 2, lid 2, van de IPA) met het beoogde doel, en derhalve kan worden toegestaan op basis van een van de beschikbare rechtsgrondslagen.

(184) Opgemerkt zij dat dit beroep op de normen van noodzakelijkheid en evenredigheid ook is opgemerkt en verwelkomd door de speciale VN-rapporteur inzake het recht op privacy, Joseph Cannataci, die met betrekking tot het bij de IPA 2016 ingevoerde systeem heeft verklaard dat "de bestaande procedures, zowel binnen de inlichtingendiensten als binnen de rechtshandhavingsinstanties, stelselmatig lijken te vereisen dat de noodzakelijkheid en evenredigheid van een bewakingsmaatregel of -operatie in aanmerking worden genomen voordat wordt aanbevolen er toestemming voor te geven, en dat deze op dezelfde gronden worden getoetst" ([281]). Hij merkte ook op dat hij tijdens zijn ontmoeting met vertegenwoordigers van de rechtshandhavingsinstanties en de nationale veiligheidsdiensten "een consensus had bereikt over het feit dat het recht op bescherming van de persoonlijke levenssfeer een eerste overweging moet zijn bij elk besluit betreffende bewakingsmaatregelen. Allen begrepen en waardeerden noodzaak en evenredigheid als de kardinale beginselen waarmee rekening moest worden gehouden".

([278]) De Code of Practice on Interception of Communications bepaalt dat andere elementen van de evenredigheidstoets zijn: "i) de omvang van de voorgestelde inmenging in de persoonlijke levenssfeer, afgezet tegen hetgeen daarmee wordt beoogd; ii) hoe en waarom de toe te passen methoden zo weinig mogelijk hinder voor de betrokkene en anderen zullen opleveren; iii) of de activiteit een passend gebruik van de wet vormt en een redelijke manier is om, na afweging van alle redelijke alternatieven, te bereiken wat wordt nagestreefd; iv) welke andere methoden, naar gelang van het geval, hetzij niet zijn toegepast, hetzij zijn gebruikt maar ontoereikend worden geacht om de operationele doelstellingen te bereiken zonder gebruikmaking van de voorgestelde onderzoeksbevoegdheid". Code of Practice on Interception of Communications, punt 4.16, te raadplegen via de volgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf

([279]) Zie de Code of Practice on Interception of Communications, punten 4.12 en 4.15, te raadplegen via de volgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf

([280]) Zie de Code of Practice on Interception of Communications, punt 4.16.

([281]) Einde van de missieverklaring van de speciale rapporteur inzake het recht op privacy bij de afsluiting van zijn missie naar het Verenigd Koninkrijk van Groot-Brittannië en Noord-Ierland, te raadplegen via de volgende link: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E, punt 1.a.

(185) De specifieke criteria voor het uitvaardigen van de verschillende bevelen, alsook de beperkingen en waarborgen die door de IPA 2016 zijn vastgesteld met betrekking tot elke onderzoeksbevoegdheid, worden nader omschreven in de overwegingen (186) tot en met (243).

3.3.1.1.1. Gerichte interceptie en onderzoek

(186) Voor gerichte interceptie bestaan er drie soorten bevelen: het gerichte interceptiebevel ([282]), het gerichte onderzoeksbevel en het bevel tot wederzijdse bijstand ([283]). De voorwaarden om dergelijke bevelen en de desbetreffende waarborgen te verkrijgen zijn uiteengezet in hoofdstuk 1 van deel 2 van de IPA 2016.

(187) Een gericht interceptiebevel geeft toestemming om de in het bevelschrift beschreven communicatie te onderscheppen tijdens de doorgifte ervan en om andere voor die communicatie relevante gegevens ([284]), waaronder secundaire gegevens, te verkrijgen ([285]). Een gericht onderzoeksbevel machtigt een persoon tot het maken van een selectie voor onderzoek van onderschepte inhoud die is verkregen op grond van een bulkinterceptiebevel ([286]).

(188) Elk bevel uit hoofde van deel 2 van de IPA 2016 kan worden uitgevaardigd door de Secretary of State ([287]) en worden goedgekeurd door een Judicial Commissioner ([288]). In alle gevallen is de duur van elk soort gericht bevel beperkt tot 6 maanden ([289]) en gelden er specifieke regels voor de wijziging ([290]) en verlenging ([291]) ervan.

(189) Alvorens het bevel uit te vaardigen, moet de Secretary of State een beoordeling maken van de noodzakelijkheid en de evenredigheid ([292]). Specifiek voor een gericht interceptiebevel en een gericht onderzoeksbevel moet de Secretary of State nagaan of de maatregel noodzakelijk is om een van de volgende redenen: het belang van de nationale veiligheid; het voorkomen of opsporen van een ernstig misdrijf; of de belangen van het economisch welzijn van het Verenigd Koninkrijk ([293]), voor zover die belangen ook relevant zijn voor de belangen van de nationale veiligheid ([294]). Anderzijds kan een bevel tot wederzijdse bijstand (zie overweging (139)) alleen worden uitgevaardigd indien de Secretary of State van oordeel is dat er sprake is van omstandigheden die gelijkwaardig zijn aan die waarin hij/zij een bevel zou uitvaardigen ter voorkoming en/of opsporing van een ernstig misdrijf ([295]).

(190) Bovendien moet de Secretary of State nagaan of de maatregel in verhouding staat tot het beoogde doel ([296]). Bij de beoordeling van de evenredigheid van de gevraagde maatregelen moet rekening worden gehouden met de algemene plichten met betrekking tot de persoonlijke levenssfeer die zijn neergelegd in artikel 2, lid 2, van de IPA 2016, met name de noodzaak om te beoordelen of hetgeen met het bevelschrift, de machtiging of de aanzegging/sommatie/beschikking wordt beoogd, redelijkerwijs ook met andere, minder ingrijpende middelen zou kunnen worden

([282]) Artikel 15, lid 2, van de IPA 2016.
([283]) Artikel 15, lid 4, van de IPA 2016.
([284]) Artikel 15, lid 2, van de IPA 2016.
([285]) Secundaire gegevens zijn gegevens die vastgehecht zijn aan of logisch geassocieerd zijn met de onderschepte communicatie, logisch daarvan kunnen worden gescheiden en, indien zij aldus zouden worden gescheiden, niets zouden onthullen van wat redelijkerwijs kan worden beschouwd als de betekenis (zou die er al zou zijn) van de communicatie. Enkele voorbeelden van secundaire gegevens zijn router- en firewallconfiguraties of de periode dat een router actief is geweest op een netwerk, wanneer deze gegevens deel uitmaken van, gekoppeld zijn aan of logisch geassocieerd zijn met de onderschepte communicatie. Zie voor meer details de definitie in artikel 16 van de IPA 2016 en de Code of Practice on Interception of Communications, punt 2.19, zie voetnoot 278.
([286]) Dit onderzoek wordt verricht als uitzondering op artikel 152, lid 4, van de IPA 2016, dat voorziet in een verbod om communicatie van personen die zich op de Britse eilanden bevinden, te trachten te identificeren. Zie overweging (229).
([287]) De Schotse minister geeft toestemming voor het bevel wanneer het betrekking heeft op ernstige criminele activiteiten in Schotland (zie de artikelen 21 en 22 van de IPA 2016), terwijl een hoge ambtenaar door de Secretary of State kan worden aangewezen om een bevel tot wederzijdse bijstand uit te vaardigen wanneer blijkt dat de interceptie betrekking zal hebben op een persoon die of een adres dat zich buiten het Verenigd Koninkrijk bevindt (artikel 40 van de IPA 2016).
([288]) Artikelen 19 en 23 van de IPA 2016.
([289]) Artikel 32 van de IPA 2016.
([290]) Artikel 39 van de IPA 2016. Beperkte wijzigingen kunnen door voorgeschreven personen worden aangebracht in de bevelen onder de voorwaarden die zijn vastgesteld in de IPA 2016. De persoon die het bevel heeft uitgevaardigd, kan een bevel te allen tijde intrekken. Die persoon moet dit doen indien het bevel om enige relevante reden niet langer noodzakelijk is of indien de bij het bevel toegestane gedraging niet langer in verhouding staat tot hetgeen wordt beoogd.
([291]) Artikel 33 van de IPA 2016. De beslissing om het bevel te verlengen moet worden goedgekeurd door een Judicial Commissioner.
([292]) Artikel 19 van de IPA 2016.
([293]) Wat het begrip "belangen van het economisch welzijn van het Verenigd Koninkrijk, voor zover die belangen ook relevant zijn voor de nationale veiligheid" betreft, kwam de Grote Kamer van het Europees Hof voor de Rechten van de Mens in de zaak Big Brother Watch e.a./Verenigd Koninkrijk (zie voetnoot 268), punt 371, tot de bevinding dat dit begrip voldoende op de nationale veiligheid was gericht. Hoewel de bevinding van het Hof in deze zaak verband hield met het gebruik van dit begrip in de RIPA 2000, wordt hetzelfde begrip gebezigd in de IPA 2016.
([294]) Artikel 20, lid 2, van de IPA 2016.
([295]) Artikel 20, lid 3, van de IPA 2016.
([296]) Artikel 19, lid 1, punt b), artikel 19, lid 2, punt b), en artikel 19, lid 3, punt b), van de IPA 2016.

bereikt, en of met betrekking tot het verkrijgen van informatie op grond van het bevel een hoger beschermingsniveau moet worden toegepast vanwege de bijzondere gevoeligheid van die informatie (zie overweging (181)).

(191) Daartoe zal de Secretary of State rekening moeten houden met alle elementen van het verzoek die zijn aangegeven door de autoriteit die het verzoek heeft ingediend, met name die welke betrekking hebben op de te onderscheppen personen en de relevantie van de maatregel voor het onderzoek. Dergelijke elementen worden behandeld in de Code of Practice on Interception of Communications en moeten met een zekere mate van specificiteit worden beschreven ([297]). Bovendien schrijft artikel 17 van de IPA 2016 voor dat elk bevel dat op grond van hoofdstuk 2 ervan wordt uitgevaardigd, de specifieke persoon of een groep personen, een organisatie of locatie die moeten worden onderschept (het "doelwit") moet noemen of beschrijven. In het geval van een gericht interceptiebevel of een gericht onderzoeksbevel kunnen deze ook betrekking hebben op een groep personen, meer dan één persoon of organisatie, of meer dan één vestiging (ook wel "thematisch bevel" genoemd) ([298]). In deze gevallen moet het bevel het gemeenschappelijke doel of de gemeenschappelijke activiteit van de groep personen of de operatie/het onderzoek beschrijven en zoveel mogelijk van deze personen/organisaties of vestiging noemen of beschrijven als redelijkerwijs haalbaar is ([299]). Ten slotte moeten in alle uit hoofde van deel 2 van de IPA 2016 uitgevaardigde bevelen de adressen, nummers, apparaten, factoren of combinatie van factoren worden gespecificeerd die moeten worden gebruikt voor het identificeren van de communicatie ([300]). In dit verband is in de Code of Practice on Interception of Communications bepaald dat in het geval van een gericht interceptiebevel en een gericht onderzoeksbevel "in het bevel de factoren of de combinatie van factoren die moeten worden gebruikt voor het identificeren van de communicatie, moeten worden gespecificeerd (of beschreven). Indien de communicatie moet worden geïdentificeerd aan de hand van (bijvoorbeeld) een telefoonnummer, moet het nummer in zijn geheel worden weergegeven. Wanneer echter voor de identificatie van het communicatieverkeer zeer complexe of voortdurend veranderende internetselectietermen moeten worden gebruikt, moeten die selectietermen zoveel mogelijk worden beschreven ([301]).

(192) Een belangrijke waarborg in dit verband is dat de beoordeling die de Secretary of State maakt om een bevel uit te vaardigen, moet worden goedgekeurd door een onafhankelijke Judicial Commissioner ([302]) die met name zal nagaan of het besluit om het bevel uit te vaardigen voldoet aan de beginselen van noodzakelijkheid en evenredigheid ([303]) (zie voor de status en de rol van Judicial Commissioners de overwegingen (251) tot en met (256)). De IPA 2016 verduidelijkt ook dat de Judicial Commissioner bij het uitvoeren van een dergelijke controle dezelfde beginselen moet toepassen als een rechter bij een verzoek om rechterlijke toetsing ([304]). Hierdoor wordt gewaarborgd dat in elk geval, en voordat inzage in gegevens wordt verleend, door een onafhankelijk orgaan systematisch wordt nagegaan of het noodzakelijkheids- en het evenredigheidsbeginsel in acht zijn genomen.

(193) De IPA 2016 voorziet in enkele specifieke en kleine uitzonderingen voor het uitvoeren van gerichte intercepties zonder een bevel. Het beperkte aantal gevallen wordt nader beschreven in de wet ([305]) en, behalve intercepties die zijn gebaseerd op de "toestemming" van de verzender/ontvanger, worden zij uitgevoerd door andere personen (particuliere of openbare instanties) dan de nationale veiligheidsdiensten. Bovendien wordt dit soort intercepties uitgevoerd voor andere doeleinden dan "inlichtingenvergaring" ([306]) en voor sommige soorten intercepties is het zeer onwaarschijnlijk dat de verzameling kan plaatsvinden in de context van een scenario van "doorgifte" (bijvoorbeeld in

([297]) De gevraagde informatie omvat nadere gegevens over de achtergrond (beschrijving van de personen/organisaties/vestiging, de te onderscheppen communicatie) en over de wijze waarop het verkrijgen van die informatie het onderzoek ten goede zal komen, alsmede een beschrijving van de toe te staan gedragingen. Indien het niet mogelijk is de personen/organisatie/panden te beschrijven, moet worden uitgelegd waarom dit niet mogelijk was of waarom slechts een algemene beschrijving werd gegeven (Code of Practice on Interception of Communications, punten 5.32 en 5.34, zie voetnoot 278).

([298]) Artikel 17, lid 2, van de IPA 2016. Zie ook de Code of Practice on Interception of Communications, punt 5.11 e.v., zie voetnoot 278.

([299]) Artikel 31, leden 4 en 5, van de IPA 2016.

([300]) Artikel 31, lid 8, van de IPA 2016.

([301]) Code of Practice on Interception of Communications, punten 5.37 en 5.38, zie voetnoot 278.

([302]) De goedkeuring door een Judicial Commissioner is niet vereist wanneer de Secretary of State van oordeel is dat er een dringende noodzakelijkheid is om het bevel uit te vaardigen (artikel 19, lid 1, van de IPA). De Judicial Commissioner moet echter op korte termijn worden geïnformeerd en moet beslissen of hij het bevel al dan niet goedkeurt. Zo niet, dan houdt het bevel op van kracht te zijn (artikelen 24 en 25 van de IPA 2016).

([303]) Artikel 23, lid 1, van de IPA 2016.

([304]) Artikel 23, lid 2, van de IPA 2016.

([305]) Zie de artikelen 44 tot en met 51 van de IPA 2016 en artikel 12 van de Interception of Communication Code of Practice (Praktijkcode inzake de interceptie van communicatie) (zie voetnoot 278).

([306]) Dit is bijvoorbeeld het geval wanneer interceptie nodig is in een gevangenis of in een psychiatrisch ziekenhuis (ter controle van het gedrag van een gedetineerde of een patiënt) of door een exploitant van postdiensten of een telecommunicatie-exploitant.

geval van interceptie in een psychiatrisch ziekenhuis of in een gevangenis). Rekening houdend met de aard van de instantie waarop deze specifieke gevallen van toepassing zijn (andere instanties dan de nationale veiligheidsinstanties), zijn alle waarborgen van deel 2 van de DPA 2018 en de UK GDPR van toepassing, met inbegrip van toezicht door de Information Commissioner en de beschikbare verhaalmechanismen. Naast de waarborgen van de DPA 2018, voorziet de IPA 2016 in bepaalde gevallen bovendien in toezicht achteraf door het IPCO ([307])

(194) Wanneer interceptie wordt uitgevoerd, zijn aanvullende beperkingen en waarborgen van toepassing met betrekking tot de specifieke status van de onderschepte persoon of personen ([308]). Zo is het onderscheppen van voorwerpen die onder de wettelijke geheimhoudingsplicht vallen alleen toegestaan in uitzonderlijke en dwingende omstandigheden; de persoon die het bevel uitvaardigt, moet rekening houden met het openbaar belang van de vertrouwelijkheid van voorwerpen die onder de wettelijke geheimhoudingsplicht vallen en met het feit dat er specifieke voorschriften zijn voor de verwerking, de bewaring en de verstrekking van dergelijk materiaal ([309]).

(195) Voorts voorziet de IPA 2016 in specifieke waarborgen met betrekking tot beveiliging, bewaring en verstrekking, waarmee de Secretary of State rekening moet houden alvorens een gericht bevel uit te vaardigen ([310]). In het bijzonder vereist artikel 53, lid 5, van de IPA 2016 dat elke kopie die wordt gemaakt van materiaal dat uit hoofde van het bevel is verzameld, op een veilige manier wordt opgeslagen en wordt vernietigd zodra er geen relevante gronden meer zijn om het te bewaren, terwijl artikel 53, lid 2, van de IPA 2016 vereist dat het aantal personen aan wie het materiaal wordt verstrekt en de mate waarin materiaal wordt verstrekt, ter beschikking gesteld of gekopieerd, wordt beperkt tot het minimum dat noodzakelijk is voor de wettelijke doeleinden.

(196) Tot slot, wanneer het materiaal dat is onderschept door middel van een gericht interceptiebevel of door middel van een bevel tot wederzijdse bijstand moet worden verstrekt aan een derde land ("overzeese verstrekking"), bepaalt de IPA 2016 dat de Secretary of State ervoor moet zorgen dat er passende regelingen worden getroffen om te waarborgen dat er in dat derde land vergelijkbare waarborgen bestaan op het gebied van beveiliging, bewaring en verstrekking ([311]). Daarnaast is in artikel 109, lid 2, van de DPA 2018 bepaald dat inlichtingendiensten alleen persoonsgegevens buiten het grondgebied van het Verenigd Koninkrijk mogen doorgeven indien de doorgifte een noodzakelijke en evenredige maatregel is die wordt uitgevoerd met het oog op de wettelijke taken van de verwerkingsverantwoordelijke of voor andere in artikel 2, lid 2, punt a), van de Security Service Act 1989 of artikel 2, lid 2, punt a), en artikel 4, lid 2, punt a), van de Intelligence Services Act 1994 vermelde doeleinden ([312]). Belangrijk is dat deze vereisten ook van toepassing zijn in gevallen waarin de nationaleveiligheidsvrijstelling overeenkomstig artikel 110 van de DPA 2018 wordt ingeroepen, aangezien in artikel 110 van de DPA 2018 artikel 109 van de DPA 2018 niet wordt genoemd als een van de bepalingen die niet hoeft te worden toegepast indien een vrijstelling van bepaalde bepalingen is vereist voor het waarborgen van de nationale veiligheid.

3.3.1.1.2. Gerichte verkrijging en bewaring van communicatiegegevens

(197) De IPA 2016 staat de Secretary of State toe om telecommunicatie-exploitanten ertoe te verplichten communicatiegegevens te bewaren voor gerichte toegang door diverse overheidsinstanties, met inbegrip van rechtshandhavingsinstanties en inlichtingendiensten. Deel 4 van de IPA 2016 voorziet in de bewaring van communicatiegegevens, terwijl deel 3 voorziet in de gerichte verkrijging van communicatiegegevens. In de delen 3 en 4 van de IPA 2016 worden ook specifieke beperkingen van de uitoefening van deze bevoegdheden uiteengezet en zijn specifieke waarborgen opgenomen.

([307]) Zie *a contrario* artikel 229, lid 4, van de IPA.

([308]) In de artikelen 26–29 van de IPA 2016 worden beperkingen ingevoerd voor het verkrijgen van gerichte interceptie- en onderzoeksbevelen met betrekking tot het onderscheppen van communicatie die wordt verzonden door of bestemd is voor een persoon die lid is van het parlement (elk parlement van het Verenigd Koninkrijk), het onderscheppen van voorwerpen die onder de wettelijk geheimhoudingsplicht vallen, het onderscheppen van communicatie waarvan de onderscheppende autoriteit denkt dat het gaat om communicatie die vertrouwelijk journalistiek materiaal bevat, en wanneer het doel van het bevel is om een bron van journalistieke informatie te identificeren of te bevestigen.

([309]) Artikel 26 van de IPA 2016.

([310]) Artikel 19, lid 1, van de IPA 2016.

([311]) Artikel 54 van de IPA 2016. Waarborgen in verband met de openbaarmaking van materiaal aan buitenlandse autoriteiten worden nader toegelicht in de praktijkcodes: zie met name de punten 9.26 et seq. en 9.87 van de Code of Practice on the Interception of Communications en de punten 9.33 et seq. en 9.41 van de Code of Practice on Equipment Interference (zie voetnoot 278).

([312]) Deze doeleinden zijn: voor de Security Service het voorkomen of opsporen van zware criminaliteit, of strafrechtelijke procedures (artikel 2, lid 2, punt a), van de Security Service Act 1989), voor de Intelligence Service het belang van de nationale veiligheid, het voorkomen of opsporen van zware criminaliteit, of strafrechtelijke procedures (artikel 2, lid 2, punt a), van de Intelligence Services Act 1994), en voor het GCHQ strafrechtelijke procedures (artikel 4, lid 2, punt a), van de Intelligence Services Act 1994). Zie ook de toelichting bij de DPA 2018, beschikbaar via de volgende link: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

(198) De term "communicatiegegevens" heeft betrekking op het "wie", "wanneer", "waar" en "hoe" van een communicatie, maar niet op de inhoud, dat wil zeggen wat er is gezegd of geschreven. Anders dan bij interceptie zijn de verkrijging en bewaring van communicatiegegevens er niet op gericht de inhoud van de communicatie te verkrijgen, maar om informatie te verkrijgen zoals de abonnee van een telefoniedienst of een gespecificeerde nota. Dit zouden het tijdstip en de duur van de communicatie, het nummer of het e-mailadres van de verzender en de ontvanger en soms de locatie van de apparaten vanaf welke de telecommunicatie is uitgegaan, kunnen zijn ([313]).

(199) Er zij opgemerkt dat de bewaring en verkrijging van communicatiegegevens doorgaans geen betrekking zal hebben op de communicatiegegevens van betrokkenen in de EU die uit hoofde van dit besluit naar het Verenigd Koninkrijk worden doorgegeven. De verplichting om communicatiegegevens te bewaren of te verstrekken overeenkomstig de delen 3 en 4 van de IPA 2016 heeft betrekking op gegevens die door telecommunicatie-exploitanten in het Verenigd Koninkrijk rechtstreeks van de gebruikers van een telecommunicatiedienst worden verzameld ([314]). Dit soort "klantgerelateerde" verwerking heeft doorgaans geen betrekking op een op dit besluit gebaseerde doorgifte, dat wil zeggen een doorgifte van een verwerkingsverantwoordelijke/verwerker in de EU aan een verwerkingsverantwoordelijke/verwerker in het Verenigd Koninkrijk.

(200) Met het oog op volledigheid worden de voorwaarden en waarborgen voor deze regelingen betreffende verkrijging en bewaring niettemin in de volgende overwegingen geanalyseerd.

(201) Vooropgesteld moet worden opgemerkt dat de bewaring en de gerichte verkrijging van communicatiegegevens ter beschikking staat van zowel nationale veiligheidsinstanties als van bepaalde rechtshandhavingsinstanties ([315]). De voorwaarden om de bewaring en/of verkrijging van communicatiegegevens te vereisen, kunnen variëren afhankelijk van de grond voor het indienen van een verzoek om de maatregel, namelijk de nationale veiligheid of rechtshandhaving als doeleinde.

(202) Hoewel met de nieuwe regeling de algemene vereiste van toestemming vooraf van een onafhankelijke instantie is ingevoerd die van toepassing zal zijn in alle gevallen waarin communicatiegegevens worden bewaard en/of verkregen (met het oog op rechtshandhaving of de nationale veiligheid), zijn naar aanleiding van het arrest in de zaak Tele2/Watson van het Europees Hof van Justitie ([316]) in het bijzonder specifieke waarborgen geïntroduceerd wanneer om rechtshandhavingsdoeleinden om de maatregel wordt verzocht. Met name wanneer de bewaring of de verkrijging van communicatiegegevens om rechtshandhavingsdoeleinden is vereist, moet de toestemming vooraf altijd worden gegeven door de Investigatory Powers Commissioner (Britse toezichthouder voor onderzoeksbevoegdheden, IPC). Dit is niet altijd het geval wanneer om de maatregel wordt verzocht met het oog op de nationale veiligheid, aangezien voor dat soort maatregelen, zoals hieronder wordt beschreven, in bepaalde gevallen toestemming kan worden gegeven door een andere "persoon die toestemming verleent". Bovendien is met de nieuwe regeling de drempel waarvoor de bewaring en de verkrijging van communicatiegegevens kan worden toegestaan verhoogd naar "ernstige strafbare feiten" ([317]).

([313]) Communicatiegegevens worden gedefinieerd in artikel 261, lid 5, van de IPA 2016. Communicatiegegevens worden ingedeeld in "gegevens over voorvallen" (dat wil zeggen gegevens die een voorval identificeren of beschrijven, al dan niet door verwijzing naar de locatie ervan, in of via een telecommunicatiesysteem waarin het voorval bestaat uit een of meer entiteiten die op een bepaald tijdstip bepaalde activiteiten uitvoeren) en "gegevens over entiteiten" (dat wil zeggen gegevens die a) betrekking hebben op i) een entiteit, ii) een samenwerking tussen een telecommunicatiedienst en een entiteit, of iii) een samenwerking tussen een deel van een telecommunicatiesysteem en een entiteit, b) bestaan uit gegevens die de entiteit identificeren of beschrijven (al dan niet door verwijzing naar de locatie van de entiteit) of die gegevens omvatten, en c) geen gegevens over voorvallen zijn).

([314]) Dit vloeit voort uit de definitie van "communicatiegegevens" in artikel 261, lid 5, van de IPA 2016, volgens welke communicatiegegevens in het bezit zijn van of worden verkregen door een telecommunicatie-exploitant en ofwel betrekking hebben op de gebruiker van een telecommunicatiedienst en verband houden met het verlenen van deze dienst, ofwel voorkomen in, deel uitmaken van, zijn vastgehecht aan of logisch geassocieerd zijn met een communicatie (zie ook de *Code of Practice on Communications Data* (Britse praktijkcode inzake communicatiegegevens), beschikbaar via de volgende link https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf, punten 2.22 tot en met 2.33). Bovendien bepaalt de definitie van "telecommunicatie-exploitant" in artikel 261, lid 10, van de IPA 2016 dat een telecommunicatie-exploitant een persoon is die een telecommunicatiedienst aanbiedt of levert aan personen in het Verenigd Koninkrijk of die een telecommunicatiesysteem beheert of aanbiedt dat zich (geheel of gedeeltelijk) in het Verenigd Koninkrijk bevindt of vanuit het Verenigd Koninkrijk wordt beheerd. Uit deze definities blijkt dat verplichtingen uit hoofde van de IPA 2016 niet kunnen worden opgelegd aan telecommunicatie-exploitanten van wie de apparatuur zich niet in het Verenigd Koninkrijk bevindt of vanuit het Verenigd Koninkrijk wordt beheerd en die geen diensten aanbieden of leveren aan personen in het Verenigd Koninkrijk (zie ook de Code of Practice on Communications Data, punt 2.1). Indien EU-abonnees (die zich hetzij in de EU, hetzij in het Verenigd Koninkrijk bevinden) gebruikmaken van diensten in het Verenigd Koninkrijk, zal het communicatieverkeer in verband met het verlenen van deze dienst rechtstreeks door de dienstverlener in het Verenigd Koninkrijk worden verzameld, en niet vanuit de EU worden doorgegeven.

([315]) De relevante autoriteiten zijn vermeld in bijlage 4 bij de IPA 2016 en omvatten de politiediensten, inlichtingendiensten, enkele ministeries en overheidsdiensten, het National Crime Agency, Her Majesty's Revenue and Customs, de Competition and Markets Authority, de Information Commissioner, ambulance-, brandweer- en reddingsdiensten, en instanties op bijvoorbeeld het gebied van gezondheid en voedselveiligheid.

([316]) Gevoegde zaken C-203/15 en C-698/15, Tele2/Watson, ECLI:EU:C:2016:970).

([317]) Zie artikel 61.7, punt b), voor de verkrijgen van communicatiegegevens en artikel 87.10A voor de bewaring van communicatiegegevens.

i) *Toestemming voor het verkrijgen van communicatiegegevens*

(203) Overeenkomstig deel 3 van de IPA 2016, mogen de betrokken overheidsinstanties communicatiegegevens verkrijgen van een telecommunicatie-exploitant of een persoon die in staat is dergelijke gegevens te verkrijgen en te verstrekken. De toestemming staat mogelijk de onderschepping van de inhoud van het communicatieverkeer ([318]) niet toe en is na één maand ([319]) niet meer geldig, waarbij verlenging door middel van een bijkomende toestemming mogelijk is ([320]). Voor de verkrijging van communicatiegegevens moet toestemming van de Investigatory Powers Commissioner ([321]) worden verkregen (zie voor de status en bevoegdheden van de IPC de overwegingen (250) en (251)). Dit is altijd het geval wanneer door een rechtshandhavingsinstantie om de verkrijging van communicatiegegevens wordt verzocht. Overeenkomstig artikel 61 van de IPA 2016, wanneer gegevens worden verkregen in het belang van de nationale veiligheid of de economische welvaart van het Verenigd Koninkrijk zo lang dit relevant is voor de nationale veiligheid, of wanneer een lid van een inlichtingendienst een aanvraag indient krachtens artikel 61, lid 7, punt b) ([322]), kan de verkrijging echter ook ([323]) worden toegestaan door de IPC of door een aangewezen hogere functionaris ([324]). De aangewezen functionaris moet onafhankelijk van het onderzoek of de operatie in kwestie zijn en praktische kennis van de beginselen en wetgeving op het gebied van mensenrechten hebben, met name wat betreft noodzaak en evenredigheid ([325]). Het besluit van de aangewezen functionaris zal worden onderworpen aan het toezicht achteraf door de IPC (zie overweging (254) voor meer gedetailleerde informatie over de taken betreffende toezicht achteraf van de IPC).

(204) De toestemming om communicatiegegevens te verkrijgen, wordt gebaseerd op een beoordeling van de noodzaak en evenredigheid van de maatregel. Meer in het bijzonder wordt de noodzaak van de maatregel beoordeeld in het licht van de in de wetgeving genoemde gronden ([326]). Gezien het gerichte karakter van deze maatregel moet deze ook noodzakelijk zijn voor een bepaald onderzoek of een bepaalde operatie ([327]). Verdere vereisten betreffende de beoordeling van de noodzaak van de maatregelen zijn neergelegd in de Code of Practice on Communication Data ([328]). In deze code staat in het bijzonder dat in de door de verzoekende autoriteit ingediende aanvraag ten minste drie elementen moeten worden vermeld die de noodzaak van het verzoek rechtvaardigen: i) het onderzochte voorval zoals een strafbaar feit of de locatie van een kwetsbare vermiste persoon; ii) de persoon van wie de gegevens worden gevraagd, zoals een verdachte, getuige of vermiste persoon, en hoe die verband houden met het voorval; en iii) de gevraagde communicatiegegevens, zoals een telefoonnummer of een IP-adres, en wat het verband is tussen deze gegevens en de persoon en het voorval ([329]).

(205) Bovendien moet de verkrijging van communicatiegegevens in verhouding staan tot het beoogde doel ([330]). In de Code of Practice on Communication Data wordt verduidelijkt dat de persoon die toestemming verleent, bij het uitvoeren van een dergelijke beoordeling een afweging moet maken tussen "de omvang van de aantasting van de rechten en

([318]) Artikel 60A, lid 6, van de IPA 2016.

([319]) Deze periode is beperkt tot drie dagen wanneer de toestemming om redenen van urgentie wordt gegeven (artikel 65, lid 3A, van de IPA 2016).

([320]) Overeenkomstig artikel 65 van de IPA 2016 is de verlengde toestemming één maand geldig vanaf de datum dat de huidige toestemming afloopt. Degene die de toestemming heeft verleend, kan de toestemming te allen tijde intrekken indien hij van oordeel is dat niet langer aan de voorwaarden wordt voldaan.

([321]) Artikel 60A, lid 1, van de IPA 2016. Het Office for Communications Data Authorisations (het Britse bureau voor toestemmingen communicatiegegevens, OCDA) voert deze functie uit namens de IPC (zie de Communication Data Codes of Practice, punt 5.6)

([322]) De aanvraag uit hoofde van artikel 61, lid 7, punt b), van de IPA 2016 wordt ingediend voor "een toepasselijk doeleinde inzake criminaliteit" in de betekenis van artikel 61, lid 7 bis, van de IPA 2016: "wanneer de communicatiegegevens geheel of gedeeltelijk uit gegevens over voorvallen bestaan, bedoeld om zware criminaliteit te voorkomen of op te sporen; in alle overige gevallen, bedoeld om criminaliteit te voorkomen of op te sporen of om ordeverstoring te voorkomen".

([323]) In de Code of Practice on Communication Data is het volgende bepaald: "Wanneer een aanvraag in verband met de nationale veiligheid kan worden ingediend overeenkomstig artikel 60A of artikel 61, wordt het besluit over welk traject voor het verlenen van toestemming in een bepaald geval het meest geschikt is, genomen door individuele overheidsinstanties. Overheidsinstanties die het traject van de aangewezen hogere functionaris willen volgen, moeten duidelijke richtsnoeren hebben over wanneer dit traject voor het verlenen van toestemming passend is" (Code of Practice on Communication Data, punt 5. 19, beschikbaar via de volgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822817/Communications_Data_Code_of_Practice.pdf).

([324]) In artikel 70, lid 3, van de IPA 2016 wordt de definitie van een "aangewezen functionaris" verstrekt, die varieert afhankelijk van de betrokken overheidsinstantie (zoals uiteengezet in bijlage 4 bij de IPA 2016).

([325]) Verdere details over de onafhankelijkheid van de aangewezen hogere functionaris worden gegeven in de Communication Data Code of practice (Code of Practice on Communications Data, punten 4.12 tot en met 4.17, zie voetnoot 323).

([326]) De gronden zijn: i) de nationale veiligheid; ii) het voorkomen of opsporen van criminaliteit of het voorkomen van ongeregeldheden (bij "gegevens over voorvallen" alleen zware criminaliteit); iii) in het belang van de economische welvaart van het Verenigd Koninkrijk voor zover dat belang ook relevant is voor het belang van de nationale veiligheid; iv) in het belang van de openbare veiligheid; v) om dood of letsel of schade aan de lichamelijke of geestelijke gezondheid van een persoon te voorkomen, of om letsel of schade aan de lichamelijke of geestelijke gezondheid van een persoon te beperken; vi) om bij te dragen aan onderzoeken naar vermeende gerechtelijke dwalingen of vii) om een overledene of een persoon te identificeren die zichzelf niet kan identificeren vanwege een bepaalde aandoening (artikel 61, lid 7, van de IPA 2016).

([327]) Artikel 60A, lid 1, punt b), van de IPA 2016.

([328]) Code of Practice on Communications Data, punt 3.3 e.v., zie voetnoot 323.

([329]) Code of Practice on Communications Data, punt 3.13, zie voetnoot 323.

([330]) Artikel 60, lid 1, punt c), van de IPA 2016.

vrijheden van een persoon en het specifieke voordeel voor het onderzoek dat of de operatie die in het algemeen belang door een betrokken overheidsinstantie wordt uitgevoerd" en dat, rekening houdend met alle overwegingen van een bepaald geval, "aantasting van de rechten van een persoon mogelijk nog steeds niet gerechtvaardigd is omdat het negatieve effect op de rechten van een andere persoon of groep personen te groot is". Om specifiek de evenredigheid van de maatregel te beoordelen, worden in de code bovendien elementen genoemd die in de door de verzoekende autoriteit ingediende aanvraag moeten worden opgenomen ([331]). Voorts moet bijzondere aandacht worden besteed aan het soort communicatiegegevens (gegevens over "entiteiten" of "voorvallen" ([332])) dat moet worden verkregen, en moet bij voorkeur gebruik worden gemaakt van een minder inbreukmakende categorie gegevens ([333]). De Code of Practice on Communication Data bevat ook specifieke instructies voor toestemming met betrekking tot de communicatiegegevens van mensen in bepaalde beroepen (zoals artsen, advocaten, journalisten, parlementariërs of geestelijken) ([334]) waarop extra waarborgen van toepassing zijn ([335]).

ii) *Aanzegging die de bewaring van communicatiegegevens vereist*

(206) In deel 4 van de IPA 2016 worden de voorschriften betreffende de bewaring van communicatiegegevens uiteengezet, en in het bijzonder de criteria die de Secretary of State toestaan een aanzegging tot bewaring af te geven ([336]). Wanneer de gegevens met het oog op rechtshandhaving worden bewaard en wanneer het gaat om de nationale veiligheid zijn dezelfde bij de IPA ingevoerde waarborgen van toepassing.

(207) Uitvaardiging van dergelijke aanzeggingen tot bewaring moet ervoor zorgen dat telecommunicatie-exploitanten relevante communicatiegegevens, die als zij niet langer vereist zijn voor zakelijke doeleinden anders zouden worden gewist, maximaal twaalf maanden bewaren ([337]). De bewaarde gegevens moeten gedurende de vereiste periode beschikbaar zijn mocht het vervolgens voor een overheidsinstantie nodig zijn om ze te verkrijgen in het kader van een toestemming voor een gerichte verkrijging van communicatiegegevens zoals bedoeld in deel 3 van de IPA 2016 en zoals beschreven in de overwegingen (203) tot en met (205).

(208) Op de uitoefening van de bevoegdheid om bewaring van bepaalde gegevens te vereisen is een aantal beperkingen en waarborgen van toepassing. De Secretary of State kan alleen een aanzegging tot bewaring aan een of meer exploitanten ([338]) afgeven indien hij/zij van oordeel is dat de vereiste om gegevens te bewaren voor een van de wettelijke doeleinden ([339]) noodzakelijk is en in verhouding staat tot het beoogde doel ([340]). Zoals verduidelijkt wordt in de IPA

([331]) Deze op te nemen informatie moet het volgende bevatten: i) een schets van de wijze waarop het verkrijgen van de gegevens ten goede zal komen aan het onderzoek of de operatie; ii) een toelichting op de relevantie van verzochte termijnen, en hoe deze termijnen in verhouding staan tot het onderzochte voorval; iii) een uitleg waarom de mate van inbreuk gerechtvaardigd is wanneer rekening wordt gehouden met het voordeel dat de gegevens zullen opleveren voor het onderzoek (voor deze rechtvaardiging moet worden nagegaan of minder ingrijpende onderzoeken kunnen worden uitgevoerd om de doelstelling te verwezenlijken); iv) aandacht voor de rechten (met name in verband met privacy en, in voorkomende gevallen, de vrijheid van meningsuiting) van de persoon, en een afweging van deze rechten tegen het voordeel voor het onderzoek; v) details over welke inbreuk op de privacy van derden kan plaatsvinden en hoe de gevraagde termijnen van invloed zijn op de inbreuk op de privacy van derden (Code of Practice on Communications Data, punten 3.22 tot en met 3.26, zie voetnoot 323).

([332]) Zie voetnoot 313.

([333]) Wanneer meer inbreukmakende communicatiegegevens (d.w.z. gegevens over voorvallen) worden gevraagd, wordt in de code gesteld dat het de voorkeur verdient om eerst gegevens over entiteiten te verkrijgen of om in een beperkt aantal specifieke spoedeisende gevallen rechtstreeks gegevens over voorvallen te verkrijgen (Code of Practice on Communications Data, punten 6.10 tot en met 6.14, zie voetnoot 323).

([334]) Code of Practice on Communications Data, punten 8.8 tot en met 8.44, zie voetnoot 323.

([335]) In de praktijkcode wordt gesteld dat "een toestemming verlenende persoon bij de behandeling van dergelijke aanvragen bijzondere zorgvuldigheid moet betrachten, onder andere door speciaal na te gaan of dergelijke aanvragen mogelijk onbedoelde gevolgen hebben en of het algemeen belang het best wordt gediend door de aanvraag" (Code of Practice on communications data, punt 8.8). Bovendien moet dit soort aanvragen in een register worden bijgehouden en moeten dergelijke aanvragen bij de volgende inspectie onder de aandacht van de IPC worden gebracht (Code of Practice on Communications Data, punt 8.10, zie voetnoot 323).

([336]) Artikelen 87 tot en met 89 van de IPA 2016.

([337]) Een telecommunicatie-exploitant aan wie een aanzegging tot bewaring is afgegeven kan uit hoofde van artikel 90 van de IPA 2016 verzoeken om een herziening door de Secretary of State die de aanzegging heeft afgegeven.

([338]) Overeenkomstig artikel 87, lid 2, punt a), van de IPA 2016 kan een aanzegging tot bewaring verband houden "met een bepaalde exploitant of een beschrijving van exploitanten".

([339]) De doeleinden zijn i) het belang van de nationale veiligheid; ii) het toepasselijke doeleinde inzake criminaliteit (zoals gedefinieerd in artikel 87.10 bis van de IPA 2016); iii) het belang van de economische welvaart van het Verenigd Koninkrijk voor zover dat belang ook relevant is voor het belang van de nationale veiligheid; iv) het belang van de openbare veiligheid; v) het doel om dood of letsel of schade aan de lichamelijke of geestelijke gezondheid van een persoon te voorkomen, of om letsel of schade aan de lichamelijke of geestelijke gezondheid van een persoon te beperken; of vi) om bij te dragen aan onderzoeken naar vermeende gerechtelijke dwalingen (artikel 87 van de IPA).

([340]) Artikel 87 van de IPA 2016. Om de evenredigheid van de aanzegging tot bewaring te beoordelen, zijn volgens de desbetreffende praktijkcode bovendien de criteria in artikel 2, lid 2, van de IPA 2016 van toepassing, met name de vereiste om te beoordelen of het beoogde doel van de aanzegging redelijkerwijs met minder ingrijpende middelen zou kunnen worden bereikt. Net zoals bij de beoordeling van de evenredigheid met betrekking tot de verkrijging van communicatiegegevens, wordt in de Code of Practice on Communications Data verduidelijkt dat voor die beoordeling "een afweging moet worden gemaakt tussen de omvang van de aantasting van het recht van een persoon op eerbiediging van zijn/haar privéleven en een bepaald voordeel voor het onderzoek (Code of Practice on Communications Data, punt 16.3, zie voetnoot 323).

2016 zelf ([341]), moet de Secretary of State, rekening houden met het volgende alvorens een aanzegging tot bewaring af te geven: de waarschijnlijke voordelen van de aanzegging ([342]); een beschrijving van de telecommunicatiediensten; de geschiktheid van beperking van de te bewaren gegevens volgens locatie, of beschrijvingen van personen aan wie de telecommunicatiediensten worden geleverd ([343]); het waarschijnlijke aantal gebruikers (indien bekend) van een telecommunicatiedienst waarop de aanzegging betrekking heeft ([344]); de technische haalbaarheid van de naleving van de aanzegging; de waarschijnlijke kosten van naleving van de aanzegging, en alle overige gevolgen van de aanzegging voor de telecommunicatie-exploitant (of de beschrijving van exploitanten) op wie de aanzegging betrekking heeft ([345]). Zoals verder uiteengezet wordt in hoofdstuk 17 van de Code of Practice on Communications Data moet in alle aanzeggingen tot bewaring elk soort te bewaren gegevens worden aangegeven, alsook op basis waarvan elk soort gegevens aan de noodzakelijke criteria voor bewaring voldoet.

(209) In alle gevallen (met het oog op zowel de nationale veiligheid als rechtshandhaving) moet het besluit van de Secretary of State om de aanzegging tot bewaring af te geven in het kader van de zogenaamde "double-lockprocedure" worden goedgekeurd door een onafhankelijke Judicial Commissioner, die in het bijzonder moet nagaan of de aanzegging tot bewaring van relevante communicatiegegevens voor een of meer van de wettelijke doeleinden noodzakelijk en evenredig is ([346]).

3.3.1.1.3. Materiële interferentie

(210) Materiële interferentie is een reeks technieken die worden gebruikt om allerlei gegevens te verkrijgen uit apparatuur ([347]), waaronder computers, tablets en smartphones, maar ook kabels, snoeren en opslagapparaten ([348]). Materiële interferentie maakt het mogelijk om zowel de inhoud van communicatie als de gegevens van apparatuur te verkrijgen ([349]).

(211) Overeenkomstig artikel 13, lid 1, van de IPA 2016 is voor het gebruik van materiële interferentie door een inlichtingendienst toestemming vereist door middel van een bevel in het kader van de bij de IPA 2016 ingestelde "double-lockprocedure", mits er sprake is van een "verband met de Britse eilanden" ([350]). In overeenstemming met de uitleg

([341]) Artikel 88 van de IPA 2016.

([342]) De voordelen kunnen bestaand of verwacht zijn en moeten in overeenstemming zijn met de wettelijke doeleinden waarvoor de gegevens kunnen worden bewaard (Code of Practice on Communications Data, punt 17.17, zie voetnoot 323).

([343]) Voor de overwegingen moet worden bepaald of de volledige geografische reikwijdte van de aanzegging noodzakelijk en evenredig is en of het noodzakelijk en evenredig is om bepaalde beschrijvingen van personen op te nemen of uit te sluiten (Code of Practice on Communications Data, punt 17.17, zie voetnoot 323).

([344]) Dit zal de Secretary of State helpen niet alleen de mate van inbreuk op de privacy van klanten in aanmerking te nemen, maar ook de waarschijnlijke voordelen van de te bewaren gegevens (Code of Practice on Communications Data, punt 17.17, zie voetnoot 323).

([345]) Artikel 88 van de IPA 2016.

([346]) Artikel 89 van de IPA 2016.

([347]) Overeenkomstig artikel 135, lid 1, en artikel 198, lid 1, van de IPA 2016 omvat "apparatuur" apparaten die elektromagnetische, akoestische of andere emissies voortbrengen en alle apparaten die in samenhang met die apparaten kunnen worden gebruikt.

([348]) *Code of Practice on Equipment Interference* (Praktijkcode inzake materiële interferentie), te raadplegen via de volgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf, punt 2.2.

([349]) In artikel 100 van de IPA 2016 worden "gegevens van apparatuur" gedefinieerd als systeemgegevens en gegevens die a) voorkomen in, deel uitmaken van, zijn vastgehecht aan of logisch geassocieerd zijn met een communicatie (door de afzender of anderszins) of een andere bron van informatie; b) logisch kunnen worden gescheiden van de rest van de communicatie of de bron van informatie, en c) indien zij aldus zijn gescheiden, niets zouden onthullen van wat redelijkerwijs zou kunnen worden beschouwd als zijnde de betekenis (indien van toepassing) van de communicatie of de bron van informatie.

([350]) Een bevel is bovendien overeenkomstig artikel 13, lid 1, van de IPA 2016 slechts verplicht indien de gedraging van de inlichtingendienst één of meer strafbare feiten zou vormen overeenkomstig de artikelen 1 tot en met 3 bis van de *Computer Misuse Act 1990* (Britse wet inzake computermisbruik van 1990), wat in veruit de meeste omstandigheden het geval zou zijn, zie de Code of Practice on Equipment Interference, punt 3.32 en de punten 3.6 tot en met 3.9). Overeenkomstig artikel 13, lid 2, van de IPA 2016, is er sprake van een "verband met de Britse eilanden" indien a) een gedraging op de Britse eilanden plaatsvindt (ongeacht de locatie van de apparatuur die wordt of kan worden verstoord), b) de inlichtingendienst meent dat apparatuur die wordt of kan worden verstoord zich op de Britse eilanden bevindt of kan bevinden op het moment dat de interferentie plaatsvindt, of c) de interferentie bedoeld is voor het verkrijgen van i) communicatie die is verzonden door of aan een persoon die zich vooralsnog op de Britse eilanden bevindt of die zich daar volgens de inlichtingendienst bevindt, ii) persoonlijke gegevens in verband met een persoon die zich vooralsnog op de Britse eilanden bevindt of die zich daar volgens de inlichtingendienst bevindt, of iii) gegevens van apparatuur die onderdeel zijn van of verband houden met communicatieverkeer of persoonlijke gegevens die onder punt i) of ii) vallen.

die door de Britse autoriteiten wordt gegeven, is er in situaties waarin binnen de reikwijdte van dit besluit gegevens van de Europese Unie worden doorgegeven aan het Verenigd Koninkrijk altijd sprake van een "verband met de Britse eilanden" en zou materiële interferentie met betrekking tot die gegevens derhalve onderhevig zijn aan de verplichting dat er een bevel is uitgevaardigd volgens artikel 13, lid 1, van de IPA 2016 ([351]).

(212) De voorschriften inzake bevelen voor gerichte materiële interferentie worden uiteengezet in deel 5 van de IPA 2016. Net als bij gerichte interceptie, moet gerichte materiële interferentie verband houden met een bepaald "doel", dat in het bevel moet worden uiteengezet ([352]). De details van de wijze waarop een "doel" moet worden geïdentificeerd is afhankelijk van de zaak en van het soort apparatuur dat moet worden verstoord. In het bijzonder in artikel 115, lid 3, van de IPA worden de elementen genoemd die in het bevel moeten worden opgenomen (bv. de naam van de persoon of organisatie, beschrijving van de locatie), bijvoorbeeld afhankelijk van de vraag of de verstoring betrekking heeft op apparatuur die eigendom is van, wordt gebruikt door of in het bezit is van een bepaalde persoon of een bepaalde organisatie of een bepaalde groep personen, of zich op een bepaalde locatie bevindt enz. ([353]). De doeleinden waarvoor bevelen voor gerichte materiële interferentie kunnen worden uitgevaardigd, zijn afhankelijk van de overheidsinstantie die het bevel aanvraagt ([354]).

(213) Net als bij gerichte interceptie moet de autoriteit van afgifte nagaan of de maatregel noodzakelijk is om een bepaald doel te bereiken en of hij in verhouding staat tot beoogde doel ([355]). Bovendien moet de autoriteit tevens nagaan of er waarborgen bestaan in verband met beveiliging, bewaring en verstrekking, en met "overzeese verstrekking" ([356]) (zie overweging (196)).

(214) De machtiging moet worden goedgekeurd door een Judicial Commissioner, behalve in spoedeisende gevallen ([357]). In het laatste geval moet een Judicial Commissioner in kennis worden gesteld van het feit dat er een bevel is uitgevaardigd en moet hij dit bevel binnen drie werkdagen goedkeuren. Indien de Judicial Commissioner weigert het bevel goed te keuren, houdt het bevel op geldig te zijn en kan dit niet worden verlengd ([358]). Bovendien heeft de Judicial Commissioner de bevoegdheid om te vereisen dat in het kader van het bevel verkregen gegevens worden verwijderd ([359]). Het feit dat een beval met spoed is afgegeven houdt geen toezicht achteraf in (zie de overwegingen (244) tot en met (255)), noch mogelijkheden voor personen om verhaal te zoeken (zie de overwegingen (260) tot en met (270)). Personen kunnen een klacht indienen bij de Information Commissioner of via de gebruikelijke weg een vordering met betrekking tot vermeende gedragingen instellen bij het Investigatory Powers Tribunal (gerecht dat toezicht uitoefent op de onderzoeksbevoegdheden). In alle gevallen is het door de Judicial Commissioner toegepaste criterium om te beslissen of een bevel al dan niet moet worden goedgekeurd het criterium inzake noodzaak en evenredigheid dat van toepassing is op verzoeken om gerichte interceptie ([360]) (zie overweging (192)).

([351]) Volledigheidshalve moet worden opgemerkt dat, zelfs in situaties waarin er geen sprake is van een "verband met de Britse eilanden" en het gebruik van materiële interferentie derhalve niet onderhevig is aan de verplichting dat er een bevel is uitgevaardigd volgens artikel 13, lid 1, van de IPA 2016, een inlichtingendienst die voornemens is zich met activiteiten in te laten waarvoor hij een bevel voor bulksgewijze materiële interferentie kan verkrijgen, dat bevel in het kader van het beleid zou moeten krijgen (zie de Code of Practice on Equipment Interference, punt 3.24). Zelfs indien een bevel voor materiële interferentie uit hoofde van de IPA 2016 niet wettelijk verplicht is, noch wordt verkregen in het kader van het beleid, zijn de acties van de inlichtingendienst onderhevig aan een aantal voorwaarden en beperkingen krachtens artikel 7 van de Intelligence Services Act 1994. Dit omvat met name de vereiste van toestemming van de Secretary of State, die zich ervan moet kunnen vergewissen dat een actie niet verder gaat dan wat noodzakelijk is voor de goede uitoefening van de taken van de inlichtingendienst.

([352]) In artikel 115 van de IPA 2016 is de inhoud van het bevel vastgelegd, waarbij wordt aangegeven dat het bevel de naam of beschrijving van de personen, de organisaties, de locatie of de groep personen die het "doel" vormen, een beschrijving van de aard van het onderzoek en een beschrijving van de activiteiten waarvoor de apparatuur wordt gebruikt moet bevatten. In het bevel moet ook het soort apparatuur worden beschreven, alsook de gedraging die voor de persoon aan wie het bevel is gericht is toegestaan.

([353]) Zie ook de Code of Practice on Equipment Interference, punt 5.7, zie voetnoot 348.

([354]) Nationale veiligheidsagentschappen kunnen een bevel tot materiële interferentie aanvragen wanneer dat noodzakelijk is voor de nationale veiligheid, voor het opsporen van zware criminaliteit en/of in het belang van de economische welvaart van het Verenigd Koninkrijk voor zover dat belang ook relevant is voor het belang van de nationale veiligheid (de artikelen 102 en 103 van de IPA 2016). Afhankelijk van het agentschap kan een bevel tot materiële interferentie worden aangevraagd met het oog op rechtshandhaving wanneer dat noodzakelijk is voor het opsporen of voorkomen van zware criminaliteit of om de dood of letsel of schade aan de lichamelijke of geestelijke gezondheid van een persoon te voorkomen, of om letsel of schade aan de lichamelijke of geestelijke gezondheid van een persoon te beperken (zie artikel 106, leden 1 en 3, van de IPA 2016).

([355]) Artikel 102, lid 1, van de IPA 2016.

([356]) Artikelen 129 tot en met 131 van de IPA 2016.

([357]) Artikel 109 van de IPA 2016.

([358]) Artikel 109, lid 4, van de IPA 2016.

([359]) Artikel 110, lid 3, punt b), van de IPA 2016. Overeenkomstig de Code of Practice on Equipment Interference, punt 5.67, wordt bepaald of iets spoedeisend is aan de hand van de vraag of het redelijkerwijs haalbaar zou zijn om toestemming van de Judicial Commissioner te verkrijgen om het bevel uit te vaardigen binnen de beschikbare tijd om in een operationele of onderzoeksbehoefte te voorzien. Urgente bevelen moet onder een van beide of beide van de volgende categorieën vallen: i) onmiddellijke bedreiging van het leven of ernstige schade — bijvoorbeeld indien een persoon is ontvoerd en er is geoordeeld dat zijn of haar leven in onmiddellijk dreigend gevaar verkeert; of (ii) een gelegenheid voor inlichtingenvergaring of onderzoek met weinig tijd om te handelen — bijvoorbeeld wanneer een zending van drugs van klasse A op het punt staat het Verenigd Koninkrijk binnen te komen en rechtshandhavingsinstanties informatie over de verdachten van ernstige strafbare feiten willen hebben om ze aan te kunnen houden. Zie voetnoot 348.

([360]) Artikel 108 van de IPA 2016.

(215) Ten slotte zijn specifieke waarborgen voor gerichte interceptie ook van toepassing op materiële interferentie met betrekking tot de duur, vernieuwing en wijziging van het bevel, alsook op de interceptie van parlementsleden, van zaken die onder het wettelijk verschoningsrecht vallen, en van journalistiek materiaal (zie voor meer informatie overweging 193).

3.3.1.1.4. Uitoefening van bevoegdheden voor bulksgewijze verzameling

(216) Bevoegdheden voor bulksgewijze verzameling worden geregeld in deel 6 van de IPA 2016. Daarnaast bevatten de praktijkcodes meer informatie over de uitoefening van bevoegdheden voor bulksgewijze verzameling. Hoewel de "bevoegdheid voor bulksgewijze verzameling" in het Britse recht niet is gedefinieerd, wordt dit begrip in de context van de IPA 2016 beschreven als het verzamelen en bewaren van grote hoeveelheden gegevens die de regering op verschillende manieren heeft verzameld (dat wil zeggen de bevoegdheden voor bulksgewijze interceptie, bulksgewijze verkrijging, bulksgewijze materiële interferentie en bulkdatasets met persoonsgegevens) en die vervolgens toegankelijk zijn voor de autoriteiten. Deze beschrijving wordt verduidelijkt door te zeggen wat "bevoegdheid voor bulksgewijze verzameling" niet is: het is niet hetzelfde als zogenaamde "grootschalige bewaking" zonder beperkingen of waarborgen. Zoals hieronder wordt uitgelegd, bevat de bevoegdheid voor bulksgewijze verzameling juist wel beperkingen en waarborgen die ervoor moeten zorgen dat de toegang tot gegevens niet op een ongedifferentieerde of ongerechtvaardigde basis wordt verleend ([361]). Bevoegdheden voor bulksgewijze verzameling kunnen in het bijzonder alleen worden uitgeoefend als een verband kan worden aangetoond tussen de technische maatregel die een nationaal veiligheidsagentschap wil gebruiken en de operationele doelstelling waarvoor om die maatregel wordt verzocht.

(217) Bovendien gelden bevoegdheden voor bulksgewijze verzameling alleen voor inlichtingendiensten en moet voor die bevoegdheden altijd een bevel door de Secretary of State worden uitgevaardigd dat door een Judicial Commissioner wordt goedgekeurd. Bij het kiezen van de middelen om inlichtingen te vergaren, moet worden nagegaan of de desbetreffende doelstelling met "minder ingrijpende middelen" kan worden verwezenlijkt ([362]). Deze aanpak vloeit voort uit het kader van de wetgeving die is gebaseerd op het evenredigheidsbeginsel en derhalve de voorkeur geeft aan gerichte verzameling boven bulksgewijze verzameling.

3.3.1.1.4.1. Bulksgewijze interceptie en bulksgewijze materiële interferentie

(218) De regeling voor bulksgewijze interceptie is opgenomen in hoofdstuk 1 van deel 6 van de IPA 2016, terwijl in hoofdstuk 3 van dat deel bulksgewijze materiële interferentie wordt behandeld. Deze regelingen zijn in wezen dezelfde, dus de voorwaarden en extra waarborgen die op die bevelen van toepassing zijn, worden gezamenlijk geanalyseerd.

i) *Voorwaarden en criteria voor de uitvaardiging van het bevel*

(219) Een bevel tot bulksgewijze interceptie is beperkt tot de interceptie van communicatieverkeer die tijdens de doorgifte ervan plaatsvindt, waarbij het gaat om berichten die worden verzonden of ontvangen door personen die zich buiten de Britse eilanden ([363]) bevinden, zogeheten "overzeese communicatie" ([364]), alsook alle overige

([361]) Het verslag inzake bevoegdheden voor bulksgewijze verzameling van Lord David Anderson, een onafhankelijke recensent van terrorismewetgeving, vóór de goedkeuring van de IPA 2016, stelt het volgende: "*het moet duidelijk zijn dat de bulksgewijze verzameling en bewaring van gegevens niet hetzelfde is als zogenaamde "grootschalige bewaking". Elk rechtsstelsel dat die benaming verdient, bevat beperkingen en waarborgen die ervoor moeten zorgen dat toegang tot de opslag van gevoelige gegevens […] niet op een ongedifferentieerde of ongerechtvaardigde basis wordt verleend*. Het wetsontwerp bevat zeker dergelijke beperkingen en waarborgen. Lord David Anderson, Report of the bulk power review, augustus 2016, punt 1.9 (cursivering toegevoegd), beschikbaar via de volgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/546925/56730_Cm9326_WEB.PDF

([362]) Artikel 2.2 van de IPA 2016. Zie bijvoorbeeld de Code of Practice on Bulk Acquisition of Communications Data, punt 4.11, beschikbaar via de volgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf

([363]) De "Britse eilanden" omvatten het Verenigd Koninkrijk, de Kanaaleilanden en Man en worden gedefinieerd in bijlage 1 bij de *Interpretation Act 1978* (Britse wet inzake interpretatie van 1978), beschikbaar via de volgende link https://www.legislation.gov.uk/ukpga/1978/30/schedule/1

([364]) Volgens artikel 136 van de IPA 2016 is "overzeese communicatie": i) communicatie die wordt verzonden door personen die zich buiten de Britse eilanden bevinden, of ii) communicatie die wordt ontvangen door personen die zich buiten de Britse eilanden bevinden. Deze regeling heeft, zoals bevestigd door de Britse autoriteiten, ook betrekking op communicatieverkeer tussen twee personen die zich beiden buiten de Britse eilanden bevinden. De Grote Kamer van het Europees Hof voor de Rechten van de Mens is in de zaak Big Brother Watch e.a./Verenigd Koninkrijk (zie voetnoot 279), punt 376, met betrekking tot een vergelijkbare beperking (verwijzend naar "externe communicatie") van communicatie die op grond van de RIPA 2000 door middel van bulksgewijze interceptie kan worden vastgelegd, tot de bevinding gekomen dat die voldoende afgebakend en voorzienbaar was.

relevante gegevens en de daarop volgende selectie voor onderzoek van het onderschepte materiaal ([365]). Een bevel tot bulksgewijze materiële interferentie ([366]) verleent degene tot wie het bevel is gericht toestemming om apparatuur te verstoren, teneinde overzees communicatieverkeer (met inbegrip van alles wat gesproken inhoud, muziek, geluiden, beelden of ongeacht welke gegevens bevat), gegevens van apparatuur (gegevens die de werking mogelijk maken of vergemakkelijken van het postverkeer, een telecommunicatiesysteem, een telecommunicatiedienst) of enige andere informatie te verkrijgen ([367]).

(220) De Secretary of State kan alleen een bevel tot bulksgewijze operaties uitvaardigen naar aanleiding van een door het hoofd van een inlichtingendienst ingediende aanvraag ([368]). Een bevel dat bulksgewijze interceptie of bulksgewijze materiële interferentie toestaat, mag alleen worden uitgevaardigd indien dat noodzakelijk is voor het belang van de nationale veiligheid en voor het voorkomen of opsporen van zware criminaliteit, of voor het belang van de economische welvaart van het Verenigd Koninkrijk indien relevant voor de nationale veiligheid ([369]). Bovendien vereist artikel 142, lid 7, van de IPA 2016 dat een bevel tot bulksgewijze interceptie gedetailleerder moet worden gespecificeerd dan alleen met een verwijzing naar het "belang van de nationale veiligheid", de "economische welvaart van het Verenigd Koninkrijk" en het "voorkomen en bestrijden van zware criminaliteit", maar dat er een verband moet worden gelegd tussen de maatregel waarom wordt verzocht en een of meer operationele doeleinden die in het bevel moeten worden opgenomen.

(221) Deze keuze van het operationele doel is het resultaat van een meerlagig proces. Artikel 142, lid 4, bepaalt dat de in het bevel opgegeven operationele doeleinden in een door de hoofden van de inlichtingendiensten bijgehouden lijst moeten zijn vermeld als doeleinden die zij beschouwen als operationele doeleinden waarvoor onderschepte inhoud of secundaire gegevens die in het kader van bevelen tot bulksgewijze interceptie zijn verkregen voor onderzoek kunnen worden geselecteerd. De lijst van operationele doeleinden moet worden goedgekeurd door de Secretary of State. De Secretary of State kan die goedkeuring alleen verlenen indien is aangetoond dat het operationele doeleinde gedetailleerder is gespecificeerd dan de algemene gronden voor het uitvaardigen van het bevel (nationale veiligheid, of nationale veiligheid en economische welvaart, of het voorkomen van zware criminaliteit) ([370]). Na afloop van de desbetreffende periode van drie maanden moet de Secretary of State een kopie van de lijst van operationele doeleinden doen toekomen aan de parlementaire Intelligence and Security Committee (Britse inlichtingen- en veiligheidscommissie van het parlement, hierna "ISC" genoemd). Ten slotte moet de Prime Minister de lijst van operationele doeleinden ten minste eenmaal per jaar herzien ([371]). Zoals opgemerkt door de High Court, "moeten deze doeleinden niet als onbeduidende waarborgen worden afgedaan, aangezien zij samen een complexe reeks verantwoordingswijzen vormen, waarbij zowel het parlement als leden van de regering op het hoogste niveau zijn betrokken" ([372]).

(222) Dergelijke operationele doeleinden beperken ook de reikwijdte van de selectie van het onderschepte materiaal voor de onderzoeksfase. De selectie van te onderzoeken materiaal dat in het kader van het bevel tot bulksgewijze operaties is verzameld, moet worden gerechtvaardigd in het licht van de operationele doeleinden. Zoals uitgelegd door de Britse autoriteiten, houdt dit in dat praktische regelingen betreffende het onderzoek reeds in de bevelfase moeten worden beoordeeld door de Secretary of State, waarbij voldoende details worden gegeven om de wettelijke taken uit hoofde van de artikelen 152 en 193 van de IPA 2016 te vervullen ([373]). De aan de Secretary of State te verstrekken details in verband met die regelingen moeten bijvoorbeeld informatie (indien van toepassing) omvatten over de wijze waarop filterregelingen kunnen variëren gedurende de geldigheidsduur van een bevel ([374]). Zie overweging (229) voor meer informatie over het proces en de waarborgen die worden toegepast op de filter- en onderzoeksfasen.

([365]) Artikel 136, lid 4, van de IPA 2016. Volgens de van de Britse regering ontvangen uitleg kan bulksgewijze interceptie bijvoorbeeld worden gebruikt om eerder onbekende bedreigingen van de nationale veiligheid van het Verenigd Koninkrijk vast te stellen, door onderschept materiaal te filteren en te analyseren teneinde communicatieverkeer dat waardevolle inlichtingen bevat, te identificeren (UK Explanatory Framework section H: National security, p. 27 – 28, zie voetnoot 29). Zoals uitgelegd door de Britse autoriteiten, kunnen dergelijke instrumenten worden gebruikt om verbanden te leggen tussen bekende personen van belang en de zoektocht naar sporen van activiteiten door personen die mogelijk nog niet bekend zijn, maar die in de loop van een onderzoek naar voren komen, en om patronen van activiteiten vast te stellen die op een dreiging voor het Verenigd Koninkrijk kunnen duiden.

([366]) Overeenkomstig artikel 13, lid 1, van de IPA 2016 is voor het gebruik van materiële interferentie door een inlichtingendienst toestemming vereist door middel van een bevel in het kader van de IPA 2016, mits er sprake is van een "verband met de Britse eilanden", zie overweging (211).

([367]) Artikel 176 van de IPA 2016. Een bevel voor bulksgewijze materiële interferentie kan geen gedraging toestaan die (tenzij die met wettige toestemming plaatsvindt) onwettige interceptie inhoudt (behalve in verband met een opgeslagen communicatie). Volgens het Explanatory Framework zou de verkregen informatie noodzakelijk kunnen zijn voor het identificeren van personen van belang en doorgaans geschikt zijn voor bulksgewijze operaties (UK Explanatory Framework, section H: National security, blz. 28, zie voetnoot 29).

([368]) Artikel 138, lid 1, en artikel 178, lid 1, van de IPA 2016.

([369]) Artikel 138, lid 2, en artikel 178, lid 2, van de IPA 2016.

([370]) Volgens de door de Britse autoriteiten gegeven uitleg kan een operationeel doeleinde bijvoorbeeld de reikwijdte van de maatregel beperken tot het bestaan van een dreiging in een bepaald geografisch gebied.

([371]) Artikel 142, leden 4 tot en met 10, van de IPA 2016.

([372]) High Court of Justice, *Liberty*, [2019] EWHC 2057 (Admin), punt 167.

([373]) De artikelen 152 en 193 van de IPA 2016 vereisen het volgende: a) de selectie voor onderzoek wordt alleen uitgevoerd voor de in het bevel opgegeven operationele doeleinden, b) de selectie voor onderzoek is onder alle omstandigheden noodzakelijk en evenredig, en c) de selectie voor onderzoek is niet in strijd met het verbod om materiaal te selecteren en communicatieverkeer te identificeren die zijn verzonden door of die bestemd zijn voor personen van wie bekend is dat zij zich op dat moment op de Britse eilanden bevinden.

([374]) Zie de Code of Practice on Interception of Communications, punt 6.6, zie voetnoot 278.

(223) Een bulkbevoegdheid kan alleen worden toegekend indien deze in verhouding staat tot het beoogde doel ([375]). Zoals uiteengezet in de Code of Practice on Interception moet voor elke evenredigheidsbeoordeling "een afweging worden gemaakt tussen de ernst van de inbreuk op de privacy (en andere in artikel 2, lid 2, genoemde omstandigheden) en de noodzaak van de activiteit in termen van onderzoek, capaciteit en in operationeel opzicht. De toegestane gedraging moet een realistisch vooruitzicht bieden op verwezenlijking van het verwachte voordeel en mag niet onevenredig of willekeurig zijn" ([376]). Zoals eerder vermeld, houdt dit in de praktijk in dat de evenredigheidsbeoordeling gebaseerd wordt op een toetsing van het evenwicht tussen het beoogde doel ("operationele doeleinden") en de beschikbare technische opties (bv. gerichte of grootschalige interceptie, materiële interferentie, verkrijging van communicatiegegevens), waarbij de voorkeur wordt gegeven aan de minst ingrijpende middelen (zie de overwegingen (181) en (182)). Wanneer meer dan één maatregel geschikt is voor het doel, moeten de minder ingrijpende middelen worden verkozen.

(224) Een extra waarborg betreffende de beoordeling van de evenredigheid van de verzochte maatregel wordt gegarandeerd door het feit dat de Secretary of State de relevante informatie moet ontvangen die nodig is om zijn/haar beoordeling naar behoren te kunnen uitvoeren. In de Code of Practice on Interception en de Code of Practice on Equipment Interference wordt met name vereist dat de door de betrokken autoriteit ingediende aanvraag de achtergrond van de aanvraag vermeldt, alsook een beschrijving van de te onderscheppen communicatie en de telecommunicatie-exploitanten die bijstand moeten verlenen, een beschrijving van de gedraging die moet worden toegestaan, de operationele doeleinden, en een uitleg waarom de gedraging noodzakelijk en evenredig is ([377]).

(225) Ten slotte is het belangrijk dat het besluit van de Secretary of State om het bevel uit te vaardigen moet worden goedgekeurd door een onafhankelijke Judicial Commissioner die de evaluatie van de noodzaak en evenredigheid van de voorgestelde maatregel beoordeelt, met toepassing van dezelfde beginselen als die welke door een rechter zouden worden gebruikt bij een verzoek om rechterlijke toetsing ([378]). Meer specifiek beoordeelt de Judicial Commissioner de conclusies van de Secretary of State over de vraag of het bevel noodzakelijk is en of de gedraging evenredig is in het licht van de in artikel 2, lid 2, van de IPA 2016 vastgestelde beginselen (algemene taken in verband met privacy). Ook beoordeelt de Judicial Commissioner de conclusies van de Secretary of State over de vraag of elk van de in het bevel genoemde operationele doeleinden een doeleinde is waarvoor selectie noodzakelijk is of kan zijn. Indien de Judicial Commissioner goedkeuring weigert van het besluit tot uitvaardiging van een bevel, kan de Secretary of State ofwel: i) het besluit aanvaarden en het bevel derhalve niet uitvaardigen; of ii) de zaak voor een besluit voorleggen aan de Investigatory Powers Commissioner (tenzij de Investigatory Powers Commissioner het oorspronkelijke besluit heeft genomen) ([379]).

ii) *Extra waarborgen*

(226) Bij de IPA 2016 zijn verdere beperkingen van de duur, de verlenging en de wijziging van een bevel tot bulksgewijze verzameling ingevoerd. Het bevel moet een duur van maximaal zes maanden hebben en elk besluit om het bevel te verlengen of te wijzigen (met uitzondering van kleine wijzigingen) moet ook door een Judicial Commissioner worden goedgekeurd ([380]). In de Code of Practice on Interception en de Code of Practice on Equipment Interference is vastgesteld dat een verandering in de operationele doeleinden van het bevel als een ingrijpende wijziging van het bevel wordt beschouwd ([381]).

([375]) Artikel 138, lid 1, punten b) en c), en artikel 178, punten b) en c), van de IPA 2016.

([376]) Code of Practice on Interception of Communications, punt 4.10, zie voetnoot 278.

([377]) De Code of Practice on Interception of Communications, punt 6.20, zie voetnoot 278, en de Code of Practice on Equipment Interference, punt 6.13, zie voetnoot 348.

([378]) Artikel 138, lid 1, punt g), en artikel 178, lid 1, punt f), van de IPA 2016. Voorafgaande toestemming door een onafhankelijke instantie is met name door het Europees Hof voor de Rechten van de Mens vastgesteld als een belangrijke waarborg tegen misbruik in de context van bulksgewijze interceptie. Europees Hof voor de Rechten van de Mens (Grote Kamer), Big Brother Watch e.a./Verenigd Koninkrijk, (zie voetnoot 269), punten 351 en 352. Er moet niet worden vergeten dat deze uitspraak betrekking had op het vorige rechtskader (RIPA 2000), die enkele van de bij de IPA 2016 ingevoerde waarborgen (waaronder voorafgaande toestemming van een onafhankelijke Judicial Commissioner) niet bevatte.

([379]) Artikel 159, leden 3 en 4, van de IPA 2016.

([380]) Artikelen 143 tot en met 146, en 184 tot en met 188 van de IPA 2016. In geval van een dringende wijziging kan de Secretary of State de wijziging zonder goedkeuring doorvoeren, maar moet hij de Commissioner in kennis stellen en moet de Commissioner vervolgens beslissen of de wijzigingen al dan niet worden goedgekeurd (artikel 147 van de IPA 2016). Bevelen moeten worden ingetrokken wanneer het bevel niet langer noodzakelijk of evenredig is, of wanneer het onderzoek van onderschept materiaal, metagegevens of andere gegevens die in het kader van het bevel zijn verkregen, niet langer noodzakelijk is voor een van de in het bevel genoemde operationele doeleinden (artikelen 148 en 189 van de IPA 2016).

([381]) Code of Practice on Interception of Communications, de punten 6.44 tot en met 6.47, zie voetnoot 278, en de Code of Practice on Equipment Interference, punt 6.48, zie voetnoot 348.

(227) Vergelijkbaar met hetgeen voor gerichte interceptie geldt, wordt in deel 6 van de IPA 2016 bepaald dat de Secretary of State ervoor moet zorgen dat er regelingen van kracht zijn waarmee waarborgen worden geboden voor de bewaring en verstrekking van materiaal dat in het kader van het bevel is verkregen ([382]), alsook voor overzeese verstrekking ([383]). In artikel 150, lid 5, en artikel 191, lid 5, van de IPA 2016 wordt met name bepaald dat elke kopie van het op grond van het bevel verzamelde materiaal op een veilige manier moet worden opgeslagen en moet worden vernietigd zodra er niet langer relevante gronden bestaan om de kopie te bewaren, terwijl in artikel 150, lid 2, en artikel 191, lid 2, wordt bepaald dat het aantal personen aan wie het materiaal wordt verstrekt en de mate waarin materiaal wordt verstrekt, beschikbaar wordt gesteld of wordt gekopieerd, moet worden beperkt tot het minimum dat voor de wettelijke doeleinden noodzakelijk is ([384]).

(228) Tot slot wordt in de IPA 2016 bepaald dat, wanneer het materiaal dat door middel van bulksgewijze interceptie of bulksgewijze materiële interferentie is onderschept aan een derde land moet worden overhandigd ("overzeese verstrekkingen"), de Secretary of State voor passende regelingen moet zorgen die waarborgen dat in dat derde land vergelijkbare waarborgen betreffende beveiliging, bewaring en verstrekking bestaan ([385]). Bovendien zijn in artikel 109 van de DPA 2018 specifieke vereisten voor internationale doorgiften van persoonsgegevens door inlichtingendiensten naar derde landen of aan internationale organisaties vastgesteld, en is daarin bepaald dat gegevens niet naar een land of gebied buiten het Verenigd Koninkrijk of aan een internationale organisatie mogen worden doorgegeven, tenzij de doorgifte noodzakelijk en evenredig is voor de wettelijke taken van de verwerkingsverantwoordelijke of voor andere in artikel 2, lid 2, punt a), van de Security Service Act 1989 of artikel 2, lid 2, punt a), en artikel 4, lid 2, punt a), van de Intelligence Services Act 1994 vermelde doeleinden ([386]). Belangrijk is dat deze vereisten ook van toepassing zijn in gevallen waarin de nationaleveiligheidsvrijstelling overeenkomstig artikel 110 van de DPA 2018 wordt ingeroepen, aangezien in artikel 110 van de DPA 2018 artikel 109 van de DPA 2018 niet wordt genoemd als een van de bepalingen die niet hoeft te worden toegepast indien een vrijstelling van bepaalde bepalingen is vereist voor het waarborgen van de nationale veiligheid.

(229) Wanneer het bevel is goedgekeurd en de gegevens bulksgewijs zijn verzameld, worden de gegevens aan een selectie onderworpen alvorens te worden onderzocht. Voor de selectie- en onderzoeksfase geldt een nadere evenredigheidsbeoordeling die wordt uitgevoerd door de analist, waarbij op basis van de in het bevel opgegeven operationele doeleinden (en de eventueel bestaande filterregelingen), de selectiecriteria worden bepaald. Zoals bepaald in de artikelen 152 en 193 van de IPA moet de Secretary of State bij het uitvaardigen van het bevel zorgen voor regelingen om te waarborgen dat de selectie van het materiaal alleen voor de opgegeven operationele doeleinden wordt uitgevoerd en onder alle omstandigheden noodzakelijk en evenredig is. In dit opzicht hebben de Britse autoriteiten verduidelijkt dat het bulksgewijs onderschepte materiaal allereerst door middel van geautomatiseerd filteren wordt geselecteerd om gegevens te verwijderen die waarschijnlijk niet van belang zijn voor de nationale veiligheid. De filters verschillen van tijd tot tijd (aangezien internetverkeerspatronen, typen en protocollen veranderen) en zijn afhankelijk van de technologie en de operationele context. Na deze fase kunnen de gegevens alleen voor onderzoek worden geselecteerd indien zij van belang zijn voor de in het bevel opgegeven operationele doeleinden ([387]). De waarborgen van de IPA 2016 voor het onderzoek van het verzamelde materiaal zijn van toepassing op alle soorten gegevens (zowel onderschepte inhoud als secundaire gegevens) ([388]). De artikelen 152 en 193 van de IPA 2016 voorzien tevens in een algemeen verbod om materiaal voor onderzoek te selecteren dat verwijst naar gesprekken die zijn verzonden door of bestemd zijn voor personen die zich op de Britse eilanden bevinden. Indien de autoriteiten dat materiaal willen onderzoeken, moeten zij een verzoek om een bevel tot gericht onderzoek krachtens de delen 2 en 4 van de IPA 2016 indienen, dat moet worden afgegeven door de Secretary of State en goedgekeurd door een Judicial Commissioner ([389]). Indien iemand bewust onderschepte inhoud voor onderzoek selecteert in strijd met de vereisten in de wetgeving ([390]), pleegt diegene een strafbaar feit ([391]).

([382]) Artikel 156 van de IPA 2016.
([383]) Artikelen 150 en 191 van de IPA 2016.
([384]) De Grote Kamer van het Europees Hof voor de Rechten van de Mens heeft in Big Brother Watch e.a./Verenigd Koninkrijk (zie voetnoot 268) het systeem van extra waarborgen voor bewaring, inzage en verstrekking van RIPA 2000 gesteund, zie de punten 392 tot en met 394 en 402 tot en met 405. De IPA 2016 voorziet in hetzelfde systeem van waarborgen.
([385]) Artikelen 151 en 192 van de IPA 2016.
([386]) Zie voor meer informatie over deze doeleinden voetnoot 312.
([387]) In dit verband stelt de Code on interception of communications het volgende: "Deze verwerkingssystemen verwerken gegevens van de communicatieverbindingen of -signalen die door de onderscheppende autoriteit zijn geselecteerd voor onderschepping. Vervolgens wordt een mate van filtering toegepast op het verkeer over die verbindingen en signalen, bedoeld om soorten communicatie te selecteren die mogelijk waardevolle inlichtingen bevatten en om communicatie te verwijderen waarvan het veel minder waarschijnlijk is dat die waardevolle inlichtingen bevatten. Als gevolg van deze filtering, die per verwerkingssysteem zal verschillen, zal een aanzienlijk deel van de communicatie over deze verbindingen en signalen automatisch worden verwijderd. Vervolgens kunnen complexere zoekopdrachten plaatsvinden om verdere communicatiegegevens uit te extraheren die waarschijnlijk waardevolle inlichtingen bevatten die verband houden met de wettelijke taken van het agentschap. Deze communicatiegegevens kunnen vervolgens voor onderzoek worden geselecteerd voor een of meer van de in het bevel opgegeven operationele doeleinden wanneer aan de voorwaarden inzake noodzaak en evenredigheid is voldaan. Alleen items die niet zijn uitgefilterd kunnen potentieel door gemachtigde personen voor onderzoek worden geselecteerd" (Code of Practice on Interception of Communications, punt 6.6, zie voetnoot 278).
([388]) Zie artikel 152, lid 1, punten a) en b), van de IPA 2016 volgens welke het onderzoek van beide soorten gegevens (onderschepte inhoud en secundaire gegevens) alleen voor het opgegeven doeleinde mag worden uitgevoerd en onder alle omstandigheden noodzakelijk en evenredig moet zijn.
([389]) Dit type bevel is niet vereist wanneer de gegevens met betrekking tot personen die zich op de Britse eilanden bevinden "secundaire gegevens" zijn (zie artikel 152, lid 1, punt c), van de IPA 2016)
([390]) Artikelen 152 en 193 van de IPA 2016.
([391]) Artikelen 155 en 196 van de IPA 2016.

(230) De door de analist uitgevoerde beoordeling van het geselecteerde materiaal wordt onderworpen aan toezicht achteraf door de IPC, die de naleving van de specifieke, in de IPA 2016 vastgestelde waarborgen voor de onderzoeksfase ([392]) evalueert (zie ook overweging (229)). De IPC moet (onder andere door middel van audit, inspectie en onderzoek) de uitoefening door overheidsinstanties van de in de IPA 2016 genoemde onderzoeksbevoegdheden beoordelen ([393]). In dit verband wordt in de Code of Practice on Interception en in de Code of Practice on Equipment Interference verduidelijkt dat het agentschap registers moet bijhouden met het oog op verder onderzoek en audits, en dat uit deze registers moet blijken waarom toegang tot het materiaal door gemachtigde personen noodzakelijk en evenredig is en wat de toepasselijke operationele doeleinden zijn ([394]). Het Investigatory Powers Commissioner Office (IPCO) ([395]) concludeerde in zijn jaarverslag van 2018 bijvoorbeeld dat de door de analisten genoteerde rechtvaardiging voor het onderzoek van bepaald materiaal dat bulksgewijs is verzameld aan de vereiste evenredigheidsnorm voldeed, doordat voldoende details werden verstrekt over de redenen van hun "zoekopdrachten" in verband met het nagestreefde doel ([396]). Het IPCO heeft in zijn verslag van 2019 met betrekking tot bevoegdheden voor bulksgewijze verzameling duidelijk gemaakt de inspecties van bulksgewijze intercepties te willen voortzetten, met inbegrip van een uitvoering onderzoek van de selectietermen en zoekcriteria ([397]). Het zal tevens per geval de keuze van bewakingsmaatregelen (gericht tegenover bulksgewijs) grondig blijven onderzoeken, zowel bij zijn behandeling van verzoeken om een bevel in het kader van de "double-lockprocedure" als tijdens inspecties ([398]). Deze verdere monitoring zal naar behoren in aanmerking worden genomen in de context van de monitoring door de Commissie van dit besluit zoals bedoeld in de overwegingen (281) tot en met (284).

3.3.1.1.4.2. Bulksgewijze verkrijging van communicatiegegevens

(231) Hoofdstuk 2 van deel 6 van de IPA 2016 regelt de bevelen tot bulksgewijze verkrijging waarbij het aan degene tot wie het bevel is gericht wordt toegestaan een telecommunicatie-exploitant ertoe te verplichten eventuele communicatiegegevens die hij in zijn bezit heeft te verstrekken of te verkrijgen. Deze bevelen staan de verzoekende autoriteit tevens toe om de gegevens voor de volgende fase van het onderzoek te selecteren. Net als bij de gerichte bewaring en verkrijging van communicatiegegevens (zie overweging (199)), heeft de bulksgewijze verkrijging van communicatiegegevens doorgaans geen betrekking op de persoonsgegevens van betrokkenen in de EU die uit hoofde van dit besluit naar het Verenigd Koninkrijk worden doorgegeven. De verplichting om communicatiegegevens te verstrekken overeenkomstig hoofdstuk 2 van deel 6 van de IPA 2016 heeft betrekking op gegevens die door telecommunicatie-exploitanten in het Verenigd Koninkrijk rechtstreeks bij de gebruikers van een telecommunicatiedienst worden verzameld ([399]). Dit soort "klantgerelateerde" verwerking heeft doorgaans geen betrekking op een op dit besluit gebaseerde doorgifte, dat wil zeggen een doorgifte van een verwerkingsverantwoordelijke/verwerker in de EU aan een verwerkingsverantwoordelijke/verwerker in het Verenigd Koninkrijk.

(232) Met het oog op volledigheid worden de voorwaarden en waarborgen voor de verkrijging van bulkcommunicatiegegevens niettemin hieronder beschreven.

([392]) Artikelen 152 en 193 van de IPA 2016.
([393]) Artikel 229 van de IPA 2016.
([394]) Code of Practice on Interception of Communications, punt 6.74, zie voetnoot 278, en de Code of Practice on Equipment Interference, punt 6.78, zie voetnoot 348.
([395]) Het IPCO is bij artikel 238 van de IPA 2016 opgericht om de IPC te voorzien van het noodzakelijke personeel, accommodatie, uitrusting en andere voorzieningen en diensten die nodig zijn voor het uitoefenen van zijn/haar functies (zie overweging (251))
([396]) In het jaarverslag van 2018 van het IPCO werd vermeld dat de door de analisten van het GCHQ genoteerde rechtvaardiging "voldeed aan de vereiste norm en dat de analisten zich voldoende gedetailleerd verantwoordden voor de evenredigheid van hun zoekopdrachten naar bulksgewijs verzamelde gegevens". Jaarverslag 2018 van de Investigatory Powers Commissioner, punt 6.22, zie voetnoot 464.
([397]) Jaarverslag 2019 van de Investigatory Powers Commissioner, punt 7.6, zie voetnoot 463.
([398]) Jaarverslag 2019 van de Investigatory Powers Commissioner, punt 10.22, zie voetnoot 463.
([399]) Dit vloeit voort uit de definitie van "communicatiegegevens" in artikel 261, lid 5, van de IPA 2016, volgens welke communicatiegegevens in het bezit zijn van of worden verkregen door een telecommunicatie-exploitant en ofwel betrekking hebben op de gebruiker van een telecommunicatiedienst en verband houden met het verlenen van deze dienst, ofwel voorkomen in, deel uitmaken van, zijn vastgehecht aan of logisch geassocieerd zijn met een communicatie (zie ook de Code of Practice on Bulk Acquisition of Communications Data, beschikbaar via de volgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf, punten 2.15 tot en met 2.22). Bovendien bepaalt de definitie van "telecommunicatie-exploitant" in artikel 261, lid 10, van de IPA 2016 dat een telecommunicatie-exploitant een persoon is die een telecommunicatiedienst aanbiedt of levert aan personen in het Verenigd Koninkrijk of die een telecommunicatiesysteem beheert of aanbiedt dat zich (geheel of gedeeltelijk) in het Verenigd Koninkrijk bevindt of vanuit het Verenigd Koninkrijk wordt beheerd. Uit deze definities blijkt dat verplichtingen uit hoofde van de IPA 2016 niet kunnen worden opgelegd aan telecommunicatie-exploitanten van wie de apparatuur zich niet in het Verenigd Koninkrijk bevindt of vanuit het Verenigd Koninkrijk wordt beheerd en die geen diensten aanbieden of leveren aan personen in het Verenigd Koninkrijk (zie ook de Code of Practice on Bulk Acquisition of Communications Data, punt 2.2). Indien EU-abonnees (die zich hetzij in de EU, hetzij in het Verenigd Koninkrijk bevinden) gebruikmaken van diensten in het Verenigd Koninkrijk, zal het communicatieverkeer in verband met het verlenen van deze dienst rechtstreeks door de dienstverlener in het Verenigd Koninkrijk worden verzameld, en niet vanuit de EU worden doorgegeven.

(233) De IPA 2016 vervangt de wetgeving betreffende de verkrijging van bulkcommunicatiegegevens die het voorwerp uitmaakte van het arrest van het Hof van Justitie van de Europese Unie in de zaak Privacy International. De wetgeving waarop die zaak betrekking had, werd ingetrokken en de nieuwe regeling voorziet in specifieke voorwaarden en waarborgen in het kader waarvan een dergelijke maatregel kan worden toegestaan.

(234) Anders dan bij de vorige regeling, volgens welke de Secretary of State volledige vrijheid had om de maatregel goed te keuren ([400]), vereist de IPA 2016 met name dat de Secretary of State alleen een bevel uitvaardigt indien de maatregel noodzakelijk en evenredig is. Dit houdt in de praktijk in dat er een verband moet bestaan tussen de inzage in de gegevens en het beoogde doel ([401]). Meer in het bijzonder zal de Secretary of State moeten beoordelen of er een verband bestaat tussen de gevraagde maatregel en een of meer in de machtiging aangegeven "operationele doeleinden" (zie overweging 219); met betrekking tot de evenredigheidsbeoordeling wordt in de relevante praktijkcode bepaald dat de Secretary of State moet overwegen of het beoogde doel redelijkerwijs met andere minder ingrijpende middelen zou kunnen worden bereikt (artikel 2, lid 2, punt a), van de wet). Bijvoorbeeld door de gewenste informatie te verkrijgen door middel van een minder ingrijpende bevoegdheid zoals de gerichte verkrijging van communicatiegegevens ([402]).

(235) De Secretary of State zal voor het uitvoeren van die beoordeling gebruikmaken van informatie die de hoofden van de inlichtingendiensten ([403]) bij hun aanvraag moeten indienen, zoals de redenen waarom de maatregel noodzakelijk wordt bevonden op een van de wettelijke gronden, en de redenen waarom het beoogde doel niet redelijkerwijs met andere minder ingrijpende middelen zou kunnen worden bereikt ([404]). Bovendien beperken de operationele doeleinden de reikwijdte waarvoor in het kader van het bevel verkregen gegevens voor onderzoek kunnen worden geselecteerd ([405]). Zoals bepaald in de desbetreffende praktijkcode, moeten de operationele doeleinden een duidelijke vereiste beschrijven en voldoende gedetailleerd zijn om de Secretary of State ervan te verzekeren dat de verkregen gegevens alleen om bepaalde redenen voor onderzoek kunnen worden geselecteerd ([406]). De Secretary of State moet, alvorens de machtiging af te geven, namelijk zorgen voor specifieke regelingen om te waarborgen dat voor het onderzoek alleen het materiaal dat voor onderzoek noodzakelijk is geacht voor een operationeel doeleinde en een wettelijk doeleinde, wordt geselecteerd en dat een en ander onder alle omstandigheden evenredig en noodzakelijk is. Deze specifieke vereiste, zoals omschreven in de artikelen 158 en 172 ([407]) van de IPA 2016, is wat betreft de voorafgaande beoordeling van de noodzaak en evenredigheid van de criteria die voor selectiedoeleinden worden gebruikt eveneens een belangrijk nieuw gegeven van de bij de IPA 2016 ingevoerde regeling, vergeleken met de vorige regeling.

(236) Bij de IPA 2016 werd ook de verplichting ingevoerd dat de Secretary of State, alvorens het bevel tot bulksgewijze verkrijging van communicatiegegevens uit te vaardigen, moet zorgen voor specifieke beperkingen op de beveiliging, de bewaring en de verstrekking van de verzamelde persoonsgegevens ([408]). Bij overzeese verstrekking zijn de in overweging (227) beschreven waarborgen voor bulksgewijze interceptie en bulksgewijze materiële interferentie ook in deze context van toepassing ([409]). Verdere beperkingen worden uiteengezet in de wetgeving inzake de duur ([410]), verlenging ([411]) en wijziging van de bevelen tot bulksgewijze operaties ([412]).

(237) Net als voor de andere bevoegdheden voor bulksgewijze verzameling is het belangrijk dat de Secretary of State, alvorens het bevel uit te vaardigen, goedkeuring van een Judicial Commissioner verkrijgt ([413]). Dit is een belangrijk onderdeel van de bij de IPA 2016 ingestelde regeling.

([400]) Artikel 94, lid 1, van de *Telecommunication Act 1984* (Britse telecommunicatiewet van 1984) bepaalde dat de Secretary of State "aanwijzingen met een algemeen karakter kon geven die de Secretary of State essentieel of nuttig achtte in het belang van de nationale veiligheid (…)" (zie voetnoot 451).

([401]) Zie de zaak Privacy International, punt 78

([402]) Zie de Code of Practice on Bulk Acquisition of Communications Data, punt 4.11, (zie voetnoot 399).

([403]) Een bevel tot bulksgewijze verkrijging kan alleen worden aangevraagd door de hoofden van de inlichtingendiensten, namelijk: i) de algemeen directeur van de Security Service; ii) het hoofd van de Secret Intelligence Service; of iii) de directeur van het GCHQ (zie de artikelen 158 en 263 van de IPA 2016).

([404]) Code of Practice on Bulk Acquisition of Communications Data, punt 4.5 (zie voetnoot 399).

([405]) Overeenkomstig artikel 161 van de IPA 2016 moeten de in het bevel opgegeven operationele doeleinden de doeleinden zijn die in een door de hoofden van de inlichtingendiensten bijgehouden lijst ("de lijst van operationele doeleinden") zijn vermeld als doeleinden die zij beschouwen als operationele doeleinden waarvoor communicatiegegevens die in het kader van bevelen tot bulksgewijze verkrijging zijn verkregen voor onderzoek kunnen worden geselecteerd.

([406]) Code of Practice on Bulk Acquisition of Communications Data, punt 6.6 (zie voetnoot 399).

([407]) Artikel 172 van de IPA 2016 vereist dat er specifieke waarborgen moeten zijn voor de fase van het filteren en selecteren voor het onderzoek van bulksgewijze verkregen communicatie. Bovendien is het opzettelijk uitvoeren van een onderzoek dat in strijd is met deze waarborgen ook een strafbaar feit (zie artikel 173 van de IPA 2016).

([408]) Artikel 171 van de IPA 2016.

([409]) Artikel 171, lid 9, van de IPA 2016.

([410]) Artikel 162 van de IPA 2016.

([411]) Artikel 163 van de IPA 2016.

([412]) Artikelen 164 tot en met 166, van de IPA 2016.

([413]) Artikel 159 van de IPA 2016.

(238) De IPC houdt achteraf toezicht op de procedure van onderzoek van het bulksgewijs verkregen materiaal (communicatiegegevens) (zie overweging (254)). In dat verband is bij de IPA 2016 de vereiste ingevoerd dat de inlichtingenanalist die het onderzoek uitvoert, voorafgaand aan het voor onderzoek selecteren van de gegevens de reden moet noteren waarom het voorgestelde onderzoek voor een opgegeven operationeel doeleinde noodzakelijk en evenredig is ([414]). In het jaarverslag 2019 van het IPCO werd met betrekking tot de praktijk van het GCHQ en MI5 vastgesteld dat "de kritieke rol van bulkcommunicatiegegevens in de waaier van bij het GCHQ uitgevoerde activiteiten duidelijk was in de zaak die wij hebben onderzocht. Wij hebben de aard van de gevraagde gegevens en de gestelde vereisten inzake inlichtingen in overweging genomen en hebben vastgesteld dat uit de documentatie is gebleken dat de aanpak van het GCHQ noodzakelijk en evenredig was" ([415]). De door MI5 vermelde rechtvaardiging was van een goed niveau en voldeed aan de beginselen van noodzaak en evenredigheid" ([416]).

3.3.1.1.4.3. Bewaring en onderzoek van bulkdatasets met persoonsgegevens

(239) Bevelen in het kader van bulkdatasets met persoonsgegevens ([417]) staan inlichtingendiensten toe datasets te bewaren en te onderzoeken die de persoonsgegevens van een aantal personen bevatten. Volgens de door de Britse autoriteiten gegeven uitleg kan de analyse van dergelijke datasets "voor UKIC de enige manier zijn om vooruitgang te boeken met onderzoeken en om terroristen te identificeren aan de hand van zeer beperkte nuttige inlichtingen, of indien hun communicatie moedwillig is achtergehouden" ([418]). Er zijn twee soorten bevelen: "bevelen voor de klasse bulkdatasets met persoonsgegevens" ([419]) die betrekking hebben op een bepaalde categorie datasets, namelijk datasets die wat betreft de inhoud en het voorgestelde gebruik vergelijkbaar zijn en aanleiding tot vergelijkbare overwegingen geven, bijvoorbeeld wat betreft de mate van inbreuk op de privacy en gevoeligheid en de evenredigheid van het gebruik van de gegevens, wat de Secretary of State in staat stelt te onderzoeken of het gelijktijdig verkrijgen van alle gegevens binnen de relevante klasse noodzakelijk en evenredig is. Een bevel voor de klasse bulkdatasets met persoonsgegevens kan bijvoorbeeld betrekking hebben op datasets met reisgegevens die verband houden met vergelijkbare routes ([420]). "Bevelen voor een specifieke bulkdataset met persoonsgegevens" ([421]) hebben daarentegen betrekking op één specifieke dataset, zoals een dataset met een nieuw of ongebruikelijk soort informatie die niet onder een bestaand bevel voor de klasse bulkdatasets met persoonsgegevens ([422]) valt, of een dataset die betrekking heeft op specifieke soorten persoonsgegevens en derhalve extra waarborgen ([423]) vereist. De bepalingen van de IPA 2016 betreffende bulkdatasets met persoonsgegevens staan het onderzoeken en bewaren van dergelijke datasets alleen toe indien dat noodzakelijk en evenredig ([424]) en in overeenstemming met de algemene verplichtingen inzake privacy ([425]) is.

(240) Op de bevoegdheid om een bevel voor bulkdatasets met persoonsgegevens af te geven is de "double-lockprocedure" van toepassing: de beoordeling van de noodzaak en evenredigheid van de maatregel wordt eerst door de Secretary of State en daarna door de Judicial Commissioner uitgevoerd ([426]). De Secretary of State moet rekening houden met de aard en de reikwijdte van het soort bevel dat wordt aangevraagd, de betreffende categorie gegevens en het aantal afzonderlijke bulkdatasets met persoonsgegevens dat waarschijnlijk onder het specifieke soort bevel zal vallen ([427]). In de Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets (Britse praktijkcode betreffende de bewaring en het gebruik door de inlichtingendiensten van bulkdatasets met persoonsgegevens) is tevens vastgesteld dat gedetailleerde registers moeten worden bijgehouden en aan audits door de IPC worden onderworpen ([428]). Het bewaren en onderzoeken van bulkdatasets met persoonsgegevens buiten de grenzen van de IPA 2016 vormt een strafbaar feit ([429]).

([414]) IPCO Jaarverslag 2019, punt 8.6, zie voetnoot 463.
([415]) IPCO Jaarverslag 2019, punt 10.4, zie voetnoot 463.
([416]) IPCO Jaarverslag 2019, punt 8.37, zie voetnoot 463.
([417]) Artikel 200 van de IPA 2016.
([418]) Het UK Explanatory Framework for Adequacy Discussions (het Britse toelichtingskader voor de adequaatheidsdiscussie), section H: National Security, blz. 34, zie voetnoot 29.
([419]) Artikel 204 van de IPA 2016.
([420]) Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets, punt 4.7, beschikbaar via de volgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715478/Bulk_Personal_Datasets_Code_of_Practice.pdf
([421]) Artikel 205 van de IPA 2016.
([422]) Zoals gevoelige persoonsgegevens, zie artikel 202 van de IPA 2016 en de Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets, punten 4.21 en 4.12, zie voetnoot 469.
([423]) Een aanvraag voor een bevel voor een specifieke bulkdataset met persoonsgegevens moet afzonderlijk door de Secretary of State worden behandeld, dat wil zeggen met betrekking tot één specifieke dataset. De inlichtingendienst is overeenkomstig artikel 205 van de IPA verplicht om in zijn aanvraag voor een bevel voor een specifieke bulkdataset met persoonsgegevens een uitvoerige toelichting over de aard en de omvang van het desbetreffende materiaal op te nemen, alsook een lijst van de "operationele doeleinden" waarvoor de betrokken inlichtingendienst de bulkdataset met persoonsgegevens wil onderzoeken (indien de inlichtingendienst een bevel tot bewaring en onderzoek en niet alleen voor bewaring wenst). Bij het afgeven van een bevel voor de klasse bulkdatasets met persoonsgegevens neemt de Secretary of State juist de hele categorie datasets in één keer in aanmerking.
([424]) Artikelen 204 en 205 van de IPA 2016.
([425]) Artikel 2 van de IPA 2016.
([426]) Artikelen 204 en 205 van de IPA 2016.
([427]) Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets, punt 5.2, zie voetnoot 420.
([428]) Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets, punten 8.1 tot en met 8.15, zie voetnoot 420.
([429]) Het UK Explanatory Framework for Adequacy Discussions (het Britse toelichtingskader voor de adequaatheidsdiscussie), section H: National Security, blz. 34, zie voetnoot 29.

3.3.2 *Verder gebruik van de verzamelde informatie*

(241) Persoonsgegevens die uit hoofde van deel 4 van de DPA 2018 worden verwerkt, mogen niet worden verwerkt op een wijze die niet verenigbaar is met de doeleinden waarvoor zij zijn verzameld ([430]). In de DPA 2018 wordt bepaald dat de verwerkingsverantwoordelijke de gegevens kan verwerken voor andere doeleinden dan de doeleinden waarvoor de gegevens zijn verzameld, wanneer deze verenigbaar zijn met de oorspronkelijke doeleinden en op voorwaarde dat het de verwerkingsverantwoordelijke wettelijk is toegestaan om de gegevens te verwerken en dat de verwerking noodzakelijk en evenredig is ([431]). Bovendien is in de Security Service Act 1989 en de Intelligence Services Act 1994 vastgesteld dat de hoofden van de inlichtingendiensten verplicht zijn erop toe te zien dat er alleen informatie wordt verkregen of verstrekt die noodzakelijk is voor de goede uitoefening van de taken van de dienst of voor de andere in de relevante bepalingen vermelde beperkte en specifieke doeleinden ([432]).

(242) Bovendien bevat artikel 109 van de DPA 2018 specifieke vereisten voor internationale doorgiften van persoonsgegevens door inlichtingendiensten naar derde landen of aan internationale organisaties. Overeenkomstig deze bepaling mogen persoonsgegevens niet naar een land of gebied buiten het Verenigd Koninkrijk of aan een internationale organisatie worden doorgegeven, tenzij de doorgifte noodzakelijk en evenredig is voor de wettelijke taken van de verwerkingsverantwoordelijke of voor andere in artikel 2, lid 2, punt a), van de Security Service Act 1989 of artikel 2, lid 2, punt a), en artikel 4, lid 2, punt a), van de Intelligence Services Act 1994 vermelde doeleinden ([433]). Belangrijk is dat deze vereisten ook van toepassing zijn in gevallen waarin de nationaleveiligheids-vrijstelling overeenkomstig artikel 110 van de DPA 2018 wordt ingeroepen, aangezien in artikel 110 van de DPA 2018 artikel 109 van de DPA 2018 niet wordt genoemd als een van de bepalingen die niet hoeft te worden toegepast indien een vrijstelling van bepaalde bepalingen is vereist voor het waarborgen van de nationale veiligheid.

(243) Zoals de Information Commissioner heeft benadrukt in zijn richtsnoeren over verwerking door inlichtingen-diensten, naast de waarborgen in deel 4 van de DPA 2018, is een inlichtingendienst bij het delen van gegevens met een inlichtingendienst in een derde land bovendien ook onderworpen aan in andere wettelijke maatregelen geboden waarborgen die op hem van toepassing zijn, om ervoor te zorgen dat persoonsgegevens op rechtmatige en verantwoordelijke wijze worden verkregen, gedeeld en behandeld ([434]). Zo worden in de IPA 2016 verdere waarborgen vastgesteld met betrekking tot doorgiften naar een derde land van materiaal dat is verzameld in het kader van gerichte interceptie ([435]), gerichte materiële interferentie ([436]), bulksgewijze interceptie ([437]), bulksgewijze verkrijging van communicatiegegevens ([438]) en bulksgewijze materiële interferentie ([439]) (zogenaamde "overzeese verstrekkingen"). De autoriteit die het bevel uitvaardigt, moet met name zorgen voor regelingen waarmee wordt gewaarborgd dat het derde land dat de gegevens ontvangt het aantal personen die het materiaal inzien, en de omvang van de verstrekking en het aantal kopieën dat van het materiaal wordt gemaakt, beperkt tot wat minimaal noodzakelijk is voor de in de IPA 2016 vastgestelde toegestane doeleinden ([440]).

3.3.3 *Toezicht*

(244) Op overheidstoegang met het oog op de nationale veiligheid wordt toezicht gehouden door een aantal verschillende organen. De Information Commissioner ziet toe op de verwerking van persoonsgegevens in het licht van de DPA 2018 (zie de overwegingen (85) tot en met (98) voor meer informatie over de onafhankelijkheid, de benoeming, de rol en de bevoegdheden van de Commissioner), terwijl de IPC onafhankelijk en gerechtelijk toezicht houdt op de

([430]) Artikel 87, lid 1, van de DPA 2018.

([431]) Artikel 87, lid 3, van de DPA 2018. Hoewel verwerkingsverantwoordelijken overeenkomstig artikel 110 van de DPA 2018 van dit beginsel kunnen worden uitgesloten voor zover die uitsluiting vereist is om de nationale veiligheid te waarborgen, moet een dergelijke uitsluiting per geval worden beoordeeld en kan die alleen worden aangevoerd voor zover de toepassing van een bepaalde bepaling negatieve gevolgen voor de nationale veiligheid zou hebben (zie overweging (132)). De nationale veiligheidscertificaten voor de inlichtingendiensten van het Verenigd Koninkrijk (beschikbaar via de volgende link: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/) hebben geen betrekking op artikel 87, lid 3, van de DPA 2018. Aangezien verwerking voor andere doeleinden wettelijk moet zijn toegestaan, moeten inlichtingendiensten bovendien een heldere juridische grondslag voor de verdere verwerking hebben.

([432]) Zie voor verdere informatie over deze doeleinden voetnoot 312.

([433]) Zie voetnoot 312.

([434]) Richtsnoeren van de Information Commissioner over verwerking door inlichtingendiensten (zie voetnoot 161).

([435]) Artikel 54 van de IPA 2016.

([436]) Artikel 130 van de IPA 2016.

([437]) Artikel 151 van de IPA 2016.

([438]) Artikel 171, lid 9, van de IPA 2016.

([439]) Artikel 192 van de IPA 2016.

([440]) De regelingen moeten maatregelen omvatten waarmee wordt gewaarborgd dat elke kopie die van dat materiaal wordt gemaakt op veilige wijze wordt opgeslagen voor de duur dat die wordt bewaard. Het in het kader van een bevel verkregen materiaal en alle kopieën daarvan moeten worden vernietigd zodra er geen relevante gronden meer bestaan om ze te bewaren (zie artikel 150, leden 2 en 5, en artikel 151, lid 2, van de IPA 2016). Op te merken valt dat gelijksoortige waarborgen, die in het vorige rechtskader (RIPA 2000) werden geboden, in overeenstemming met de door het Europees Hof voor de Rechten van de Mens vastgestelde vereisten voor het delen van door middel van bulksgewijze interceptie verkregen materiaal met andere staten of internationale organisaties werden bevonden (het Europees Hof voor de Rechten van de Mens (Grote Kamer), Big Brother Watch e.a./Verenigd Koninkrijk, (zie voetnoot 279), punten 362 en 399).

uitoefening van onderzoeksbevoegdheden uit hoofde van de IPA 2016. De IPC ziet toe op de uitoefening van de onderzoeksbevoegdheden uit hoofde van de IPA 2016 door zowel rechtshandhavingsinstanties als nationale veiligheidsagentschappen. Politiek toezicht wordt gewaarborgd door de Intelligence Service Committee (commissie die toezicht houdt op de Britse inlichtingendiensten) van het parlement.

3.3.3.1. Toezicht uit hoofde van deel 4 van de DPA

(245) Op de verwerking van persoonsgegevens door de inlichtingendiensten uit hoofde van deel 4 van de DPA 2018 wordt toezicht gehouden door de Information Commissioner ([441]).

(246) De algemene functies van de Information Commissioner met betrekking tot de verwerking van persoonsgegevens door inlichtingendiensten uit hoofde van deel 4 van de DPA 2018 zijn vastgesteld in bijlage 13 bij de DPA 2018. De taken omvatten, maar zijn niet beperkt tot, het controleren en handhaven van deel 4 van de DPA 2018, het bewustmaken van het publiek, het adviseren van het parlement, de regering en andere instellingen over wettelijke en bestuursrechtelijke maatregelen, het bewustmaken van verwerkingsverantwoordelijken en verwerkers van hun verplichtingen, het verstrekken van informatie aan betrokkenen betreffende de uitoefening van hun rechten, het verrichten van onderzoek enz.

(247) Wat betreft deel 3 van de DPA 2018 heeft de Commissioner de bevoegdheid om verwerkingsverantwoordelijken in kennis te stellen van mogelijke inbreuken en om waarschuwingen te doen uitgaan dat een verwerking waarschijnlijk de regels schendt, en geeft hij reprimandes wanneer de inbreuk wordt bevestigd. Hij kan tevens sommaties tot nakoming en sanctiebeschikkingen afgeven voor schending van bepaalde bepalingen van de wet opleggen ([442]). Anders dan in andere delen van de DPA 2018, kan de Commissioner echter geen aanzeggingen tot beoordeling aan een nationale veiligheidsdienst afgeven ([443]).

(248) Bovendien voorziet artikel 110 van de DPA 2018 in een uitzondering voor de uitoefening van bepaalde bevoegdheden van de Commissioner wanneer dit vereist is voor het waarborgen van de nationale veiligheid. Dit omvat de bevoegdheid van de Commissioner om een (ongeacht welke) aanzegging/sommatie/beschikking af te geven uit hoofde van de DPA (aanzeggingen tot informatie, beoordeling, sommaties tot nakoming en sanctiebeschikkingen), de bevoegdheid om inspecties uit te voeren in overeenstemming met internationale verplichtingen, de toegangs- en inspectiebevoegdheden, en de voorschriften inzake strafbare feiten ([444]). Zoals uitgelegd in overweging (126) zijn deze uitzonderingen alleen van toepassing indien zij noodzakelijk en evenredig zijn, en indien per geval een analyse wordt gemaakt.

(249) Het ICO en de inlichtingendiensten van het Verenigd Koninkrijk hebben een memorandum van overeenstemming ([445]) ondertekend waarmee een kader wordt vastgesteld voor samenwerking rond een aantal kwesties, met inbegrip van kennisgevingen van inbreuken in verband met gegevens en de afhandeling van klachten van betrokkenen. Er is met name in bepaald dat het ICO, na een klacht te hebben ontvangen, beoordeelt of een toepassing van een vrijstelling in verband met de nationale veiligheid naar behoren is gebruikt. Vragen van het ICO in de context van het onderzoek van individuele klachten moeten binnen twintig werkdagen door de betrokken inlichtingendienst worden beantwoord, met gebruikmaking van passende veilige kanalen indien daarbij gerubriceerde informatie is betrokken. Het ICO heeft vanaf april 2018 tot heden 21 klachten over de inlichtingendiensten ontvangen van personen. Elke klacht is beoordeeld en de uitkomst is aan de betrokkene meegedeeld ([446]).

([441]) Artikel 116 van de DPA 2018.

([442]) Overeenkomstig bijlage 13, punt 2, bij de DPA 2018, kunnen sommaties tot nakoming en sanctiebeschikkingen worden afgegeven aan een verwerkingsverantwoordelijke of verwerker in verband met schendingen van hoofdstuk 2 van deel 4 van de DPA 2018 (verwerkingsbeginselen), een bepaling van deel 4 van de DPA 2018 inzake de toekenning van rechten aan een betrokkene, een vereiste om een inbreuk in verband met persoonsgegevens aan de Commissioner mee te delen op grond van artikel 108 van de DPA 2018, en de beginselen voor de doorgifte van persoonsgegevens naar derde landen, niet door het verdrag gebonden landen en internationale organisaties in artikel 109 van de DPA 2018 (zie overweging (92) voor meer informatie over sommaties tot nakoming en sanctiebeschikkingen).

([443]) Uit hoofde van artikel 147, lid 6, van de DPA 2018 mag de Information Commissioner een aanzegging tot beoordeling niet afgeven aan een in artikel 23, lid 3, van de Freedom of Information Act 2000 vermelde dienst. Daaronder vallen de Security Service (MI5), de Secret Intelligence Service (MI6) en de Government Communications Headquarters).

([444]) De volgende bepalingen kunnen worden vrijgesteld: artikel 108 (mededeling van een inbreuk in verband met persoonsgegevens aan de Commissioner), artikel 119 (inspectie in overeenstemming met internationale verplichtingen); de artikelen 142 tot en met 154 en bijlage 15 (aanzeggingen en toegangs- en inspectiebevoegdheden van de Commissioner); en de artikelen 170 tot en met 173 (strafbare feiten in verband met persoonsgegevens). Voorts in verband met de verwerking door de inlichtingendiensten in bijlage 13 (andere algemene taken van de Commissioner): punt 1, onder a) en g), en punt 2.

([445]) Memorandum van overeenstemming tussen het Information Commission's Office en de inlichtingendiensten van het Verenigd Koninkrijk, zie voetnoot 165.

([446]) In zeven van deze gevallen adviseerde het ICO de klager om de klacht voor te leggen aan de verwerkingsverantwoordelijke (dit is het geval wanneer een persoon een klacht heeft ingediend bij het ICO, maar dat eerst bij de verwerkingsverantwoordelijke had moeten doen), in één van deze gevallen gaf het ICO algemeen advies aan de verwerkingsverantwoordelijke (dit wordt gedaan wanneer de acties van de verwerkingsverantwoordelijke geen inbreuk op de wetgeving lijken te hebben gemaakt, maar een verbetering van de praktijken had kunnen voorkomen dat de klacht bij het ICO werd ingediend), en in de overige dertien gevallen was geen actie van de verwerkingsverantwoordelijke vereist (dit is het geval wanneer de door de persoon ingediende klachten wel onder de Data Protection Act 2018 vallen omdat zij betrekking hebben op de verwerking van persoonsgegevens, maar de verwerkingsverantwoordelijke op basis van de verstrekte informatie geen inbreuk op de wetgeving lijkt te hebben gemaakt).

3.3.3.2. Toezicht op de uitoefening van onderzoeksbevoegdheden uit hoofde van de IPA 2016

(250) Overeenkomstig deel 8 van de IPA 2016 wordt op de uitoefening van onderzoeksbevoegdheden toezicht gehouden door de Investigatory Powers Commissioner (IPC). De IPC wordt bijgestaan door andere Judicial Commissioners, die gezamenlijk Judicial Commissioners ([447]) worden genoemd. In de IPA 2016 worden de waarborgen vastgesteld die de onafhankelijkheid van de Judicial Commissioners beschermen. Judicial Commissioners moeten een hoger rechterlijk ambt bekleden of hebben bekleed (d.w.z. dat zij lid van de hoogste rechterlijke instanties moeten zijn of moeten zijn geweest) ([448]) en, als lid van de rechterlijke macht, onafhankelijk van de regering zijn ([449]). Overeenkomstig artikel 227 van de IPA 2016 is de Prime Minister degene die de IPC en zo veel Judicial Commissioners als hij noodzakelijk acht, benoemt. Alle Commissioners, ongeacht of zij huidige of voormalige leden van de rechterlijke macht zijn, kunnen uitsluitend worden benoemd op gezamenlijke voordracht van de drie Chief Justices voor Engeland en Wales, Schotland en Noord-Ierland, en de Lord Chancellor ([450]). De Secretary of State moet de IPC van personeel, accommodatie, uitrusting en andere voorzieningen en diensten voorzien ([451]). De Commissioners dienen drie jaar en kunnen worden herbenoemd ([452]). Als een verdere garantie voor hun onafhankelijkheid, kunnen Judicial Commissioners alleen onder strikte hoogdrempelige voorwaarden van hun functie worden ontheven: ofwel door de Prime Minister onder de in artikel 228, lid 5, van de IPA 2016 uitvoerig omschreven specifieke omstandigheden (zoals een faillissement of gevangenisstraf), of als een resolutie tot goedkeuring van de ontheffing door het Hoger- en Lagerhuis wordt aangenomen ([453]).

(251) De IPC en de Judicial Commissioners worden in hun taken bijgestaan door het Investigatory Powers Commissioner's Office (IPCO). Het personeel van het IPCO bestaat uit een team van inspecteurs, interne juridische en technische deskundigen, en een adviserende commissie die deskundig advies op het gebied van technologie verstrekt. Evenals voor de individuele Judicial Commissioners, wordt de onafhankelijkheid van het IPCO beschermd. Het IPCO is een arm's-length body van het ministerie van Binnenlandse Zaken, dat wil zeggen een orgaan dat financiering van het ministerie van Binnenlandse Zaken ontvangt, maar zijn taken onafhankelijk vervult ([454]).

(252) De voornaamste taken van de Judicial Commissioners worden uiteengezet in artikel 229 van de IPA 2016 ([455]). De Judicial Commissioners hebben in het bijzonder een uitgebreide bevoegdheid tot voorafgaande goedkeuring, die deel uitmaakt van de waarborgen die bij de IPA 2016 in het rechtskader van het Verenigd Koninkrijk zijn ingevoerd. Bevelen in verband met gerichte interceptie, materiële interferentie, bulkdatasets met persoonsgegevens, bulksgewijze verkrijging van communicatiegegevens alsook aanzeggingen tot bewaring voor communicatiegegevens moeten alle door een Judicial Commissioner worden goedgekeurd ([456]). De IPC moet ook altijd vooraf toestemming geven voor de verkrijging van communicatiegegevens met het oog op rechtshandhaving ([457]). Indien een Commissioner weigert goedkeuring voor een bevel te geven, kan de Secretary of State in beroep gaan bij de Investigatory Powers Commissioner, wiens besluit definitief is.

([447]) Overeenkomstig artikel 227, leden 7 en 8, van de IPA 2016, is de Investigatory Powers Commissioner een Judicial Commissioner, en worden de Investigatory Powers Commissioner en de andere Judicial Commissioners gezamenlijk aangeduid als de Judicial Commissioners. Momenteel zijn er 15 Judicial Commissioners.

([448]) Overeenkomstig deel 3, artikel 60, lid 2, van de *Constitutional Reform Act 2005* (Britse grondwettelijke hervormingswet van 2005) is een "hoger rechterlijk ambt" het ambt van rechter bij een van de volgende gerechten: Supreme Court; Court of Appeal in Engeland en Wales; iii) de High Court in Engeland en Wales; iv) de *Court of Session* (het hoogste gerecht voor civiele zaken in Schotland); v) de Court of Appeal in Noord-Ierland; vi) de High Court in Noord-Ierland; of Lord of Appeal in Ordinary (lid van het Britse Hogerhuis met rechterlijke bevoegdheid vóór de oprichting van de Supreme Court).

([449]) De onafhankelijkheid van de rechterlijke macht is gebaseerd op verdragen en wordt sinds de *1701 Act of Settlement* (Britse opvolgingswet van 1701) breed erkend.

([450]) Artikel 227, lid 3, van de IPA 2016. Judicial Commissioners moeten ook worden voorgedragen door de Investigatory Powers Commissioner, artikel 227, lid 4, onder e), van de IPA 2016.

([451]) Artikel 238 van de IPA 2016.

([452]) Artikel 227, lid 2, van de IPA 2016.

([453]) De afzettingsprocedure is identiek aan de afzettingsprocedure voor andere rechters in het Verenigd Koninkrijk (zie bijvoorbeeld artikel 11, lid 3, van de *Senior Courts Act 1981* (Britse wet inzake hooggerechtshoven van 1981) en artikel 33 van de Constitutional Reform Act 2005, waarvoor eveneens een resolutie na goedkeuring door het Hoger- en Lagerhuis is vereist). Tot op heden zijn er geen Judicial Commissioners van hun functie ontheven.

([454]) Een arm's-length body is een organisatie die of een agentschap dat financiering van de overheid ontvangt, maar tevens in staat is om onafhankelijk te handelen (zie voor een definitie en meer informatie over een arm's length body het handboek van de Cabinet Office (regeringskanselarij) over de indeling van overheidsinstanties, beschikbaar via de volgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/519571/Classification-of-Public_Bodies-Guidance-for-Departments.pdf en het First Report of session 2014-2015 van de Public Administration Select Committee (commissie die de administratie van overheidsdiensten onderzoekt) van het Britse Lagerhuis, beschikbaar via de volgende link: https://publications.parliament.uk/pa/cm201415/cmselect/cmpubadm/110/110.pdf).

([455]) Overeenkomstig artikel 229 of the IPA 2016 beschikken de Judicial Commissioners over uitgebreide bevoegdheden op het gebied van toezicht die ook het toezicht op de bewaring en verstrekking van de door de inlichtingendiensten verzamelde gegevens omvatten.

([456]) Beslissingen over de vraag of een besluit van de Secretary of State om een bevel uit te vaardigen moet worden goedgekeurd, moeten door de Judicial Commissioners zelf worden genomen. Indien een Commissioner weigert goedkeuring voor een bevel te geven, kan de Secretary of State in beroep gaan bij de Investigatory Powers Commissioner, wiens besluit definitief is.

([457]) De toestemming van de IPC moet altijd worden verkregen wanneer communicatiegegevens worden verkregen met het oog op rechtshandhaving (artikel 60A van de IPA 2016). Wanneer communicatiegegevens zijn verkregen met het oog op de nationale veiligheid, kan de toestemming worden verleend door de IPC of anders door een aangewezen hogere functionaris van de betrokken overheidsinstantie (zie de artikelen 61 en 61A van de IPA 2016 en overweging (203)).

(253) De speciale VN-rapporteur inzake het recht op privacy was zeer ingenomen met de instelling van de Judicial Commissioners bij de IPA 2016, aangezien "gevoelige of ingrijpende verzoeken om toezicht uit te oefenen moeten worden goedgekeurd door zowel een minister van het kabinet als het Investigatory Powers Commissioner's Office". Hij benadrukte met name dat "dit aspect van rechterlijke toetsing [door middel van de rol van de IPC] met behulp van een beter uitgerust team van ervaren inspecteurs en technologiedeskundigen één van de belangrijkste nieuwe waarborgen is die bij de IPA werden ingevoerd, in de plaats van het eerdere versnipperde systeem van toezichthoudende autoriteiten en als aanvulling op de rol van de Intelligence and Security Committee (inlichtingen- en veiligheidscommissie) van het parlement, en van het Investigatory Powers Tribunal" ([458]).

(254) Bovendien heeft de IPC de bevoegdheden om toezicht achteraf te houden, onder andere door middel van audit, inspectie en onderzoek, op de uitoefening van onderzoeksbevoegdheden uit hoofde van IPA 2016 ([459]) en enkele andere in de relevante wetgeving vastgestelde bevoegdheden en functies ([460]). De resultaten van dat toezicht achteraf worden opgenomen in het verslag dat de IPC jaarlijks moet opstellen en indienen bij de Prime Minister ([461]) en dat moet worden gepubliceerd en voorgelegd aan het parlement ([462]). Het verslag bevat relevante statistieken en informatie over de uitoefening van de onderzoeksbevoegdheden door inlichtingendiensten en rechtshandhavingsinstanties alsook de introductie van de waarborgen in verband met zaken die onder het wettelijk verschoningsrecht vallen, vertrouwelijk journalistiek materiaal en bronnen van journalistieke informatie, informatie over de getroffen regelingen en de operationele doeleinden die in de context van bevelen voor bulksgewijze operaties zijn gebruikt. Tot slot is in het jaarverslag van het IPCO vastgesteld op welk gebied aanbevelingen aan overheidsinstanties zijn gedaan en hoe daaraan gevolg is gegeven ([463]).

(255) Overeenkomstig artikel 231 van de IPA 2016, moet de IPC, indien hij kennis krijgt van fouten die overheidsinstanties hebben gemaakt bij de uitoefening van hun onderzoeksbevoegdheden, de betrokkene in kennis stellen indien hij van mening is dat de fout ernstig is en het in het algemeen belang is om de persoon in kennis te stellen ([464]). In het bijzonder wordt in artikel 231 van de IPA 2016 vastgesteld dat de IPC, bij het in kennis stellen van een persoon van een fout, informatie moet verstrekken over de eventuele rechten die de persoon heeft om zich tot het Investigatory Powers Tribunal te richten, en de details moet geven die de Commissioner noodzakelijk acht voor de uitoefening van die rechten, waarbij hij moet nagaan of openbaarmaking van de details in het algemeen belang is ([465]).

([458]) Verklaring bij de beëindiging van zijn opdracht van de speciale rapporteur inzake het recht op privacy bij de afsluiting van zijn missie naar het Verenigd Koninkrijk van Groot-Brittannië en Noord-Ierland (zie voetnoot 281).

([459]) Artikel 229 van de IPA 2016. De voornaamste bevoegdheden van de Judicial Commissioner op het gebied van onderzoek en informatie worden uiteengezet in artikel 235 van de IPA 2016.

([460]) Dit omvat toezichtmaatregelen uit hoofde van de RIPA 2000, de uitoefening van taken op grond van deel 3 van de Police Act 1997 (Britse politiewet van 1997) (goedkeuring van acties met betrekking tot eigendom), en de uitoefening door de Secretary of State van taken uit hoofde van de artikelen 5 tot en met 7 van de Intelligence Services Act 1994 (bevelen tot verstoring van radiotelegrafie, toegang tot en verstoring van eigendom (artikel 229 van de IPA 2016).

([461]) Artikel 230 van de IPA 2016. De IPC kan ook op eigen initiatief verslag uitbrengen aan de Prime Minister over aangelegenheden in verband met zijn taken. De IPC moet ook verslag uitbrengen aan de Prime Minister op diens verzoek en de Prime Minister kan de IPC opdragen taken van de inlichtingendiensten te herzien.

([462]) Bepaalde delen kunnen worden uitgesloten indien publicatie ervan in strijd met de nationale veiligheid zou zijn.

([463]) In het jaarverslag van 2019 van het IPCO (punt 6.38) wordt bijvoorbeeld vermeld dat MI5 was aanbevolen zijn bewaarbeleid voor bulkdatasets met persoonsgegevens aan te passen, aangezien de dienst een aanpak had moet hanteren waarin rekening werd gehouden met de evenredigheid van de bewaring van alle velden in in het bezit zijnde bulkdatasets met persoonsgegevens en voor elke bewaarde bulkdataset met persoonsgegevens. Eind 2018 had het IPCO niet vastgesteld dat deze aanbeveling was opgevolgd en in het verslag van 2019 werd uitgelegd dat MI5 nu een nieuwe procedure aan het invoeren is om aan deze vereiste te voldoen. In het jaarverslag 2019 (punt 8.22) wordt ook vermeld dat aan het GCHQ een reeks aanbevelingen is gedaan betreffende het register waaruit de evenredigheid van hun zoekopdrachten naar bulkgegevens blijkt. In het verslag werd bevestigd dat eind 2018 verbeteringen waren doorgevoerd op dit gebied. Jaarverslag 2019 van het Investigatory Powers Commissioner Office, beschikbaar via de volgende link: https://www.ipco.org.uk/docs/IPC%20Annual%20Report%202019_Web%20Accessible%20version_final.pdf. Bovendien wordt elke inspectie door het IPCO van een overheidsinstantie afgesloten met een verslag dat aan de instantie wordt overhandigd en aanbevelingen bevat die uit de inspectie zijn voortgekomen. Het IPCO start elke daarna volgende inspectie met een evaluatie van eventuele eerdere aanbevelingen van de vorige keer en vermeldt in het nieuwe inspectieverslag of de vorige aanbevelingen zijn opgevolgd of overgebracht.

([464]) Een fout wordt als "ernstig" beschouwd wanneer de Commissioner van mening is dat die schade van betekenis aan de betrokkene heeft berokkend (artikel 231, lid 2, van de IPA 2016). In 2018 werden 22 fouten gemeld waarvan er acht als ernstig werden beschouwd en resulteerden in kennisgeving aan de betrokkene. Zie het jaarverslag van 2018 van het Investigatory Powers Commissioner Office, bijlage C (zie https://www.ipco.org.uk/docs/IPCO%20Annual%20Report%202018%20final.pdf). In 2019 werden 14 fouten als ernstig aangemerkt. Zie het jaarverslag van 2019 van het Investigatory Powers Commissioner Office, bijlage C, zie voetnoot 463.

([465]) In artikel 231 van de IPA 2016 is vastgesteld dat de IPC bij het in kennis stellen van een persoon van een fout de details moet geven die de Commissioner noodzakelijk acht voor de uitoefening van die rechten, waarbij met name rekening wordt gehouden met de mate waarin openbaarmaking van de details in strijd zou zijn met het algemeen belang of nadelige gevolgen zou hebben voor de preventie of opsporing van zware criminaliteit, de economische welvaart van het Verenigd Koninkrijk, of de verdere uitoefening van de taken van elk van de inlichtingendiensten.

3.3.3.3. Parlementair toezicht op de inlichtingendiensten

(256) Het parlementaire toezicht door de Intelligence and Security Committee (ISC) is wettelijk verankerd in de Justice and Security Act 2013 (wet inzake toezicht op de Britse inlichtingendiensten, hierna "JSA 2013" genoemd) ([466]). Bij de wet wordt de ISC opgericht als een commissie van het Britse parlement. De ISC heeft sinds 2013 meer bevoegdheden gekregen, waaronder het toezicht op de operationele activiteiten van veiligheidsdiensten. De ISC heeft uit hoofde van deel 2 van de JSA 2013 de taak om toe te zien op de uitgaven, de administratie, het beleid en de operaties van nationale veiligheidsdiensten. In de JSA 2013 is vastgesteld dat de ISC onderzoeken naar operationele aangelegenheden mag uitvoeren wanneer die geen verband houden met lopende operaties ([467]). In het door de Prime Minister en de ISC ([468]) overeengekomen memorandum van overeenstemming wordt uitvoerig beschreven welke elementen in aanmerking moeten worden genomen wanneer wordt overwogen of een activiteit al dan niet onderdeel van een lopende operatie is ([469]). De ISC kan ook worden verzocht lopende operaties van de Prime Minister te onderzoeken en kan vrijwillig door de diensten verstrekte informatie onderzoeken.

(257) De ISC kan de hoofden van elk van de drie inlichtingendiensten krachtens bijlage 1 bij de JSA 2013 verzoeken om informatie te verstrekken. De dienst moet die informatie ter beschikking stellen, tenzij de Secretary of State daar een veto tegen uitspreekt ([470]). Volgens de uitleg van de Britse autoriteiten wordt in de praktijk zeer weinig informatie achtergehouden voor de ISC ([471]).

(258) De ISC bestaat uit leden die behoren tot het Lager- of het Hogerhuis en die door de Prime Minister zijn benoemd na overleg met de leider van de oppositie ([472]). De ISC is verplicht een jaarverslag bij het parlement in te dienen over de uitoefening van haar taken en andere verslagen die zij passend acht ([473]). Bovendien heeft de ISC het recht om elke drie maanden de lijst te ontvangen van operationele doeleinden die worden gebruikt om het verkregen bulkmateriaal te onderzoeken ([474]). Kopieën van de onderzoeken, inspecties of audits van de Investigatory Power Commissioner worden door de Prime Minister met de ISC gedeeld wanneer de inhoud van de verslagen van belang is voor de wettelijke bevoegdheden van de commissie ([475]). Ten slotte kan de commissie de IPC vragen een onderzoek uit te voeren en moet de Commissioner de ISC in kennis stellen van het besluit om dat onderzoek al dan niet uit te voeren ([476]).

(259) De ISC heeft ook een bijdrage geleverd aan het ontwerp van de IPA 2016, wat tot een aantal wijzigingen heeft geleid die nu in de IPA 2016 zijn overgenomen ([477]). De ISC heeft met name aanbevolen om de bescherming van de persoonlijke levenssfeer te versterken door een reeks privacybeschermingen in te voeren die op alle onderzoeksbe-

([466]) Zoals uitgelegd door de Britse autoriteiten werd met de JSA de toepassing van de ISC verruimd om een rol in het toezicht op de inlichtingendiensten op te nemen die verder gaat dan de drie diensten en toezicht met terugwerkende kracht mogelijk te maken ten aanzien van de operationele activiteiten van de diensten met betrekking tot aangelegenheden van aanzienlijk nationaal belang.

([467]) Artikel 2 van de JSA 2013.

([468]) Memorandum van overeenstemming tussen de Prime minister en de ISC, beschikbaar via de volgende link: http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf

([469]) Memorandum van overeenstemming tussen de Prime minister en de ISC, punt 14, zie voetnoot 468.

([470]) De Secretary of State kan op slechts twee gronden een veto ten aanzien van de verstrekking van informatie uitspreken: de informatie is gevoelig en moet niet aan de ISC worden verstrekt in het belang van de nationale veiligheid; of de informatie is van dien aard dat, indien de Secretary of State zou worden gevraagd om die informatie aan een Departmental Select Committee (toezichtcommissie) van het Britse Lagerhuis te overleggen, de Secretary of State het (op gronden die niet tot de nationale veiligheid zijn beperkt) niet passend acht dat te doen (bijlage 1, punt 4, onder 2), bij de JSA 2013).

([471]) Het UK Explanatory Framework for Adequacy Discussions, section H: National Security, blz. 43, zie voetnoot 31.

([472]) Artikel 1 van de JSA 2013. Ministers kunnen niet tot leden worden benoemd. Leden vervullen hun functie in de ISC voor de zittingsperiode van het parlement gedurende welke zij werden benoemd. Zij kunnen worden afgezet door een resolutie van het huis waardoor zij zijn benoemd, of indien zij geen parlementslid meer zijn, of indien zij minister worden. Een lid kan ook zijn ambt neerleggen.

([473]) Verslagen en verklaringen van de commissie zijn online beschikbaar via de volgende link: https://isc.independent.gov.uk/publications/ . De ISC heeft in 2015 een verslag uitgebracht getiteld "Privacy and Security: A modern and transparent legal framework" (zie: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf), waarin de commissie het rechtskader voor door de inlichtingendiensten gebruikte surveillancetechnieken in ogenschouw heeft genomen en een reeks aanbevelingen heeft gedaan die vervolgens werden beoordeeld en opgenomen in de Investigatory Powers Bill (wetsontwerp inzake onderzoeksbevoegdheden), dat vervolgens werd aangenomen als wetgeving: de IPA 2016. Het antwoord van de regering op het verslag inzake privacy en veiligheid is beschikbaar via de volgende link: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20151208_Privacy_and_Security_Government_Response.pdf

([474]) Artikelen 142, 161 en 183 van de IPA 2016.

([475]) Artikel 234 van de IPA 2016.

([476]) Artikel 236 van de IPA 2016.

([477]) Intelligence and Security Committee van het parlement, verslag betreffende de Investigatory Powers Bill, beschikbaar via de volgende link: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20160209_ISC_Rpt_IPBillweb.pdf

voegdheden van toepassing zijn ([478]). Tevens stelde de commissie wijzigingen voor van de voorgestelde capaciteiten met betrekking tot materiële interferentie, bulkdatasets met persoonsgegevens en communicatiegegevens, en verzocht zij om andere specifieke wijzigingen ter versterking van de beperkingen en waarborgen voor de uitoefening van onderzoeksbevoegdheden ([479]).

3.3.4 *Verhaalmogelijkheden*

(260) Met betrekking tot overheidstoegang om redenen van nationale veiligheid moeten betrokkenen de mogelijkheid hebben een rechtsvordering in te stellen bij een onafhankelijke en onpartijdige rechterlijke instantie om inzage te krijgen in hun persoonsgegevens of om deze gegevens te laten corrigeren of wissen ([480]). Een dergelijke rechterlijke instantie moet met name de bevoegdheid hebben om bindende besluiten over de inlichtingendienst te nemen ([481]). Zoals in de overwegingen (261) tot en met (271) uiteengezet, biedt een aantal verhaalsmogelijkheden betrokkenen in het Verenigd Koninkrijk de mogelijkheid om die rechtsmiddelen te verkrijgen en in te zetten.

3.3.4.1. Beschikbare verhaalmogelijkheden uit hoofde van deel 4 van de DPA

(261) Een betrokkene heeft uit hoofde van artikel 165 van de DPA 2018 het recht een klacht in te dienen bij de Information Commissioner indien de betrokkene van mening is dat er in verband met hem of haar betreffende gegevens sprake is van een inbreuk op deel 4 van de DPA 2018. De Information Commissioner heeft de bevoegdheid de naleving door de verwerkingsverantwoordelijke en de verwerker van de DPA 2018 te beoordelen en hen ertoe te verplichten de noodzakelijke maatregelen te nemen. Bovendien hebben personen krachtens deel 4 van de DPA 2018 het recht de High Court (of de Court of Session in Schotland) te verzoeken om een beschikking die de verwerkingsverantwoordelijke ertoe verplicht het recht op inzage in gegevens ([482]), het recht om bezwaar te maken tegen de verwerking ([483]) en het recht op rectificatie of wissing ([484]) te eerbiedigen.

(262) Personen hebben tevens het recht om vergoeding te vorderen van de schade die zij hebben geleden als gevolg van niet-naleving van een vereiste in deel 4 van de DPA 2018 door de verwerkingsverantwoordelijke of een verwerker ([485]). Schade omvat zowel financiële verliezen als schade zonder financiële verliezen, zoals smart ([486]).

3.3.4.2. Beschikbare verhaalmogelijkheden uit hoofde van de IPA 2016

(263) Personen kunnen bij het Investigatory Powers Tribunal beroep instellen tegen schendingen van de IPA 2016.

(264) Het Investigatory Powers Tribunal is opgericht bij de RIPA 2000 en treedt onafhankelijk op ten opzichte van de uitvoerende macht ([487]). Overeenkomstig artikel 65 van de RIPA 2000 worden de leden van dat Tribunal door Hare Majesteit benoemd voor een periode van vijf jaar. Een lid van dat Tribunal kan door Hare Majesteit van zijn functie worden ontheven op basis van een address ([488]) door het Lager- en het Hogerhuis ([489]).

([478]) Deze algemene taken in verband met de persoonlijke levenssfeer worden nu uiteengezet in artikel 2, lid 2, van de IPA 2016, waarin wordt bepaald dat een overheidsinstantie die uit hoofde van de IPA 2016 handelt, moet nagaan of hetgeen met het bevel, de toestemming of aanzegging wordt nagestreefd redelijkerwijs zou kunnen worden bereikt met andere minder ingrijpende middelen, of een hoger beschermingsniveau in verband met de verkrijging van informatie op grond van het bevel, de toestemming of aanzegging moet worden geboden met het oog op het bijzonder gevoelige karakter van die informatie, het algemene belang van de integriteit en veiligheid van telecommunicatiesystemen en posterijen, en alle overige aspecten van het algemene belang van de bescherming van de persoonlijke levenssfeer.

([479]) Zo is het aantal dagen dat een "urgent" bevel kan gelden voordat de Judicial Commissioner deze moet goedkeuren op verzoek van de ISC bijvoorbeeld teruggebracht van vijf naar drie werkdagen, en heeft de ISC de bevoegdheid gekregen om zaken voor onderzoek naar de Investigatory Powers Commissioner door te verwijzen.

([480]) Schrems II, punt 194.

([481]) Schrems II, punt 197.

([482]) Artikel 94, lid 11, van de DPA 2018.

([483]) Artikel 99, lid 4, van de DPA 2018.

([484]) Artikel 100, lid 1, van de DPA 2018.

([485]) Artikel 169 van de DPA 2018 staat vorderingen toe van "Een persoon die schade lijdt als gevolg van niet-naleving van een vereiste van de wetgeving inzake gegevensbescherming". Volgens de door de Britse autoriteiten verstrekte informatie wordt een vordering of klacht tegen de inlichtingendiensten in de praktijk waarschijnlijk ingediend bij het Investigatory Powers Tribunal, dat ruime bevoegdheid heeft en schadevergoeding kan toekennen, en waarbij het instellen van een vorderingen geen kosten met zich brengt.

([486]) Artikel 169, lid 5, van de DPA 2018.

([487]) De leden moeten krachtens bijlage 3 bij de RIPA 2000 specifieke juridische ervaring hebben en kunnen worden herbenoemd.

([488]) Een "address" is een motie die wordt voorgelegd aan het parlement, waarmee ernaar wordt gestreefd de vorst op de hoogte te stellen van de standpunten van het parlement over een bepaalde kwestie.

([489]) Bijlage 3, punt 1, onder 5), bij de RIPA 2000.

(265) Het Tribunal is krachtens artikel 65 van de RIPA 2000 de passende rechterlijke instantie voor klachten van personen die zich benadeeld achten door gedragingen in het kader van de IPA 2016, de RIPA 2000 of andere gedragingen van de inlichtingendiensten ([490]).

(266) Om zich tot het Investigatory Powers Tribunal te wenden ("procesbevoegdheidsvereiste"), moet een persoon overeenkomstig artikel 65 van de RIPA 2000 ervan overtuigd zijn ([491]) dat de gedraging van een inlichtingendienst heeft plaatsgevonden met betrekking tot hem, zijn eigendom, eventuele door of aan hem verzonden of voor hem bedoelde communicatie, of zijn gebruik van de posterijen, telecommunicatiediensten of telecommunicatiesystemen" ([492]). Bovendien moet de klager ervan overtuigd zijn dat de gedraging onder "betwistbare omstandigheden" ([493]) of "door of namens de inlichtingendiensten" ([494]) heeft plaatsgevonden. Doordat met name deze norm betreffende de "overtuiging" van de betrokkene nogal breed geïnterpreteerd is ([495]), gelden voor het aanhangig maken van een zaak bij dat Tribunal geringe procesbevoegdheidsvereisten.

(267) Wanneer het Investigatory Powers Tribunal een bij hem ingediende klacht behandelt, is het de plicht van het Tribunal om te onderzoeken of de personen tegen wie beschuldigingen worden geuit in de klacht gedragingen met betrekking tot de klager hebben vertoond, en om onderzoek te doen naar de autoriteit die naar verluidt betrokken was bij de schendingen, en om na te gaan of de vermeende gedraging heeft plaatsgevonden ([496]). Wanneer een zaak aan dat Tribunal wordt voorgelegd, moet het dezelfde beginselen hanteren om in die zaak tot een vaststelling te komen als de beginselen die door een rechter zouden worden toegepast bij een verzoek om rechterlijke toetsing ([497]). Bovendien hebben degenen tot wie de bevelen of aanzeggingen/sommaties/beschikkingen uit hoofde van de IPA 2016 zijn gericht, en iedere andere persoon die een functie van de kroon bekleedt, in dienst is bij de politie of de Police Investigations and Review Commissioner (overheidsinstantie van de Schotse regering) de plicht om dat Tribunal alle documenten en informatie te verstrekken of te doen toekomen die het Tribunal kan vragen om het in staat te stellen zijn bevoegdheid uit te oefenen ([498]).

(268) Het Investigatory Powers Tribunal moet de klager meedelen of er al dan niet een vaststelling in zijn voordeel is gedaan ([499]). Het Tribunal heeft krachtens artikel 67, leden 6 en 7, van de RIPA 2000 de bevoegdheid om een uitspraak in kort geding te doen en om vergoeding toe te kennen of andere beschikkingen uit te vaardigen die het passend acht. Het kan hierbij gaan om een beschikking tot vernietiging of intrekking van bevelen of toestemmingen

([490]) Artikel 65, lid 5, van de RIPA 2000.

([491]) Zie wat betreft de norm betreffende de toets van "overtuiging" van de betrokkene de zaak Human Rights Watch/Secretary of State [2016] UKIPTrib15_165-CH, punt 41. In deze zaak heeft het Investigatory Powers Tribunal, onder verwijzing naar de rechtspraak van het Europees Hof voor de Rechten van de Mens, geoordeeld dat moet worden nagegaan of er, met betrekking tot de aangevoerde overtuiging dat onder subartikel 68, lid 5, van de RIPA 2000 vallende gedragingen door of namens een van de inlichtingendiensten hebben plaatsgevonden, enige reden voor die overtuiging bestaat, zodanig dat de persoon slechts kan aanvoeren slachtoffer te zijn geworden van een schending die is veroorzaakt door het louter bestaan van geheime maatregelen of wetgeving die geheime maatregelen toestaat, indien hij kan aantonen dat hij vanwege zijn persoonlijke situatie mogelijk het risico loopt om aan die maatregelen te worden onderworpen.

([492]) Artikel 65, lid 4, punt a), van de RIPA 2000.

([493]) Dergelijke omstandigheden hebben betrekking op gedragingen van overheidsinstanties die met autoriteit (bv. een bevel, een toestemming voor/aanzegging tot de verkrijging van communicatiegegevens enz.) plaatsvinden, of indien de omstandigheden dusdanig zijn dat (ongeacht of dergelijke autoriteit er is) het niet passend zou zijn als de gedraging zonder die autoriteit had plaatsgevonden, of ten minste zonder dat naar behoren is nagegaan of die autoriteit zou moeten worden aangezocht. Door een Judicial Commissioner goedgekeurde gedragingen worden geacht onder betwistbare omstandigheden te hebben plaatsgevonden (artikel 65 (7ZA) van de RIPA 2000), terwijl andere gedragingen die plaatsvinden met toestemming van een persoon die een rechterlijk ambt bekleedt niet worden geacht onder betwistbare omstandigheden te hebben plaatsgevonden (artikel 65, leden 7 en 8, van de RIPA 2000).

([494]) Volgens de door de Britse autoriteiten verstrekte informatie leidt de lage drempel voor het indienen van een klacht ertoe dat het niet ongebruikelijk is dat op basis van het onderzoek van het Tribunal wordt bepaald dat de klager in feite nooit onderwerp van een onderzoek door een overheidsinstantie is geweest. In het meest recente statistisch overzicht van het Investigatory Powers Tribunal staat dat het Tribunal in 2016 209 klachten heeft ontvangen, dat 52 % van die klachten als onbelangrijk of ongerechtvaardigd werd beschouwd en dat voor 25 % "geen vaststelling" werd gedaan. De Britse autoriteiten hebben uitgelegd dat dit betekent dat er ofwel geen geheime activiteiten zijn uitgevoerd of geheime bevoegdheden zijn uitgeoefend met betrekking tot de klager, ofwel geheime technieken zijn gebruikt en dat het Tribunal heeft bepaald dat de activiteit legitiem was. Bovendien werd 11 % als irrelevant terzijde geschoven, ingetrokken of ongeldig verklaard, werd 5 % te laat ingediend en werd 7 % in het voordeel van de klager verklaard. Statistisch overzicht van 2016 van het Investigatory Powers Tribunal, beschikbaar via de volgende link: https://www.ipt-uk.com/docs/IPT%20Statisical%20Report%202016.pdf

([495]) Zie zaak Human Rights Watch/Secretary of State [2016] UKIPTrib15_165-CH. In deze zaak heeft het Investigatory Powers Tribunal, onder verwijzing naar de rechtspraak van het Europees Hof voor de Rechten van de Mens, geoordeeld dat met betrekking tot de overtuiging dat onder subartikel 68, lid 5, van de RIPA 2000 vallende gedragingen door of namens een van de inlichtingendiensten hebben plaatsgevonden, moet worden nagegaan of er enige reden voor die overtuiging bestaat, waaronder het feit dat een persoon slechts kan aanvoeren slachtoffer te zijn geworden van een schending die is veroorzaakt door het louter bestaan van geheime maatregelen of wetgeving die geheime maatregelen toestaat, indien hij kan aantonen dat hij vanwege zijn persoonlijke situatie mogelijk het risico loopt om aan die maatregelen te worden onderworpen (zie de zaak Human Rights Watch/Secretary of State, punt 41).

([496]) Artikel 67, lid 3, van de RIPA 2000.

([497]) Artikel 67, lid 2, van de RIPA 2000.

([498]) Artikel 68, leden 6 en 7 van de RIPA 2000.

([499]) Artikel 68, lid 4, van de RIPA 2000.

en een beschikking tot vernietiging van opgeslagen informatie die is verkregen bij de uitoefening van bevoegdheden die zijn toegekend in het kader van een bevel, toestemming of aanzegging/sommatie/beschikking, of die anderszins door overheidsinstanties worden uitgeoefend met betrekking tot een persoon ([500]). Overeenkomstig artikel 67 bis van de RIPA 2000 kan tegen een vaststelling van het Tribunal beroep worden ingesteld, afhankelijk van toestemming van het Tribunal of de relevante beroepsinstantie.

(269) Ten slotte valt op te merken dat de rol van het Investigatory Powers Tribunal in de context van bij het Europees Hof voor de Rechten van de Mens aanhangige zaken herhaaldelijk is besproken, met name in de zaak Kennedy/het Verenigd Koninkrijk ([501]), en meer recentelijk in de zaak Big Brother Watch e.a./Verenigd Koninkrijk ([502]), waarin de rechter verklaarde dat "het Investigatory Powers Tribunal een solide voorziening in rechte heeft geboden aan eenieder die vermoedde dat zijn of haar communicatie door de inlichtingendiensten was onderschept" ([503]).

3.3.4.3. Andere beschikbare verhaalmogelijkheden

(270) Zoals uitgelegd in de overwegingen (109) tot en met (111), zijn de verhaalsmogelijkheden uit hoofde van de Human Rights Act 1998 en voor het Europees Hof voor de Rechten van de Mens ([504]) ook beschikbaar op het gebied van de nationale veiligheid. In artikel 65, lid 2, van de RIPA 2000 wordt aan het Investigatory Powers Tribunal exclusieve bevoegdheid verleend voor alle rechtsvorderingen uit hoofde van de Human Rights Act in verband met de inlichtingendiensten ([505]). Zoals opgemerkt door de High Court, betekent dit het volgende: "de vraag of er inbreuk is gemaakt op de Human Rights Act met betrekking tot de feiten van een bepaalde zaak kan in principe worden gesteld en beantwoord door een onafhankelijk tribunaal dat toegang kan hebben tot al het relevante materiaal, met inbegrip van geheim materiaal. […] Wij houden in dit verband ook rekening met het feit dat hiermee tegen het Tribunal zelf beroep kan worden ingesteld bij een geschikte beroepsinstantie (in Engeland en Wales zou dat het Court of Appeal zijn); en dat de Supreme Court onlangs heeft besloten dat het Tribunal in principe vatbaar is voor rechterlijke toetsing: zie R (Privacy International)/Investigatory Powers Tribunal [2019] UKSC 22; [2019] 2 WLR 1219" ([506]).

(271) Uit het bovenstaande volgt dat wanneer Britse rechtshandhavingsinstanties of nationale veiligheidsdiensten toegang hebben tot persoonsgegevens die binnen het toepassingsgebied van dit besluit vallen, die toegang wordt geregeld door wetgeving waarin de voorwaarden worden vastgesteld waaronder toegang kan plaatsvinden en wordt gewaarborgd dat de toegang en het verdere gebruik van de gegevens worden beperkt tot hetgeen noodzakelijk en evenredig is voor het nagestreefde doel inzake de rechtshandhaving of de nationale veiligheid. Bovendien moet voor die toegang in de meeste gevallen voorafgaande toestemming worden verkregen van een rechterlijke instantie, door middel van de goedkeuring van een bevel of een beschikking tot overlegging, en in elk geval onafhankelijk toezicht worden uitgeoefend. Wanneer overheidsinstanties eenmaal toegang hebben tot gegevens, gelden voor de verwerking van die gegevens, met inbegrip van verdere deling en verdere doorgifte, specifieke waarborgen inzake gegevensbescherming uit hoofde van deel 3 van de DPA 2018, die in overeenstemming zijn met de in Richtlijn (EU) 2016/680 geboden waarborgen, wanneer er sprake is van verwerking door rechtshandhavingsinstanties, en van deel 4 van de DPA 2018, wanneer er sprake is van verwerking door inlichtingendiensten. Ten slotte genieten betrokkenen op dit gebied effectieve administratieve rechten en rechten op gerechtelijk verhaal, waaronder inzage in hun gegevens of rectificatie of wissing van dergelijke gegevens.

(272) Gezien het belang van die voorwaarden, beperkingen en waarborgen voor de toepassing van dit besluit, zal de Commissie de toepassing en interpretatie van de Britse voorschriften betreffende toegang van de overheid tot gegevens van nabij blijven volgen. Dit omvat relevante ontwikkelingen in de wet- en regelgeving en de jurisprudentie, alsook de activiteiten van de Information Commissioner en andere toezichthoudende autoriteiten op dit gebied. Ook zal bijzondere aandacht worden besteed aan de uitvoering door het Verenigd Koninkrijk van

([500]) Een voorbeeld van de toepassing van die bevoegdheden is de zaak Liberty & Others/the Security Service, SIS, GCHQ, [2015] UKIP Trib 13_77-H_2. Het Tribunal deed een vaststelling in het voordeel van twee klagers, omdat hun communicatie in één zaak buiten de vastgestelde beperkingen werd bewaard en omdat in de andere zaak de onderzoeksprocedure niet was gevolgd zoals neergelegd in de interne voorschriften van het GCHQ. In de eerste zaak droeg de rechter de inlichtingendiensten op de communicatie te vernietigen die langer dan de desbetreffende termijn was bewaard. In de tweede zaak werd geen beschikking tot vernietiging gegeven, omdat de communicatie niet was bewaard.

([501]) *Kennedy,* zie voetnoot 129.

([502]) Europees Hof voor de Rechten van de Mens, Big Brother Watch e.a./Verenigd Koninkrijk, (zie voetnoot 268), punten 413 tot en met 415.

([503]) Europees Hof voor de Rechten van de Mens, Big Brother Watch, punt 425.

([504]) Zoals onder meer blijkt uit de recente uitspraak van de Grote Kamer van het Europees Hof voor de Rechten van de Mens in de zaak Big Brother Watch e.a./Verenigd Koninkrijk (zie voetnoot 279), staat dit doeltreffende rechterlijke toetsing toe — vergelijkbaar met de toetsing waaraan EU-lidstaten onderhevig zijn — door een internationale rechter met betrekking tot de naleving door overheidsinstanties van de grondrechten wanneer zij tot persoonsgegevens verkrijgen. Bovendien is de uitvoering van de rechtspraak van het Europees Hof voor de Rechten van de Mens onderhevig aan specifiek toezicht door de Raad van Europa.

([505]) In Belhaj & others [2017] UKSC 3 was de vaststelling van onrechtmatigheid van de onderschepping van wettelijk beschermd materiaal rechtstreeks gebaseerd op artikel 8 van het EVRM (zie vaststelling 11).

([506]) High Court of Justice, Liberty, [2019] EWHC 2057 (Admin), punt 170.

relevante rechtspraak van het Europees Hof voor de Rechten van de Mens, met inbegrip van de maatregelen die zijn vastgesteld in de "actieplannen" en "verslagen over acties" die bij het Comité van Ministers worden ingediend in de context van het toezicht op de naleving van de uitspraken van het Hof.

4. **CONCLUSIE**

(273) De Commissie is van oordeel dat de UK GDPR en de DPA 2018 een beschermingsniveau voor uit de Europese Unie doorgegeven persoonsgegevens waarborgen dat in feite overeenkomt met het niveau dat bij Verordening (EU) 2016/679 wordt gegarandeerd.

(274) Bovendien is de Commissie van oordeel dat, als geheel genomen, de toezichtsmechanismen en de verhaalsmogelijkheden waarin het Britse recht voorziet, het mogelijk maken om inbreuken in de praktijk vast te stellen en te bestraffen, en betrokkenen rechtsmiddelen bieden om toegang te krijgen tot de hen betreffende persoonsgegevens en, uiteindelijk, om deze gegevens te laten corrigeren of wissen.

(275) Op basis van de beschikbare informatie over de Britse rechtsorde, is de Commissie ten slotte van oordeel dat inbreuken op de grondrechten van de personen wier persoonsgegevens vanuit de Europese Unie door Britse overheidsinstanties naar het Verenigd Koninkrijk worden doorgegeven met het oog op het algemeen belang, met name rechtshandhaving en de nationale veiligheid, zullen worden beperkt tot wat strikt noodzakelijk is om de desbetreffende legitieme doelstelling te verwezenlijken, en dat er sprake is van doeltreffende rechtsbescherming tegen dergelijke inbreuken.

(276) Derhalve moet in het licht van de bevindingen van dit besluit worden besloten dat het Verenigd Koninkrijk een passend beschermingsniveau biedt in de zin van artikel 45 van Verordening (EU) 2016/679, geïnterpreteerd in het licht van het Handvest van de grondrechten van de Europese Unie.

(277) Deze conclusie wordt gebaseerd op de relevante nationale regeling van het Verenigd Koninkrijk en zijn internationale verplichtingen, in het bijzonder de toetreding tot het Europees Verdrag voor de rechten van de mens en onderwerping aan de jurisdictie van het Europees Hof voor de Rechten van de Mens. Voortdurende naleving van dergelijke internationale verplichtingen is derhalve een zeer belangrijk onderdeel van de beoordeling waarop dit besluit is gebaseerd.

5. **GEVOLGEN VAN DIT BESLUIT EN INGRIJPEN VAN GEGEVENSBESCHERMINGSAUTORITEITEN**

(278) De lidstaten en hun organen moeten de maatregelen nemen die noodzakelijk zijn om te voldoen aan de handelingen van de instellingen van de Unie, aangezien deze laatste geacht worden rechtsgeldig te zijn en bijgevolg rechtsgevolgen in het leven roepen zolang zij niet zijn verlopen, ingetrokken, nietig verklaard in een beroep tot nietigverklaring of ongeldig verklaard na een prejudiciële verwijzing of op een exceptie van onwettigheid.

(279) Daarom is een krachtens artikel 45, lid 3, van Verordening (EU) 2016/679 vastgesteld adequaatheidsbesluit van de Commissie bindend voor alle organen van de lidstaten waartoe het is gericht, met inbegrip van hun onafhankelijke toezichthoudende autoriteiten. In het bijzonder kunnen doorgiften van een verwerkingsverantwoordelijke of verwerker in de Europese Unie aan verwerkingsverantwoordelijken of verwerkers in het Verenigd Koninkrijk gedurende de toepassingsperiode van dit besluit plaatsvinden zonder dat daarvoor verdere toestemming is vereist.

(280) Er zij aan herinnerd dat, overeenkomstig artikel 58, lid 5, van Verordening (EU) 2016/679 en zoals door het Hof van Justitie uitgelegd in het arrest in de zaak Schrems ([507]), wanneer een nationale gegevensbeschermingsautoriteit, ook indien na ontvangst van een klacht, de verenigbaarheid van een adequaatheidsbesluit van de Commissie met de grondrechten van de persoon op privacy en gegevensbescherming in twijfel trekt, het nationale recht moet voorzien in een rechtsmiddel voor die persoon om die grieven aan een nationale rechter voor te leggen die eventueel bij prejudiciële verwijzing het Hof van Justitie om beoordeling moet verzoeken ([508]).

([507]) Schrems, punt 65.

([508]) Schrems, punt 65: "In dat verband staat het aan de nationale wetgever om in beroepsgangen te voorzien waarmee bedoelde autoriteit de grieven die zij gegrond acht aan de nationale rechter kan voorleggen, zodat die laatste, wanneer hij de twijfel ten aanzien van de geldigheid van de beschikking van de Commissie deelt, de vraag naar de geldigheid van die beschikking prejudicieel kan verwijzen".

6. **TOEZICHT OP, EN OPSCHORTING, INTREKKING OF WIJZIGING VAN DIT BESLUIT**

(281) Overeenkomstig artikel 45, lid 4, van Verordening (EU) 2016/679 moet de Commissie na de aanneming van dit besluit doorlopend toezicht houden op relevante ontwikkelingen in het Verenigd Koninkrijk om te beoordelen of met het besluit nog altijd een beschermingsniveau wordt gewaarborgd dat in feite overeenkomend is. Dat toezicht is met name in dit geval van belang, aangezien het Verenigd Koninkrijk een nieuw stelsel voor gegevensbescherming zal uitvoeren, toepassen en handhaven, dat niet langer onder het recht van de Europese Unie valt en dat mogelijk nog zal worden gewijzigd. In dat opzicht zal bijzondere aandacht worden besteed aan de toepassing in de praktijk van de Britse voorschriften betreffende de doorgifte van persoonsgegevens naar derde landen, en aan het effect dat die kan hebben op het niveau van de bescherming van gegevens die in het kader van dit besluit worden doorgegeven; aan de doeltreffendheid van de uitoefening van individuele rechten, met inbegrip van relevante ontwikkelingen in de rechtspraktijk met betrekking tot de uitzonderingen op of de beperkingen van die rechten (met name het recht in verband met de instandhouding van een doeltreffende controle van de immigratie); alsook naleving van de beperkingen en waarborgen met betrekking tot overheidstoegang. Ontwikkelingen in de jurisprudentie en het toezicht door de Information Commissioner en andere onafhankelijke instanties zullen onder andere als basis dienen voor de controletaak van de Commissie.

(282) Om deze controle mogelijk te maken, moeten de Britse autoriteiten de Commissie onverwijld in kennis stellen van wezenlijke wijzigingen van de Britse rechtsorde die gevolgen hebben voor het rechtskader waarop dit besluit van toepassing is, alsook van ontwikkelingen in praktijken in verband met de verwerking van persoonsgegevens die in dit besluiten wordt onderzocht, zowel met betrekking tot de verwerking van persoonsgegevens door verwerkingsverantwoordelijken en gegevensverwerkers op grond van de UK GDPR, als tot de beperkingen en waarborgen die op de toegang tot persoonsgegevens door overheidsinstanties van toepassing zijn. Dit moet ook gelden voor ontwikkelingen met betrekking tot de in overweging (281) genoemde elementen.

(283) Teneinde de Commissie in staat te stellen haar toezichthoudende taak doeltreffend uit te voeren, moeten de lidstaten de Commissie bovendien op de hoogte brengen van desbetreffende maatregelen van de nationale gegevensbeschermingsautoriteiten, met name inzake vragen of klachten van betrokkenen uit de EU betreffende de doorgifte van persoonsgegevens vanuit de Europese Unie aan verwerkingsverantwoordelijken of verwerkers in het Verenigd Koninkrijk. Voorts moet de Commissie geïnformeerd worden over eventuele aanwijzingen dat de maatregelen van de Britse overheidsinstanties die verantwoordelijk zijn voor de preventie, het onderzoek, de opsporing of de vervolging van strafbare feiten, of voor de nationale veiligheid, met inbegrip van toezichthoudende instanties, niet het vereiste beschermingsniveau waarborgen.

(284) Wanneer uit de beschikbare informatie, met name informatie die voortvloeit uit het toezicht op dit besluit of verstrekt wordt door de autoriteiten in het Verenigd Koninkrijk of in de lidstaten, blijkt dat het door het Verenigd Koninkrijk geboden beschermingsniveau niet langer passend is, moet de Commissie de bevoegde Britse autoriteiten daarvan onverwijld in kennis stellen en verzoeken dat binnen een opgegeven termijn van maximaal drie maanden geschikte maatregelen worden genomen. Indien nodig kan deze periode voor een bepaalde tijd worden verlengd, rekening houdend met de aard van de problematiek en/of de maatregelen die moeten worden genomen. Een dergelijke procedure zou bijvoorbeeld in gang worden gezet in gevallen waarin verdere doorgifte, onder andere op basis van nieuwe adequaatheidsbepalingen die door de Secretary of State worden aangenomen of door het Verenigd Koninkrijk gesloten internationale overeenkomsten, niet langer zou worden uitgevoerd in het kader van waarborgen die de continuïteit van de bescherming garanderen in de zin van artikel 44 van Verordening (EU) 2016/679.

(285) Indien de bevoegde Britse autoriteiten die maatregelen bij het verstrijken van die opgegeven termijn niet hebben genomen of anderszins niet aannemelijk hebben kunnen maken dat dit besluit op een passend beschermingsniveau gebaseerd blijft, leidt de Commissie de in artikel 93, lid 2, van Verordening (EU) 2016/679 bedoelde procedure in teneinde dit besluit geheel of gedeeltelijk op te schorten of in te trekken.

(286) Als alternatief zal de Commissie deze procedure inleiden met het oog op wijziging van dit besluit, met name door voor gegevensdoorgiften aanvullende voorwaarden te stellen of door de reikwijdte van de vaststelling van adequaatheid te beperken tot gegevensdoorgiften waarvoor een passend beschermingsniveau blijft gewaarborgd.

(287) De Commissie zal om naar behoren gerechtvaardigde dwingende urgente redenen gebruikmaken van de mogelijkheid om overeenkomstig de in artikel 93, lid 3, van Verordening (EU) 2016/679 bedoelde procedure onmiddellijk toepasselijke uitvoeringshandelingen tot opschorting, intrekking of wijziging van het besluit vast te stellen.

7. **DUUR EN VERLENGING VAN DIT BESLUIT**

(288) De Commissie moet rekening houden met het feit dat het Verenigd Koninkrijk, na afloop van de bij het terugtrekkingsakkoord vastgestelde overgangsperiode en zodra de overgangsbepaling uit hoofde van artikel 782 van de handels- en samenwerkingsovereenkomst tussen de Europese Unie en het Verenigd Koninkrijk niet langer van toepassing is, een nieuwe gegevensbeschermingsregeling zal uitvoeren, toepassen en handhaven ten opzichte van de regeling die gold toen het Verenigd Koninkrijk nog gebonden was door het EU-recht. Dit kan met name betrekking hebben op wijzigingen of veranderingen in het kader voor gegevensbescherming dat in dit besluit wordt beoordeeld, alsook op andere relevante ontwikkelingen.

(289) Derhalve moet worden bepaald dat dit besluit van toepassing zal zijn gedurende een periode van vier jaar vanaf de inwerkingtreding ervan.

(290) Indien uit bepaalde uit het toezicht op dit besluit voortvloeiende informatie blijkt dat de bevindingen in verband met de adequaatheid van het in het Verenigd Koninkrijk geboden beschermingsniveau nog steeds feitelijk en juridisch gerechtvaardigd zijn, moet de Commissie uiterlijk zes maanden voordat dit besluit niet meer van toepassing zal zijn, de procedure inleiden tot wijziging van dit besluit door verlenging van de toepassingsduur ervan, in beginsel met een bijkomende periode van vier jaar. Uitvoeringshandelingen tot wijziging van dit besluit moeten overeenkomstig de in artikel 93, lid 2, van Verordening (EU) 2016/679 bedoelde procedure worden vastgesteld.

8. **SLOTOVERWEGINGEN**

(291) Het Europees Comité voor gegevensbescherming heeft zijn advies ([509]) gepubliceerd, waarmee bij het opstellen van dit besluit rekening is gehouden.

(292) De in dit besluit vervatte maatregelen zijn in overeenstemming met het advies van het bij artikel 93 van Verordening (EU) 2016/679 ingestelde comité,

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

Artikel 1

1. Het Verenigd Koninkrijk waarborgt met het oog op de toepassing van artikel 45 van Verordening (EU) 2016/679 een passend beschermingsniveau voor persoonsgegevens die binnen het toepassingsgebied van Verordening (EU) 2016/679 worden doorgegeven vanuit de Europese Unie naar het Verenigd Koninkrijk.

2. Dit besluit heeft geen betrekking op persoonsgegevens die worden doorgegeven met het oog op controle van de immigratie door het Verenigd Koninkrijk of die anderszins vallen binnen de omvang van de vrijstelling van bepaalde rechten van de betrokkene met het oog op instandhouding van doeltreffende controle van de immigratie overeenkomstig paragraaf 4, punt 1, van bijlage 2 bij de DPA 2018.

Artikel 2

Wanneer de bevoegde toezichthoudende autoriteiten in de lidstaten, om personen te beschermen in verband met de verwerking van hun persoonsgegevens, hun bevoegdheden uit hoofde van artikel 58 van Verordening (EU) 2016/679 uitoefenen met betrekking tot gegevensdoorgiften die onder het in artikel 1 vastgestelde toepassingsgebied vallen, stelt de betrokken lidstaat de Commissie daarvan onverwijld in kennis.

Artikel 3

1. De Commissie houdt voortdurend toezicht op de toepassing van het rechtskader waarop dit besluit is gebaseerd, met inbegrip van de voorwaarden voor verdere doorgifte, voor de uitoefening van individuele rechten en voor toegang van Britse overheidsinstanties tot gegevens die op basis van dit besluit worden doorgegeven, teneinde te beoordelen of het Verenigd Koninkrijk een passend beschermingsniveau in de zin van artikel 1 blijft waarborgen.

2. De lidstaten en de Commissie stellen elkaar in kennis van gevallen waarin de Information Commissioner of enige andere bevoegde Britse autoriteit niet garandeert dat het rechtskader waarop dit besluit is gebaseerd wordt geëerbiedigd.

3. De lidstaten en de Commissie stellen elkaar in kennis van eventuele aanwijzingen dat inmenging van de Britse overheidsdiensten in het recht van personen op de bescherming van hun persoonsgegevens verder gaat dan hetgeen strikt noodzakelijk is, of dat er geen doeltreffende rechtsbescherming tegen dergelijke inmenging bestaat.

4. Wanneer de Commissie over aanwijzingen beschikt dat niet langer een passend beschermingsniveau wordt gewaarborgd, stelt zij de bevoegde autoriteiten van het Verenigd Koninkrijk daarvan in kennis en kan zij dit besluit opschorten, intrekken of wijzigen.

([509]) Advies 14/2021 betreffende het ontwerp van uitvoeringsbesluit van de Europese Commissie overeenkomstig Verordening (EU) 2016/679 betreffende de passende bescherming van persoonsgegevens in het Verenigd Koninkrijk, via de volgende link te raadplegen: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-142021-regarding-european-commission-draft_en

5. De Commissie kan dit besluit opschorten, intrekken of wijzigen indien zij door gebrek aan medewerking van de Britse regering niet kan bepalen of er sprake is van beïnvloeding van de bevinding in artikel 1, lid 1.

Artikel 4

Dit besluit verstrijkt op 27 juni 2025, tenzij verlengd volgens de in artikel 93, lid 2, van Verordening (EU) 2016/679 bedoelde procedure.

Artikel 5

Dit besluit is gericht tot de lidstaten.

Gedaan te Brussel, 28 juni 2021.

Voor de Commissie
Didier REYNDERS
Lid van de Commissie

UITVOERINGSBESLUIT (EU) 2021/1773 VAN DE COMMISSIE

van 28 juni 2021

overeenkomstig Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad betreffende de adequate bescherming van persoonsgegevens door het Verenigd Koninkrijk

(Kennisgeving geschied onder nummer C(2021) 4801)

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad ([1]), en met name artikel 36, lid 3,

Overwegende hetgeen volgt:

1. INLEIDING

(1) In Richtlijn (EU) 2016/680 worden de regels uiteengezet voor de doorgifte van persoonsgegevens door bevoegde autoriteiten in de Unie aan derde landen en internationale organisaties voor zover die doorgifte valt onder het toepassingsgebied van die richtlijn. De regels betreffende internationale doorgiften van gegevens door bevoegde autoriteiten zijn vastgesteld in hoofdstuk V van Richtlijn (EU) 2016/680, meer bepaald in de artikelen 35 tot en met 40. De stroom van persoonsgegevens naar en van landen buiten de Europese Unie is van essentieel belang voor doeltreffende samenwerking op het gebied van de rechtshandhaving, maar wel moet worden gewaarborgd dat het beschermingsniveau voor persoonsgegevens in de Europese Unie door dergelijke doorgiften niet wordt aangetast ([2]).

(2) Op grond van artikel 36, lid 3, van Richtlijn (EU) 2016/680 kan de Commissie aan de hand van een uitvoeringshandeling besluiten dat een derde land, een gebied of één of meerdere nader bepaalde sectoren in een derde land, of een internationale organisatie een adequaat beschermingsniveau verzekert. Onder deze voorwaarde mogen doorgiften van persoonsgegevens aan een derde land plaatsvinden zonder dat daarvoor verdere toelating moet worden verkregen (behalve wanneer een andere lidstaat waarvan de gegevens zijn verkregen zijn toestemming aan de doorgifte moet geven), zoals bepaald in artikel 35, lid 1, en overweging 66 van Richtlijn (EU) 2016/680.

(3) Zoals bepaald in artikel 36, lid 2, van Richtlijn (EU) 2016/680 moet de beoordeling van de vraag of het beschermingsniveau adequaat is, gebaseerd zijn op een grondige analyse van de rechtsorde van het derde land. Bij haar beoordeling moet de Commissie nagaan of het betrokken derde land een beschermingsniveau waarborgt dat "in wezen overeenkomt" met het niveau dat in de Europese Unie wordt verzekerd (overweging 67 van Richtlijn (EU) 2016/680). De norm die wordt toegepast om die "wezenlijke overeenkomst" te beoordelen, is de norm die is vastgesteld door de EU-wetgeving, met name Richtlijn (EU) 2016/680, evenals de jurisprudentie van het Hof van Justitie van de Europese Unie ([3]). Ook het vademecum over adequaatheid van het Europees Comité voor gegevensbescherming is in dit verband van belang ([4]).

(4) Zoals het Hof van Justitie van de Europese Unie heeft opgemerkt, is het hiervoor niet noodzakelijk dat hetzelfde beschermingsniveau ([5]) wordt geboden. Met name mogen de middelen die het betrokken derde land tot zijn beschikking heeft voor de bescherming van persoonsgegevens anders zijn dan de middelen die binnen de Europese Unie worden ingezet, zolang zij in de praktijk doeltreffend genoeg blijken om een adequaat beschermingsniveau te bieden ([6]). De adequaatheidsnorm vereist daarom niet dat de voorschriften van de Unie integraal worden overgenomen. Het gaat er veeleer om of het betreffende buitenlandse systeem als geheel het vereiste beschermingsniveau biedt, door de invulling van het recht op privacy, de doeltreffende toepassing en afdwingbaarheid daarvan en het toezicht dat wordt uitgeoefend ([7]).

([1]) PB L 119 van 4.5.2016, blz. 89.

([2]) Zie overweging 64 van Richtlijn (EU) 2016/680.

([3]) Zie voor de recentste jurisprudentie, zaak C-311/18, Maximilian Schrems/Data Protection Commissioner (hierna "Schrems II" genoemd), ECLI:EU:C:2020:559.

([4]) Zie Aanbevelingen 01/2021 over de adequaatheidsreferentie in het kader van de richtlijn gegevensbescherming bij rechtshandhaving, vastgesteld in februari 2021 en beschikbaar via de volgende link: https://edpb.europa.eu/our-work-tools/general-guidance/police-justice-guidelines-recommendations-best-practices_en

([5]) Zaak C-362/14, Maximilian Schrems/Data Protection Commissioner, ECLI:EU:C:2015:650, (hierna "Schrems" genoemd), punt 73.

([6]) Schrems, punt 74.

([7]) Mededeling van de Commissie aan het Europees Parlement en de Raad, "Uitwisseling en bescherming van persoonsgegevens in een geglobaliseerde wereld", COM(2017)7 final van 10.1.2017, punt 3.1., blz. 6-7, beschikbaar via de volgende link: https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52017DC0007&from=EN

(5) De Commissie heeft het relevante recht en de rechtspraktijk van het Verenigd Koninkrijk zorgvuldig geanalyseerd. Op grond van haar bevindingen, die hieronder worden uiteengezet, concludeert de Commissie dat het Verenigd Koninkrijk een adequaat beschermingsniveau verzekert voor persoonsgegevens die onder het toepassingsgebied van Richtlijn (EU) 2016/680 vallen en die door bevoegde autoriteiten in de Unie worden doorgegeven aan bevoegde autoriteiten in het Verenigd Koninkrijk die vallen onder het toepassingsgebied van deel 3 van de *Data Protection Act 2018* (de Britse wet gegevensbescherming, hierna "DPA 2018" genoemd) ([8]).

(6) Dit besluit heeft tot gevolg dat dergelijke doorgiften mogen plaatsvinden gedurende een periode van vier jaar, die mogelijk kan worden verlengd, zonder dat er verdere toelating moet worden verkregen en onverminderd de voorwaarden van artikel 35 van Richtlijn (EU) 2016/680.

2. REGELS DIE GELDEN VOOR DE VERWERKING VAN PERSOONSGEGEVENS DOOR BEVOEGDE AUTORITEITEN MET HET OOG OP DE HANDHAVING VAN HET STRAFRECHT

2.1. Het grondwettelijk kader

(7) Het Verenigd Koninkrijk is een parlementaire democratie. Het land heeft een soeverein parlement, dat boven alle andere overheidsinstellingen staat, een uitvoerende macht die uit leden van het parlement is samengesteld en die aan het parlement verantwoording moet afleggen, en een onafhankelijke rechterlijke macht. Het gezag van de uitvoerende macht berust op het vertrouwen dat zij kan afdwingen van het gekozen *House of Commons* (Lagerhuis) en de uitvoerende macht moet verantwoording afleggen aan beide kamers van het parlement (het House of Commons en het *House of Lords* of Hogerhuis), die verantwoordelijk zijn voor het toezicht op de regering en voor het bespreken en aannemen van wetten. Het Britse parlement heeft bevoegdheden gedelegeerd aan het Schotse parlement, het parlement van Wales (*Senedd Cymru*) en de assemblee van Noord-Ierland om wetgeving vast te stellen met betrekking tot interne kwesties in Schotland, Wales en Noord-Ierland. Hoewel gegevensbescherming een aangelegenheid is die voorbehouden is voor het Britse parlement, d.w.z. dat voor het hele land dezelfde wetgeving geldt, zijn andere beleidsgebieden die voor dit besluit van belang zijn, gedelegeerd. Zo zijn de strafrechtsystemen, met inbegrip van het politiewerk (de activiteiten verricht door de politie) van Schotland en Noord-Ierland gedelegeerd aan het Schots parlement respectievelijk de assemblee van Noord-Ierland ([9]).

(8) Hoewel het Verenigd Koninkrijk niet beschikt over een gecodificeerde grondwet in de zin van een document waarin de grondwet vast verankerd is, zijn de grondwettelijke beginselen van het land, die meer bepaald uit de jurisprudentie en conventies werden afgeleid, in de loop der tijd duidelijk naar voren gekomen. De grondwettelijke waarde van bepaalde *statutes* (geschreven wetten), zoals de *Magna Carta*, de *Bill of Rights* van 1689 en de *Human Rights Act* van 1998 werd erkend. De grondrechten van personen, als onderdeel van de grondwet, werden ontwikkeld aan de hand van common law (rechtsvorming waarin de jurisprudentie leidend is), statutes en internationale verdragen, met name het Europees Verdrag voor de rechten van de mens (EVRM), dat in 1951 door het Verenigd Koninkrijk werd geratificeerd. In 1987 heeft het Verenigd Koninkrijk tevens het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens van de Raad van Europa (hierna "Verdrag 108" genoemd) geratificeerd ([10]).

(9) Met de *Human Rights Act 1998* (mensenrechtenwet 1998) worden de rechten uit het EVRM opgenomen in het recht van het Verenigd Koninkrijk. Deze wet verleent elke persoon de grondrechten en fundamentele vrijheden waarin is voorzien bij de artikelen 2 tot en met 12 en artikel 14 EVRM en bij de artikelen 1, 2 en 3, van het Protocol nr. 1 en artikel 1 van Protocol nr. 13 bij het EVRM, gelezen in samenhang met de artikelen 16, 17 en 18 EVRM. Dit omvat het recht op eerbiediging van privéleven, familie- en gezinsleven, dat op zijn beurt het recht op gegevensbescherming omvat, en het recht op een onpartijdig gerecht ([11]). Overeenkomstig artikel 8 EVRM is geen inmenging van enig openbaar gezag toegestaan in de uitoefening van het recht op eerbiediging van privéleven, familie- en gezinsleven, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van ordeverstoring en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

([8]) Data Protection Act 2018, beschikbaar via de volgende link: https://www.legislation.gov.uk/ukpga/2018/12/contents

([9]) *Explanatory Framework for Adequacy Discussion, section F: Law enforcement* (toelichting van het Verenigd Koninkrijk in het kader van de adequaatheidsdiscussie), beschikbaar via de volgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf

([10]) De beginselen van Verdrag 108 werden aanvankelijk in het recht van het Verenigd Koninkrijk uitgevoerd aan de hand van de Data Protection Act van 1984, die werd vervangen door de DPA 1998 en vervolgens door de DPA 2018 (gelezen in samenhang met de algemene rechtshandeling met betrekking tot gegevensbescherming van het Verenigd Koninkrijk). Het Verenigd Koninkrijk heeft in 2018 eveneens het Protocol tot wijziging van het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (bekend onder de naam "Verdrag 108+") ondertekend en werkt momenteel aan de ratificatie daarvan.

([11]) Artikelen 6 en 8 EVRM (zie ook bijlage 1 bij de Human Rights Act 1998).

(10) Overeenkomstig de Human Rights Act 1998 moet elk optreden van de overheid verenigbaar zijn met een recht dat door het EVRM wordt gewaarborgd ([12]). Bovendien moet primaire en secundaire wetgeving op een wijze worden uitgelegd en uitgevoerd die verenigbaar is met die rechten ([13]). Voor zover personen van mening zijn dat hun rechten, waaronder het recht op eerbiediging van het privéleven en het recht op gegevensbescherming, door een overheidsdienst zijn geschonden, kunnen zij op grond van de Human Rights Act 1998 rechtsherstel vorderen bij de rechtbanken van het Verenigd Koninkrijk en kunnen zij, wanneer hun beroepsmogelijkheden in eigen land uitgeput zijn, uiteindelijk bij het Europees Hof voor de Rechten van de Mens rechtsherstel vorderen voor inbreuken op de uit hoofde van het EVRM gewaarborgde rechten.

2.2. **Het kader voor gegevensbescherming van het Verenigd Koninkrijk**

(11) Op 31 januari 2020 heeft het Verenigd Koninkrijk zich teruggetrokken uit de Unie. Op grond van het Akkoord inzake de terugtrekking van het Verenigd Koninkrijk van Groot-Brittannië en Noord-Ierland uit de Europese Unie en de Europese Gemeenschap voor Atoomenergie ([14]) bleef het Unierecht tijdens de overgangsperiode tot en met 31 december 2020 gelden in het Verenigd Koninkrijk. Vóór de terugtrekking en tijdens de overgangsperiode bestond het rechtskader inzake de bescherming van persoonsgegevens in het Verenigd Koninkrijk waarmee de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de preventie, het onderzoek, de opsporing of de vervolging van strafbare feiten en de uitvoering van straffen wordt geregeld, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid, uit de toepasselijke delen van de Data Protection Act 2018, waarmee Richtlijn (EU) 2016/680 werd omgezet.

(12) Als voorbereiding op de terugtrekking uit de EU stelde de regering van het Verenigd Koninkrijk de *European Union (Withdrawal) Act 2018 (EUWA)* ([15]) (wet inzake de terugtrekking uit de Europese Unie 2018) vast, waarin rechtstreeks toepasselijk Unierecht werd omgezet in het recht van het Verenigd Koninkrijk en waarin werd bepaald dat zogenoemde „*EU-derived domestic legislation*" (van de EU afgeleide interne wetgeving) verder rechtsgevolgen zou blijven hebben na afloop van de overgangsperiode. Deel 3 van de DPA 2018 ([16]) tot omzetting van Richtlijn (EU) 2016/680 vormt „*EU-derived domestic legislation*" in de zin van de EUWA. Overeenkomstig de EUWA moet de ongewijzigde van de EU afgeleide interne wetgeving door de rechtbanken van het Verenigd Koninkrijk worden uitgelegd overeenkomstig de relevante jurisprudentie van het Hof van Justitie van de Europese Unie (hierna "Hof van Justitie" genoemd) en de algemene beginselen van het Unierecht zoals deze onmiddellijk vóór het einde van de overgangsperiode van toepassing waren (respectievelijk „*retained EU case law*" (gehandhaafde EU-jurisprudentie) en „*retained general principles of EU law*" (gehandhaafde algemene beginselen van het Unierecht) genoemd) ([17]).

(13) De ministers van het Verenigd Koninkrijk zijn uit hoofde van de EUWA bevoegd om aan de hand van *statutory instruments* (gedelegeerde handelingen van de uitvoerende macht) secundaire wetgeving in te voeren teneinde in het gehandhaafde Unierecht de nodige wijzigingen door te voeren die voortvloeien uit de terugtrekking van het Verenigd Koninkrijk uit de Unie. Deze bevoegdheid werd uitgeoefend met de *Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (DPPEC Regulations)* ([18]). Met deze rechtshandelingen werd de gegevensbeschermingswetgeving van het Verenigd Koninkrijk, waaronder de DPA 2018, gewijzigd en aangepast aan de binnenlandse context ([19]).

([12]) Artikel 6 van de Human Rights Act 1998.

([13]) Artikel 3 van de Human Rights Act 1998.

([14]) Akkoord inzake de terugtrekking van het Verenigd Koninkrijk van Groot-Brittannië en Noord-Ierland uit de Europese Unie en de Europese Gemeenschap voor Atoomenergie (2019/C 384 I/01), XT/21054/2019/INIT, PB C 384 I van 12.11.2019, blz. 1 (hierna het "Terugtrekkingsakkoord" of "TA"), beschikbaar via de volgende link: https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=EN

([15]) European Union Withdrawal Act 2018, beschikbaar via de volgende link: https://www.legislation.gov.uk/ukpga/2018/16/contents

([16]) Data Protection Act 2018, beschikbaar via de volgende link: https://www.legislation.gov.uk/ukpga/2018/12/contents

([17]) Artikel 6 van de EUWA 2018.

([18]) Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019, beschikbaar via de volgende link: https://www.legislation.gov.uk/uksi/2019/419/contents/made, als gewijzigd bij DPPEC 2020, beschikbaar via de volgende link: https://www.legislation.gov.uk/ukdsi/2020/9780348213522

([19]) In de *Exit Regulations* wordt een aantal wijzigingen aangebracht aan deel 3 van de DPA 2018. Dit zijn veelal technische wijzigingen, zoals de verwijdering van verwijzingen naar "lidstaat" of naar de "richtlijn rechtshandhaving" (zie bijvoorbeeld artikel 48, lid 8, of artikel 73, lid 5, punt a), van de DPA 2018 met "intern recht") zodat deel 3 na afloop van de overgangsperiode doeltreffend werkt als intern recht. Op bepaalde plaatsen waren andere soorten wijzigingen noodzakelijk, bijvoorbeeld in verband met "wie" er "adequaatheidsbesluiten" neemt voor de toepassing van het rechtskader van het Verenigd Koninkrijk inzake gegevensbescherming (zie artikel 74A DPA 2018), namelijk de *Secretary of State* (minister) en niet langer de Europese Commissie.

(14) Bijgevolg zullen de rechtsnormen inzake de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de preventie, het onderzoek, de opsporing of de vervolging van strafbare feiten en de uitvoering van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid in het Verenigd Koninkrijk na de overgangsperiode uit hoofde van het Terugtrekkingsakkoord in de relevante delen van de DPA 2018 uiteengezet blijven, maar wel zoals gewijzigd bij de DPPEC Regulations, met name deel 3 van die rechtshandeling. De Britse *General Data Protection Regulation* (hierna de "UK GDPR" genoemd), de algemene rechtshandeling met betrekking tot gegevensbescherming, is niet van toepassing op dit type verwerking.

(15) Deel 3 van de DPA 2018 voorziet in de regels voor de verwerking van persoonsgegevens met het oog op de handhaving van het strafrecht, met inbegrip van beginselen inzake gegevensbescherming, rechtsgrondslagen van de verwerking (rechtmatigheid), rechten van de betrokkenen, verplichtingen van de bevoegde autoriteiten in hun hoedanigheid van verwerkingsverantwoordelijke en beperkingen op verdere doorgifte. In de delen 5 en 6 van de DPA 2018 wordt meteen ook voorzien in toepasselijke regels inzake toezicht, handhaving en verhaal op het gebied van rechtshandhaving.

(16) In het licht van de belangrijke rol die de politiediensten vervullen op het gebied van rechtshandhaving moeten bovendien de regels voor het politiewerk in beschouwing worden genomen. Aangezien politiewerk een gedecentraliseerde aangelegenheid is, zijn verschillende stukken wetgeving, die inhoudelijk echter vaak niet veel van elkaar verschillen, van toepassing op het politiewerk in a) Engeland en Wales, b) Schotland en c) Noord-Ierland ([20]). Bovendien verschaffen verschillende richtsnoeren aanvullende toelichtingen op de manier waarop de politie haar bevoegdheden moet gebruiken. Er zijn drie belangrijke soorten richtsnoeren voor de politie: 1) wettelijke richtsnoeren die zijn uitgevaardigd uit hoofde van de wetgeving, zoals de *Code of Ethics* ([21]) (gedragscode) en de *Code of Practice on the Management of Police Information* (MoPI Code of Practice, de praktijkcode beheer politie-informatie, MoPI-praktijkcode) ([22]) uitgevaardigd uit hoofde van de *Police Act 1996* ([23]) of PACE-codes ([24]) uitgevaardigd uit hoofde van de *Police and Criminal Evidence Act* ([25]), 2) toegestane beroepspraktijken in verband met het beheer van politie-informatie (*Authorised Professional Practice on the Management of Police Information*, APP-richtsnoeren) ([26]), uitgevaardigd door het *College of Policing* (College van politiezaken) en 3) operationele richtsnoeren (die door de politie zelf worden gepubliceerd). De *National Police Chiefs' Council* (een coördinerend orgaan voor alle politiediensten in het Verenigd Koninkrijk) publiceert operationele richtsnoeren die alle politiediensten hebben goedgekeurd en die derhalve nationaal van toepassing zijn ([27]). Deze richtsnoeren moeten zorgen voor samenhang in de manier waarop informatie door alle politiediensten wordt beheerd ([28]).

(17) De MoPI-praktijkcode werd in 2005 uitgevaardigd door de *Secretary of State* (minister), die daarvoor gebruikmaakte van de bevoegdheden zoals bepaald in artikel 39A van de Police Act 1996 ([29]). Elke praktijkcode die uit hoofde van de *Police Act* wordt uitgevaardigd, moet worden goedgekeurd door de Secretary of State en voor overleg worden voorgelegd aan het *National Crime Agency* (NCA — nationale recherche) voordat deze praktijkcode aan het parlement wordt voorgelegd. Volgens artikel 39A, lid 7, van de Police Act moet de politie codes die uit hoofde van

([20]) Voor een uitvoeriger toelichting over de politiediensten in het Verenigd Koninkrijk en hun bevoegdheden, raadpleeg: *Explanatory Framework for Adequacy Discussion, section F: Law Enforcement* (zie voetnoot 9).

([21]) De gedragscode inzake de beginselen en normen voor het gedrag van politiemedewerkers in Engeland en Wales bij de uitoefening van hun beroep, beschikbaar via de volgende link: https://www.college.police.uk/What-we-do/Ethics/Documents/Code_of_Ethics.pdf; de gedragscode van de politiediensten in Noord-Ierland, beschikbaar via de volgende link: https://www.nipolicingboard.org.uk/psni-code-ethics; de gedragscode voor politiewerk in Schotland, beschikbaar via de volgende link: https://www.scotland.police.uk/about-us/code-of-ethics-for-policing-in-scotland/

([22]) De praktijkcode inzake het beheer van politie-informatie, beschikbaar via de volgende link: http://library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf

([23]) De Police Act 1996, beschikbaar via de volgende link: https://www.legislation.gov.uk/ukpga/1996/16/contents

([24]) Praktijkcodes in verband met de *Police and Criminal Evidence Act 1984 (PACE)* (wet op het verzamelen van bewijs door de politie en het gebruik ervan in strafzaken), beschikbaar via de volgende link: https://www.gov.uk/guidance/police-and-criminal-evidence-act-1984-pace-codes-of-practice

([25]) Police and Criminal Evidence Act 1984 beschikbaar via de volgende link: https://www.legislation.gov.uk/ukpga/1984/60/contents

([26]) Toegestane beroepspraktijken in verband met het beheer van politie-informatie, beschikbaar via de volgende link: https://www.app.college.police.uk/app-content/information-management/management-of-police-information/

([27]) Handleiding gegevensbescherming voor politiemedewerkers met een gegevensbeschermingsopdracht, beschikbaar via de volgende link: https://www.npcc.police.uk/2019%20FOI/IMORCC/225%2019%20NPCC%20DP%20Manual%20Draft%200.11%20Mar%202019.pdf

([28]) De MoPI-praktijkcode (zie voetnoot 22) geldt bijvoorbeeld voor het bewaren van operationele politie-informatie (zie overweging 47 van dit besluit).

([29]) Volgens informatie die door de Britse autoriteiten werd verstrekt, was het College of Policing tijdens de periode van de gesprekken over adequaatheid bezig met de opstelling van een praktijkcode in verband met informatie- en dossierbeheer ter vervanging van de MoPI-praktijkcode. Het ontwerp van die gedragscode werd op 25 januari 2021 gepubliceerd met het oog op een openbare raadpleging en is beschikbaar via de volgende link: https://www.college.police.uk/article/information-records-management-consultation

die wet worden uitgevaardigd naar behoren in acht nemen en wordt dus verwacht dat de politie zich aan die codes houdt ([30]). Bovendien moeten niet-wettelijke richtsnoeren (zoals de APP-richtsnoeren in verband met het beheer van politie-informatie) altijd in overeenstemming zijn met de MoPI-praktijkcode, die voorrang heeft ([31]). Hoewel er bepaalde operationele situaties kunnen bestaan waarin politieagenten van deze richtsnoeren moeten afwijken, moeten zij steeds de voorschriften van deel 3 van de DPA 2018 naleven ([32]).

(18) Verdere richtsnoeren in verband met de gegevenbeschermingswetgeving van het Verenigd Koninkrijk voor de verwerking van gegevens op het gebied van rechtshandhaving worden verstrekt door de *Information Commissioner's Office* (het bureau van de toezichthouder informatie, hierna ook "ICO" genoemd) ([33]) (nadere informatie over het ICO is te vinden in de overwegingen 93 tot en met 109). Hoewel de richtsnoeren geen juridisch bindend karakter hebben, zouden rechtbanken in een rechtszaak verplicht zijn rekening te houden met een inbreuk op die richtsnoeren, aangezien zij van belang zijn voor de interpretatie en aangeven hoe de gegevensbeschermingswetgeving in de praktijk door de *Information Commissioner* wordt uitgelegd en gehandhaafd ([34]).

(19) Tot slot moeten de Britse rechtshandhavingsinstanties, zoals vermeld in de overwegingen 8, 9 en 10, de naleving van het EVRM en Verdrag 108 waarborgen.

(20) Het juridisch kader voor de gegevensverwerking door Britse strafrechtelijke handhavingsinstanties vertoont qua structuur en hoofdonderdelen dus grote gelijkenis met het juridisch kader dat in de EU van toepassing is. Dit omvat het feit dat dit kader niet alleen berust op in het interne recht neergelegde verplichtingen, die zijn vormgegeven door het Unierecht, maar ook op verplichtingen die zijn verankerd in het internationaal recht, met name doordat het Verenigd Koninkrijk zich houdt aan het EVRM en Verdrag 108 en zich onderwerpt aan de rechtspraak van het Europees Hof voor de Rechten van de Mens. Deze verplichtingen die voortvloeien uit juridisch bindende internationale instrumenten, met name betreffende de bescherming van persoonsgegevens, zijn daarom een zeer belangrijk onderdeel van het juridisch kader dat in dit besluit wordt beoordeeld.

2.3. **Materieel en territoriaal toepassingsgebied**

(21) Het materiële toepassingsgebied van deel 3 van de DPA 2018 valt samen met het toepassingsgebied van Richtlijn (EU) 2016/680 zoals bepaald in artikel 2, lid 2, van die richtlijn. Deel 3 van de DPA 2018 is van toepassing op de geheel of gedeeltelijk geautomatiseerde, alsmede op de niet-geautomatiseerde verwerking door een bevoegde autoriteit van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

(22) Om onder het toepassingsgebied van deel 3 van de DPA 2018 te vallen, moet de verwerkingsverantwoordelijke bovendien een bevoegde autoriteit ("*competent authority*") zijn en moet de verwerking worden verricht met het oog op rechtshandhaving ("*law enforcement purpose*"). De gegevensbeschermingsregeling die in dit besluit wordt beoordeeld, is derhalve van toepassing op alle rechtshandhavingsactiviteiten van deze bevoegde autoriteiten.

(23) Het begrip "bevoegde autoriteit" wordt in artikel 30 van de DPA 2018 gedefinieerd als een persoon die is opgenomen in bijlage 7 bij de DPA 2018 evenals elke andere persoon voor zover die persoon wettelijke taken vervult ten behoeve van rechtshandhaving. De bevoegde autoriteiten die in bijlage 7 zijn opgenomen, omvatten niet alleen politiediensten, maar ook alle Britse ministeriële overheidsinstanties evenals andere autoriteiten met een onderzoeksopdracht (bv. de *Commissioner for Her Majesty's Revenue and Customs, de Welsh Revenue Authority, de Competition and Markets Authority, Her Majesty's Land Register of het National Crime Agency*), met vervolging belaste instanties, andere

([30]) In zaak *R v the Commissioner of Police of the Metropolis* [2014] EWCA Civ 585, werd de juridische status van de MoPI-praktijkcode bevestigd en verklaarde *Lord Justice* (rechter in hogere instantie) Laws dat de commissaris van de grootstedelijke politie verplicht is de MoPI-praktijkcode en de APP-richtsnoeren in verband met het beheer van politie-informatie uit hoofde van artikel 39A van de Police Act 1996 in acht te nemen.

([31]) De naleving van de MoPI-praktijkcode door de politie wordt gecontroleerd door *Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services* (HMICFRS, koninklijke inspectiedienst van politie, brandweer en reddingsdiensten).

([32]) Zie in dit verband het standpunt van het College of Policing met betrekking tot de naleving van de APP-richtsnoeren inzake alle onderdelen van het politiewerk, luidens hetwelk "de APP door de beroepsvereniging voor politiewerk (het College of Policing) is erkend als de officiële bron van beroepspraktijken inzake politiewerk. Van politieagenten en -medewerkers wordt verwacht dat zij de APP naleven wanneer zij zich van hun verantwoordelijkheden kwijten. In bepaalde omstandigheden kan een politiedienst echter een legitieme operationele reden hebben om van de APP af te wijken, op voorwaarde dat het duidelijk is waarom dat gebeurt. De politiedienst draagt dan de verantwoordelijkheid voor eventuele plaatselijke en nationale risico's die samenhangen met een optreden dat niet strookt met nationaal overeengekomen richtsnoeren, en als er zich ten gevolge daarvan een incident voordoet of een onderzoek plaatsvindt (bijvoorbeeld door het *Independent Office of Police Conduct*, onafhankelijk bureau voor het politieoptreden), dan is de betrokken politiedienst aansprakelijk voor die risico's", zie https://www.app.college.police.uk/faq-page/.

([33]) *Guide to Law Enforcement Processing*, beschikbaar via de volgende link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/

([34]) Zie de zaak *Bridges v the Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin) waarbij de *High Court* (Hooggerechtshof) opmerkte dat de richtsnoeren van de Information Commissioner weliswaar wettelijk niet-bindend zijn, "maar dat een rechtbank die nagaat of een verwerkingsverantwoordelijke de verplichting uit hoofde van artikel 64 [om een effectbeoordeling inzake de gegevensbescherming uit te voeren met betrekking tot verwerking met een hoog risico] al dan niet heeft nageleefd, rekening zal houden met de richtsnoeren die door de Information Commissioner zijn uitgevaardigd in verband met effectbeoordelingen inzake de gegevensbescherming".

strafrechtelijke instanties en andere functionarissen of organisaties die zijn belast met rechtshandhaving ([35]). Deel 3 van de DPA 2018 geldt ook voor rechtbanken en hoven wanneer zij hun rechterlijke taken uitoefenen, met uitzondering van het gedeelte in verband met de rechten van betrokkenen en ICO-toezicht ([36]). De lijst met bevoegde autoriteiten in bijlage 7 is niet definitief en kan door de Secretary of State aan de hand van *regulations* (een van de eerder genoemde statutory instruments) worden geactualiseerd, met inachtneming van wijzigingen in de organisatie van de openbare diensten ([37]).

(24) De desbetreffende verwerking moet ook dienen voor een "rechtshandhavingsdoeleinde", dat wordt gedefinieerd als de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de uitvoering van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid ([38]). Verwerking door een bevoegde autoriteit wordt niet geregeld in deel 3 van de DPA 2018 wanneer dit niet gebeurt ten behoeve van rechtshandhaving. Dat is bijvoorbeeld het geval wanneer de *Competition and Markets Authority* (Autoriteit Concurrentie en Markten) zaken onderzoekt die niet strafbaar zijn gesteld (bijvoorbeeld fusies tussen ondernemingen). In dat geval zal de UK GDPR, samen met deel 2 van de DPA 2018, van toepassing zijn aangezien de verwerking van persoonsgegevens door bevoegde autoriteiten wordt verricht voor andere doeleinden dan rechtshandhavingsdoeleinden. Om te bepalen welke gegevensbeschermingsregeling (deel 3 of deel 2 van de DPA 2018) van toepassing is op de verwerking van de betrokken persoonsgegevens, moet de bevoegde autoriteit, d.w.z. de verwerkingsverantwoordelijke, nagaan of het hoofddoel van de verwerking een van de rechtshandhavingsdoeleinden in de zin van de DPA 2018 is.

(25) Wat het territoriale toepassingsgebied van deel 3 van de DPA 2018 betreft, is in artikel 207, lid 2, bepaald dat de DPA geldt voor de verwerking van persoonsgegevens in het kader van de activiteiten van een persoon die een vestiging heeft op het gehele grondgebied van het Verenigd Koninkrijk. Dit omvat overheidsinstanties van het grondgebied van Engeland, Wales, Schotland en Noord-Ierland die vallen onder het materiële toepassingsgebied van deel 3 van de DPA 2018 ([39]).

2.3.1. *Definitie van persoonsgegevens en verwerking*

(26) De sleutelbegrippen "persoonsgegevens" en "verwerking" zijn gedefinieerd in artikel 3 van de DPA 2018 en zijn van toepassing in de gehele DPA. De definities sluiten nauw aan bij de overeenkomstige definities in artikel 3 van Richtlijn (EU) 2016/680. Krachtens de DPA 2018 zijn persoonsgegevens alle informatie over een geïdentificeerde of identificeerbare levende persoon ([40]). Op grond van artikel 3, lid 3, van de DPA 2018 is een persoon identificeerbaar als hij/zij direct of indirect kan worden geïdentificeerd aan de hand van de informatie, onder meer met behulp van een verwijzing naar een naam of een identificatiemiddel of naar een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die persoon. Het begrip "verwerking" wordt gedefinieerd als een bewerking of een geheel van bewerkingen met betrekking tot informatie of een geheel van informatie, zoals a) het verzamelen, vastleggen, ordenen, structureren of opslaan; b) het bijwerken of wijzigen; c) het opvragen, raadplegen of gebruiken; d) het verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen; e) het aligneren of combineren; of f) het afschermen, wissen of vernietigen van gegevens. Bovendien wordt "gevoelige verwerking" in de wet gedefinieerd als "a) de verwerking van persoonsgegevens die ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond onthult; b) de verwerking van genetische gegevens of van biometrische gegevens met het oog op de unieke identificatie van een persoon; c) de verwerking van gegevens over gezondheid; d) de verwerking van gegevens betreffende het seksuele gedrag of de seksuele gerichtheid van een persoon" ([41]). In dit verband wordt in artikel 205 van de DPA 2018 de definitie verstrekt van "biometrische gegevens" ([42]), "gegevens over gezondheid" ([43]) en "genetische gegevens" ([44]).

([35]) In bijlage 7 bij de DPA 2018 zijn onder meer de *Director of Service Prosecutions* (hoofd Openbaar Ministerie in strafzaken waarbij leger of politie betrokken zijn), de *Director of Public Prosecutions for Northern Ireland* (hoofd Openbaar Ministerie voor Noord-Ierland) en de Information Commissioner opgenomen.

([36]) Artikel 43, lid 3, van de DPA 2018.

([37]) Artikel 30, lid 3, van de DPA 2018. De inlichtingendiensten (*Secret Intelligence Service, Security Service* en de *Government Communications Headquarters*) worden niet tot de bevoegde autoriteiten (zie artikel 30, lid 2, van de DPA 2018) gerekend en deel 3 van de DPA 2018 geldt niet voor hun activiteiten. Hun activiteiten vallen onder het toepassingsgebied van deel 4 van de DPA 2018.

([38]) Artikel 31 van de DPA 2018.

([39]) Dit betekent dat de DPA 2018 en derhalve dit besluit niet van toepassing zijn op de van de Britse Kroon afhankelijke gebieden en de andere Britse overzeese gebieden, zoals bijvoorbeeld de Falklandeilanden en het grondgebied van Gibraltar.

([40]) Persoonsgegevens met betrekking tot een overleden persoon vallen niet onder het toepassingsgebied van de DPA 2018.

([41]) Artikel 35, lid 8, van de DPA 2018.

([42]) "Biometrische gegevens" zijn persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een persoon op grond waarvan eenduidige identificatie van die persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens.

([43]) "Gegevens over gezondheid" zijn persoonsgegevens die betrekking hebben op de fysieke of mentale gezondheid van een persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn/haar gezondheidstoestand wordt gegeven.

([44]) "Genetische gegevens" zijn persoonsgegevens betreffende de overgeërfde of verworven genetische kenmerken van een persoon die unieke informatie verschaffen over de fysiologie of de gezondheid van die persoon en die met name zijn verkregen door een analyse van een biologisch monster van die persoon.

(27) Artikel 32 van de DPA 2018 verduidelijkt de definities van "verwerkingsverantwoordelijke" en "verwerker" in verband met de verwerking van persoonsgegevens ten behoeve van rechtshandhaving; die definities sluiten nauw aan bij de equivalente definities in Richtlijn (EU) 2016/680. De verwerkingsverantwoordelijke is de bevoegde autoriteit die de doeleinden van en de middelen voor de verwerking van persoonsgegevens vaststelt. Wanneer de verwerking volgens de wet vereist is, is de verwerkingsverantwoordelijke de bevoegde autoriteit waaraan die verplichting door de betrokken wet is opgelegd. Een verwerker is elke persoon die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt (en die geen werknemer is van de verwerkingsverantwoordelijke).

2.4. **Waarborgen, rechten en verplichtingen**

2.4.1. *Rechtmatigheid en behoorlijkheid van de verwerking*

(28) Krachtens artikel 35 van de DPA 2018 moet de verwerking van persoonsgegevens rechtmatig en eerlijk zijn, zoals ook wordt vermeld in artikel 4, lid 1, punt a), van Richtlijn (EU) 2016/680. Overeenkomstig artikel 35, lid 2, van de DPA 2018 is de verwerking van persoonsgegevens ten behoeve van rechtshandhaving alleen rechtmatig als die verwerking gebaseerd is op het recht en ofwel de betrokkene toestemming heeft gegeven voor de verwerking voor dat doel ofwel de verwerking noodzakelijk is voor de vervulling van een taak die met dat doel door een bevoegde autoriteit wordt verricht.

2.4.1.1. Verwerking op basis van het recht

(29) Net als in artikel 8 van Richtlijn (EU) 2016/680 is bepaald, moet een verwerking die valt onder deel 3 van de DPA 2018 op het recht zijn gebaseerd om rechtmatig te zijn. "Rechtmatige" verwerking betekent dat de verwerking is toegestaan op grond van een statute, common law of koninklijk prerogatief ([45]).

(30) De bevoegdheden van de bevoegde autoriteiten worden in het algemeen geregeld door statutes, hetgeen betekent dat hun taken en bevoegdheden duidelijk zijn uiteengezet in door het parlement aangenomen wetgeving ([46]). In bepaalde gevallen kunnen de politie en andere bevoegde autoriteiten die zijn opgenomen in de lijst van bijlage 7 bij de DPA 2018 op common law steunen voor de verwerking van gegevens ([47]). De common law is opgebouwd via precedenten die door beslissingen van de rechtbanken zijn vastgesteld. De common law is relevant in het kader van de bevoegdheden waarover de politie beschikt, die uit deze rechtsbron haar kernopdracht afleidt, namelijk het publiek beschermen door misdrijven op te sporen en te voorkomen ([48]). De politiediensten hebben echter zowel bevoegdheden uit hoofde van de common

([45]) Memorie van toelichting bij de DPA 2018, punt 181, beschikbaar via de volgende link: https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpgaen_20180012_en.pdf.

([46]) Zo ontleent het National Crime Agency zijn bevoegdheden aan de *Crime and Courts Act 2013*, die beschikbaar is via de volgende link: https://www.legislation.gov.uk/ukpga/2013/22/contents. Evenzo zijn de bevoegdheden van het *Food Standards Agency* (het agentschap voor voedselnormen) vastgesteld in de *Food Standards Act 1999*, beschikbaar via de volgende link: https://www.legislation.gov.uk/ukpga/1999/28/contents. Andere voorbeelden zijn de *Prosecution of Offenders Act 1985*, op grond waarvan de *Crown Prosecution Service* (Openbaar Ministerie van de Kroon) is opgericht (zie https://www.legislation.gov.uk/ukpga/1985/23/contents); de *Commissioners for Revenue and Customs Act 2005* op grond waarvan *Her Majesty's Revenue and Customs* (belastingdienst en douaneautoriteit) werd opgericht (zie https://www.legislation.gov.uk/ukpga/2005/11/contents); de *Criminal Procedure (Scotland) Act 1995*, op grond waarvan de *Scottish Criminal Cases Review Commission* werd opgericht (een commissie die vermeende gerechtelijke dwalingen van Schotse rechtbanken onderzoekt, zie https://www.legislation.gov.uk/ukpga/1995/46/contents); de *Justice (Northern Ireland) Act 2002*, op grond waarvan het Openbaar Ministerie voor Noord-Ierland (zie https://www.legislation.gov.uk/ukpga/2002/26/contents) werd opgericht en de *Criminal Justice Act 1987* uit hoofde waarvan het *Serious Fraud Office* (bureau ernstige fraude) werd opgericht en zijn bevoegdheden ontving (zie https://www.legislation.gov.uk/ukpga/1987/38/contents).

([47]) Uit de door de Britse autoriteiten verstrekte informatie blijkt bijvoorbeeld dat de *Lord Advocate*, het hoofd van het Openbaar Ministerie in Schotland binnen de *Crown Office and Procurator Fiscal Service* die verantwoordelijk is voor de vervolging van zaken in Schotland, zijn bevoegdheden om sterfgevallen te onderzoeken en strafbare feiten te vervolgen ontleent aan de common law, terwijl verschillende van zijn taken in een statute zijn vastgelegd. Bovendien ontleent de Kroon, en ontlenen bij uitbreiding verschillende regeringsinstanties, departementen en ministers, hun bevoegdheden aan een combinatie van wetgeving, common law en het koninklijk prerogatief (dit zijn commonlaw-bevoegdheden die aan de Kroon zijn toegewezen, maar die door ministers worden uitgeoefend).

([48]) *Explanatory Framework for Adequacy Discussion, section F: Law Enforcement*, blz. 8 (zie voetnoot 9).

law als uit hoofde van de wet ([49]) om die opdracht uit te voeren. Wanneer de politie een bevoegdheid heeft die op een statute (een geschreven wet) gebaseerd is, komt deze in de plaats van een bevoegdheid op grond van de common law ([50]).

(31) Zoals erkend is door de rechtbanken omvatten de bevoegdheden en verplichtingen van politieagenten op grond van de common law "alle stappen die volgens hen nodig zijn om de vrede te bewaren, misdrijven te voorkomen of eigendom te beschermen tegen geweldmisdrijven" ([51]). Bevoegdheden op grond van de common law zijn geen absolute bevoegdheden. Zij zijn onderworpen aan een reeks beperkingen, onder meer beperkingen die zijn vastgesteld door de rechtbanken ([52]) en door de wetgeving, met name de Human Rights Act 1998 en de *Equality Act 2010* (gelijkheidswet 2010) ([53]). Voor bevoegde autoriteiten die gegevens verwerken krachtens deel 3 van de DPA 2018 houdt dit bovendien in dat zij hun bevoegdheden op grond van de common law moeten uitoefenen in overeenstemming met de voorschriften van de DPA 2018 ([54]). In een besluit om eender welke vorm van gegevensverwerking te verrichten moet voorts rekening worden gehouden met de voorschriften van de toepasselijke richtsnoeren, zoals de MoPI-praktijkcode, en van richtsnoeren die specifiek in een van de landen van het Verenigd Koninkrijk geldig zijn ([55]). De regering en de operationele politie hebben een aantal richtsnoeren uitgevaardigd om ervoor te zorgen dat politieagenten hun bevoegdheden uitoefenen binnen de grenzen die zijn vastgelegd in de common law of de betrokken statute ([56]).

(32) Koninklijke prerogatieven vormen een ander bestanddeel van het recht; zij verwijzen naar bepaalde bevoegdheden waarover de Kroon beschikt en die door de uitvoerende macht mogen worden uitgeoefend, en die niet gebaseerd zijn op een statute, maar voortvloeien uit de soevereiniteit van de vorst ([57]). In de context van de rechtshandhaving zijn slechts enkele voorbeelden van prerogatieve bevoegdheden relevant. Daartoe behoren onder meer het kader voor wederzijdse rechtsbijstand aan de hand waarvan een Secretary of State (minister) met derde landen gegevens kan delen ten behoeve van rechtshandhaving. De bevoegdheid om op deze manier gegevens te delen is niet altijd

([49]) De belangrijkste wetgevingshandelingen waarin de voornaamste politiebevoegdheden zijn vastgelegd (arrestaties, huiszoekingen, verlenging van verzekerde bewaring, afnemen van vingerafdrukken, afnemen van monsters uit de schaamstreek, gerechtelijk bevel tot onderschepping van communicatie, toegang tot communicatiegegevens), zijn: i) voor Engeland en Wales, de *Police and Criminal Evidence Act 1984 (PACE)*, beschikbaar via de volgende link: https://www.legislation.gov.uk/ukpga/1984/60/contents (als gewijzigd bij de *Protection of Freedoms Act 2012 (PoFA)*, beschikbaar via de volgende link: https://www.legislation.gov.uk/ukpga/2012/9/contents) en de *Investigatory Powers Act 2016 (IPA)*, beschikbaar via de volgende link: https://www.legislation.gov.uk/ukpga/2016/25/contents), ii) voor Schotland, de *Criminal Justice (Scotland) Act 2016*, beschikbaar via de volgende link: https://www.legislation.gov.uk/asp/2016/1/contents en de *Criminal Procedure (Scotland) Act 1995*, beschikbaar via de volgende link: https://www.legislation.gov.uk/ukpga/1995/46/contents) iii) voor Noord-Ierland, de *Police and Criminal Evidence (Northern Ireland) Order 1989*, beschikbaar via de volgende link: https://www.legislation.gov.uk/nisi/1989/1341/contents.

([50]) De Britse autoriteiten hebben toegelicht dat de voorrang van statutes (*statutory law*) reeds lang geldt in het Verenigd Koninkrijk, en dateert van het arrest in *Entick v Carrington* [1765] EWHC KB J98, waarin werd erkend dat er grenzen waren aan de uitoefening van bevoegdheden door de uitvoerende macht en het beginsel werd vastgelegd dat de bevoegdheden op grond van de common law en de prerogatieve bevoegdheden van de vorst en de regering ondergeschikt zijn aan de wetten van het land.

([51]) Zie zaak *Rice v Connolly* [1966] 2 QB 414.

([52]) Zie zaak *R(Catt) v Association of Chief Police Officers* [2015] AC 1065, waarin Lord Sumption in verband met de bevoegdheid van de politie om de informatie over een persoon (die een misdrijf had gepleegd) te verkrijgen en te bewaren oordeelde dat de politie volgens de common law de bevoegdheid heeft om informatie te verkrijgen en te bewaren met het oog op politiewerk, d.w.z. in ruime zin voor de handhaving van de openbare orde en de preventie en opsporing van misdrijven. Deze bevoegdheden laten echter geen indringende methoden voor het verkrijgen van informatie toe, zoals de toegang tot privédomein of een handeling (met uitzondering van een arrestatie overeenkomstig de bevoegdheden volgens de common law) die een gewelddaad zou vormen. De rechter was in dit geval van oordeel dat de bevoegdheden op grond van de common law meer dan toereikend waren om toestemming te geven voor het verkrijgen en bewaren van de openbare informatie waarover deze beroepszaken handelden.

([53]) Equality Act 2010, beschikbaar via de volgende link: https://www.legislation.gov.uk/ukpga/2010/15/contents

([54]) Voor een voorbeeld van een zaak waarin de commonlaw-bevoegdheden van de politie werden beoordeeld in het kader van de DPA 1998, zie het besluit van de High Court in *Bridges v the Chief Constable of South Wales Police* (zie voetnoot 33). Zie ook de zaken *Vidal-Hall v Google Inc* [2015] EWCA Civ 311 en *Richard v BBC* [2018] EWHC 1837 (Ch).

([55]) Zie bijvoorbeeld de dienstvoorschriften van de *Police Service of Northern Ireland* (PSNI — de politiedienst van Noord-Ierland) over archiefbeheer, beschikbaar via de volgende link: https://www.psni.police.uk/globalassets/advice–information/our-publications/policies-and-service-procedures/records-management-080819.pdf

([56]) Het Lagerhuis heeft een achtergrondnota gepubliceerd waarin wordt uiteengezet over welke belangrijke bevoegdheden de politie in Engeland en Wales beschikt op grond van de common law en de statutory law (zie https://researchbriefings.files.uk/documents/CBP-8637/CBP-8637.pdf). Zo zijn de bevoegdheden om de vrede van de Kroon te bewaren volgens dit document afgeleid uit de common law, terwijl het gebruik van geweld en de bevoegdheid om mensen aan te houden en te fouilleren altijd afgeleid zijn uit statutes. Daarnaast verstrekt de Schotse regering op haar website informatie over de bevoegdheden van de politie om mensen te arresteren en om ze aan te houden en te fouilleren (zie https://www.gov.scot/policies/police/police-powers/).

([57]) Volgens de door de Britse autoriteiten verstrekte informatie omvatten de prerogatieve bevoegdheden die door de regering worden uitgeoefend onder meer de opstelling en ratificering van verdragen, het voeren van diplomatie en het inzetten van de strijdkrachten binnen het Verenigd Koninkrijk om de politie steun te verlenen bij het bewaren van de vrede.

vastgesteld in een statute ([58]). Koninklijke prerogatieven zijn gebonden door commonlaw-beginselen ([59]) en zijn ondergeschikt aan de statutes, met als gevolg dat zij onderworpen zijn aan de grenzen die zijn bepaald in de Human Rights Act 1998 en de DPA 2018 ([60]).

(33) Net als artikel 8 van Richtlijn (EU) 2016/680 vereist ook de Britse regeling dat de bevoegde autoriteiten om te voldoen aan het rechtmatigheidsbeginsel ervoor moeten zorgen dat, wanneer de verwerking gebaseerd is op het recht, die verwerking ook "noodzakelijk" moet zijn voor de uitvoering van een taak ten behoeve van rechtshandhaving. Het ICO verstrekt hierover richtsnoeren waarin wordt verduidelijkt dat "er sprake moet zijn van een doelgericht en evenredig middel om het doel te bereiken. De rechtsgrondslag is niet van toepassing als het doel redelijkerwijs kan worden bereikt met behulp van andere, minder indringende middelen. Volgens het ICO volstaat het niet dat iemand stelt dat de verwerking noodzakelijk is omdat hij/zij ervoor heeft gekozen zijn/haar bedrijf op een bepaalde manier te runnen. De vraag is of de verwerking noodzakelijk is voor het vermelde doel" ([61]).

2.4.1.2. Verwerking op grond van de toestemming van de betrokkene

(34) Zoals vermeld in overweging 28, is in artikel 35, lid 2, van de DPA 2018 voorzien in de mogelijkheid om persoonsgegevens te verwerken op basis van de toestemming ("*consent*") van de betrokkene.

(35) Toestemming blijkt echter geen rechtsgrond te zijn die relevant is voor de verwerkingsactiviteiten die onder het toepassingsgebied van dit besluit vallen. In feite zullen de verwerkingsactiviteiten die onder dit besluit vallen altijd betrekking hebben op gegevens die uit hoofde van Richtlijn (EU) 2016/680 door een bevoegde autoriteit van een lidstaat zijn doorgegeven aan een Britse bevoegde autoriteit. Die activiteiten zullen daarom doorgaans geen betrekking hebben op de directe interactie (het verzamelen van gegevens) tussen een overheid en betrokkenen die gebaseerd kan zijn op toestemming uit hoofde van artikel 35, lid 2, punt a), van de DPA 2018.

(36) Hoewel het gebruik van toestemming niet relevant wordt geacht voor de beoordeling die uit hoofde van dit besluit wordt verricht, is het volledigheidshalve wel vermeldenswaard dat verwerking in het kader van de rechtshandhaving nooit uitsluitend gebaseerd is op toestemming aangezien een bevoegde autoriteit altijd moet beschikken over een onderliggende bevoegdheid waardoor zij gemachtigd is de gegevens te verwerken ([62]). Meer specifiek en vergelijkbaar met wat is toegestaan uit hoofde van Richtlijn (EU) 2016/680 ([63]), betekent dit dat toestemming dient als een aanvullende voorwaarde om bepaalde begrensde en specifieke verwerkingsactiviteiten mogelijk te maken die anders niet uitgevoerd zouden kunnen worden, bijvoorbeeld de verzameling en verwerking van een DNA-monster van een persoon die geen verdachte is. In dat geval zou de verwerking niet uitgevoerd worden als de toestemming niet wordt gegeven of wordt ingetrokken ([64]).

([58]) Zie in dit verband de beoordeling van de Britse regeling van verdere doorgiften in de overwegingen 74-87.

([59]) Zie zaak *Bancoult v Secretary of State for Foreign and Commonwealth Affairs* [2008] UKHL 61, waarbij de rechters oordeelden dat de prerogatieve bevoegdheid om *Orders in Council* vast te stellen (een koninklijk prerogatief) ook onderworpen was aan de gewone grondslagen van de rechterlijke toetsing.

([60]) Zie zaak *Attorney-General v De Keyser's Royal Hotel Ltd* [1920] [1920] AC 508, waarin de rechter oordeelde dat prerogatieve bevoegdheden niet kunnen worden gebruikt wanneer zij door bevoegdheden op grond van statutes zijn vervangen; zaak *Laker Airways Ltd v Department of Trade* [1977] QB 643, waarin de rechter oordeelde dat prerogatieve bevoegdheden niet kunnen worden gebruikt om statutes terzijde te schuiven; zaak *R v Secretary of State for the Home Department, ex p. Fire Brigades Union* [1995] UKHL 3, waarin de rechter oordeelde dat prerogatieve bevoegdheden niet kunnen worden gebruikt wanneer ze indruisen tegen vastgestelde wetgeving, zelfs wanneer die vastgestelde wetgeving nog niet in werking is getreden; zaak *R (Miller) v Secretary of State for Exiting the European Union* [2017] UKSC 5, waarin de rechter bevestigde dat met statutes prerogatieve bevoegdheden kunnen worden aangepast en opgeheven. Voor een algemeen overzicht van de relatie tussen bevoegdheden op grond van koninklijke prerogatieven en statutes dan wel de common law kunt u de achtergrondnota van het Lagerhuis raadplegen via de volgende link: https://researchbriefings.files.parliament.uk/documents/SN03861/SN03861.pdf

([61]) "What is the first principle about?" in de *Guide to Law Enforcement Processing*, beschikbaar via de volgende link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/#ib2

([62]) Dit volgt uit de formulering van de relevante bepaling van de DPA 2018, waarin is vastgesteld dat de verwerking van persoonsgegevens met het oog op rechtshandhaving alleen rechtmatig is als en voor zover die verwerking gebaseerd is op het recht en ofwel a) de betrokkene toestemming heeft gegeven voor de verwerking voor dat doel, ofwel b) de verwerking noodzakelijk is voor de uitvoering van een taak die met dat doel door een bevoegde autoriteit wordt verricht.

([63]) Zie de overwegingen 35 en 37 van Richtlijn (EU) 2016/680.

([64]) De Britse autoriteiten hebben opgemerkt dat toestemming bijvoorbeeld een passende grondslag voor de verwerking kan zijn wanneer de politie een DNA-monster afneemt met betrekking tot een vermiste persoon om dit te vergelijken met het DNA wanneer er een overledene wordt aangetroffen. In die omstandigheden zou het niet passend zijn dat de politie de betrokkene ertoe dwingt een monster te verstrekken; in plaats daarvan zou de politie de toestemming van de betrokkene moeten vragen, die vrij wordt gegeven en te allen tijde kan worden ingetrokken. Als de toestemming wordt ingetrokken, mogen de gegevens niet langer worden verwerkt, tenzij er een nieuwe rechtsgrond wordt vastgesteld om het monster verder te verwerken (bijvoorbeeld als de betrokkene een verdachte wordt). Een ander voorbeeld doet zich voor wanneer een politiedienst een misdrijf onderzoekt waarin een slachtoffer (van een overval, seksueel misdrijf, huiselijk geweld, of verwanten van een vermoorde persoon of van een ander slachtoffer van een misdrijf) baat zou kunnen hebben bij een doorverwijzing naar *Victim Support* (een onafhankelijke charitatieve instelling die slachtoffers van misdaden en traumatische incidenten ondersteunt). In die omstandigheden zal de politie uitsluitend de persoonlijke informatie, zoals de naam en contactgegevens van de betrokkene, met Victim Support delen als zij daarvoor de toestemming van het slachtoffer heeft.

(37) In gevallen waarin de toestemming van de betrokkene vereist is, moet die toestemming ondubbelzinnig zijn en een duidelijke actieve handeling behelzen ([65]). De politiediensten moeten een privacyverklaring hebben, waarin onder meer de nodige informatie is opgenomen in verband met het geldige gebruik van toestemming. Daarnaast publiceren sommige politiediensten aanvullende informatie over de manier waarop zij de gegevensbeschermingswetgeving naleven, onder meer hoe en wanneer zij toestemming als rechtsgrond zouden gebruiken ([66]).

2.4.1.3. Verwerking van gevoelige gegevens

(38) Wanneer bijzondere categorieën gegevens worden verwerkt, moet worden voorzien in bijzondere waarborgen. In dit verband worden, naar analogie van het bepaalde in artikel 10 van Richtlijn (EU) 2016/680, in deel 3 van de DPA 2018 sterkere waarborgen geboden voor zogenoemde „*sensitive processing*" (verwerking van gevoelige gegevens) ([67]).

(39) Volgens artikel 35, lid 3, van de DPA 1998 kunnen gevoelige gegevens slechts in twee gevallen door bevoegde autoriteiten met het oog op rechtshandhaving worden verwerkt: 1) de betrokkene heeft toestemming gegeven voor de verwerking met het oog op rechtshandhaving en de verwerkingsverantwoordelijke beschikt op het ogenblik waarop de verwerking plaatsvindt over een passend beleidsdocument ([68]); of 2) de verwerking is strikt noodzakelijk ten behoeve van rechtshandhaving, de verwerking voldoet aan ten minste een van de voorwaarden in bijlage 8 bij de DPA 2018, en de verwerkingsverantwoordelijke beschikt op het ogenblik waarop de verwerking plaatsvindt over een passend beleidsdocument ([69]).

(40) Wat het eerste geval betreft, en zoals uiteengezet in overweging 38, wordt het inroepen van toestemming niet relevant geacht voor de doorgiftesituaties als bedoeld in dit besluit ([70]).

(41) Wanneer de verwerking van gevoelige gegevens niet op toestemming berust, kan deze worden verricht aan de hand van een van de voorwaarden die zijn opgenomen in bijlage 8 bij de DPA 2018. Deze voorwaarden hebben betrekking op verwerking die noodzakelijk is voor wettelijke doeleinden; de rechtsbedeling; de bescherming van de vitale belangen van de betrokkene of een andere persoon; de bescherming van kinderen en van personen die risico lopen; rechtsvorderingen; gerechtelijke uitspraken; de voorkoming van fraude; archivering; wanneer

([65]) Er is geen afzonderlijke definitie voor toestemming ("consent") met het oog op de verwerking van persoonsgegevens uit hoofde van deel 3 van de DPA 2018. Het ICO heeft richtsnoeren verstrekt over het begrip toestemming in verband met deel 3 van de DPA 2018 en daarbij verduidelijkt dat dit dezelfde betekenis heeft en strookt met de definitie die in de algemene verordening gegevensbescherming wordt verstrekt, met name dat toestemming een vrije, specifieke en geïnformeerde wilsuiting is en dat de toestemming om de gegevens te laten verwerken gebaseerd moet zijn op een echte keuze ("What is the first principle about?" in de *Guide to Law Enforcement Processing* (zie voetnoot 64) en *Guide to Data Protection* over toestemming, beschikbaar via de volgende link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/).

([66]) Zie bijvoorbeeld de informatie op de webpagina van de politie van Lincolnshire (zie https://www.lincs.police.uk/resource-library/data-protection/law-enforcement-processing/) of op de webpagina van de politie van West Yorkshire (zie https://www.westyorkshire.police.uk/sites/default/files/2018-06/data_protection.pdf).

([67]) Artikel 35, lid 8, van de DPA 2018.

([68]) Artikel 35, lid 4, van de DPA 2018.

([69]) Artikel 35, lid 5, van de DPA 2018.

([70]) Volledigheidshalve is het vermeldenswaard dat, wanneer de verwerking gebaseerd is op toestemming, dit een vrije, specifieke en geïnformeerde wilsuiting moet zijn en dat er een specifieke keuze moet bestaan in verband met de toestemming om de gegevens te laten verwerken. Bovendien moet de verwerkingsverantwoordelijke, wanneer deze een verwerking verricht op grond van de toestemming van de betrokkene, beschikken over een passend beleidsdocument (*appropriate policy document*, APD). Artikel 42 van de DPA 2018 schetst de vereisten waaraan het APD moet voldoen. Daarin wordt gepreciseerd dat in het document ten minste de procedures moeten worden toegelicht die de verwerkingsverantwoordelijke gebruikt om naleving van de gegevensbeschermingsbeginselen te garanderen alsook de beleidsmaatregelen die de verwerkingsverantwoordelijke heeft getroffen in verband met de bewaring en wissing van persoonsgegevens. Overeenkomstig artikel 42 van de DPA 2018 betekent dit dat de verwerkingsverantwoordelijke een document moet voorleggen waarin a) de procedures worden toegelicht die de verwerkingsverantwoordelijke gebruikt om naleving van de gegevensbeschermingsbeginselen te garanderen, en b) de beleidsmaatregelen worden toegelicht die de verwerkingsverantwoordelijke heeft getroffen in verband met de bewaring en wissing van persoonsgegevens op basis van de toestemming van de betrokkene of waarbij een aanwijzing wordt gegeven over hoelang die persoonsgegevens waarschijnlijk zullen worden bewaard. In het beleidsdocument moet meer bepaald zijn vereist dat de verwerkingsverantwoordelijke, bij de naleving van zijn/haar verplichting om de verwerkingsactiviteiten te registreren, altijd rekening moet houden met de in de punten a) en b) genoemde elementen. Het ICO heeft een modeldocument gepubliceerd ("Conditions for sensitive processing", in de *Guide to Law Enforcement* Processing, beschikbaar via de volgende link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/conditions-for-sensitive-processing) en kan dwingende maatregelen treffen als de verwerkingsverantwoordelijken niet aan deze vereisten voldoen. Het APD wordt ook onderzocht door rechtbanken bij de beoordeling van mogelijke inbreuken op de DPA 2018. In de recente zaak *R (Bridges) v Chief Constable of South Wales Police*, bijvoorbeeld, onderzochten de rechters het APD van de verwerkingsverantwoordelijke en kwamen daarbij tot de vaststelling dat dit toereikend was maar dat verdere bijzonderheden nuttig zouden zijn geweest. Bijgevolg herzag de politie van Zuid-Wales dit APD en bracht zij dit in overeenstemming met de nieuwe ICO-richtsnoeren (zie voetnoot 33). Voorts moet het APD krachtens artikel 42, lid 3, van de DPA 2018 regelmatig door de verwerkingsverantwoordelijke worden geëvalueerd. Tot slot is er krachtens artikel 42, lid 4, van de DPA 2018 voorzien in een extra waarborg: de verwerkingsverantwoordelijke moet een uitgebreid register van de verwerkingsactiviteiten bijhouden, met extra elementen in vergelijking met de algemene verplichting van de verwerkingsverantwoordelijke om registers over de verwerkingsactiviteiten bij te houden, zoals vastgesteld in artikel 61 van de DPA 2018.

persoonsgegevens kennelijk openbaar gemaakt zijn door de betrokkene. Met uitzondering van het geval waarin de gegevens kennelijk openbaar zijn gemaakt, worden alle voorwaarden van bijlage 8 aan een toetsing van strikte noodzakelijkheid (“*strict necessity*”) onderworpen. Zoals door het ICO wordt verduidelijkt, “betekent “strikt noodzakelijk” in dit verband dat de verwerking verband moet houden met een dringende sociale behoefte, en dat daaraan redelijkerwijze niet kan worden tegemoetgekomen met minder indringende middelen” ([71]). Bovendien gelden er voor sommige voorwaarden aanvullende beperkingen. Om bijvoorbeeld de voorwaarde “wettelijke doeleinden” of “bescherming” (bijlage 8, punten 1 en 4) te kunnen inroepen, moet er een aanvullende uitgebreide toetsing van het openbaar belang worden verricht. In verband met de voorwaarden met betrekking tot de bescherming van het kind (bijlage 8, punt 4) moet de betrokkene ook een welbepaalde leeftijd hebben en aangemerkt zijn als een persoon die risico loopt. Bovendien kan de verwerkingsverantwoordelijke de in bijlage 8, punt 4, vastgestelde voorwaarde uitsluitend toepassen in welbepaalde omstandigheden ([72]). Evenzo gelden er beperkingen voor de voorwaarden “gerechtelijke uitspraken” en “voorkoming van fraude” (bijlage 8, punten 7 en 8). Beide zijn alleen op specifieke verwerkingsverantwoordelijken van toepassing. Wat gerechtelijke uitspraken betreft, mag alleen een rechtbank of een andere rechterlijke instantie gebruikmaken van een dergelijke voorwaarde, en in het geval van fraudepreventie kunnen alleen verwerkingsverantwoordelijken die fraudebestrijdingsorganisaties zijn deze voorwaarde inroepen.

(42) Wanneer de verwerking tot slot berust op een van de in bijlage 8 vermelde voorwaarden, respectievelijk geschiedt uit hoofde van artikel 42 van de DPA 2018, moet er een passend beleidsdocument bestaan — waarin de procedures worden toegelicht die de verwerkingsverantwoordelijke gebruikt om naleving van de gegevensbeschermingsbeginselen te garanderen en de beleidsmaatregelen worden toegelicht die de verwerkingsverantwoordelijke heeft getroffen in verband met de bewaring en wissing van persoonsgegevens — en gelden de verplichtingen inzake het bijhouden van een uitgebreid register.

2.4.2. *Doelbinding*

(43) Persoonsgegevens moeten worden verwerkt voor een specifiek doel en mogen vervolgens uitsluitend worden gebruikt voor doeleinden die niet onverenigbaar zijn met het doel van de verwerking. Dit gegevensbeschermingsbeginsel wordt gewaarborgd door artikel 36 van de DPA 2018. Net als artikel 4, lid 1, punt b), van Richtlijn (EU) 2016/680 vereist deze bepaling dat a) persoonsgegevens in elk geval voor welbepaalde, uitdrukkelijk omschreven en legitieme rechtshandhavingdoeleinden moeten worden verzameld en b) niet op een met die doeleinden onverenigbare wijze mogen worden verwerkt.

(44) Wanneer bevoegde autoriteiten gegevens verwerken ten behoeve van rechtshandhaving, kan het daarbij gaan om archivering, wetenschappelijk of historisch onderzoek of statistische doeleinden ([73]). In deze gevallen wordt in de DPA 2018 ook verduidelijkt dat archivering (of de verwerking met het oog op wetenschappelijk of historisch onderzoek of voor statistische doeleinden) niet is toegestaan wanneer dit wordt verricht met betrekking tot besluiten in verband met een welbepaalde betrokkene of indien dit wellicht zou leiden tot aanzienlijke schade of leed voor deze betrokkene ([74]).

2.4.3. *Juistheid en gegevensminimalisatie*

(45) De gegevens moeten juist zijn en moeten zo nodig worden bijgewerkt. Zij moeten ook toereikend zijn, ter zake dienend en niet bovenmatig in verhouding tot de doeleinden waarvoor zij worden verwerkt. Deze beginselen worden, naar analogie van het bepaalde in artikel 4, lid 1, punten c), d) en e), van Richtlijn (EU) 2016/680, gewaarborgd in de artikelen 37 en 38 van de DPA 2018. Alle redelijke maatregelen moeten worden genomen om te waarborgen dat onjuiste persoonsgegevens ([75]) onverwijld worden gewist of

([71]) “Conditions for sensitive processing” in de *Guide to Law Enforcement Processing* (zie voetnoot 70).

([72]) De verwerking wordt zonder de toestemming van de betrokkene verricht wanneer: a) de betrokkene geen toestemming tot verwerking kan geven; b) van de verwerkingsverantwoordelijke redelijkerwijs niet kan worden verwacht dat hij/zij de toestemming van de betrokkene voor de verwerking krijgt; c) de verwerking moet worden verricht zonder de toestemming van de betrokkene omdat het verkrijgen van de toestemming van de betrokkene het bieden van bescherming, zoals vermeld in alinea 1, punt a), zou schaden.

([73]) Artikel 41, lid 1, van de DPA 2018.

([74]) Artikel 41, lid 2, van de DPA 2018.

([75]) Volgens artikel 205 van de DPA 2018 wordt onder de term “onjuist” (“*inaccurate*”) verstaan foutieve of misleidende (“*incorrect or misleading*”) persoonsgegevens. De Britse autoriteiten hebben opgemerkt dat gegevens in verband met strafrechtelijke onderzoeken vaak onvolledig, maar desondanks juist kunnen zijn.

rechtgezet ([76]), in het licht van het rechtshandhavingsdoel waarvoor zij worden verwerkt ([77]), en om te waarborgen dat onjuiste, onvolledige of niet langer actuele persoonsgegevens niet worden doorgegeven of beschikbaar worden gesteld voor een van de rechtshandhavingsdoelen ([78]).

(46) Voorts wordt, net als in artikel 7 van Richtlijn (EU) 2016/680, ook in de Britse gegevensbeschermingsregeling gespecificeerd dat persoonsgegevens die op feiten zijn gebaseerd, voor zover mogelijk moeten worden onderscheiden van persoonsgegevens die op een persoonlijk oordeel zijn gebaseerd ([79]). Waar relevant en voor zover mogelijk moet een duidelijk onderscheid worden gemaakt tussen persoonsgegevens in verband met verschillende categorieën van betrokkenen, zoals verdachten, personen die voor een strafbaar feit zijn veroordeeld, slachtoffers van een strafbaar feit en getuigen ([80]).

2.4.4. *Opslagbeperking*

(47) Krachtens artikel 5 van Richtlijn (EU) 2016/680 mogen gegevens in principe niet langer worden bewaard dan nodig is voor de doeleinden waarvoor de persoonsgegevens worden verwerkt. Overeenkomstig artikel 39 van de DPA 2018 en naar analogie van artikel 5 van die richtlijn is het verboden om persoonsgegevens die werden verwerkt met het oog op rechtshandhaving langer te bewaren dan nodig is in verband met het doel waarvoor ze worden verwerkt. Volgens de rechtsorde van het Verenigd Koninkrijk moeten passende termijnen worden vastgelegd voor een periodieke evaluatie van de noodzaak van verdere opslag van persoonsgegevens ten behoeve van rechtshandhaving. Verdere regels voor werkwijzen in verband met de bewaring van persoonsgegevens en de toepasselijke termijnen zijn uiteengezet in de relevante wetgeving en richtsnoeren voor de bevoegdheden en de werking van de politie. In Engeland en Wales, bijvoorbeeld, voorziet de MoPI-praktijkcode van het College of Policing, samen met de APP-richtsnoeren in verband met het beheer van politie-informatie, in een kader dat een consistent op risico's gebaseerd bewarings-, evaluatie- en verwijderingsproces voor het beheer van operationele politie-informatie moet waarborgen ([81]). In dit kader wordt duidelijk uiteengezet wat er van alle diensten wordt verwacht in verband met de manier waarop informatie wordt aangemaakt, gedeeld, gebruikt en beheerd bij en tussen afzonderlijke politiediensten en andere instanties ([82]). Van de politie wordt verwacht dat zij de praktijkcode naleeft en die naleving wordt gecontroleerd door *Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services* ([83]).

(48) De *Police Service of Northern Ireland* (PSNI) is wettelijk niet verplicht om zich aan de MoPI-praktijkcode te houden. Het in 2011 vastgestelde MoPI-kader is echter aangevuld met een *PSNI Handbook* ([84]) waarin beleidsmaatregelen en procedures zijn uiteengezet over de manier waarop de MoPI-praktijkcode in Noord-Ierland wordt toegepast.

([76]) Artikel 38, lid 1, punt b), van de DPA 2018.

([77]) Volgens het Britse *Explanatory Framework for Adequacy Discussion* "zorgt dit ervoor dat zowel de rechten van betrokkenen als de operationele behoeften van rechtshandhavingsinstanties worden erkend. Bovenstaand punt werd zorgvuldig in overweging genomen tijdens de ontwerpstadia van de *Data Protection Bill*, aangezien er specifieke en beperkte operationele redenen kunnen zijn waarom gegevens niet kunnen worden gerectificeerd. Dit zal hoogstwaarschijnlijk het geval zijn als de onjuiste persoonsgegevens in kwestie in hun oorspronkelijke vorm moeten worden bewaard voor gebruik als bewijs" (zie *Explanatory Framework for Adequacy Discussion, section F: Law Enforcement*, blz. 21, zie voetnoot 9).

([78]) Artikel 38, lid 4, van de DPA 2018. Krachtens artikel 38, lid 5, van de DPA 2018 moet daarnaast de kwaliteit van persoonsgegevens worden gecontroleerd voordat zij worden doorgezonden of beschikbaar worden gesteld, en moet in alle doorzendingen van persoonsgegevens de nodige informatie worden opgenomen aan de hand waarvan de ontvanger de mate van juistheid, volledigheid en betrouwbaarheid van de gegevens kan beoordelen evenals de mate waarin de gegevens actueel zijn; indien na doorzending van de persoonsgegevens blijkt dat de gegevens onjuist waren of dat de doorzending onrechtmatig was, moet de ontvanger daarvan onverwijld in kennis worden gesteld.

([79]) Artikel 38, lid 2, van de DPA 2018.

([80]) Artikel 38, lid 3, van de DPA 2018.

([81]) Dit kader waarborgt een consistente bewaring van de verkregen persoonsgegevens. De evaluatieperiode is afhankelijk van de strafbare feiten die in vier groepen zijn ingedeeld: 1) bepaalde aangelegenheden in verband met bescherming van de bevolking; 2) andere seksueel-geweldsdelicten en ernstige strafbare feiten; 3) alle andere strafbare feiten; 4) diversen. Meer informatie is te vinden in de APP-richtsnoeren in verband met het beheer van politie-informatie (zie voetnoot 26).

([82]) Volgens de door de Britse autoriteiten verstrekte informatie staat het andere organisaties vrij zich desgewenst te houden aan de beginselen van de MoPI-praktijkcode. Her Majesty's Revenue and Customs (de belastingdienst en douaneautoriteit) en het National Crime Agency (nationale recherche), bijvoorbeeld, hebben vrijwillig een groot aantal beginselen van de MoPI-praktijkcode overgenomen om consistentie in de rechtshandhaving te waarborgen. Over het algemeen zullen de meeste organisaties voorzien in specifieke beleidsmaatregelen en richtsnoeren voor al hun medewerkers zodat deze weten hoe zij in hun specifieke functie en organisatie moeten omgaan met persoonsgegevens. Dit omvat doorgaans eveneens een verplichte opleiding.

([83]) De MoPI-praktijkcode werd uitgevaardigd op grond van bevoegdheden waarin de Police Act 1996 voorziet en die de College of Policing in staat stellen praktijkcodes in verband met de doeltreffende werking van de politie uit te vaardigen. Elke praktijkcode die uit hoofde van die wet wordt uitgevaardigd, moet worden goedgekeurd door de Secretary of State en voor overleg worden voorgelegd aan de National Crime Agency voordat deze praktijkcode aan het parlement wordt voorgelegd. Volgens artikel 39A, lid 7, van de Police Act 1996 moet de politie codes die uit hoofde van die wet worden uitgevaardigd naar behoren in acht nemen.

([84]) PSNI MoPI Handbook, hoofdstukken 1 tot en met 6.

(49) In Schotland maken de politiediensten gebruik van de *Record Retention Standard Operating Procedure (SOP)* ([85]), een operationele standaardprocedure die dient ter ondersteuning van hun beleid voor archiefbeheer ([86]). In de SOP zijn specifieke archiveringsregels vastgesteld voor de dossiers van de Schotse politie.

(50) Naast het overkoepelende vereiste om dossiers te controleren, dat geldt in het gehele Verenigd Koninkrijk, zijn in plaatselijke regelgeving nadere bijzonderheden vastgesteld. Een paar voorbeelden: met betrekking tot Engeland en Wales zijn in de Police and Criminal Evidence Act, zoals gewijzigd bij de *Protection of Freedom Act 2012 (PoFA)* bepalingen opgenomen betreffende de bewaring van vingerafdrukken en DNA-profielen en betreffende een specifieke regeling voor niet-veroordeelde personen ([87]). Met de PoFA werd ook de functie van *Commissioner for the Retention and Use of Biometric Material* (de *Biometrics Commissioner,* de toezichthouder bewaring en gebruik van biometrische materialen) in het leven geroepen ([88]). Specifieke regels in verband met beeldmateriaal van mensen in verzekerde bewaring zijn vastgesteld in de *Custody Image Review* van 2017 ([89]). Voor Schotland voorziet de *Criminal Procedure (Scotland) Act 1995* in regels voor het verkrijgen en bewaren van vingerafdrukken en biologische monsters ([90]). Net als in Engeland en Wales is de bewaring van biometrische gegevens in verschillende gevallen bij wet geregeld ([91]).

2.4.5. *Beveiliging van gegevens*

(51) Persoonsgegevens moeten op een dusdanige manier worden verwerkt dat de beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. Daartoe moeten overheidsinstanties passende technische of organisatorische maatregelen treffen om de persoonsgegevens te beschermen tegen mogelijke bedreigingen. Bij de beoordeling van die maatregelen moet rekening worden gehouden met de stand van de techniek en de ermee gemoeide kosten.

(52) Deze beginselen komen tot uitdrukking in artikel 40 van de DPA 2018, waarin, naar analogie van het bepaalde in artikel 4, lid 1, punt f), van Richtlijn (EU) 2016/680, is vastgesteld dat persoonsgegevens die worden verwerkt met het oog op rechtshandhaving met gebruikmaking van passende technische of organisatorische middelen op een dusdanige manier moeten worden verwerkt dat de beveiliging ervan gewaarborgd is. Dit behelst ook dat de

([85]) De Record Retention Standard Operating Procedure (SOP) is beschikbaar via de volgende link: https://www.scotland.police.uk/spa-media/nhobty5i/record-retention-sop.pdf

([86]) Raadpleeg voor meer informatie over archiefbeheer de informatie in verband met de *National Records of Scotland* (het nationaal archief van Schotland), beschikbaar via de volgende link: https://www.nrscotland.gov.uk/record-keeping/records-management.

([87]) De bewaartermijnen verschillen naargelang van de vraag of een persoon al dan niet veroordeeld werd (artikelen 63I tot en met 63KI van de PACE 1984). Wanneer bijvoorbeeld een volwassene is veroordeeld voor een strafbaar feit waarover de politie een dossier moet bijhouden, is het mogelijk dat zijn/haar vingerafdrukken en DNA-profiel voor onbepaalde tijd worden bewaard (artikel 63I, lid 2, van de PACE 1984), terwijl die bewaartermijn beperkt blijft als de veroordeelde jonger is dan 18 jaar, als het gaat om een minder zwaar strafbaar feit waarvoor een dossier moet worden bijgehouden en als de desbetreffende persoon niet eerder veroordeeld werd (artikel 63K van de PACE 1984). Voor een persoon die werd gearresteerd en aangeklaagd, maar niet veroordeeld, is de bewaartermijn beperkt tot drie jaar (artikel 63F van de PACE 1984). De verlenging van deze bewaartermijn moet worden goedgekeurd door een rechterlijke instantie (artikel 63F, lid 7, van de PACE 1984). Indien iemand werd gearresteerd of aangeklaagd, maar niet werd veroordeeld voor een minder zwaar strafbaar feit, mogen zijn/haar vingerafdrukken en DNA-profiel niet worden bewaard (artikel 63D en artikel 63H van de PACE 1984).

([88]) Bij artikel 20 van de PoFA 2012 werd de functie van Biometrics Commissioner in het leven geroepen. De Biometrics Commissioner beslist onder meer of de politie al dan niet DNA-profielen en vingerafdrukken mag bewaren die werden verkregen van gearresteerden die niet werden beschuldigd van een strafbaar feit dat hiervoor in aanmerking komt (artikel 63G van de PACE 1984). Bovendien heeft de Biometrics Commissioner de algemene verantwoordelijkheid om toezicht uit te oefenen op de bewaring en het gebruik van DNA en vingerafdrukken, en de bewaring om redenen van nationale veiligheid (artikel 20, lid 2, van de POFA 2012). De Biometrics Commissioner wordt benoemd conform de *Code for Public Appointments* (code voor benoemingen bij de overheid; de code is beschikbaar via de volgende link: Governance Code for Public Appointments - GOV.UK (www.gov.uk)) en in zijn/haar benoemings-voorwaarden staat duidelijk dat hij/zij alleen onder bepaalde nauwkeurig omschreven omstandigheden uit zijn/haar functie kan worden ontheven door de minister van Binnenlandse Zaken; het gaat daarbij onder meer om het niet uitvoeren van zijn/haar taken gedurende een periode van drie maanden, veroordeling wegens een strafbaar feit of niet-naleving van de voorwaarden van zijn/haar benoeming.

([89]) Beoordeling van het gebruik en de bewaring van beeldmateriaal van mensen in verzekerde bewaring, beschikbaar via de volgende link: https://www.gov.uk/government/publications/custody-images-review-of-their-use-and-retention

([90]) Artikel 18 en volgende van de Criminal Procedure (Scotland) Act 1995.

([91]) De bewaartermijnen verschillen naargelang het feit of de persoon al dan niet veroordeeld werd (artikel 18, lid 3, van de Criminal Procedure (Scotland) Act 1995) of al dan niet minderjarig is. In het laatste geval is de bewaartermijn drie jaar vanaf de veroordeling ter terechtzitting van het kind (artikel 18E, lid 8, van de Criminal Procedure (Scotland) Act 1995). Gegevens van gearresteerden die niet zijn veroordeeld mogen niet worden bewaard (artikel 18, lid 3, van de Criminal Procedure (Scotland) Act 1995) tenzij in specifieke gevallen en afhankelijk van de ernst van het strafbare feit (artikel 18A van de Criminal Procedure (Scotland) Act 1995). Bij de *Scottish Biometrics Commissioner Act 2020* (zie https://www.legislation.gov.uk/asp/2020/8/contents) wordt de functie van *Scottish Biometrics Commissioner* gecreëerd, de Schotse toezichthouder biometrische gegevens, die (door het Schots parlement goedgekeurde) praktijkcodes moet opstellen en herzien betreffende de verwerving, de bewaring, het gebruik en de vernietiging van biometrische gegevens voor strafrechtelijke en politiële doeleinden (artikel 7 van de Scottish Biometrics Commissioner Act 2020).

gegevens beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging ([92]). In artikel 66 van de DPA 2018 is voorts bepaald dat elke verwerkingsverantwoordelijke en elke verwerker passende technische en organisatorische maatregelen moet treffen om een beveiligingsniveau te waarborgen dat is afgestemd op de risico's die voortvloeien uit de verwerking van persoonsgegevens. Volgens de memorie van toelichting moet de verwerkingsverantwoordelijke de risico's analyseren en passende veiligheidsmaatregelen toepassen op basis van deze analyse, bijvoorbeeld encryptie of veiligheidsmachtigingen van een bepaald niveau voor de medewerkers die de gegevens verwerken ([93]). In de analyse moet ook rekening worden gehouden met, bijvoorbeeld, de aard van de verwerkte gegevens en andere relevante factoren of omstandigheden die de veiligheid van de verwerking nadelig zouden kunnen beïnvloeden.

(53) De regeling in verband met de naleving van de gegevensbeschermingsbeginselen loopt sterk gelijk met de regeling die is vastgesteld bij de artikelen 29, 30 en 31 van Richtlijn (EU) 2016/680. Wanneer zich een inbreuk in verband met persoonsgegevens voordoet waarvoor de verwerkingsverantwoordelijke verantwoordelijk is, moet deze laatste, overeenkomstig artikel 67, lid 1, van de DPA 2018, zonder onnodige vertraging en indien mogelijk niet meer dan 72 uur nadat hij/zij ervan kennis heeft genomen, deze inbreuk melden aan de Information Commissioner ([94]). Deze meldingsplicht geldt niet wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk geen risico met zich meebrengt voor de rechten en vrijheden van personen ([95]). De verwerkingsverantwoordelijke moet de feiten omtrent een inbreuk, de gevolgen ervan en de genomen corrigerende maatregelen dusdanig documenteren dat de Information Commissioner de naleving van de DPA kan controleren ([96]). Als een verwerker in kennis wordt gesteld van een inbreuk op de beveiliging, moet deze die inbreuk zonder onnodige vertraging melden aan de verwerkingsverantwoordelijke ([97]).

(54) Als een inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van personen, moet de verwerkingsverantwoordelijke, krachtens artikel 68, lid 1, van de DPA 2018, de betrokkene zonder onnodige vertraging in kennis stellen van die inbreuk ([98]). De melding moet dezelfde informatie bevatten als de in overweging 53 bedoelde kennisgeving aan de Information Commissioner. Deze verplichting geldt niet wanneer de verwerkingsverantwoordelijke passende technische en organisatorische beschermingsmaatregelen heeft genomen, die zijn toegepast op de persoonsgegevens waarop de inbreuk in verband met persoonsgegevens betrekking heeft. Deze verplichting geldt evenmin als de verwerkingsverantwoordelijke achteraf maatregelen heeft genomen om ervoor te zorgen dat het hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen. Tot slot hoeft de verwerkingsverantwoordelijke de betrokkene geen melding te doen als dit een onevenredige inspanning zou vergen ([99]). In dat geval moet de informatie op een andere, even doeltreffende manier aan de betrokkene beschikbaar worden gesteld, bijvoorbeeld via een openbare mededeling ([100]). Indien de verwerkingsverantwoordelijke de inbreuk in verband met persoonsgegevens nog niet aan de betrokkene heeft meegedeeld, kan de Information Commissioner, na ontvangst van de melding krachtens artikel 67 van de DPA en na te hebben nagegaan of de inbreuk in verband met persoonsgegevens een hoog risico met zich meebrengt, de verwerkingsverantwoordelijke ertoe verplichten de inbreuk te melden aan de betrokkene ([101]).

([92]) Overeenkomstig de memorie van toelichting bij de DPA 2018 (zie voetnoot 45) moet de verwerkingsverantwoordelijke meer bepaald: zijn/haar beveiliging dusdanig ontwerpen en organiseren dat deze past bij de aard van de persoonsgegevens die hij/zij bijhoudt en bij de schade die uit een inbreuk op de beveiliging kan voortvloeien; duidelijk aangeven wie in zijn/haar organisatie verantwoordelijk is voor de informatiebeveiliging; ervoor zorgen dat hij/zij over de juiste fysieke en technische beveiliging beschikt, ondersteund door robuuste beleidsmaatregelen en procedures en betrouwbare, goed opgeleide medewerkers, en klaarstaan om snel en doeltreffend te reageren op elke inbreuk op de beveiliging.

([93]) Punt 221 van de memorie van toelichting bij de DPA 2018 (zie voetnoot 45).

([94]) In artikel 67, lid 4, van de DPA 2018 is bepaald dat de kennisgeving een beschrijving moet bevatten van de aard van de inbreuk in verband met persoonsgegevens (met, zo mogelijk, vermelding van de categorieën van betrokkenen en gegevensbestanden in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensbestanden in kwestie), de naam en contactgegevens van een contactpunt, een beschrijving van de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens en een beschrijving van de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken (waaronder in voorkomend geval maatregelen ter beperking van de eventuele nadelige gevolgen daarvan).

([95]) Artikel 67, lid 2, van de DPA 2018.

([96]) Artikel 67, lid 6, van de DPA 2018.

([97]) Artikel 67, lid 9, van de DPA 2018.

([98]) Krachtens artikel 68, lid 7, van de DPA 2018 mag de verwerkingsverantwoordelijke de informatieverstrekking aan de betrokkene geheel of gedeeltelijk beperken in de mate dat en voor zover de beperking ten aanzien van de grondrechten en legitieme belangen van de betrokkene een noodzakelijke en evenredige maatregel is om a) belemmering van officiële of gerechtelijke onderzoeken of procedures te voorkomen; b) nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek of de vervolging van strafbare feiten of de uitvoering van straffen te voorkomen; c) de openbare veiligheid te beschermen; d) de nationale veiligheid te beschermen; e) de rechten en vrijheden van anderen te beschermen.

([99]) Artikel 68, lid 3, van de DPA 2018.

([100]) Artikel 68, lid 5, van de DPA 2018.

([101]) Artikel 68, lid 6, van de DPA 2018, met inachtneming van de beperking vastgesteld in artikel 68, lid 8, van de DPA 2018.

2.4.6. *Transparantie*

(55) Betrokkenen moeten worden ingelicht over de belangrijkste kenmerken van de verwerking van hun persoonsgegevens. Dit beginsel komt tot uitdrukking in artikel 44 van de DPA 2018 waarin, net als in artikel 13 van Richtlijn (EU) 2016/680, is bepaald dat de verwerkingsverantwoordelijke de algemene verplichting heeft om de betrokkenen informatie over de verwerking van hun persoonsgegevens te bezorgen (door die informatie algemeen beschikbaar of op een andere manier ter beschikking te stellen) ([102]). De informatie die ter beschikking moet worden gesteld, omvat a) de identiteit en contactgegevens van de verwerkingsverantwoordelijke; b) in voorkomend geval, de contactgegevens van de functionaris voor gegevensbescherming; c) de doeleinden van de verwerking waarvoor de persoonsgegevens zijn bestemd; d) het bestaan van het recht van de betrokkenen om de verwerkingsverantwoordelijke te verzoeken om toegang tot en rectificatie of wissing van hun persoonsgegevens, of beperking van de verwerking ervan; e) het bestaan van het recht een klacht in te dienen bij de Information Commissioner en de desbetreffende contactgegevens ([103]).

(56) In specifieke gevallen met als doel de uitoefening van de rechten van een betrokkene krachtens de DPA 2018 mogelijk te maken (bijvoorbeeld wanneer de verwerkte persoonsgegevens werden verzameld zonder medeweten van de betrokkene), moet de verwerkingsverantwoordelijke de betrokkene informatie geven over a) de rechtsgrond van de verwerking; b) de periode gedurende welke de persoonsgegevens zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen; c) in voorkomend geval, de categorieën van ontvangers van de persoonsgegevens, ook in derde landen of internationale organisaties; d) indien noodzakelijk, extra informatie die nodig is om de betrokkene in staat te stellen zijn/haar rechten uit hoofde van deel 3 van de DPA 2018 uit te oefenen ([104]).

2.4.7. *Individuele rechten*

(57) Aan betrokkenen moet een aantal afdwingbare rechten worden verleend. In deel 3, hoofdstuk 3, van de DPA 2018 is bepaald dat personen recht hebben op inzage, rectificatie, wissing en beperking ([105]); deze rechten zijn vergelijkbaar met de rechten als bedoeld in hoofdstuk III van Richtlijn (EU) 2016/680.

(58) Het inzagerecht is neergelegd in artikel 45 van de DPA 2018. Ten eerste heeft de betrokkene het recht om van de verwerkingsverantwoordelijke uitsluitsel te krijgen over de al dan niet verwerking van hem/haar betreffende persoonsgegevens ([106]). Ten tweede heeft de betrokkene, wanneer zijn/haar persoonsgegevens worden verwerkt, het recht om die persoonsgegevens in te zien en om de volgende informatie over de verwerking te verkrijgen: a) de doeleinden van en de rechtsgrond voor de verwerking; b) de betrokken gegevenscategorieën; c) de ontvanger aan wie de gegevens zijn bekendgemaakt; d) de periode gedurende welke de persoonsgegevens worden opgeslagen; e) het recht van de betrokkene om de persoonsgegevens te laten rectificeren of wissen; f) het recht om een klacht in te dienen, en g) alle informatie over de oorsprong van de desbetreffende persoonsgegevens ([107]).

(59) Krachtens artikel 46 van de DPA 2018 heeft de betrokkene het recht van de verwerkingsverantwoordelijke rectificatie van hem/haar betreffende persoonsgegevens te verlangen. De verwerkingsverantwoordelijke moet de gegevens zonder onnodige vertraging rectificeren (of aanvullen wanneer de gegevens onjuist zijn omdat ze onvolledig zijn). Als de persoonsgegevens als bewijsmateriaal moeten worden bewaard, moet de verwerkingsverantwoordelijke de verwerking van de persoonsgegevens beperken (in plaats van ze te rectificeren) ([108]).

([102]) In de *Guide to Law Enforcement Processing* wordt het volgende voorbeeld gegeven: "op uw website staat een algemene privacyverklaring met basisinformatie over de organisatie, het doel waarvoor u persoonsgegevens verwerkt, de rechten van betrokkenen en hun recht om klacht in te dienen bij de Information Commissioner. U bent te weten gekomen dat een persoon aanwezig was toen er een misdrijf werd gepleegd. Tijdens uw eerste ondervraging van deze persoon moet u de algemene informatie verstrekken, evenals de verdere ondersteunende informatie, zodat de persoon zijn/haar rechten kan uitoefenen. U mag de informatie die u verstrekt over behoorlijke verwerking uitsluitend beperken als die informatie nadelige gevolgen zal hebben voor het door u gevoerde onderzoek." ("What information should we supply to an individual?" in de *Guide to Law Enforcement Processing*, beschikbaar via de volgende link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib3).

([103]) In de *Guide to Law Enforcement Processing* is vermeld dat de informatie die over de verwerking van persoonsgegevens wordt verstrekt beknopt, begrijpelijk en gemakkelijk toegankelijk moet zijn; in een duidelijke en eenvoudige taal moet zijn opgesteld, die aangepast is aan de behoeften van kwetsbare personen zoals kinderen; en kosteloos moet worden verstrekt ("How should we provide this information?" in de *Guide to Law Enforcement Processing*, beschikbaar via de volgende link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib1).

([104]) Artikel 44, lid 2, van de DPA 2018.

([105]) Raadpleeg voor een uitvoerige analyse van de rechten van betrokkenen: *Guide to Law Enforcement Processing* over individuele rechten ("*individual rights*"), beschikbaar via de volgende link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/

([106]) Artikel 45, lid 1, van de DPA 2018.

([107]) Artikel 45, lid 2, van de DPA 2018.

([108]) Artikel 46, lid 4, van de DPA 2018.

(60) In artikel 47 van de DPA 2018 is bepaald dat personen het recht hebben hun persoonsgegevens te laten wissen en de verwerking ervan te beperken. De verwerkingsverantwoordelijke moet ([109]) persoonsgegevens zonder onnodige vertraging wissen wanneer de verwerking van de persoonsgegevens in strijd is met een van de gegevensbeschermingsbeginselen, de rechtsgronden van de verwerking of de waarborgen in verband met archivering en de verwerking van gevoelige gegevens. De verwerkingsverantwoordelijke moet de gegevens ook wissen als hij/zij daartoe wettelijk verplicht is. Als de persoonsgegevens moeten worden bewaard als bewijsmateriaal, moet de verwerkingsverantwoordelijke de verwerking van de persoonsgegevens beperken (in plaats van ze te wissen) ([110]). De verwerkingsverantwoordelijke moet de verwerking van persoonsgegevens beperken als een betrokkene de juistheid van de persoonsgegevens betwist en er niet kan worden vastgesteld of deze al dan niet juist zijn ([111]).

(61) Wanneer een betrokkene verzoekt om rectificatie of wissing van zijn/haar persoonsgegevens of om beperking van de verwerking ervan, moet de verwerkingsverantwoordelijke de betrokkene er schriftelijk van in kennis stellen of dit verzoek al dan niet is ingewilligd en in het geval van afwijzing de betrokkene in kennis stellen van de redenen voor die weigering en van de mogelijkheden om een beroep in te stellen (het recht van de betrokkene om de Information Commissioner te verzoeken een onderzoek in te stellen naar de rechtmatigheid van de beperking, het recht om een klacht in te dienen bij de Information Commissioner en het recht om te verzoeken om een rechterlijk bevel tot naleving) ([112]).

(62) Wanneer de verwerkingsverantwoordelijke persoonsgegevens rectificeert die afkomstig zijn van een andere bevoegde autoriteit, moet hij/zij die andere autoriteit daarvan in kennis stellen ([113]). Wanneer de verwerkingsverantwoordelijke de rectificatie, wissing of beperking uitvoert van persoonsgegevens die door de verwerkingsverantwoordelijke zijn bekendgemaakt, moet de verwerkingsverantwoordelijke de ontvangers in kennis stellen, en moeten de ontvangers de persoonsgegevens dienovereenkomstig rectificeren, wissen of de verwerking ervan beperken (voor zover zij daarvoor verantwoordelijk blijven) ([114]).

(63) De betrokkene heeft bovendien het recht om zonder onnodige vertraging door de verwerkingsverantwoordelijke in kennis te worden gesteld van een inbreuk in verband met zijn/haar persoonsgegevens indien die inbreuk waarschijnlijk een hoog risico voor de rechten en vrijheden van personen met zich meebrengt ([115]).

(64) In verband met al die rechten van de betrokkene en naar analogie van het bepaalde in artikel 12 van Richtlijn (EU) 2016/680 is de verwerkingsverantwoordelijke verplicht ervoor te zorgen dat informatie aan de betrokkene in een beknopte, begrijpelijke en gemakkelijk toegankelijke vorm ([116]) wordt verstrekt en dat deze, waar mogelijk, in dezelfde vorm wordt verstrekt als de vorm van het verzoek ([117]). De verwerkingsverantwoordelijke moet zonder onnodige vertraging ingaan op een verzoek van de betrokkene, of in elk geval, in beginsel, binnen één maand na de indiening van het verzoek ([118]). Wanneer de verwerkingsverantwoordelijke gerede twijfel heeft over de identiteit van een persoon, kan hij/zij verzoeken om aanvullende informatie en de behandeling van het verzoek uitstellen totdat de identiteit bevestigd is. De verwerkingsverantwoordelijke mag een redelijke vergoeding aanrekenen of weigeren gevolg te geven aan het verzoek wanneer hij/zij dit kennelijk ongegrond acht ([119]). Het ICO heeft richtsnoeren verstrekt over de gevallen waarin een verzoek kennelijk ongegrond of buitensporig wordt geacht en een vergoeding mag worden gevraagd ([120]).

(65) Op grond van artikel 53, lid 4, van de DPA 2018 kan de Secretary of State door middel van regulations het maximumbedrag van een vergoeding bepalen.

([109]) Een betrokkene mag de verwerkingsverantwoordelijke verzoeken zijn/haar persoonsgegevens te wissen of de verwerking ervan te beperken (maar de verplichting van de verwerkingsverantwoordelijke om de gegevens te wissen of de verwerking ervan te beperken is van toepassing ongeacht of er al dan niet een verzoek daartoe is ingediend).

([110]) Artikel 46, lid 4, en artikel 47, lid 2, van de DPA 2018.

([111]) Artikel 47, lid 3, van de DPA 2018.

([112]) Artikel 48, lid 1, van de DPA 2018.

([113]) Artikel 48, lid 7, van de DPA 2018.

([114]) Artikel 48, lid 9, van de DPA 2018.

([115]) Artikel 68 van de DPA 2018.

([116]) Artikel 52, lid 1, van de DPA 2018.

([117]) Artikel 52, lid 3, van de DPA 2018.

([118]) In artikel 54 van de DPA 2018 wordt de betekenis omschreven van „*applicable time period*" (toepasselijke periode); dit is de periode van één maand, of een langere periode die is vastgesteld in regulations, die begint op het relevante tijdstip (waarop de verwerkingsverantwoordelijke het betrokken verzoek ontvangt; waarop de verwerkingsverantwoordelijke de informatie ontvangt die (eventueel) werd gevraagd in verband met een verzoek uit hoofde van artikel 52, lid 4, van de DPA; of waarop de eventuele vergoeding die in verband met het verzoek uit hoofde van artikel 53 van de DPA wordt aangerekend, is betaald).

([119]) Artikel 53, lid 1, van de DPA 2018.

([120]) Volgens de ICO-richtsnoeren mag een verwerkingsverantwoordelijke besluiten om een betrokkene een vergoeding aan te rekenen als het verzoek kennelijk ongegrond of buitensporig is, maar die verwerkingsverantwoordelijke toch besluit om op dat verzoek in te gaan. De vergoeding moet redelijk zijn en gerechtvaardigd zijn in het licht van de kosten. "Manifestly unfounded and excessive requests" in de *Guide to Law Enforcement Processing*, beschikbaar via de volgende link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/manifestly-unfounded-and-excessive-requests/

2.4.7.1. Beperkingen van de rechten van de betrokkene en transparantieverplichtingen

(66) Een bevoegde autoriteit kan in bepaalde omstandigheden bepaalde rechten van de betrokkene beperken: het inzagerecht ([121]), het recht om op de hoogte te worden gebracht ([122]), om ingelicht te worden over een inbreuk in verband met de persoonsgegevens ([123]), en om ingelicht te worden over de reden van de weigering van een verzoek om rectificatie of wissing ([124]). Net als is bepaald in de regeling die in hoofdstuk III van Richtlijn (EU) 2016/680 is opgenomen, kan de bevoegde autoriteit de beperking uitsluitend toepassen wanneer deze, met inachtneming van de grondrechten en de legitieme belangen van de betrokkene, noodzakelijk en evenredig is om: a) belemmering van officiële of gerechtelijke onderzoeken of procedures te voorkomen; b) nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek of de vervolging van strafbare feiten of de uitvoering van straffen te voorkomen; c) de openbare veiligheid te beschermen; d) de nationale veiligheid te beschermen; e) de rechten en vrijheden van anderen te beschermen.

(67) Het ICO heeft richtsnoeren uitgevaardigd in verband met de toepassing van die beperkingen. Volgens die richtsnoeren moeten de verwerkingsverantwoordelijken elk geval afzonderlijk analyseren om de rechten van de persoon af te wegen tegen de schade die bekendmaking zou veroorzaken. Zij moeten met name de noodzakelijkheid en evenredigheid van elke toegepaste beperking rechtvaardigen en mogen de verstrekking uitsluitend beperken als die de bovenvermelde doeleinden zou ondermijnen ([125]).

(68) De bevoegde autoriteiten hebben ook enkele andere richtsnoeren opgesteld, waarin zij uitvoerige informatie verstrekken over alle aspecten van de gegevensbeschermingswetgeving, onder meer over de toepassing van beperkingen van de rechten van betrokkenen ([126]). In verband met artikel 45, lid 4, van de DPA 2018 staat in de *Data Protection Manual* (handleiding gegevensbescherming) van de National Police Chiefs" Council het volgende vermeld: "er zij opgemerkt dat de beperkingen uitsluitend kunnen worden toegepast voor zover dat noodzakelijk is en zolang als nodig is. Bijgevolg is een algemene toepassing van de beperking op alle persoonsgegevens van een aanvrager of een permanente toepassing van de beperking niet toegestaan. Wat het laatste punt betreft, is het vaak zo dat persoonsgegevens die worden verzameld zonder medeweten van de betrokkene die een verdachte in een onderzoek is, aanvankelijk moeten worden beschermd tegen bekendmaking aan die betrokkene zelf om te voorkomen dat het onderzoek tijdens de uitvoering in gevaar wordt gebracht, maar dat die persoonsgegevens achteraf zonder nadelige gevolgen wel mogen worden bekendgemaakt als de persoonsgegevens aan de betrokkene bekendgemaakt zijn tijdens een verhoor. De politie moet procedures vaststellen om ervoor te zorgen dat deze beperkingen slechts worden toegepast voor zover zij noodzakelijk zijn en slechts zolang als nodig is" ([127]). In deze richtsnoeren worden ook voorbeelden gegeven van gevallen waarin elk van de beperkingen waarschijnlijk zal worden toegepast ([128]).

(69) In verband met de mogelijkheid om de bovenvermelde rechten te beperken met het oog op de bescherming van de nationale veiligheid ("*national security*") mag een verwerkingsverantwoordelijke bovendien een aanvraag indienen voor een certificaat dat ondertekend is door een minister of door de *Attorney General* (procureur-generaal) of de *Advocate General for Scotland* (advocaat-generaal van Schotland), waarin wordt verklaard dat een beperking van die rechten een noodzakelijke en evenredige maatregel is voor de bescherming van de nationale veiligheid ([129]). De Britse regering heeft richtsnoeren uitgevaardigd over de nationaleveiligheidscertificaten uit hoofde van de DPA 2018 waarin met name wordt benadrukt dat elke beperking van de rechten van betrokkenen met het oog op de bescherming van de nationale veiligheid evenredig en noodzakelijk moet zijn ([130]) (zie de overwegingen 131 tot en met 134 voor nadere informatie over nationaleveiligheidscertificaten).

([121]) Artikel 45, lid 4, van de DPA 2018.

([122]) Artikel 44, lid 4, van de DPA 2018.

([123]) Artikel 68, lid 7, van de DPA 2018.

([124]) Artikel 48, lid 3, van de DPA 2018.

([125]) Zie bijvoorbeeld de *Guide to Law Enforcement Processing* over het inzagerecht ("*the right of access*"), beschikbaar via de volgende link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-of-access/#ib8

([126]) Zie bijvoorbeeld de Data Protection Manual for Police Data Protection Professionals, een handleiding uitgevaardigd door de National Police Chiefs" Council (zie voetnoot 27) of de richtsnoeren uitgevaardigd door het Serious Fraud Office, beschikbaar via de volgende link: https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/data-protection/

([127]) *Data Protection Manual* van de National Police Chiefs" Council, blz. 140 (zie voetnoot 27).

([128]) Volgens de *Data Protection Manual* van de National Police Chiefs" Council is "het voorkómen van de belemmering van officiële of justitiële onderzoeken of procedures" waarschijnlijk relevant voor persoonsgegevens die worden verwerkt voor forensische onderzoeken, zaken die voor een familierechtbank worden behandeld, niet-strafrechtelijke interne disciplinaire onderzoeken, en onderzoeken zoals die van de *Independent Inquiry into Child Sexual Abuse* (onafhankelijke commissie voor onderzoek naar seksueel misbruik van kinderen), terwijl "de bescherming van de rechten en vrijheden van anderen relevant is voor persoonsgegevens die niet alleen betrekking hebben op de aanvrager, maar ook op andere personen" (*Data Protection Manual* van de National Police Chiefs" Council, blz. 140, zie voetnoot 27).

([129]) Artikel 79 van de DPA 2018.

([130]) Richtsnoeren van de Britse regering inzake nationaleveiligheidscertificaten, beschikbaar via de volgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf

(70) Wanneer er een beperking op een recht van een betrokkene geldt, moet de bevoegde autoriteit bovendien de betrokkene er zonder onnodige vertraging van in kennis stellen dat zijn/haar rechten zijn beperkt, van de redenen voor die beperking en van de beschikbare beroepsmogelijkheden, tenzij het verstrekken van die informatie de reden voor de toepassing van de beperking zou ondermijnen ([131]). Als extra waarborg tegen het misbruik van beperkingen moet de verwerkingsverantwoordelijke de redenen registreren waarom hij/zij de informatie beperkt en die registratie, op verzoek, beschikbaar stellen aan de Information Commissioner ([132]).

(71) Als de verwerkingsverantwoordelijke aanvullende transparantiegegevens weigert te verstrekken, of inzage weigert te verlenen, of als hij/zij een verzoek tot rectificatie, wissing of beperking van de verwerking afwijst, kan de betrokkene de Information Commissioner vragen te onderzoeken of de verwerkingsverantwoordelijke de beperking rechtmatig heeft toegepast ([133]). De betrokkene kan ook een klacht indienen bij de Information Commissioner of zich tot een rechter wenden om de verwerkingsverantwoordelijke te bevelen gevolg te geven aan het verzoek ([134]).

2.4.7.2. Geautomatiseerde besluitvorming

(72) De artikelen 49 en 50 van de DPA 2018 hebben respectievelijk betrekking op de rechten in verband met geautomatiseerde besluitvorming en de toe te passen waarborgen ([135]). Naar analogie van artikel 11 van Richtlijn (EU) 2016/680, kan de verwerkingsverantwoordelijke slechts een doorslaggevend besluit nemen dat uitsluitend op de geautomatiseerde verwerking van persoonsgegevens gebaseerd is als dit krachtens het recht vereist of toegestaan is ([136]). Een besluit is doorslaggevend als het voor de betrokkene nadelige rechtsgevolgen zou hebben of hem/haar in aanmerkelijke mate zou treffen ([137]).

(73) Wanneer de verwerkingsverantwoordelijke volgens het recht een doorslaggevend besluit moet of mag nemen, worden in artikel 50 van de DPA 2018 de waarborgen vermeld die van toepassing zullen zijn op dat besluit (dat wordt gedefinieerd als een "*qualifying significant decision*"). De verwerkingsverantwoordelijke moet de betrokkene er zo spoedig mogelijk van in kennis stellen dat een dergelijk besluit is genomen. De betrokkene kan vervolgens, binnen een maand, een verzoek richten aan de verwerkingsverantwoordelijke om het besluit te herzien of een nieuw besluit te nemen dat niet uitsluitend op geautomatiseerde verwerking is gebaseerd. De verwerkingsverantwoordelijke moet het verzoek onderzoeken en de betrokkene informeren over de uitkomst van dat onderzoek. De DPA 2018 verleent de Secretary of State de bevoegdheid om regelgeving ("regulations") vast te stellen in verband met aanvullende waarborgen ([138]). Er is nog geen dergelijke regelgeving vastgesteld.

2.4.8. *Verdere doorgiften*

(74) Het beschermingsniveau voor persoonsgegevens die vanuit een rechtshandhavingsinstantie van een lidstaat worden doorgegeven aan een rechtshandhavingsinstantie in het Verenigd Koninkrijk mag niet worden ondermijnd door de verdere doorgifte van die gegevens aan ontvangers in een derde land. Dergelijke "verdere doorgiften", die uit het oogpunt van de Britse rechtshandhavingsinstantie internationale doorgiften vanuit het Verenigd Koninkrijk vormen, mogen slechts worden toegestaan wanneer de verdere ontvanger buiten het Verenigd Koninkrijk zelf is onderworpen aan voorschriften die zorgen voor een vergelijkbaar beschermingsniveau zoals wordt gegarandeerd binnen de Britse rechtsorde.

([131]) Artikel 44, leden 5 en 6; artikel 45, leden 5 en 6; artikel 48, lid 4, van de DPA 2018.
([132]) Artikel 44, lid 7; artikel 45, lid 7; artikel 48, lid 6, van de DPA 2018.
([133]) Artikel 51 van de DPA 2018.
([134]) Artikel 167 van de DPA 2018.
([135]) In de memorie van toelichting bij de DPA 2018 is het volgende vermeld over het toepassingsgebied van geautomatiseerde verwerking: "deze bepalingen hebben betrekking op volledig geautomatiseerde besluitvorming en niet op geautomatiseerde verwerking. Geautomatiseerde verwerking (met inbegrip van profilering) vindt plaats wanneer op gegevens een activiteit wordt verricht zonder dat daarbij menselijke tussenkomst vereist is. Dit wordt regelmatig gebruikt bij de rechtshandhaving om grote datasets te filteren en op die manier te reduceren tot een beheersbare hoeveelheid gegevens die vervolgens door een menselijke operator kunnen worden gebruikt. Geautomatiseerde besluitvorming is een vorm van geautomatiseerde verwerking en vereist dat het definitieve besluit wordt genomen zonder enige menselijke tussenkomst." (Memorie van toelichting bij de DPA, punt 204, zie voetnoot 45).
([136]) Naast de bescherming waarin de DPA voorziet, zijn er andere wettelijke beperkingen opgenomen in het rechtskader van het Verenigd Koninkrijk, die van toepassing zijn op rechtshandhavingsinstanties en die geautomatiseerde verwerking (met inbegrip van profilering) die leidt tot onrechtmatige discriminatie, zouden voorkomen. Met de Human Rights Act 1998 worden de rechten uit het EVRM opgenomen in het recht van het Verenigd Koninkrijk, met inbegrip van het recht van artikel 14 van het Verdrag, het verbod op discriminatie. Evenzo verbiedt de Equality Act 2010 discriminatie van mensen met beschermde kenmerken (waaronder geslacht, ras, handicap enz.).
([137]) Artikel 49, lid 2, van de DPA 2018.
([138]) Artikel 50, lid 4, van de DPA 2018.

(75) De Britse regeling voor internationale doorgiften is opgenomen in deel 3, hoofdstuk 5, van de DPA 2018 ([139]) en weerspiegelt de aanpak van hoofdstuk V van Richtlijn (EU) 2016/680. Om persoonsgegevens te kunnen doorgeven aan een derde land, moet een bevoegde autoriteit aan drie voorwaarden voldoen: a) de doorgifte moet noodzakelijk zijn voor rechtshandhavingsdoeleinden; b) de doorgifte moet gebaseerd zijn op: i) een adequaatheidsbesluit met betrekking tot het derde land, ii) passende waarborgen (bij ontstentenis van een adequaatheidsbesluit), of iii) bijzondere omstandigheden (bij ontstentenis van een adequaatheidsbesluit of passende waarborgen), en c) de ontvanger van de doorgifte moet: i) een relevante autoriteit (d.w.z. het equivalent van een bevoegde autoriteit) in het derde land zijn; ii) een relevante internationale organisatie zijn, bijvoorbeeld een internationaal orgaan dat taken uitoefent die overeenstemmen met een van de rechtshandhavingsdoeleinden; of iii) een persoon zijn die geen relevante autoriteit is, maar uitsluitend wanneer de doorgifte strikt noodzakelijk is voor de uitvoering van een van de rechtshandhavingsdoeleinden; er geen grondrechten en vrijheden van de betrokkene zijn die voorrang hebben op het openbaar belang dat de doorgifte noodzakelijk maakt; een doorgifte van persoonsgegevens naar een relevante autoriteit in het derde land ondoeltreffend of ongeschikt zou zijn, en de ontvanger wordt ingelicht over het doel waarvoor de gegevens mogen worden verwerkt ([140]).

(76) Adequaatheidsbesluiten met betrekking tot een derde land, gebied of sector in dat derde land, een internationale organisatie, of een beschrijving ([141]) van dat land, dat gebied, die sector of die organisatie worden vastgesteld door de Secretary of State. Wat de in acht te nemen normen betreft, moet de Secretary of State beoordelen of een gebied/sector/organisatie voorziet in een adequaat beschermingsniveau voor persoonsgegevens. In artikel 74A, lid 4, van de DPA 2018 is bepaald dat de Secretary of State daartoe rekening moet houden met een aantal aspecten die overeenstemmen met de aspecten die zijn opgesomd in artikel 36 van Richtlijn (EU) 2016/680 ([142]). In dit opzicht vormt deel 3 van de DPA 2018 sinds het einde van de overgangsperiode "EU-derived domestic legislation" (van de EU afgeleide interne wetgeving) die, zoals reeds toegelicht, door de rechtbanken in het Verenigd Koninkrijk zal worden uitgelegd overeenkomstig de relevante rechtspraak van het Hof van Justitie die dateert van vóór de terugtrekking van het Verenigd Koninkrijk uit de Europese Unie en algemene beginselen van het Unierecht zoals deze onmiddellijk vóór het einde van de overgangsperiode van toepassing waren. Hieronder valt de norm van "wezenlijke overeenkomst" die aldus van toepassing zal zijn voor de adequaatheidsbeoordelingen die door de Britse autoriteiten worden verricht.

(77) Wat de procedure betreft, gelden voor de besluiten de "algemene" procedurevoorschriften als bepaald in artikel 182 van de DPA 2018. In het kader van deze procedure moet de Secretary of State overleg plegen met de Information Commissioner wanneer hij/zij voorstellen voor toekomstige Britse adequaatheidsbesluiten

([139]) Dit nieuwe kader is in werking getreden aan het einde van de overgangsperiode, met inbegrip van de bevoegdheid van de Secretary of State om adequaatheidsbesluiten vast te stellen. In de DPPEC Regulations (met name in de punten 10, 11 en 12 van bijlage 21 waarbij deze Regulations in de DPA 2018 worden opgenomen) is bepaald dat bepaalde doorgiften van persoonsgegevens tijdens en na afloop van de overgangsperiode worden behandeld alsof zij op adequaatheidsbesluiten gebaseerd zouden zijn. Deze doorgiften omvatten doorgiften naar derde landen die aan het einde van de overgangsperiode onder een adequaatheidsbesluit van de EU vallen alsook doorgiften naar EU-lidstaten, de EVA-staten en het grondgebied van Gibraltar aangezien deze de richtlijn rechtshandhaving toepassen op de verwerking van rechtshandhavingsgegevens (de EVA-staten passen Richtlijn (EU) 2016/680 toe op grond van hun verplichtingen uit hoofde van het Schengenacquis). Dit betekent dat de doorgiften naar deze landen aan het einde van de overgangsperiode kunnen worden voortgezet zoals vóór de terugtrekking van het Verenigd Koninkrijk uit de EU. Na afloop van de overgangsperiode moet de Secretary of State binnen vier jaar de adequaatheidsbevindingen beoordelen.

([140]) Artikelen 73 en 77 van de DPA 2018.

([141]) De Britse autoriteiten hebben opgemerkt dat de beschrijving van een land of een internationale organisatie verwijst naar een situatie waarin het noodzakelijk zou zijn een specifieke en gedeeltelijke bepaling van de adequaatheid te verrichten met doelgerichte beperkingen (bijvoorbeeld een adequaatheidsbesluit dat uitsluitend betrekking heeft op een bepaald type gegevensdoorgiften).

([142]) Zie artikel 74A, lid 4, van de DPA 2018, waarin is bepaald dat "de Secretary of State" bij de beoordeling van de vraag of het beschermingsniveau adequaat is, "met name rekening moet houden met a) de rechtsstatelijkheid, de eerbiediging van de mensenrechten en de fundamentele vrijheden, de relevante algemene en sectorale wetgeving, onder meer inzake openbare veiligheid, defensie, nationale veiligheid en strafrecht en toegang van overheidsinstanties tot persoonsgegevens, evenals de uitvoering van die wetgeving, gegevensbeschermingsregels, beroepsregels en de veiligheidsmaatregelen, met inbegrip van regels voor verdere doorgifte van persoonsgegevens aan een ander derde land of een andere internationale organisatie, die in dat land of die internationale organisatie worden nageleefd, rechtspraak, alsmede het bestaan van effectieve en afdwingbare rechten van betrokkenen en daadwerkelijke mogelijkheden om administratief beroep of beroep in rechte in te stellen voor betrokkenen van wie persoonsgegevens worden doorgegeven, b) het bestaan en het effectief functioneren van een of meer onafhankelijke toezichthoudende autoriteiten in het derde land of waaraan een internationale organisatie is onderworpen, welke tot taak heeft of hebben de naleving van de gegevensbeschermingsregels te verzekeren en deze te handhaven, met inbegrip van passende handhavingsbevoegdheden, om betrokkenen bij de uitoefening van hun rechten bij te staan en te adviseren en met de Commissioner samen te werken; en c) de internationale verbintenissen die het derde land of de internationale organisatie in kwestie heeft aangegaan, of andere verplichtingen die voortvloeien uit juridisch bindende overeenkomsten of instrumenten, alsmede uit de deelname van dat derde land of die internationale organisatie aan multilaterale of regionale regelingen, in het bijzonder met betrekking tot de bescherming van persoonsgegevens."

opstelt ([143]). Zodra deze adequaatheidsbesluiten door de Secretary of State zijn vastgesteld, worden ze voorgelegd aan het parlement en onderworpen aan de zogenoemde negative resolution procedure; dit betekent dat beide kamers van het parlement het besluit kunnen onderzoeken en binnen veertig dagen een motie kunnen aannemen tot nietigverklaring van het besluit ([144]).

(78) Overeenkomstig artikel 74 ter, lid 1, van de DPA 2018 moeten adequaatheidsbesluiten worden geëvalueerd met tussenpozen van niet meer dan vier jaar en moet de Secretary of State voortdurend de ontwikkelingen volgen in derde landen en internationale organisaties die van invloed kunnen zijn op besluiten tot vaststelling, wijziging of intrekking van adequaatheidsbesluiten. Wanneer de Secretary of State vaststelt dat een bepaald land of een organisatie niet langer een adequaat beschermingsniveau voor persoonsgegevens verzekert, moet hij/zij, indien nodig, de adequaatheidsbesluiten wijzigen of intrekken en overleg plegen met het betrokken derde land of de betrokken internationale organisatie om het gebrek aan een adequaat beschermingsniveau te verhelpen.

(79) Naar analogie van artikel 37 van Richtlijn (EU) 2016/680 zou, bij ontbreken van een adequaatheidsbesluit, een doorgifte van persoonsgegevens in het kader van de rechtshandhaving kunnen plaatsvinden wanneer in passende waarborgen is voorzien. Dergelijke waarborgen worden geboden aan de hand van a) een juridisch bindend instrument waarin passende waarborgen voor de bescherming van persoonsgegevens zijn opgenomen; of b) een beoordeling door de verwerkingsverantwoordelijke die alle omstandigheden in verband met de doorgifte van persoonsgegevens heeft beoordeeld en heeft geconcludeerd dat er passende waarborgen bestaan voor de bescherming van persoonsgegevens ([145]). Indien doorgiften gebaseerd zijn op passende waarborgen, is in de DPA 2018 voorts bepaald dat de bevoegde autoriteiten, in aanvulling op de normale toezichthoudende rol van het ICO, specifieke informatie over de doorgiften moeten verstrekken aan het ICO ([146]).

(80) Als een doorgifte niet op een adequaatheidsbesluit of passende waarborgen is gebaseerd, kan die doorgifte uitsluitend plaatsvinden in bepaalde, welomschreven omstandigheden die "*special circumstances*" (bijzondere omstandigheden) worden genoemd ([147]). Dit is het geval wanneer de doorgifte noodzakelijk is: a) om de vitale belangen van de betrokkene of van een andere persoon te beschermen; b) om de legitieme belangen van de betrokkene te beschermen; c) om een onmiddellijke en ernstige bedreiging van de openbare veiligheid van een derde land te voorkomen; d) in afzonderlijke gevallen met het oog op rechtshandhaving; of e) in afzonderlijke gevallen met een juridisch doel (bijvoorbeeld in gerechtelijke procedures of voor het inwinnen van juridisch advies) ([148]). Er zij op gewezen dat de punten d) en e) niet van toepassing zijn indien de rechten en vrijheden van de betrokkene zwaarder wegen dan het openbaar belang van de doorgifte ([149]). Deze reeks omstandigheden stemt overeen met de specifieke situaties en voorwaarden die als "afwijkingen" gelden uit hoofde van artikel 38 van Richtlijn (EU) 2016/680.

(81) In die omstandigheden moeten de datum, het tijdstip en de reden van de doorgifte worden gedocumenteerd, evenals de naam van de ontvanger en andere relevante informatie over de ontvanger, en een beschrijving van de doorgegeven persoonsgegevens, en moet dit alles, op verzoek, beschikbaar worden gesteld aan de Information Commissioner ([150]).

(82) Artikel 78 van de DPA 2018 regelt het scenario van "*subsequent transfers*" (verdere doorgiften), namelijk wanneer persoonsgegevens die vanuit het Verenigd Koninkrijk aan een derde land zijn doorgegeven vervolgens aan een ander derde land of een internationale organisatie worden doorgegeven. Ingevolge artikel 78, lid 1, moet de Britse verwerkingsverantwoordelijke die de doorgifte verricht, die doorgifte afhankelijk stellen van de voorwaarde dat de gegevens niet verder worden doorgegeven aan een derde land zonder toestemming van de verwerkingsverantwoordelijke die de doorgifte verricht. Daarnaast zijn er, conform artikel 78, lid 3, en naar analogie van het bepaalde in artikel 35, lid 1, punt e), van Richtlijn (EU) 2016/680, een aantal inhoudelijke vereisten van toepassing indien een dergelijke toestemming vereist is. Meer bepaald moet een bevoegde autoriteit bij de beoordeling of zij al dan niet

([143]) Memorandum van overeenstemming tussen de Secretary of State van het *Department for Digital, Culture, Media and Sport* (DCMS — het ministerie van Digitale Aangelegenheden, Cultuur, Media en Sport) en het *Information Commissioner's Office* (ICO — het bureau van de toezichthouder informatie) over de rol van het ICO in verband met de nieuwe adequaatheidsbeoordelingen van het Verenigd Koninkrijk, beschikbaar via de volgende link: https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments.

([144]) Tijdens deze termijn van veertig dagen hebben beide kamers van het parlement, indien gewenst, de mogelijkheid om tegen het besluit te stemmen; in het geval van een dergelijke stemming zal het besluit uiteindelijk geen verdere rechtsgevolgen hebben.

([145]) Artikel 75 van de DPA 2018.

([146]) Overeenkomstig artikel 75, lid 3, van de DPA 2018 moet, wanneer een doorgifte van gegevens plaatsvindt op basis van passende waarborgen: a) deze doorgifte gedocumenteerd worden, b) de documentatie desgevraagd ter beschikking worden gesteld van de Commissioner en moet c) de documentatie met name i) de datum en tijd van doorgifte, ii) de naam van de ontvanger en andere relevante informatie over de ontvanger, iii) de reden voor de doorgifte en iv) een beschrijving van de doorgegeven persoonsgegevens bevatten.

([147]) "Are there any special circumstances?" in de *Guide to Law Enforcement Processing*, beschikbaar via de volgende link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/international-transfers/#ib3).

([148]) Artikel 76 van de DPA 2018.

([149]) Artikel 76 van de DPA 2018.

([150]) Artikel 76, lid 3, van de DPA 2018.

toestemming zal verlenen voor de doorgifte, verifiëren of de verdere doorgifte noodzakelijk is met het oog op rechtshandhaving en moet zij daarbij een aantal factoren in aanmerking nemen, zoals onder meer a) de ernst van de omstandigheden die tot het verzoek om toestemming hebben geleid, b) het doel waarvoor de persoonsgegevens oorspronkelijk waren doorgegeven en c) de normen voor de bescherming van persoonsgegevens die van toepassing zijn in het derde land of de internationale organisatie waaraan de persoonsgegevens verder zouden worden doorgegeven.

(83) Wanneer de gegevens die vanuit het Verenigd Koninkrijk verder worden doorgegeven, oorspronkelijk vanuit de Europese Unie werden doorgegeven, gelden er bovendien aanvullende waarborgen.

(84) Ten eerste is er in artikel 73, lid 1, punt b), van de DPA 2018, net als in artikel 35, lid 1, onder c), van Richtlijn (EU) 2016/680, bepaald dat een lidstaat die de persoonsgegevens oorspronkelijk aan de verwerkingsverantwoordelijke of een andere bevoegde autoriteit heeft verstrekt of op een andere manier beschikbaar heeft gesteld, die lidstaat of een andere persoon in die lidstaat die een bevoegde autoriteit is in de zin van Richtlijn (EU) 2016/680, toestemming moet hebben gegeven voor de doorgifte overeenkomstig het recht van die lidstaat.

(85) Net als in artikel 35, lid 2, van Richtlijn (EU) 2016/680 is bepaald, is die toestemming echter niet vereist wanneer a) de doorgifte noodzakelijk is met het oog op de voorkoming van een acute en ernstige bedreiging van de openbare veiligheid van een lidstaat of een derde land of voor de fundamentele belangen van een lidstaat, en b) de toestemming niet tijdig kan worden verkregen. In dat geval moet de voor het geven van de toestemming verantwoordelijke autoriteit daarvan onverwijld in kennis worden gesteld ([151]).

(86) Ten tweede geldt dezelfde aanpak in het geval van gegevens die oorspronkelijk vanuit de Europese Unie aan het Verenigd Koninkrijk zijn doorgegeven en die vervolgens door het Verenigd Koninkrijk verder worden doorgegeven aan een derde land, dat ze vervolgens verder zou doorgeven aan een derde land. In dat geval kan de bevoegde autoriteit van het Verenigd Koninkrijk krachtens artikel 78, lid 4, geen toestemming geven voor de laatstbedoelde doorgifte conform artikel 78, lid 1, tenzij de "lidstaat [die de betrokken gegevens oorspronkelijk heeft doorgegeven] of een in die lidstaat gevestigde persoon die een bevoegde autoriteit in de zin van de richtlijn rechtshandhaving is, in overeenstemming met het recht van die lidstaat toestemming heeft gegeven voor de doorgifte." Deze waarborgen zijn belangrijk omdat zij de autoriteiten van de lidstaten in staat stellen de continuïteit van de bescherming, in overeenstemming met het EU-recht inzake gegevensbescherming, in de hele "doorgifteketen" te waarborgen.

(87) Dit nieuwe kader voor internationale doorgiften werd van toepassing aan het einde van de overgangsperiode ([152]). In bijlage 21, punt 10, 11 en 12 (ingevoerd door de DPPC Regulations) is echter bepaald dat bepaalde doorgiften van persoonsgegevens vanaf het einde van de overgangsperiode worden behandeld alsof ze gebaseerd zouden zijn op adequaatheidsbesluiten. Deze doorgiften zijn onder meer doorgiften naar een EU-lidstaat, een EVA-staat, een derde land dat aan het einde van de overgangsperiode onder een adequaatheidsbesluit van de EU valt en het grondgebied van Gibraltar. Bijgevolg kunnen de doorgiften naar deze landen worden voortgezet zoals dat gebeurde vóór de terugtrekking van het Verenigd Koninkrijk uit de Europese Unie. Na afloop van de overgangsperiode moet de Secretary of State binnen vier jaar, d.w.z. uiterlijk eind december 2024, deze adequaatheidsbevindingen beoordelen. Volgens de toelichting die door de Britse autoriteiten werd verstrekt moet de Secretary of State die beoordeling weliswaar uiterlijk eind december 2024 verrichten, maar omvatten de overgangsbepalingen geen vervalbepaling en zullen de relevante overgangsbepalingen niet automatisch buiten werking treden als die beoordeling eind december 2024 niet is afgerond.

2.4.9. *Verantwoordingsplicht*

(88) Volgens het beginsel van de verantwoordingsplicht moeten overheidsinstanties die gegevens verwerken passende technische en organisatorische maatregelen nemen om doeltreffend aan hun verplichtingen inzake gegevensbescherming te voldoen, en moeten zij die naleving kunnen aantonen, in het bijzonder jegens de bevoegde toezichthoudende autoriteit.

(89) Dit beginsel komt tot uitdrukking in artikel 56 van de DPA 2018, waarin een algemene verantwoordingsplicht voor de verwerkingsverantwoordelijke wordt ingevoerd, d.w.z. een verplichting om passende technische en organisatorische maatregelen te nemen om te verzekeren, en te kunnen aantonen, dat de verwerking van persoonsgegevens voldoet aan de voorschriften van deel 3 van de DPA 2018. De toegepaste maatregelen moeten waar nodig worden geëvalueerd en geactualiseerd, en zij moeten, wanneer dit in verhouding staat tot de verwerking, passende beleidsmaatregelen in verband met gegevensbescherming omvatten.

([151]) Artikel 73, lid 5, van de DPA 2018.

([152]) De toepasselijkheid van dit nieuwe kader moet worden gelezen in het licht van artikel 782 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 (PB L 444 van 31.12.2020, blz. 14) (hierna "de EU-UK TCA" genoemd), beschikbaar via de volgende link: https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:22020A1231(01)&from=EN

(90) In overeenstemming met hoofdstuk IV van Richtlijn (EU) 2016/680 wordt in de artikelen 55 tot en met 71 van de DPA 2018 voorzien in verschillende mechanismen om de verantwoordingsplicht te garanderen en verwerkingsverantwoordelijken en verwerkers in staat te stellen aan te tonen dat zij hun verplichtingen nakomen. Van verwerkingsverantwoordelijken wordt met name verlangd dat zij gegevensbeschermingsmaatregelen door ontwerp en door standaardinstellingen toepassen, namelijk om te verzekeren dat de beginselen inzake gegevensbescherming op een doeltreffende manier worden toegepast, dat zij registers bijhouden van alle categorieën van onder hun verantwoordelijkheid vallende verwerkingsactiviteiten (onder meer informatie over de identiteit van de verwerkingsverantwoordelijke, contactgegevens van de functionaris voor gegevensbescherming, de verwerkingsdoeleinden, de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden bekendgemaakt, en een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens) en dat zij deze registers, op verzoek, ter beschikking stellen van de Information Commissioner. De verwerkingsverantwoordelijke en de verwerker moeten voor bepaalde verwerkingsactiviteiten ook logbestanden bijhouden en deze ter beschikking stellen van de Information Commissioner ([153]). De verwerkingsverantwoordelijken zijn ook specifiek verplicht om samen te werken met de Information Commissioner bij de uitvoering van zijn/haar taken.

(91) In de DPA 2018 zijn tevens aanvullende vereisten opgenomen voor verwerking die waarschijnlijk een hoog risico voor de rechten en vrijheden van personen zal opleveren. Deze omvatten een verplichting om effectbeoordelingen van de gegevensbescherming te verrichten en vóór de verwerking overleg te plegen met de Information Commissioner indien uit een dergelijke beoordeling blijkt dat de verwerking zou leiden tot een hoog risico voor de rechten en vrijheden van personen (bij ontstentenis van maatregelen om dit risico te beperken).

(92) De verwerkingsverantwoordelijken moeten voorts een functionaris voor gegevensbescherming aanstellen, tenzij de verwerkingsverantwoordelijke een gerecht of een andere rechterlijke instantie is, tijdens de uitoefening van zijn/haar rechterlijke taken ([154]). De verwerkingsverantwoordelijke moet ervoor zorgen dat de functionaris voor gegevensbescherming wordt betrokken bij alle aangelegenheden die met de bescherming van persoonsgegevens verband houden, beschikt over de benodigde middelen en toegang krijgt tot persoonsgegevens en verwerkingsactiviteiten en dat deze functionaris zijn/haar taken onafhankelijk kan vervullen. De taken van de functionaris voor gegevensbescherming worden uiteengezet in artikel 71 van de DPA 2018. Daartoe behoren onder meer informeren en adviseren, toezien op de naleving en samenwerken met en als contactpunt fungeren voor de Information Commissioner. Bij de uitvoering van zijn/haar taken moet de functionaris voor gegevensbescherming rekening houden met de risico's in verband met verwerkingsactiviteiten, met inachtneming van de aard, de reikwijdte, de context en het doel van de verwerking.

2.5. **Toezicht en handhaving**

2.5.1. *Onafhankelijk toezicht*

(93) Om ervoor te zorgen dat ook in de praktijk een passend niveau van bescherming van persoonsgegevens wordt gewaarborgd, moet er een onafhankelijke toezichthoudende autoriteit worden opgericht die bevoegd is voor het toezicht op en de handhaving van de naleving van de gegevensbeschermingsvoorschriften. Deze autoriteit moet bij de uitvoering van haar taken en de uitoefening van haar bevoegdheden volledig onafhankelijk en onpartijdig optreden.

(94) In het Verenigd Koninkrijk worden het toezicht op en de handhaving van de naleving van de UK GDPR en de DPA 2018 verricht door de Information Commissioner ([155]). De Information Commissioner houdt tevens toezicht op de verwerking van persoonsgegevens door bevoegde autoriteiten die vallen onder het toepassingsgebied van deel 3 van de DPA 2018 ([156]). De Information Commissioner is een zogenoemde *Corporation Sole*: een afzonderlijke juridische entiteit die bestaat uit een enkele persoon. De Information Commissioner wordt in zijn/haar werkzaamheden bijgestaan door een bureau. Op 31 maart 2020 telde het bureau van de Information Commissioner 768 vaste medewerkers ([157]). De ondersteunende dienst van de Information Commissioner is het *Department for Digital, Culture, Media and Sport* ([158]).

([153]) Artikel 62 van de DPA 2018.

([154]) Artikel 69 van de DPA 2018.

([155]) Artikel 36, lid 2, punt b), van Richtlijn (EU) 2016/680.

([156]) Artikel 116 van de DPA 2018.

([157]) Het jaarverslag van de Information Commissioner en de jaarrekening 2019-2020 zijn beschikbaar via de volgende link: https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf

([158]) De onderlinge betrekkingen worden geregeld in een Management Agreement (beheerscontract). De belangrijkste verantwoordelijkheden van het DCMS, als ondersteunende dienst, zijn onder meer: ervoor zorgen dat het ICO beschikt over toereikende financiële, technische en personele middelen; de belangen van het ICO behartigen bij het parlement en andere regeringsinstanties; voorzien in een robuust nationaal kader voor gegevensbescherming; en het ICO richtsnoeren en bijstand verlenen met betrekking tot interne aangelegenheden, zoals vastgoedkwesties, huurcontracten en aanbestedingen (Management Agreement 2018-2021, beschikbaar via de volgende link: https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf).

(95) De onafhankelijkheid van de Commissioner is uitdrukkelijk vastgelegd in artikel 52 van de UK GDPR dat de in artikel 52, leden 1, 2 en 3, van Verordening (EU) 2016/679 van het Europees Parlement en de Raad ([159]) vastgelegde vereisten weerspiegelt. De Commissioner moet volledig onafhankelijk optreden bij de uitvoering van zijn/haar taken en de uitoefening van zijn/haar bevoegdheden die hem/haar overeenkomstig de UK GDPR zijn toegewezen, hij/zij moet vrij blijven van al dan niet rechtstreekse invloed in verband met die taken en bevoegdheden, en hij/zij mag geen instructies van wie dan ook vragen of aanvaarden. De Commissioner mag voorts geen handelingen verrichten die onverenigbaar zijn met zijn/haar taken en hij/zij mag, gedurende zijn/haar ambtstermijn, geen al dan niet bezoldigde beroepswerkzaamheden verrichten die onverenigbaar zijn met zijn/haar taken.

(96) De voorwaarden voor de aanstelling en het ontslag van de Information Commissioner zijn opgenomen in bijlage 12 bij de DPA 2018. De Information Commissioner wordt op voordracht van de regering door Hare Majesteit aangesteld in het kader van een eerlijk en algemeen vergelijkend onderzoek. De kandidaat moet beschikken over de passende kwalificaties, vaardigheden en competenties. Overeenkomstig de *Governance Code on Public Appointments* ([160]) (bestuurscode voor benoemingen bij de overheid) stelt een adviespanel een lijst van geschikte kandidaten op. Voordat de Secretary of State bij het Department for Digital, Culture, Media and Sport een definitieve beslissing neemt, moet het desbetreffende selectiecomité van het parlement voorafgaand aan de aanstelling een doorlichting verrichten. Het standpunt van het comité wordt openbaar gemaakt ([161]).

(97) De Information Commissioner bekleedt deze functie gedurende maximaal zeven jaar. De Information Commissioner kan uit zijn/haar functie worden ontheven door Hare Majesteit na een *Address* van beide kamers van het parlement ([162]). Er kan alleen een verzoek tot ontslag van de Information Commissioner bij een van de kamers van het parlement worden ingediend indien een minister aan een van die kamers een verslag heeft voorgelegd waarin is vermeld dat hij/zij het bewezen acht dat de Information Commissioner zich schuldig heeft gemaakt aan ernstig wangedrag en/of dat de Commissioner niet langer voldoet aan de voorwaarden die zijn vereist voor de uitvoering van zijn/haar taken ([163]).

(98) De financiële middelen voor de Information Commissioner zijn afkomstig uit drie bronnen: i) door verwerkingsverantwoordelijken betaalde bijdragen voor gegevensbescherming die zijn vastgesteld in regulations van een Secretary of State ([164]) en die goed zijn voor 85 tot 90 % van de jaarlijkse begroting van het Bureau van de Information Commissioner ([165]); ii) subsidies die door de regering worden betaald aan de Information Commissioner en voornamelijk worden gebruikt om de bedrijfskosten van de Information Commissioner te financieren met betrekking tot taken die geen verband houden met gegevensbescherming ([166]); iii) vergoedingen die voor de dienstverlening worden aangerekend ([167]). Dergelijke vergoedingen worden momenteel niet in rekening gebracht.

(99) In bijlage 13 bij de DPA 2018 zijn de algemene taken van de Information Commissioner in verband met de verwerking van persoonsgegevens die vallen onder het toepassingsgebied van deel 3 van de DPA 2018 vastgelegd. De taken omvatten toezicht op en handhaving van deel 3 van de DPA 2018, voorlichting van het publiek, advisering van het parlement, de regering en andere instellingen over wetgevings- en bestuursrechtelijke maatregelen, de verwerkingsverantwoordelijken en de verwerkers beter bekendmaken met hun verplichtingen,

---

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

([160]) Governance Code on Public Appointments, beschikbaar via de volgende link: https://www.gov.uk/government/publications/governance-code-for-public-appointments.

([161]) *Second Report of Session 2015-2016* van het Culture, Media and Sports Committee in het Lagerhuis, beschikbaar via de volgende link: https://publications.parliament.uk/pa/cm201516/cmselect/cmcumeds/990/990.pdf

([162]) Een *Address* is een motie die bij het parlement wordt ingediend, met als doel de vorst in kennis te stellen van de standpunten van het parlement over een welbepaalde aangelegenheid.

([163]) Bijlage 12, punt 3, van de DPA 2018.

([164]) Artikel 137 van de DPA 2018.

([165]) De artikelen 137 en 138 van de DPA 2018 bevatten een aantal waarborgen die ervoor moeten zorgen dat de vergoedingen op een passend niveau worden vastgesteld. In artikel 137, lid 4, van de DPA 2018 worden de aangelegenheden opgesomd waarmee de Secretary of State rekening moet houden wanneer hij/zij regulations vaststelt waarin het bedrag wordt gespecificeerd dat de verschillende organisaties moeten betalen. Artikel 138, lid 1, en artikel 182 van de DPA 2018 bevatten daarnaast een wettelijk vereiste voor de Secretary of State om de Information Commissioner en andere vertegenwoordigers of personen voor wie de regelingen waarschijnlijk gevolgen zullen hebben, te raadplegen alvorens deze regelingen vast te stellen, zodat rekening kan worden gehouden met hun standpunten. Daarnaast is de Information Commissioner uit hoofde van artikel 138, lid 2, van de DPA 2018 verplicht de werking van de regulations in verband met de kosten regelmatig te beoordelen en kan hij/zij bij de Secretary of State voorstellen indienen om de regulations te wijzigen. Tot slot zijn de regulations onderworpen aan een bekrachtigingsprocedure en kunnen zij niet worden aangenomen zonder voorafgaande goedkeuring door elk van de kamers van het parlement door middel van een resolutie, behalve wanneer deze regulations louter bedoeld zijn om rekening te houden met een stijging van het indexcijfer van de consumentenprijzen (in dat geval geldt een procedure van stilzwijgende goedkeuring).

([166]) In de Management Agreement wordt verduidelijkt dat "de Secretary of State de Information Commissioner mag betalen uit middelen die door het parlement worden verstrekt uit hoofde van punt 9 van bijlage 12 bij de DPA 2018. Na overleg met de Information Commissioner (IC) zal het DCMS de passende bedragen (subsidies) betalen voor de administratieve kosten van het ICO en de uitoefening van de werkzaamheden van de IC in verband met een aantal specifieke taken, waaronder de vrijheid van informatie" (Management Agreement 2018-2021, punt 1.12, zie voetnoot 158).

([167]) Artikel 134 van de DPA 2018.

informatie verstrekken aan een betrokkene over de uitoefening van zijn/haar rechten, en onderzoeken uitvoeren. Om de onafhankelijkheid van de rechterlijke macht te waarborgen, is de Information Commissioner niet gemachtigd zijn/haar taken uit te oefenen in verband met de verwerking van persoonsgegevens door een persoon die rechterlijke taken uitoefent, of door een gerecht tijdens de uitoefening van zijn rechterlijke taken. Het toezicht op de rechterlijke macht wordt evenwel door gespecialiseerde organen gewaarborgd, zoals hieronder wordt uiteengezet.

2.5.1.1. Handhaving, met inbegrip van sancties

(100) De Commissioner heeft algemene bevoegdheden tot onderzoek, correctie, autorisatie en advies met betrekking tot de verwerking van persoonsgegevens waarop deel 3 van de DPA 2018 van toepassing is. De Information Commissioner is bevoegd om de verwerkingsverantwoordelijke of de verwerker te melden dat er vermoedelijk een inbreuk op deel 3 wordt gemaakt, om de verwerkingsverantwoordelijke of verwerker te waarschuwen dat met de voorgenomen verwerkingen waarschijnlijk een inbreuk op de bepalingen van deel 3 wordt gemaakt, en de verwerkingsverantwoordelijke of de verwerker een berisping te geven wanneer met bepaalde verwerkingsactiviteiten een inbreuk op bepalingen van deel 3 is gemaakt. De Information Commissioner mag voorts, op eigen initiatief of op verzoek, aan het Britse parlement, de regering of andere instellingen en organen, evenals aan het publiek, adviezen verstrekken over alle aangelegenheden in verband met de bescherming van persoonsgegevens ([168]).

(101) Bovendien is de Information Commissioner bevoegd om:

— de verwerkingsverantwoordelijke en de verwerker (en in bepaalde omstandigheden andere personen) te bevelen de nodige informatie te verstrekken door een *information notice* (informatienota) uit te vaardigen ([169]);

— onderzoeken en controles uit te voeren door een *assessment notice* (beoordelingsnota) uit te vaardigen, waarin de verwerkingsverantwoordelijke of de verwerker kan worden verzocht de Commissioner toe te staan bepaalde gebouwen te betreden, documenten of apparatuur te inspecteren of te onderzoeken, en personen te ondervragen die namens de verwerker persoonsgegevens verwerken ([170]);

— zich op andere wijze toegang te verschaffen tot documenten van verwerkingsverantwoordelijken en verwerkers en tot hun gebouwen overeenkomstig artikel 154 van de DPA 2018 (*powers of entry and inspection*);

— corrigerende maatregelen te treffen, onder meer door middel van waarschuwingen en berispingen, of bevelen te geven door middel van een *enforcement notice* (handhavingsnota), waarin verwerkingsverantwoordelijken/verwerkers wordt verzocht bepaalde stappen te ondernemen of hiervan af te zien ([171]), en

— administratieve boeten op te leggen in de vorm van een *penalty notice* (boetenota) ([172]).

(102) In de *Regulatory Action Policy* (beleidsdocument inzake regelgevingsmaatregelen) van het ICO, wordt uiteengezet onder welke omstandigheden de Information Commissioner een informatie-, beoordelings-, handhavings- of boetenota zal uitvaardigen ([173]). Met een handhavingsnota kan de Information Commissioner vereisten opleggen die hij/zij passend acht om de inbreuk recht te zetten. Met een boetenota wordt de persoon verplicht aan de Information Commissioner het bedrag te betalen dat in die nota is vermeld. Een boetenota kan worden uitgevaardigd wanneer niet is voldaan aan bepaalde bepalingen van de DPA 2018 ([174]) of kan worden verstrekt aan een verwerkingsverantwoordelijke of verwerker die geen gevolg heeft gegeven aan een informatie-, beoordelings- of handhavingsnota.

(103) Bij de beslissing of aan een verwerkingsverantwoordelijke of verwerker een boetenota moet worden verstrekt en bij de bepaling van het bedrag van de boete moet de Information Commissioner rekening houden met de elementen die zijn vermeld in artikel 155, lid 3, van de DPA 2018, onder meer de aard en ernst van de inbreuk, de vraag of de inbreuk opzettelijk of uit onachtzaamheid is gepleegd, eventuele maatregelen die de verwerkingsverantwoordelijke of de verwerker heeft genomen om de schade voor betrokkenen te beperken, de mate van verantwoordelijkheid van

([168]) Punt 2 van bijlage 13 bij de DPA 2018.
([169]) Artikel 142 van de DPA 2018 (met inachtneming van de beperkingen in artikel 143 van de DPA 2018).
([170]) Artikel 146 van de DPA 2018 (met inachtneming van de beperkingen in artikel 147 van de DPA 2018).
([171]) Artikel 149, 150 en 151 van de DPA 2018 (met inachtneming van de beperkingen in artikel 152 van de DPA 2018).
([172]) Artikel 155 van de DPA 2018 (met inachtneming van de beperkingen in artikel 156 van de DPA 2018).
([173]) Regulatory Action Policy, beschikbaar via de volgende link: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf
([174]) Het ICO kan met name een boetenota uitvaardigen als niet voldaan is aan de bepalingen van artikel 149, lid 2, 3, 4 of 5, van de DPA 2018.

de verwerkingsverantwoordelijke of de verwerker (met inachtneming van de technische en organisatorische maatregelen die zij hebben genomen) en eventuele relevante eerdere inbreuken die door de verwerkingsverantwoordelijke of de verwerker werden gemaakt, de categorieën van persoonsgegevens die door de inbreuk zijn getroffen en de vraag of de boete doeltreffend, evenredig en afschrikkend is.

(104) Het maximumbedrag van de boete die via een boetenota kan worden opgelegd is a) 17 500 000 GBP in verband met het niet naleven van gegevensbeschermingsbeginselen (artikelen 35, 36 en 37, artikel 38, lid 1, artikel 39, lid 1, en artikel 40 van de DPA 2018), transparantieverplichtingen en individuele rechten (artikelen 44, 45, 46, 47, 48, 49, 52 en 53 van de DPA 2018), en de beginselen in verband met de internationale doorgiften van persoonsgegevens (artikelen 73, 75, 76, 77 of 78 van de DPA 2018), en b) 8 700 000 GBP in alle andere gevallen ([175]). Bij niet-naleving van een informatie-, beoordelings- of handhavingsnota is het maximumbedrag van de boete die via een boetenota kan worden opgelegd 17 500 000 GBP.

(105) Volgens haar laatste jaarverslagen (2018-2019 ([176]) en 2019-2020 ([177])) heeft de Information Commissioner een aantal onderzoeken verricht naar de verwerking van persoonsgegevens door strafrechtelijke handhavingsinstanties. Zo heeft zij in oktober 2019 een onderzoek uitgevoerd en een advies gepubliceerd over het gebruik door rechtshandhavingsinstanties van gezichtsherkenningstechnologie in openbare ruimten. Het onderzoek richtte zich met name op het gebruik van live gezichtsherkenning door de politie van Zuid-Wales en de *Metropolitan Police Service* (Londense Politie, MPS). Bovendien heeft de Information Commissioner een onderzoek ingesteld naar de "Gangs matrix" ([178]) van de MPS en daarbij een reeks ernstige inbreuken op de gegevensbeschermingswet vastgesteld die het vertrouwen van het publiek in de matrix en het gebruik van de gegevens kunnen ondermijnen.

(106) In november 2018 gaf de Information Commissioner een handhavingsnota af, waarna de MPS de nodige maatregelen trof om de beveiliging en verantwoordingsplicht te versterken en ervoor te zorgen dat de gegevens op evenredige wijze worden gebruikt.

(107) Een ander voorbeeld van een recente handhavingsmaatregel is de boete van 325 000 GBP die in mei 2018 door de Information Commissioner werd opgelegd aan de *Crown Prosecution Service* (het Britse openbaar ministerie) omdat dit ongecodeerde dvd's met opnames van politieverhoren was kwijtgeraakt. Bovendien stelde de Information Commissioner onderzoeken in naar bredere onderwerpen, zoals — in de eerste helft van 2020 — het gebruik van uit mobiele telefoons gehaalde gegevens voor politiedoeleinden en de verwerking van gegevens van slachtoffers door de politie.

(108) Naast de handhavingsbevoegdheden van de Information Commissioner, kunnen bepaalde inbreuken op de gegevensbeschermingswetgeving strafbare feiten zijn en als zodanig aan strafrechtelijke sancties worden onderworpen (artikel 196 van de DPA 2018). Dit geldt bijvoorbeeld voor het verkrijgen of bekendmaken van persoonsgegevens zonder de toestemming van de verwerkingsverantwoordelijke en voor het bewerkstelligen van de bekendmaking van persoonsgegevens aan een andere persoon zonder de toestemming van de verwerkingsverantwoordelijke ([179]); het opnieuw identificeerbaar maken van niet-identificeerbare persoonsgegevens zonder de toestemming van de verwerkingsverantwoordelijke die verantwoordelijk is voor het anonimiseren van de persoonsgegevens ([180]); het opzettelijk hinderen van de Information Commissioner bij de uitoefening van zijn/haar bevoegdheden in verband met de inspectie van persoonsgegevens overeenkomstig internationale verplichtingen ([181]), het afleggen van valse verklaringen in antwoord op een informatienota, of het vernietigen van informatie in verband met een informatie- of beoordelingsnota ([182]).

(109) De Information Commissioner is krachtens artikel 139 van de DPA 2018 tevens verplicht om aan elke kamer van het parlement een algemeen verslag voor te leggen over de uitoefening van zijn/haar taken uit hoofde van die wet ([183]).

([175]) Artikel 157 van de DPA 2018.

([176]) Het jaarverslag van de Information Commissioner en de jaarrekening 2018-2019 zijn beschikbaar via de volgende link: https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf

([177]) Jaarverslag 2019-2020 van de Information Commissioner (zie voetnoot 157).

([178]) Een databank met inlichtingen over vermoedelijke bendeleden en slachtoffers van bendecriminaliteit.

([179]) Artikel 170 van de DPA 2018.

([180]) Artikel 171 van de DPA 2018.

([181]) Artikel 119 van de DPA 2018.

([182]) Artikelen 144 en 148 van de DPA 2018.

([183]) Zoals is uiteengezet in de Management Agreement, moet het jaarverslag: i) handelen over ondernemingen, dochterondernemingen of gemeenschappelijke ondernemingen waarover het ICO zeggenschap heeft; ii) de handleiding voor financiële verslaglegging van het ministerie van Financiën (*Financial Reporting Manual (FReM)*) naleven; iii) een verklaring inzake governance bevatten, waarin is uiteengezet hoe de rekenplichtige de in de organisatie aangewende middelen heeft beheerd en gecontroleerd in de loop van het jaar en wordt aangetoond hoe goed de organisatie omgaat met risico's voor de verwezenlijking van haar doelstellingen, en iv) de belangrijkste activiteiten en resultaten van het vorige boekjaar beschrijven en een beknopt overzicht geven van de toekomstplannen (Management Agreement 2018-2021, punt 3.26, zie voetnoot 158).

2.5.2. *Toezicht op de rechterlijke macht*

(110) Het toezicht op de verwerking van persoonsgegevens door rechters en de rechterlijke macht is tweeledig. Wanneer gerechtsambtenaren of rechters geen rechterlijke taken uitoefenen, wordt het toezicht verricht door de Information Commissioner. Wanneer de verwerkingsverantwoordelijke rechterlijke taken uitoefent, kan het ICO zijn toezichthoudende taken niet uitoefenen ([184]) en wordt het toezicht uitgeoefend door speciale organen. Dit sluit aan bij de aanpak van artikel 32 van Richtlijn (EU) 2016/680.

(111) In het tweede scenario wordt dat toezicht met name uitgeoefend door het *Judicial Data Protection Panel* ([185]) wanneer het de rechtbanken van Engeland en Wales en de gerechten in eerste aanleg (*First-tier Tribunals*) en in tweede aanleg (*Upper Tibunals*) van Engeland en Wales betreft. Daarnaast hebben de *Lord Chief Justice* (hoogste rechter) en de *Senior president of Tribunals* (eerste voorzitter van de rechtbanken) een *Privacy Notice* (privacyverklaring) ([186]) uitgevaardigd waarin wordt uiteengezet hoe de rechtbanken in Engeland en Wales persoonsgegevens verwerken bij de uitoefening van gerechtelijke taken. De rechterlijke macht van Noord-Ierland ([187]) en van Schotland ([188]) hebben een soortgelijke verklaring uitgevaardigd.

(112) In Noord-Ierland heeft de *Lord Chief Justice* van Noord-Ierland bovendien een rechter van de High Court aangesteld als *Data Supervisory Judge* (DSJ — toezichthoudend rechter in verband met gegevens) ([189]). Deze heeft ook richtsnoeren uitgevaardigd voor de Noord-Ierse rechterlijke macht over wat moet worden gedaan in het geval van verlies of mogelijk verlies van gegevens en over de procedure voor de aanpak van de daaruit voortvloeiende problemen ([190]).

(113) In Schotland heeft de *Lord president* (hoogste rechter) een *Data Supervisory Judge* (toezichthoudend rechter in verband met gegevens) aangesteld die klachten in verband met gegevensbescherming onderzoekt. Dit is uiteengezet in de regels betreffende gerechtelijke klachten, die vergelijkbaar zijn met de regels die voor Engeland en Wales zijn vastgesteld ([191]).

(114) Tot slot wordt een van de rechters van de *Supreme Court* benoemd om toezicht te houden op de gegevensbescherming.

([184]) Artikel 117 van de DPA 2018.

([185]) Dit panel is verantwoordelijk voor het verstrekken van richtsnoeren en opleiding aan het gerechtelijk apparaat. Het behandelt tevens klachten van betrokkenen in verband met de verwerking van persoonsgegevens door rechtbanken, hoven en personen die rechterlijke taken uitoefenen. Het panel streeft ernaar de middelen te verschaffen aan de hand waarvan klachten kunnen worden opgelost. Als de klager niet tevreden was met het besluit van het panel en aanvullende bewijzen heeft verstrekt, kan het panel zijn besluit heroverwegen. Het panel legt zelf geen financiële sancties op, maar als het van oordeel is dat de inbreuk op de DPA 2018 voldoende ernstig is, kan het deze doorverwijzen naar het *Judicial Conduct Investigation Office* (JCIO — onderzoeksbureau gerechtelijk optreden), dat de klacht vervolgens zal onderzoeken. Als de klacht gegrond wordt verklaard, is het aan de *Lord Chancellor* en de *Lord Chief Justice* (of een hooggeplaatste rechter aan wie hij/zij deze taak delegeert) om te beslissen welke maatregelen er tegen de ambtsdrager zullen worden getroffen. Deze maatregelen zijn, van licht naar zwaar: een terechtwijzing, een formele waarschuwing, een berisping en, uiteindelijk, ontslag. Als een persoon niet tevreden is met de manier waarop het JCIO de klacht heeft onderzocht, kan hij/zij een klacht indienen bij de *Judicial Appointments and Conduct Europese Ombudsman* (zie https://www.gov.uk/government/organisations/judicial-appointments-and-conduct-ombudsman). De Europese Ombudsman is bevoegd het JCIO te verzoeken een klacht opnieuw te onderzoeken en kan voorstellen dat de klager een vergoeding uitbetaald krijgt wanneer hij van oordeel is dat deze schade heeft geleden als gevolg van wanbeheer.

([186]) De privacyverklaring van de Lord Chief Justice en de Senior president of Tribunals is beschikbaar via de volgende link: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice

([187]) De privacyverklaring van de Lord Chief Justice van Noord-Ierland is beschikbaar via de volgende link: https://judiciaryni.uk/data-privacy

([188]) De privacyverklaring van de Schotse rechtbanken en hoven is beschikbaar via de volgende link: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice

([189]) De DSJ verstrekt richtsnoeren aan de rechterlijke macht en onderzoekt inbreuken en/of klachten in verband met de verwerking van persoonsgegevens door rechters of personen die rechterlijke taken uitoefenen.

([190]) Wanneer de klacht of inbreuk ernstig wordt geacht, wordt deze doorverwezen naar de *Judicial Complaints Officer* (functionaris "gerechtelijke klachten") voor verder onderzoek overeenkomstig de praktijkcode inzake klachten van de Lord Chief Justice van Noord-Ierland. Het resultaat van een dergelijke klacht kan onder meer zijn: geen verdere actie, advies, opleiding of begeleiding, een informele waarschuwing, een formele waarschuwing, een laatste waarschuwing, de beperking van de werkzaamheden of doorverwijzing naar een *statutory tribunal*. De praktijkcode inzake klachten van de Lord Chief Justice van Noord-Ierland is beschikbaar via de volgende link: https://judiciaryni.uk/sites/judiciary/files/media-files/14G.%20CODE%20OF%20PRACTICE%20Judicial%20~%2028%20Feb%2013%20%28Final%29%20updated%20with%20new%20comp..__1.pdf

([191]) Gegronde klachten worden onderzocht door de Data Supervisory Judge en doorverwezen naar de Lord president, die de bevoegdheid heeft advies, een formele waarschuwing of een berisping te geven, indien hij/zij dit nodig acht (voor leden van hoven bestaan er soortgelijke regels die beschikbaar zijn via de volgende link: https://www.judiciary.scot/docs/librariesprovider3/judiciarydocuments/complaints/complaintsaboutthejudiciaryscotlandrules2017_1d392ab6e14f6425aa0c7f48d062f5cc5.pdf?sfvrsn=5d3eb9a1_2).

2.5.3. *Beroep*

(115) Om een adequate rechtsbescherming en met name de handhaving van individuele rechten te garanderen, moeten aan de betrokkene daadwerkelijke mogelijkheden om administratief beroep of beroep in rechte in te stellen worden toegekend, met inbegrip van een recht op schadeloosstelling.

(116) Ten eerste heeft een betrokkene het recht om een klacht in te dienen bij de Information Commissioner, indien de betrokkene van mening is dat de verwerking van hem/haar betreffende persoonsgegevens inbreuk maakt op deel 3 van de DPA 2018 ([192]). Zoals beschreven in de overwegingen 100 en 109, is de Information Commissioner bevoegd om de naleving van de DPA 2018 door de verwerkingsverantwoordelijke en de verwerker te beoordelen, om van hen te verlangen dat zij de nodige stappen ondernemen of hiervan afzien in het geval van niet-naleving, en om boeten op te leggen.

(117) Ten tweede voorziet de DPA 2018 in een recht op een voorziening in rechte tegen de Information Commissioner. Indien de Information Commissioner geen vooruitgang boekt ([193]) met een klacht die door een betrokkene is ingediend, heeft de klager toegang tot een voorziening in rechte aangezien hij/zij de zaak aanhangig kan maken bij een *First Tier Tribunal* ([194]) (rechter in eerste aanleg) om de Information Commissioner te bevelen passende stappen te ondernemen om op de klacht te reageren, of om de klager in kennis te stellen van de voortgang van de klacht ([195]). Bovendien kan eenieder die een van de genoemde nota's (informatie-, beoordelings-, handhavings- of boetenota's) van de Information Commissioner heeft gekregen, beroep instellen bij een First Tier Tribunal. Als het Tribunal van oordeel is dat het besluit van de Information Commissioner niet strookt met het recht of dat deze zijn/haar discretionaire bevoegdheid anders had moeten gebruiken, moet het Tribunal dit beroep toewijzen, of de nota of het besluit vervangen door een andere nota of een ander besluit die of dat de Information Commissioner had kunnen afgeven of nemen ([196]).

(118) Ten derde kunnen personen uit hoofde van artikel 167 van de DPA 2018 rechtstreeks beroep in rechte instellen tegen verwerkingsverantwoordelijken en verwerkers. Als een betrokkene een zaak aanhangig heeft gemaakt bij een rechtbank en deze van oordeel is dat er een inbreuk is gepleegd op de rechten van de betrokkene in het kader van de gegevensbeschermingswetgeving, kan de rechtbank de verwerkingsverantwoordelijke in verband met de verwerking, of een verwerker die namens die verwerkingsverantwoordelijke optreedt, bevelen de in de rechterlijke beslissing vermelde stappen te ondernemen of hiervan af te zien. Op grond van artikel 169 van de DPA 2018 heeft elke persoon die schade lijdt ten gevolge van een inbreuk op een vereiste van de gegevensbeschermingswetgeving (met inbegrip van deel 3 van de DPA 2018), met uitzondering van de UK GDPR, bovendien recht op een schadevergoeding van de verwerkingsverantwoordelijke of de verwerker, tenzij de verwerkingsverantwoordelijke of de verwerker aantoont dat hij/zij in geen geval verantwoordelijk is voor de schadeveroorzakende gebeurtenis. Schade omvat zowel financieel verlies als niet-financieel verlies, zoals leed.

(119) Ten vierde kan een persoon die van mening is dat de overheid inbreuk heeft gepleegd op zijn/haar rechten, met inbegrip van het recht op privacy en het recht op gegevensbescherming, een beroep instellen bij de Britse rechtbanken uit hoofde van de Human Rights Act 1998. De verwerkingsverantwoordelijken in de zin van deel 3 van de DPA 2018, d.w.z. de bevoegde autoriteiten, zijn altijd overheidsinstanties ("*public authorities*") in de zin van de Human Rights Act 1998. Een persoon die stelt dat een overheidsinstantie heeft gehandeld (of voorstelt te handelen) op een wijze die niet verenigbaar is met een EVRM-recht en die bijgevolg onrechtmatig is op grond van artikel 6, lid 1, van de Human Rights Act 1998, kan een rechtsvordering instellen bij de bevoegde rechtbank, of kan zich beroepen op de desbetreffende rechten in een gerechtelijke procedure wanneer hij/zij slachtoffer is (of zou worden) van de onrechtmatige handeling ([197]).

([192]) Artikel 165 van de DPA 2018.

([193]) Artikel 166 van de DPA 2018 verwijst specifiek naar de volgende situaties: a) de Information Commissioner neemt niet de passende stappen om op de klacht te reageren, b) de Information Commissioner geeft de klager geen informatie over de voortgang van de klacht, of over het resultaat ervan, vóór het verstrijken van een periode van drie maanden vanaf de ontvangst van de klacht door de Information Commissioner, of c) de Information Commissioner heeft de behandeling van de klacht niet binnen die termijn afgerond en heeft de klager die informatie niet verstrekt binnen een verdere periode van drie maanden.

([194]) De First Tier Tribunal is de rechterlijke instantie die bevoegd is beroepen tegen besluiten van regelgevende overheidsinstanties te behandelen. Wat het besluit van de Information Commissioner betreft, is de bevoegde kamer de *General Regulatory Chamber*, die bevoegd is voor het gehele Verenigd Koninkrijk

([195]) Artikel 166 van de DPA 2018.

([196]) Artikelen 161 en 162 van de DPA 2018.

([197]) Zie de zaak *Brown v Commissioner of the Met 2016*, waarin de rechter in het kader van gegevensbescherming verzoekster schadeloos stelde in een gerechtelijke procedure tegen de politie. De rechter oordeelde ten gunste van verzoekster, die stelde dat er inbreuk was gepleegd op de verplichtingen uit hoofde van de DPA 1998 en inbreuk op de Human Rights Act 1998 (en het daarmee samenhangende recht op grond van artikel 8 EVRM) en dat er sprake was van misbruik van persoonsgegevens. (Verweerder gaf uiteindelijk toe dat er inbreuk was gepleegd op de DPA en het EVRM, en het vonnis was bijgevolg gericht op de vraag welke vorm van genoegdoening passend was). Ten gevolge van deze inbreuken kende de rechter verzoekster een financiële schadevergoeding toe.

(120) Indien rechters oordelen dat een overheidsinstantie onrechtmatig handelt, kunnen zij binnen de eigen bevoegdheden een compensatie of genoegdoening verschaffen, of een bevel in die zin uitvaardigen, voor zover zij dit rechtvaardig en passend achten ([198]). Een rechter kan ook verklaren dat een bepaling van het primaire recht onverenigbaar is met een door het EVRM gewaarborgd recht.

(121) Tot slot kan een persoon die alle nationale rechtsmiddelen heeft uitgeput, een beroep instellen bij het Europees Hof voor de Rechten van de Mens wegens schending van de door het EVRM gewaarborgde rechten.

2.6. **Verder delen**

(122) Volgens het Britse recht is het toegestaan dat een rechtshandhavingsinstantie gegevens deelt met andere instanties voor andere doeleinden dan de doeleinden waarvoor die gegevens oorspronkelijk werden verzameld (*onward sharing* genoemd), maar uitsluitend onder bepaalde voorwaarden.

(123) Naar analogie van het bepaalde in artikel 4, lid 2, van Richtlijn (EU) 2016/680, staat artikel 36, lid 3, van de DPA 2018 toe dat persoonsgegevens die voor een rechtshandhavingsdoel door een bevoegde autoriteit zijn verzameld, verder worden verwerkt (door dezelfde of een andere verwerkingsverantwoordelijke) voor andere rechtshandhavingsdoeleinden, op voorwaarde dat de verwerkingsverantwoordelijke overeenkomstig het recht gemachtigd is deze persoonsgegevens voor een dergelijk doel te verwerken en de verwerking noodzakelijk is en in verhouding staat tot dat andere doel ([199]). In dit geval zijn alle waarborgen die worden geboden door deel 3 van de DPA 2018 en die hierboven werden geanalyseerd van toepassing op de verwerking door de ontvangende autoriteit.

(124) In de Britse rechtsorde zijn er verschillende wetten die verder delen uitdrukkelijk toestaan. Zo zijn er met name i) de *Digital Economy Act* 2017 (wet inzake de digitale economie), op grond waarvan overheidsinstanties gegevens mogen delen voor verschillende doeleinden, bijvoorbeeld als er sprake is van fraude ten nadele van de overheidssector waarbij een overheidsinstantie verlies lijdt of zou kunnen lijden ([200]) of in het geval van schulden aan een overheidsinstantie of de Kroon ([201]); ii) de *Crime and Courts Act 2013* (wet inzake criminaliteit en rechtbanken), op grond waarvan het delen van informatie met de National Crime Agency (NCA — nationale recherche) ([202]) is toegestaan in het kader van de bestrijding, het onderzoek en de rechtsvervolging van zware en georganiseerde criminaliteit; iii) de *Serious Crime Act 2007* (wet inzake zware criminaliteit), op grond waarvan overheidsinstanties informatie mogen verstrekken aan fraudebestrijdingsorganisaties met het oog op de voorkoming van fraude ([203]).

(125) In deze wetten is uitdrukkelijk bepaald dat het delen van gegevens in overeenstemming moet zijn met in de DPA 2018 vastgestelde regels. Bovendien heeft het College of Policing een *Authorised Professional Practice on Information Sharing* ([204]) (toegestane beroepspraktijken in verband met het delen van gegevens) uitgevaardigd om de politie bij te staan bij de naleving van haar gegevensbeschermingsverplichtingen uit hoofde van de UK GDPR, de DPA en de Human Rights Act 1998. De vraag of bij het delen van gegevens het toepasselijke rechtskader in verband met de gegevensbescherming is nageleefd, kan uiteraard door de rechter worden getoetst ([205]).

(126) Naar analogie van het bepaalde in artikel 9 van Richtlijn (EU) 2016/680, is in de DPA 2018 bovendien vastgesteld dat persoonsgegevens die voor rechtshandhavingsdoeleinden worden verzameld, mogen worden verwerkt voor een doel dat geen rechtshandhavingsdoel is wanneer de verwerking volgens het recht is toegestaan ([206]). Deze vorm van het delen van gegevens betreft twee scenario's: 1) wanneer een strafrechtelijke handhavingsinstantie gegevens deelt met een niet-strafrechtelijke handhavingsinstantie die geen inlichtingendienst is (bijvoorbeeld met een financiële

([198]) Artikel 8, lid 1, van de Human Rights Act 1998.

([199]) Artikel 36, lid 3, van de DPA 2018.

([200]) Artikel 56 van de *Digital Economy Act 2017*, beschikbaar via de volgende link: https://www.legislation.gov.uk/ukpga/2017/30/contents

([201]) Artikel 48 van de Digital Economy Act 2017.

([202]) Artikel 7 van de Crime and Courts Act 2013, beschikbaar via de volgende link: https://www.legislation.gov.uk/ukpga/2013/22/contents

([203]) Artikel 68 van de Serious Crime Act 2007, beschikbaar via de volgende link: https://www.legislation.gov.uk/ukpga/2007/27/contents

([204]) *Authorised Professional Practice on Information Sharing*, beschikbaar via de volgende link: https://www.app.college.police.uk/app-content/information-management/sharing-police-information

([205]) Zie bijvoorbeeld de zaak *M v the Chief Constable of Sussex Police* [2019] EWHC 975 (Admin), waarbij aan de High Court werd gevraagd zich te buigen over het delen van gegevens tussen de politie en een *Business Crime Reduction Partnership (BCRP)*, een organisatie die bevoegd is om uitsluitingsbevelen uit te vaardigen waarbij bepaalde personen de toegang wordt ontzegd tot de bedrijfsruimten van haar leden. De rechter onderzocht het delen van gegevens dat plaatsvond op basis van een overeenkomst die tot doel had het publiek te beschermen en criminaliteit te voorkomen, en concludeerde uiteindelijk dat de meeste aspecten van het delen van gegevens rechtmatig waren, behalve met betrekking tot enkele gevoelige gegevens die tussen de politie en de BCRP werden gedeeld. Een ander voorbeeld is de zaak *Cooper v NCA* [2019] EWCA Civ 16, waarbij het Court of Appeal (hof van beroep) het delen van gegevens tussen de politie en het *Serious Organised Crime Agency (SOCA)*, het agentschap voor de bestrijding van zware georganiseerde criminaliteit dat momenteel deel uitmaakt van de NCA, bekrachtigde.

([206]) Artikel 36, lid 4, van de DPA 2018.

autoriteit, een belastingdienst, een mededingingsautoriteit, een jeugdzorginstantie); 2) wanneer een strafrechtelijke handhavingsinstantie gegevens deelt met een inlichtingendienst. In het eerste scenario valt de verwerking van persoonsgegevens onder het toepassingsgebied van de UK GDPR en deel 2 van de DPA 2018. Zoals vermeld in het besluit vastgesteld uit hoofde van Verordening (EU) 2016/679, verschaffen de waarborgen waarin is voorzien bij de UK GDPR en deel 2 van de DPA 2018 een beschermingsniveau dat in wezen overeenkomt met het niveau dat in de Unie wordt verzekerd ([207]).

(127) In het tweede scenario, waarbij door een strafrechtelijke handhavingsinstantie verzamelde gegevens worden gedeeld met een inlichtingendienst met het oog op de nationale veiligheid, is het delen van gegevens toegestaan op grond van de *Counter Terrorism Act 2008* (CTA 2008 — antiterrorismewet) ([208]). Krachtens de CTA 2008 mag elke persoon inlichtingen verstrekken aan de inlichtingendiensten met het oog op de uitvoering van de taken van die dienst, onder meer de "nationale veiligheid".

(128) Gegevens kunnen slechts onder bepaalde voorwaarden worden gedeeld met het oog op de nationale veiligheid. In dat verband wordt de mogelijkheid voor de inlichtingendiensten om gegevens te verkrijgen door de *Intelligence Services Act* (wet op de inlichtingendiensten) en de *Security Services Act* (wet op de veiligheidsdiensten) beperkt tot datgene wat noodzakelijk is om hun wettelijke taken uit te oefenen. Bevoegde autoriteiten die vallen onder het toepassingsgebied van deel 3 van de DPA 2018 en die gegevens wensen te delen met de inlichtingendiensten zullen rekening moeten houden met een aantal factoren/beperkingen, naast de wettelijke taken van die diensten die zijn uiteengezet in de Intelligence Services Act en de Security Services Act ([209]). In artikel 20 van de CTA 2008 is duidelijk bepaald dat het delen van gegevens uit hoofde van artikel 19 van de CTA 2008 ook altijd moet voldoen aan de gegevensbeschermingswetgeving; dit betekent dat alle beperkingen en vereisten van de DPA 2018 van toepassing zijn. Voorts zijn de rechtshandhavingsinstanties en inlichtingendiensten "public authorities" (overheidsinstanties) in de zin van de Human Rights Act 1998 en moeten zij er derhalve voor zorgen dat zij handelen in overeenstemming met de rechten die uit hoofde van het EVRM, met inbegrip van artikel 8, zijn gewaarborgd. Met andere woorden, deze vereisten houden in dat het delen van gegevens tussen rechtshandhavingsinstanties en inlichtingendiensten altijd moet voldoen aan de gegevensbeschermingswetgeving en het EVRM.

(129) Voor de verwerking door inlichtingendiensten van persoonsgegevens die zij ontvangen of verkrijgen van rechtshandhavingsinstanties met het oog op de nationale veiligheid gelden een aantal voorwaarden en waarborgen ([210]). Deel 4 van de DPA 2018 geldt voor elke verwerking door of namens de inlichtingendiensten. Dat

([207]) Uitvoeringsbesluit van de Commissie overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad betreffende de adequate bescherming van persoonsgegevens door het Verenigd Koninkrijk; C(2021) 4800.

([208]) Artikel 19 van de Counter Terrorism Act 2008, beschikbaar via de volgende link: https://www.legislation.gov.uk/ukpga/2008/28/section/19

([209]) In artikel 2, lid 2, van de Intelligence Service Act 1994 (zie https://www.legislation.gov.uk/ukpga/1994/13/contents) is bepaald dat "het hoofd van de inlichtingendienst verantwoordelijk is voor de doeltreffendheid van die dienst en dat het zijn/haar taak is ervoor te zorgen — a) dat er regelingen zijn aan de hand waarvan gegarandeerd is dat de inlichtingendienst geen informatie verkrijgt tenzij dit noodzakelijk is voor de correcte uitoefening van zijn taken en dat de inlichtingendienst geen informatie verstrekt tenzij dit noodzakelijk is — i) voor dat doel; ii) in het belang van de nationale veiligheid; iii) voor de voorkoming of opsporing van ernstige misdrijven; of iv) ten behoeve van een strafrechtelijke procedure; en b) dat de inlichtingendienst geen maatregelen treft om de belangen van een Britse politieke partij te bevorderen." In artikel 2, lid 2, van de Security Service Act 1989 (zie https://www.legislation.gov.uk/ukpga/1989/5/contents) is bepaald dat "de directeur-generaal verantwoordelijk is voor de doeltreffendheid van de dienst en dat het zijn/haar taak is ervoor te zorgen — a) dat er regelingen zijn aan de hand waarvan gegarandeerd is dat de dienst geen informatie verkrijgt tenzij dit noodzakelijk is voor de correcte uitoefening van zijn taken en dat de dienst geen informatie bekendmaakt tenzij dit noodzakelijk is voor dat doel of voor de voorkoming of opsporing van ernstige misdrijven of in het kader van een strafrechtelijke procedure; en b) dat de dienst geen maatregelen treft om de belangen van een politieke partij te bevorderen; en c) dat er met de directeur-generaal van het National Crime Agency overeengekomen regelingen zijn om de activiteiten van de dienst conform artikel 1, lid 4, van deze wet te coördineren met de activiteiten van de politiediensten, het National Crime Agency en andere rechtshandhavingsinstanties."

([210]) Waarborgen betreffende de bevoegdheden van de inlichtingendiensten en beperkingen op die bevoegdheden zijn ook neergelegd in de *Investigatory Powers Act 2016* (de wet onderzoeksbevoegdheden) die, samen met de *Regulation of Investigatory Powers Act 2000* voor Engeland, Wales en Noord-Ierland en de *Regulation of Investigatory Powers (Scotland) Act 2000* voor Schotland, de rechtsgrondslag vormt voor het gebruik van die bevoegdheden. Die bevoegdheden zijn echter niet relevant in de context van het "verder delen" aangezien zij de rechtstreekse verzameling van persoonsgegevens door inlichtingendiensten betreffen. Voor een beoordeling van de bevoegdheden die in het kader van de Investigatory Powers Act aan de inlichtingendiensten zijn verleend, zie het uitvoeringsbesluit van de Commissie overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad betreffende de adequate bescherming van persoonsgegevens door het Verenigd Koninkrijk; C(2021)4800.

deel bevat de belangrijkste gegevensbeschermingsbeginselen (rechtmatigheid, eerlijkheid en transparantie ([211]); doelbinding ([212]); gegevensminimalisatie ([213]); juistheid ([214]); opslagbeperking ([215]) en beveiliging ([216])), de voorwaarden voor de verwerking van bijzondere gegevenscategorieën ([217]), de rechten van betrokkenen ([218]), het vereiste dat gegevensbescherming door ontwerp wordt toegepast ([219]) en de regeling voor de internationale doorgiften van persoonsgegevens ([220]).

(130) Bovendien voorziet artikel 110 van de DPA 2018 in een vrijstelling van sommige bepalingen van deel 4 van de DPA 2018 wanneer een dergelijke vrijstelling vereist is om de nationale veiligheid te waarborgen. In artikel 110, lid 2, van de DPA 2018 worden de bepalingen opgesomd waarvan kan worden afgeweken. Het omvat gegevensbeschermingsbeginselen (met uitzondering van het rechtmatigheidsbeginsel), de rechten van betrokkenen, de verplichting om de Information Commissioner in kennis te stellen van een inbreuk in verband met persoonsgegevens, de inspectiebevoegdheden van de Information Commissioner op grond van internationale verplichtingen, bepaalde handhavingsbevoegdheden van de Information Commissioner, de bepalingen die bepaalde inbreuken op de gegevensbeschermingswetgeving strafbaar stellen, en de bepalingen in verband met bijzondere verwerkingsdoeleinden, zoals journalistieke, academische of artistieke doeleinden. Van deze afwijking kan gebruik worden gemaakt op basis van een analyse per geval ([221]). Zoals toegelicht door de Britse autoriteiten en bevestigd door de rechtspraak van Britse rechtbanken moet "de verwerkingsverantwoordelijke rekening houden met de daadwerkelijke gevolgen voor de nationale veiligheid of defensie als hij/zij de desbetreffende gegevensbeschermingsbepaling zou naleven; hij moet ook nagaan of hij/zij redelijkerwijs de normale regel zou kunnen naleven zonder afbreuk te doen aan de nationale veiligheid of defensie" ([222]). Het ICO houdt toezicht op de correcte toepassing van de vrijstelling ([223]).

([211]) Op grond van artikel 86, lid 6, van de DPA 2018 moet de methode aan de hand waarvan de gegevens zijn verkregen in aanmerking worden genomen om de behoorlijkheid en transparantie van de verwerking te beoordelen. In dit verband is aan het vereiste van behoorlijkheid en transparantie voldaan als de gegevens zijn verkregen van een persoon die rechtmatig toestemming heeft gekregen of die rechtmatig verplicht is om die gegevens te verstrekken.

([212]) Op grond van artikel 87 van de DPA 2018 moet er sprake zijn van welbepaalde, uitdrukkelijk omschreven en legitieme doeleinden van de verwerking. De gegevens mogen niet op een met die doeleinden onverenigbare wijze worden verwerkt. Ingevolge artikel 87, lid 3, kan de verenigbare verdere verwerking van persoonsgegevens uitsluitend worden toegestaan indien de verwerkingsverantwoordelijke overeenkomstig het recht gemachtigd is deze gegevens voor dat doel te verwerken en de verwerking noodzakelijk is en in verhouding staat tot dat andere doel. De verwerking moet verenigbaar worden geacht als zij bestaat uit verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of gebruik voor statistische doeleinden, en mits er passende waarborgen worden geboden (artikel 87, lid 4, van de DPA 2018).

([213]) Persoonsgegevens moeten toereikend, ter zake dienend en niet bovenmatig zijn (artikel 88 van de DPA 2018).

([214]) Persoonsgegevens moeten juist en geactualiseerd zijn (artikel 89 van de DPA 2018).

([215]) Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk is (artikel 90 van de DPA 2018).

([216]) Het zesde gegevensbeschermingsbeginsel houdt in dat bij de verwerking van persoonsgegevens onder meer passende veiligheidsmaatregelen worden getroffen betreffende risico's die voortvloeien uit de verwerking van persoonsgegevens. Deze risico's zijn onder meer (maar zijn niet beperkt tot) onopzettelijke of ongeoorloofde toegang tot en onopzettelijk of ongeoorloofd verlies, gebruik, wijziging of bekendmaking van persoonsgegevens (artikel 91 van de DPA 2018). In artikel 107 is ook bepaald 1) dat elke verwerkingsverantwoordelijke veiligheidsmaatregelen moet nemen die passen bij de risico's ten gevolge van de verwerking van persoonsgegevens en 2) dat als er sprake is van geautomatiseerde verwerking, elke verwerkingsverantwoordelijke en elke verwerker preventieve of mitigerende maatregelen moet nemen die op een risicoanalye zijn gebaseerd.

([217]) Artikel 86, lid 2, punt b), van de DPA 2018 en bijlage 10 bij de DPA 2018.

([218]) Hoofdstuk 3 van deel 4 van de DPA 2018, met name: het recht op toegang, rectificatie en wissing, het recht om bezwaar aan te tekenen tegen de verwerking en niet aan geautomatiseerde besluitvorming te worden onderworpen, het recht om in te grijpen in geautomatiseerde besluitvorming en over de besluitvorming te worden ingelicht. Bovendien moet de verwerkingsverantwoordelijke de betrokkene informatie geven over de verwerking van zijn/haar persoonsgegevens.

([219]) Artikel 103 van de DPA 2018.

([220]) Artikel 109 van de DPA 2018. Doorgiften van persoonsgegevens aan internationale organisaties of landen buiten het Verenigd Koninkrijk zijn mogelijk als de doorgifte een noodzakelijke en evenredige maatregel is die wordt uitgevoerd in het kader van de wettelijke taken van de verwerkingsverantwoordelijke of voor andere doeleinden die zijn bepaald in specifieke artikelen van de Security Service Act 1989 en de Intelligence Services Act 1994.

([221]) Zie de zaak *Baker v Secretary of State for the Home Department* [2001] UKIT NSA2 ("*Baker v Secretary of State*").

([222]) *Explanatory Framework for Adequacy Discussion, section H: National Security Data Protection and Investigatory Powers Framework*, blz. 15-16, beschikbaar via de volgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf. Zie ook *Baker v Secretary of State* (zie voetnoot 220 hierboven), waarin het Tribunal een nationaleveiligheidscertificaat nietig verklaarde dat door de minister van Binnenlandse Zaken was afgegeven en dat de toepassing van de vrijstelling in verband met de nationale veiligheid bevestigde; het Tribunal oordeelde dat er geen reden was om te voorzien in een algemene vrijstelling op de verplichting om verzoeken om toegang te beantwoorden en dat het toestaan van een dergelijke vrijstelling in alle omstandigheden, zonder onderzoek per geval, verder ging dan wat noodzakelijk en evenredig was voor de bescherming van de nationale veiligheid.

([223]) Zie het memorandum van overeenstemming tussen het ICO en het UKIC, waarin staat "dat wanneer het ICO een klacht van een betrokkene ontvangt, het ICO zal nagaan of de aangelegenheid correct is afgehandeld en, in voorkomend geval, of een eventuele vrijstelling op correcte wijze is toegepast" (memorandum van overeenstemming tussen het Bureau van de Information Commissioner en de Britse inlichtingendiensten, punt 16, beschikbaar via de volgende link: https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf).

(131) In verband met de mogelijkheid om de bovenvermelde rechten te beperken met het oog op de bescherming van de "nationale veiligheid" wordt in artikel 79 van de DPA 2018 bovendien bepaald dat een verwerkingsverantwoordelijke een aanvraag mag indienen voor een certificaat dat ondertekend is door een minister of door de Attorney General, waarin wordt verklaard dat een beperking van die rechten een noodzakelijke en evenredige maatregel is, of was, voor de bescherming van de nationale veiligheid ([224]). De Britse regering heeft richtsnoeren uitgevaardigd over de nationaleveiligheidscertificaten uit hoofde van de DPA 2018, waarin met name wordt benadrukt dat elke beperking van de rechten van betrokkenen met het oog op de bescherming van de nationale veiligheid evenredig en noodzakelijk moet zijn ([225]). Alle nationale veiligheidscertificaten moeten op de website van het ICO worden gepubliceerd ([226]).

(132) Het certificaat moet geldig zijn voor een vaste periode van maximaal vijf jaar om ervoor te zorgen dat het regelmatig door de uitvoerende macht wordt geëvalueerd ([227]). In een certificaat moeten de persoonsgegevens of categorieën van persoonsgegevens zijn vermeld waarvoor de vrijstelling geldt, evenals de bepalingen van de DPA 2018 waarop de vrijstelling van toepassing is ([228]).

(133) Het is belangrijk op te merken dat nationaleveiligheidscertificaten geen extra grond vormen voor het beperken van gegevensbeschermingsrechten om redenen van nationale veiligheid. De verwerkingsverantwoordelijke of de verwerker kan zich met andere woorden uitsluitend op een certificaat beroepen wanneer hij/zij het noodzakelijk acht om een beroep te doen op de vrijstelling inzake de nationale veiligheid, die per geval moet worden aangevraagd. Zelfs als een nationaleveiligheidscertificaat van toepassing is op de betreffende aangelegenheid, kan het ICO onderzoeken of het al of niet gerechtvaardigd was in een specifiek geval een beroep te doen op de vrijstelling inzake de nationale veiligheid ([229]).

(134) Elke persoon die directe gevolgen ondervindt van de afgifte van het certificaat kan bij het *Upper Tribunal* ([230]) (de rechter in tweede aanleg) een beroep instellen tegen het certificaat ([231]) of, wanneer in het certificaat gegevens worden geïdentificeerd door middel van een algemene beschrijving, de toepassing van het certificaat op specifieke gegevens aanvechten ([232]).

(135) De rechter in tweede aanleg zal het besluit om een certificaat af te geven beoordelen en nagaan of er al dan niet redelijke gronden waren om het certificaat af te geven ([233]). De rechter kan een hele reeks aangelegenheden in overweging nemen, onder meer de noodzakelijkheid, evenredigheid en rechtmatigheid, rekening houdend met de gevolgen voor de rechten van betrokkenen en een afweging van de noodzaak om de nationale veiligheid te waarborgen. Bijgevolg kan de rechter tot de conclusie komen dat het certificaat niet van toepassing is op specifieke persoonsgegevens die het onderwerp zijn van het beroep ([234]).

([224]) Bij de DPA 2018 is de mogelijkheid om op grond van artikel 28, lid 2, van de Data Protection Act 1998 een certificaat af te geven, ingetrokken. Het is echter wel nog mogelijk om "oude certificaten" af te geven voor zover er sprake is van betwistingen uit het verleden op grond van de 1998 Act (zie punt 17 van deel 5 van bijlage 20 bij de DPA 2018). Deze mogelijkheid lijkt zich echter zeer zelden voor te doen en zal slechts in een beperkt aantal gevallen van toepassing zijn, bijvoorbeeld wanneer een betrokkene het gebruik van de vrijstelling inzake de nationale veiligheid aanvecht met betrekking tot een verwerking die door een overheidsinstantie is uitgevoerd op grond van de 1998 Act. Opgemerkt zij dat artikel 28 van de DPA 1998 in die gevallen volledig van toepassing zal zijn, met inbegrip derhalve van de mogelijkheid voor de betrokkene om het certificaat aan te vechten. Momenteel zijn er geen nationaleveiligheidscertificaten afgegeven uit hoofde van de DPA 1998.

([225]) Richtsnoeren van de Britse regering inzake nationaleveiligheidscertificaten uit hoofde van de DPA 2018, beschikbaar via de volgende link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf

([226]) Volgens artikel 130 van de DPA 2018 kan het ICO besluiten de tekst van het certificaat geheel of gedeeltelijk niet te publiceren, indien dit zou indruisen tegen 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. In deze gevallen maakt het ICO echter wel bekend dat het certificaat is afgegeven.

([227]) Richtsnoeren van de Britse regering inzake nationaleveiligheidscertificaten, punt 15, zie voetnoot 225.

([228]) Richtsnoeren van de Britse regering inzake nationaleveiligheidscertificaten, punt 5, zie voetnoot 225.

([229]) Overeenkomstig artikel 102 van de DPA 2018 moet de verwerkingsverantwoordelijke kunnen aantonen dat hij/zij de DPA 2018 heeft nageleefd. Dit betekent dat een inlichtingendienst aan het ICO zou moeten aantonen dat hij, wanneer hij een beroep deed op de vrijstelling, de specifieke omstandigheden van het geval in overweging heeft genomen. Het ICO publiceert ook een register van de nationaleveiligheidscertificaten, dat beschikbaar is via de volgende link: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/.

([230]) Het Upper Tribunal is de rechtbank die bevoegd is voor beroepszaken tegen besluiten van lagere administratieve rechtbanken en heeft specifieke bevoegdheid voor rechtstreekse beroepen tegen besluiten van bepaalde overheidsorganen.

([231]) Artikel 111, lid 3, van de DPA 2018.

([232]) Artikel 111, lid 5, van de DPA 2018.

([233]) In de zaak *Baker v Secretary of State* (zie voetnoot 221) verklaarde het Information Tribunal een nationaleveiligheidscertificaat nietig dat door de minister van Binnenlandse Zaken was afgegeven, met de overweging dat er geen reden was om te voorzien in een algemene vrijstelling op de verplichting om verzoeken om toegang te beantwoorden en dat het toestaan van een dergelijke vrijstelling in alle omstandigheden, zonder onderzoek per geval, verder ging dan wat noodzakelijk en evenredig was voor de bescherming van de nationale veiligheid.

([234]) Richtsnoeren van de Britse regering inzake nationaleveiligheidscertificaten, punt 25, zie voetnoot 225.

(136) Een andere reeks mogelijke beperkingen zijn de beperkingen die ingevolge bijlage 11 bij de DPA 2018 van toepassing zijn op sommige bepalingen van deel 4 van de DPA 2018 ([235]) en waarbij andere belangrijke doelstellingen van algemeen openbaar belang of beschermde belangen, zoals de parlementaire onschendbaarheid, de vertrouwelijkheid van de communicatie tussen advocaat en cliënt, het voeren van gerechtelijke procedures of de paraatheid van de strijdkrachten, worden gewaarborgd. De toepassing van deze bepalingen is ofwel vrijgesteld voor bepaalde gegevenscategorieën ("*class based*", op grond van categorie), ofwel vrijgesteld voor zover de toepassing van die bepalingen het beschermde belang zou kunnen schaden ("*prejudice based*", op grond van schade) ([236]). Op vrijstellingen op grond van schade kan uitsluitend een beroep worden gedaan als de toepassing van de vermelde gegevensbeschermingsbepaling het betrokken specifieke belang zou kunnen schaden. Het gebruik van een vrijstelling moet dan ook altijd worden gerechtvaardigd door te verwijzen naar de desbetreffende schade die zich in het afzonderlijke geval zou kunnen voordoen. Op vrijstellingen op grond van categorie kan uitsluitend een beroep worden gedaan in verband met de specifieke, strikt afgebakende gegevenscategorie waarvoor de vrijstelling wordt verleend. Deze lijken qua doel en effect sterk op veel van de uitzonderingen op de UK GDPR (uit hoofde van bijlage 2 bij de DPA 2018) die, op hun beurt, een weerspiegeling zijn van de uitzonderingen van artikel 23 AVG.

(137) Uit het bovenstaande volgt dat de toepasselijke wettelijke bepalingen van het Verenigd Koninkrijk, zoals uitgelegd door de rechtbanken en de Information Commissioner, beperkingen en voorwaarden bevatten aan de hand waarvan wordt gegarandeerd dat deze vrijstellingen en beperkingen binnen de grenzen blijven van wat noodzakelijk en evenredig is om de nationale veiligheid te beschermen.

(138) Op de verwerking van persoonsgegevens door de inlichtingendiensten uit hoofde van deel 4 van de DPA 2018 wordt toezicht gehouden door de Information Commissioner ([237]).

(139) In bijlage 13 bij de DPA 2018 zijn de algemene taken van de Information Commissioner in verband met de verwerking van persoonsgegevens door inlichtingendiensten uit hoofde van deel 4 van de DPA 2018 vastgelegd. De taken omvatten, maar zijn niet beperkt tot, toezicht op en handhaving van deel 4 van de DPA 2018, voorlichting van het publiek, adviseren van het parlement, de regering en andere instellingen over wetgevings- en bestuursrechtelijke maatregelen, de verwerkingsverantwoordelijken en de verwerkers beter bekendmaken met hun verplichtingen, informatie verstrekken aan een betrokkene over de uitoefening van zijn/haar rechten, en onderzoeken uitvoeren.

(140) Wat deel 3 van de DPA 2018 betreft, heeft de Information Commissioner de bevoegdheid aan verwerkingsverantwoordelijken te melden dat er vermoedelijk een inbreuk is gepleegd, hen te waarschuwen dat een verwerking waarschijnlijk een inbreuk vormt op de regels, en berispingen te geven wanneer de inbreuk is bevestigd. De Information Commissioner kan tevens handhavings- en boetenota's afgeven voor inbreuken op bepaalde bepalingen van de wet ([238]). Anders dan voor andere delen van de DPA 2018 kan de Information Commissioner evenwel geen beoordelingsnota afgeven aan een nationale veiligheidsdienst ([239]).

(141) Bovendien voorziet artikel 110 van de DPA 2018 in een uitzondering op de uitoefening van bepaalde bevoegdheden van de Information Commissioner wanneer dit vereist is om de nationale veiligheid te waarborgen. Dit omvat de bevoegdheid van de Information Commissioner om nota's uit hoofde van de DPA af te geven, van welke aard ook (informatie-, beoordelings-, handhavings- en boetenota's), de bevoegdheid om inspecties te verrichten overeenkomstig internationale verplichtingen, de bevoegdheid tot toegang en inspectie, en de regels inzake strafbare

([235]) Hieronder vallen: i) de gegevensbeschermingsbeginselen van deel 4, behalve het vereiste in verband met de rechtmatigheid van de verwerking conform het eerste beginsel en het feit dat de verwerking moet voldoen aan een van de relevante voorwaarden als bepaald in de bijlagen 9 en 10; ii) de rechten van betrokkenen; en iii) de verplichtingen in verband met het melden van inbreuken aan het ICO.

([236]) Volgens het *Explanatory Framework* van het Verenigd Koninkrijk zijn de "class based" (op categorieën gebaseerde) uitzonderingen: i) informatie over de toekenning van eerbewijzen en adelbrieven door de Kroon; ii) de vertrouwelijkheid van de communicatie tussen advocaat en cliënt; iii) vertrouwelijke referenties in verband met werk, opleiding of onderwijs; en iv) examenteksten en cijfers. De "prejudice based" uitzonderingen (op grond van schade) betreffen de volgende aangelegenheden: i) voorkoming of opsporing van criminaliteit; de aanhouding en gerechtelijke vervolging van daders; ii) parlementaire onschendbaarheid; iii) gerechtelijke procedures; iv) de paraatheid van de strijdkrachten van de Kroon; v) het economisch welzijn van het Verenigd Koninkrijk; vi) onderhandelingen met de betrokkene; vii) wetenschappelijk of historisch onderzoek, of statistische doeleinden; viii) archivering in het algemeen belang. *Explanatory Framework for Adequacy Discussion, section H: National Security*, blz. 13, zie voetnoot 222).

([237]) Artikel 116 van de DPA 2018.

([238]) Uit een gecombineerde lezing van artikel 149, punt 2, en artikel 155 van de DPA 2018 volgt, dat handhavings- en boetenota's kunnen worden afgegeven aan een verwerkingsverantwoordelijke of verwerker in verband met inbreuken op hoofdstuk 2 van deel 4 van de DPA 2018 (beginselen van de verwerking), een bepaling van deel 4 van de DPA 2018 waarin rechten worden verleend aan een betrokkene, een vereiste om een inbreuk op persoonsgegevens aan de Information Commissioner mede te delen op grond van artikel 108 van de DPA 2018, en de beginselen voor doorgiften van persoonsgegevens aan derde landen, landen die niet door het EVRM zijn gebonden en internationale organisaties in artikel 109 van de DPA 2018 (zie de overwegingen 102 en 103 voor meer informatie over handhavings- en boetenota's).

([239]) Uit hoofde van artikel 147, lid 6, van de DPA 2018 mag de Information Commissioner geen beoordelingsnota afgeven aan een instantie die vermeld is in artikel 23, lid 3, van de *Freedom of Information Act 2000*. Daaronder vallen de veiligheidsdienst (MI5), de geheime dienst (MI6) en de *Government Communications Headquarters* (communicatiehoofdkwartier van de regering).

feiten ([240]). Zoals uiteengezet in overweging 136, zijn deze uitzonderingen uitsluitend per geval van toepassing en moeten zij noodzakelijk en evenredig zijn. De toepassing van deze uitzonderingen kan door de rechter worden getoetst ([241]).

(142) Het ICO en de Britse inlichtingendiensten hebben een memorandum van overeenstemming ([242]) ondertekend waarin een kader voor samenwerking op een aantal gebieden is vastgesteld, onder meer in verband met nota's betreffende gegevensinbreuken en de behandeling van klachten van betrokkenen. In dit kader is met name bepaald dat het ICO bij ontvangst van een klacht zal beoordelen of er terecht een beroep is gedaan op een uitzondering in verband met de nationale veiligheid. Vragen van het ICO in het kader van het onderzoek van individuele klachten moeten binnen twintig werkdagen worden beantwoord met behulp van de betrokken richtsnoeren van de Britse regering inzake nationaleveiligheidscertificaten uit hoofde van de Data Protection Act, en via passende beveiligde kanalen als er sprake is van gerubriceerde informatie. Van april 2018 tot heden heeft het ICO 21 klachten van personen over inlichtingendiensten ontvangen. Elke klacht werd beoordeeld en de uitkomst werd aan de betrokkene meegedeeld ([243]).

(143) Daarnaast oefent het *Intelligence and Security Committee* (ISC — Inlichtingen- en veiligheidscomité) parlementair toezicht uit op de gegevensverwerking door inlichtingendiensten. Dit comité is opgericht uit hoofde van de *Justice and Security Act 2013* (JSA 2013 — wet justitie en veiligheid) ([244]). Bij deze wet wordt het ISC ingesteld als een comité van het Britse parlement. Het ISC is samengesteld uit leden die tot een van de kamers van het parlement behoren en die aangesteld zijn door de premier na overleg met de leider van de oppositie ([245]). Het ISC moet aan het parlement een jaarverslag voorleggen over de uitoefening van zijn taken, en andere verslagen die het passend acht ([246]).

(144) Sinds 2013 beschikt het ISC over ruimere bevoegdheden, waaronder het toezicht op de operationele activiteiten van de veiligheidsdiensten. Krachtens artikel 2 van de JSA 2013 heeft het ISC tot taak toezicht te houden op de uitgaven, de administratie, het beleid en de activiteiten van de nationale veiligheidsdiensten. In de JSA 2013 is bepaald dat het ISC onderzoeken naar operationele aangelegenheden mag uitvoeren wanneer deze geen betrekking hebben op

([240]) Voor de volgende bepalingen zijn vrijstellingen mogelijk: artikel 108 (mededeling van een inbreuk op persoonsgegevens aan de Information Commissioner), artikel 119 (inspectie overeenkomstig internationale verplichtingen); de artikelen 142 tot en met 154 en bijlage 15 (nota's en toegangs- en inspectiebevoegdheden van de Information Commissioner); en de artikelen 170 tot en met 173 (strafbare feiten in verband met persoonsgegevens). Vrijstellingen zijn ook mogelijk in verband met de verwerking door de inlichtingendiensten in bijlage 13 (andere algemene taken van de Commissioner): punt 1, onder a) en g), en punt 2.

([241]) Zie bijvoorbeeld de zaak *Baker v Secretary of State for the Home Department* (zie voetnoot 221)

([242]) Memorandum van overeenstemming tussen het ICO en de Britse inlichtingendiensten, zie voetnoot 231.

([243]) In zeven van deze gevallen adviseerde het ICO de klager om de klacht voor te leggen aan de verwerkingsverantwoordelijke (dit is het geval wanneer een persoon een klacht heeft ingediend bij het ICO, maar dat eerst bij de verwerkingsverantwoordelijke had moeten doen), in één van de gevallen gaf het ICO algemeen advies aan de verwerkingsverantwoordelijke (dit wordt gedaan wanneer de acties van de verwerkingsverantwoordelijke geen inbreuk op de wetgeving lijken te hebben gemaakt, maar een verbetering van de praktijken had kunnen voorkomen dat de klacht bij het ICO werd ingediend), en in de overige dertien gevallen was geen actie van de verwerkingsverantwoordelijke vereist (dit is het geval wanneer de door de persoon ingediende klachten wel onder de Data Protection Act 2018 vallen omdat zij betrekking hebben op de verwerking van persoonsgegevens, maar de verwerkingsverantwoordelijke op basis van de verstrekte informatie geen inbreuk op de wetgeving lijkt te hebben gemaakt).

([244]) Zoals uitgelegd door de Britse autoriteiten werd met de JSA de toepassing van het ISC verruimd om een rol in het toezicht op de inlichtingendiensten op te nemen die verder gaat dan de drie diensten en toezicht met terugwerkende kracht mogelijk te maken ten aanzien van de operationele activiteiten van de diensten met betrekking tot aangelegenheden van aanzienlijk nationaal belang.

([245]) Artikel 1 van de JSA 2013. ministers kunnen niet tot leden worden benoemd. Leden vervullen hun functie in het ISC voor de zittingsperiode van het parlement gedurende welke zij werden benoemd. Zij kunnen worden afgezet door een resolutie van de kamer die hen heeft benoemd, of als zij geen parlementslid meer zijn, of als zij minister worden. Een lid kan ook zijn/haar ambt neerleggen.

([246]) Verslagen en verklaringen van het comité zijn online te vinden op: http://isc.independent.gov.uk/committee-reports. In 2015 heeft het ISC een verslag uitgebracht met als titel *Privacy and Security: A modern and transparent legal framework* (Privacy en veiligheid: een modern en transparant rechtskader, zie https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf) waarin het comité het rechtskader voor door de inlichtingendiensten gebruikte surveillancetechnieken in ogenschouw heeft genomen en een reeks aanbevelingen heeft gedaan die vervolgens werden beoordeeld en opgenomen in het wetsvoorstel inzake onderzoeksbevoegdheden, dat vervolgens werd aangenomen als wetgeving: de IPA 2016. Het antwoord van de regering op het verslag inzake privacy en veiligheid is te vinden op: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20151208_Privacy_and_Security_Government_Response.pdf

lopende operaties ([247]). In het memorandum van overeenstemming tussen de premier en het ISC ([248]) zijn nadere bijzonderheden opgenomen over de elementen waarmee rekening moet worden gehouden wanneer wordt bekeken of een activiteit al dan niet deel uitmaakt van een lopende operatie ([249]). Het ISC kan door de premier ook worden verzocht lopende operaties te onderzoeken en kan informatie beoordelen die vrijwillig door de diensten wordt verstrekt.

(145) Krachtens bijlage 1 bij de JSA 2013 mag het ISC het hoofd van elk van de drie inlichtingendiensten vragen om informatie te verstrekken. De betrokken dienst moet die informatie beschikbaar stellen, tenzij de Secretary of State daar een veto tegen uitspreekt ([250]). Volgens de Britse autoriteiten wordt er in de praktijk zeer weinig informatie achtergehouden voor het ISC ([251]).

(146) Wat het verhaalsrecht betreft, kan een betrokkene eerst en vooral uit hoofde van artikel 165, lid 2, van de DPA 2018 een klacht indienen bij het ICO indien hij/zij van mening is dat er in verband met de hem/haar betreffende persoonsgegevens een inbreuk heeft plaatsgevonden op deel 4 van de DPA 2018, met inbegrip van misbruik van de vrijstellingen en beperkingen in verband met de nationale veiligheid.

(147) Bovendien hebben personen krachtens deel 4 van de DPA 2018 het recht de High Court (of de Court of Session in Schotland) te verzoeken om een beschikking die de verwerkingsverantwoordelijke ertoe verplicht het recht op inzage in gegevens ([252]), het recht om bezwaar te maken tegen de verwerking ([253]) en het recht op rectificatie of wissing te eerbiedigen.

(148) Personen hebben tevens het recht om vergoeding te vorderen van de schade die zij hebben geleden als gevolg van niet-naleving van een vereiste in deel 4 van de DPA 2018 door de verwerkingsverantwoordelijke of een verwerker ([254]). Schade omvat zowel financieel verlies als niet-financieel verlies, zoals leed ([255]).

(149) Tot slot kan een persoon een klacht indienen bij het *Investigatory Powers Tribunal* (IPT) voor het handelen van of namens de Britse inlichtingendiensten ([256]). Het IPT is een rechterlijke instantie die is opgericht bij de Regulation of Investigatory Powers Act 2000 voor Engeland, Wales en Noord-Ierland en de Regulation of Investigatory Powers (Scotland) Act 2000 voor Schotland (RIPA 2000) en is onafhankelijk van de uitvoerende macht ([257]). Overeenkomstig artikel 65 van de RIPA 2000 worden de leden van het IPT door Hare Majesteit benoemd voor een periode van vijf jaar.

(150) Een lid van het Tribunal kan uit zijn/haar functie worden ontheven door Hare Majesteit na een *Address* ([258]) van beide kamers van het parlement ([259]).

(151) Om zich tot het IPT te wenden ("*standing requirement*", procesbevoegdheidsvereiste), moeten personen overeenkomstig artikel 65 van de RIPA 2000 ervan overtuigd zijn i) dat het gedrag van een inlichtingendienst heeft plaatsgevonden met betrekking tot henzelf, hun eigendom, mededelingen die door of naar hen zijn verzonden of voor hen bedoeld waren, of hun gebruik van een postdienst, telecommunicatiedienst of telecommunicatiesysteem ([260]), en ii) dat het gedrag heeft plaatsgevonden in betwistbare omstandigheden ("*challengeable*

([247]) Artikel 2 van de JSA 2013.
([248]) Memorandum van overeenstemming tussen de premier en het ISC, beschikbaar via de volgende link: http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf
([249]) Memorandum van overeenstemming tussen de premier en het ISC, punt 14, zie voetnoot 248.
([250]) De Secretary of State kan op slechts twee gronden een veto ten aanzien van de verstrekking van informatie uitspreken: de informatie is gevoelig en mag niet aan het ISC worden verstrekt in het belang van de nationale veiligheid; of de informatie is van dien aard dat, indien de Secretary of State zou worden gevraagd om die informatie aan een *Departmental Select Committee* (toezichtscommissie) van het Britse Lagerhuis te overleggen, de Secretary of State het (op gronden die niet tot de nationale veiligheid zijn beperkt) niet passend acht dat te doen (bijlage 1, punt 4, onder 2), van de JSA 2013).
([251]) *Explanatory Framework — section H: National Security*, blz. 43.
([252]) Artikel 94, lid 11, van de DPA 2018.
([253]) Artikel 99, lid 4, van de DPA 2018.
([254]) Volgens artikel 169 van de DPA 2018 kunnen "personen die schade lijden ten gevolge van een overtreding van een voorschrift van de gegevensbeschermingswetgeving, een schadevordering instellen."
([255]) Artikel 169, lid 5, van de DPA 2018.
([256]) Artikel 65, lid 2, punt b), van de RIPA.
([257]) De leden moeten krachtens bijlage 3 bij de RIPA 2000 specifieke juridische ervaring hebben en zij kunnen worden herbenoemd.
([258]) Zie voetnoot 183 voor het begrip *Address*.
([259]) Bijlage 3, punt 1, onder 5), van de RIPA 2000.
([260]) Artikel 65, lid 4, van de RIPA 2000.

circumstances") ([261]) of is uitgevoerd door of namens de inlichtingendiensten ([262]). Aangezien het criterium inzake deze "overtuiging" ruim is opgevat ([263]), worden er voor het aanhangig maken van een zaak voor het Tribunal relatief lage eisen ("*standing requirements*") gesteld.

(152) Wanneer het Tribunal een bij hem ingediende klacht behandelt, is het zijn plicht te onderzoeken of de personen tegen wie in de klacht een beschuldiging is geuit, jegens de klager zijn opgetreden en om onderzoek te doen naar de autoriteit die de inbreuken zou hebben gepleegd en na te gaan of het vermeende gedrag heeft plaatsgevonden ([264]). Wanneer een zaak aan dat Tribunal wordt voorgelegd, moet het dezelfde beginselen hanteren om in die zaak tot een vaststelling te komen als de beginselen die door een rechter zouden worden toegepast bij een verzoek om rechterlijke toetsing ([265]).

(153) Het Tribunal moet de klager meedelen of er al dan niet een vaststelling in zijn/haar voordeel is gedaan ([266]). Het Tribunal heeft krachtens artikel 67, leden 6 en 7, van de RIPA 2000 de bevoegdheid om een uitspraak in kort geding te doen en om vergoeding toe te kennen of andere beschikkingen uit te vaardigen die het passend acht ([267]). Overeenkomstig artikel 67A van de RIPA 2000 kan tegen een vaststelling van het Tribunal beroep worden ingesteld, afhankelijk van toestemming van het Tribunal of de relevante beroepsinstantie.

(154) Personen kunnen meer bepaald een vordering instellen — en verhaal halen — bij het IPT wanneer zij van mening zijn dat een overheidsinstantie heeft gehandeld (of voorstelt te handelen) op een wijze die onverenigbaar is met de EVRM-rechten, met inbegrip van het recht op privacy en gegevensbescherming, en die bijgevolg onrechtmatig is op grond van artikel 6, lid 1, van de Human Rights Act 1998. Aan het IPT is exclusieve rechtsbevoegdheid verleend voor alle vorderingen in verband met de Human Rights Act waar het de inlichtingendiensten betreft. Dit betekent volgens de High Court het volgende: "de vraag of er inbreuk is gemaakt op de Human Rights Act met betrekking tot de feiten van een bepaalde zaak kan in principe worden gesteld aan en beantwoord door een onafhankelijke rechtbank die toegang kan hebben tot al het relevante materiaal, met inbegrip van geheim materiaal. […] Wij houden in dit verband ook rekening met het feit dat hiermee tegen het IPT zelf beroep kan worden ingesteld bij een geschikte beroepsinstantie (in Engeland en Wales zou dat de Court of Appeal zijn); en dat de Supreme Court onlangs heeft besloten dat het Tribunal in principe vatbaar is voor rechterlijke toetsing: zie *R (Privacy International) v Investigatory Powers Tribunal* [2019] UKSC 22; [2019] 2 WLR 1219" ([268]). Indien het IPT oordeelt dat een overheidsinstantie onrechtmatig handelt, kan het binnen de eigen bevoegdheden een compensatie of genoegdoening verschaffen, of een bevel in die zin uitvaardigen, voor zover het dat rechtvaardig en passend acht ([269]).

([261]) Dergelijke omstandigheden hebben betrekking op gedragingen van overheidsinstanties wanneer zij het gezag uitoefenen (bv. een bevel, een toestemming voor/aanzegging tot de verkrijging van communicatiegegevens enz.), of indien de omstandigheden dusdanig zijn dat (ongeacht of er sprake is van gezagsuitoefening) het niet passend zou zijn als de gedraging zonder gezagsuitoefening had plaatsgevonden, of ten minste zonder dat naar behoren is nagegaan of gezagsuitoefening noodzakelijk was. Door een Judicial Commissioner goedgekeurde gedragingen worden geacht onder betwistbare omstandigheden te hebben plaatsgevonden (artikel 65 (7ZA) van de RIPA 2000), terwijl andere gedragingen die plaatsvinden met toestemming van een persoon die een rechterlijk ambt bekleedt niet worden geacht onder betwistbare omstandigheden te hebben plaatsgevonden (artikel 65, leden 7 en 8, van de RIPA 2000).

([262]) Volgens de door de Britse autoriteiten verstrekte informatie leidt de lage drempel voor het indienen van een klacht ertoe dat het niet ongebruikelijk is dat op basis van het onderzoek van het Tribunal wordt bepaald dat de klager in feite nooit onderwerp van een onderzoek door een overheidsinstantie is geweest. In het meest recente statistisch overzicht van het IPT staat dat het Tribunal in 2016 209 klachten heeft ontvangen, dat 52 % van die klachten als onbelangrijk of ongerechtvaardigd werd beschouwd en dat voor 25 % "geen vaststelling" werd gedaan. De Britse autoriteiten hebben uitgelegd dat dit betekent dat er ofwel geen geheime activiteiten zijn uitgevoerd of geheime bevoegdheden zijn uitgeoefend met betrekking tot de klager, ofwel geheime technieken zijn gebruikt en dat het Tribunal heeft bepaald dat de activiteit legitiem was. Bovendien werd 11 % van de klachten onontvankelijk verklaard, ingetrokken of ongeldig verklaard, werd 5 % te laat ingediend en werd 7 % in het voordeel van de klager beslist. Statistisch overzicht van 2016 van het IPT, beschikbaar via de volgende link: https://www.ipt-uk.com/docs/IPT%20Statisical%20Report%202016.pdf

([263]) Zie zaak *Human Rights Watch v Secretary of State* [2016] UKIPTrib15_165-CH. In deze zaak heeft het IPT, onder verwijzing naar de rechtspraak van het Europees Hof voor de Rechten van de Mens, geoordeeld dat met betrekking tot de overtuiging dat onder subartikel 68, lid 5, van de RIPA 2000 vallende gedragingen door of namens een van de inlichtingendiensten hebben plaatsgevonden, moet worden nagegaan of er enige reden voor die overtuiging bestaat, waaronder het feit dat een persoon slechts kan aanvoeren slachtoffer te zijn geworden van een schending die is veroorzaakt door het louter bestaan van geheime maatregelen of wetgeving die geheime maatregelen toestaat, indien hij/zij kan aantonen dat hij/zij vanwege zijn/haar persoonlijke situatie mogelijk het risico loopt om aan die maatregelen te worden onderworpen (zie de zaak *Human Rights Watch v Secretary of State*, punt 41).

([264]) Artikel 67, lid 3, van de RIPA 2000.

([265]) Artikel 67, lid 2, van de RIPA 2000.

([266]) Artikel 68, lid 4, van de RIPA 2000.

([267]) Het kan hierbij gaan om een bevel tot vernietiging van informatiebestanden die door een overheidsinstantie met betrekking tot een persoon worden bijgehouden.

([268]) High Court of Justice, *Liberty*, [2019] EWHC 2057 (Admin), punt 170.

([269]) Artikel 8, lid 1, van de Human Rights Act 1998.

(155) Een persoon die alle nationale rechtsmiddelen heeft uitgeput, kan een beroep instellen bij het Europees Hof voor de Rechten van de Mens wegens schending van de door het EVRM gewaarborgde rechten, onder meer het recht op privacy en gegevensbescherming.

(156) Uit het bovenstaande volgt dat het delen door Britse strafrechtelijke handhavingsinstanties van gegevens in het kader van dit besluit met andere overheidsinstanties, onder meer inlichtingendiensten, onderworpen is aan beperkingen en voorwaarden die garanderen dat dat verder delen noodzakelijk en evenredig is en onderworpen is aan specifieke gegevensbeschermingswaarborgen uit hoofde van de DPA 2018. Bovendien wordt op de verwerking van gegevens door de betrokken overheidsinstanties toezicht uitgeoefend door onafhankelijke instanties en hebben de betrokken personen toegang tot doeltreffende voorzieningen in rechte.

3. **CONCLUSIE**

(157) De Commissie is van mening dat met deel 3 van de DPA 2018 voor persoonsgegevens die door bevoegde autoriteiten in de Unie met het oog op de handhaving van het strafrecht worden doorgegeven aan bevoegde autoriteiten in het Verenigd Koninkrijk, een beschermingsniveau verzekerd is dat in wezen overeenkomt met het beschermingsniveau dat door Richtlijn (EU) 2016/680 wordt gewaarborgd.

(158) Bovendien is de Commissie van mening dat, als geheel genomen, de toezichtsmechanismen en de verhaalsmogelijkheden waarin het Britse recht voorziet, het mogelijk maken om inbreuken in de praktijk vast te stellen en te bestraffen, en de betrokkene rechtsmiddelen bieden om toegang te krijgen tot de hem/haar betreffende persoonsgegevens en, uiteindelijk, om deze gegevens te laten rectificeren of wissen.

(159) Op grond van de beschikbare informatie over de rechtsorde van het Verenigd Koninkrijk is de Commissie tot slot van mening dat elke inmenging in de grondrechten van personen van wie persoonsgegevens vanuit de Europese Unie aan het Verenigd Koninkrijk worden doorgegeven, door Britse overheidsinstanties met het oog op het algemeen belang, ook in het kader van het delen van persoonsgegevens tussen rechtshandhavingsinstanties en andere overheidsinstanties zoals nationale veiligheidsagentschappen, beperkt zal zijn tot hetgeen strikt noodzakelijk is om het desbetreffende legitieme doel te bereiken, en dat er tegen dergelijke inmenging doeltreffende rechtsbescherming bestaat.

(160) Er moet derhalve worden besloten dat het Verenigd Koninkrijk een adequaat beschermingsniveau in de zin van artikel 36, lid 2, van Richtlijn (EU) 2016/680 waarborgt, uitgelegd in het licht van het Handvest van de grondrechten.

(161) Deze conclusie is gebaseerd op de relevante interne regeling van het Verenigd Koninkrijk en zijn internationale verplichtingen, in het bijzonder de toetreding tot het Europees Verdrag voor de rechten van de mens en de onderwerping aan de jurisdictie van het Europees Hof voor de Rechten van de Mens. De voortgezette nakoming van dergelijke internationale verplichtingen is derhalve een zeer belangrijk aspect van de beoordeling waarop dit besluit is gebaseerd.

4. **GEVOLGEN VAN DIT BESLUIT EN MAATREGELEN VAN GEGEVENSBESCHERMINGSAUTORITEITEN**

(162) De lidstaten en hun organen moeten de maatregelen nemen die noodzakelijk zijn om te voldoen aan de handelingen van de instellingen van de Unie, aangezien deze laatste geacht worden rechtsgeldig te zijn en bijgevolg rechtsgevolgen in het leven roepen zolang zij niet zijn verlopen, ingetrokken, nietig verklaard in een beroep tot nietigverklaring of ongeldig verklaard na een prejudiciële verwijzing of op een exceptie van onwettigheid.

(163) Daarom is een krachtens artikel 36, lid 3, van Richtlijn (EU) 2016/680 vastgesteld adequaatheidsbesluit van de Commissie bindend voor alle organen van de lidstaten waaraan het is gericht, met inbegrip van hun onafhankelijke toezichthoudende autoriteiten. Tijdens de periode waarin dit besluit van toepassing is, mogen doorgiften van een verwerkingsverantwoordelijke of verwerker in de Europese Unie aan verwerkingsverantwoordelijken of verwerkers in het Verenigd Koninkrijk met name plaatsvinden zonder dat daarvoor verdere toestemming vereist is.

(164) Tegelijkertijd moet erop worden gewezen dat, overeenkomstig artikel 47, lid 5, van Richtlijn (EU) 2016/680 en zoals uitgelegd door het Hof van Justitie in het arrest in de zaak Schrems, de nationale wetgever, wanneer een nationale gegevensbeschermingsautoriteit, ook bij een klacht, de verenigbaarheid van een adequaatheidsbesluit van de Commissie met het grondrecht van de persoon op privacy en gegevensbescherming in twijfel trekt, moet voorzien in een rechtsmiddel waarmee deze grieven kunnen worden voorgelegd aan een nationale rechter, die eventueel een prejudiciële verwijzing naar het Hof van Justitie moet doen ([270]).

([270]) Schrems, punt 65.

5. TOEZICHT OP, EN SCHORSING, INTREKKING OF WIJZIGING VAN DIT BESLUIT

(165) Op grond van artikel 36, lid 4, van Richtlijn (EU) 2016/680 moet de Commissie na de vaststelling van dit besluit doorlopend toezicht houden op relevante ontwikkelingen in het Verenigd Koninkrijk om te beoordelen of het besluit nog steeds een in essentie overeenkomend beschermingsniveau verzekert. Dat toezicht is in dit geval bijzonder belangrijk aangezien het Verenigd Koninkrijk een nieuw gegevensbeschermingsstelsel zal beheren, toepassen en handhaven, dat niet langer aan het Unierecht onderworpen is en dat wellicht nog zal evolueren. In dat verband zal bijzondere aandacht worden besteed aan de toepassing in de praktijk van de voorschriften van het Verenigd Koninkrijk inzake de doorgifte van persoonsgegevens aan derde landen, onder meer door het sluiten van internationale overeenkomsten, en aan de gevolgen die dit kan hebben voor het beschermingsniveau dat wordt geboden voor gegevens die uit hoofde van dit besluit worden doorgegeven; alsmede aan de doeltreffendheid van de uitoefening van individuele rechten op de onder dit besluit vallende gebieden. De Commissie zal bij haar toezicht onder meer rekening houden met de ontwikkelingen in de jurisprudentie en met het toezicht door het ICO en andere onafhankelijke instanties.

(166) Om dit toezicht te vergemakkelijken, moeten de Britse autoriteiten de Commissie onverwijld en regelmatig in kennis te stellen van elke materiële wijziging van de Britse rechtsorde die van invloed is op het rechtskader dat het onderwerp van dit besluit vormt, alsook van veranderingen in de in dit besluit beoordeelde praktijken in verband met de verwerking van persoonsgegevens, met name met betrekking tot de in overweging 165 genoemde elementen.

(167) Teneinde de Commissie in staat te stellen haar toezichthoudende taak doeltreffend uit te voeren, moeten de lidstaten de Commissie bovendien in kennis stellen van relevante maatregelen van de nationale gegevensbeschermingsautoriteiten, met name inzake vragen of klachten van betrokkenen uit de EU betreffende de doorgifte van persoonsgegevens vanuit de Europese Unie aan bevoegde autoriteiten in het Verenigd Koninkrijk. Voorts moet de Commissie worden geïnformeerd over eventuele aanwijzingen dat de maatregelen van de Britse overheidsinstanties die verantwoordelijk zijn voor de preventie, het onderzoek, de opsporing of de vervolging van strafbare feiten, met inbegrip van toezichthoudende instanties, niet het vereiste beschermingsniveau waarborgen.

(168) Wanneer uit beschikbare informatie, in het bijzonder uit informatie die voortvloeit uit het toezicht op dit besluit of informatie die is verstrekt door de autoriteiten van het Verenigd Koninkrijk of de lidstaten, blijkt dat het Verenigd Koninkrijk mogelijk niet langer een adequaat beschermingsniveau verzekert, moet de Commissie de bevoegde Britse autoriteiten daarvan onverwijld in kennis stellen en vragen om binnen een welbepaalde termijn, die niet meer dan drie maanden mag bedragen, passende maatregelen te nemen. Indien nodig kan deze termijn met een bepaalde periode worden verlengd, rekening houdend met de aard van de betrokken kwestie en/of van de te nemen maatregelen.

(169) Indien de bevoegde autoriteiten van het Verenigd Koninkrijk die maatregelen bij het verstrijken van die termijn niet hebben genomen of anderszins niet aannemelijk kunnen maken dat dit besluit op een passend beschermingsniveau gebaseerd blijft, leidt de Commissie de in artikel 58, lid 2, van Richtlijn (EU) 2016/680 bedoelde procedure in teneinde dit besluit geheel of gedeeltelijk te schorsen of in te trekken.

(170) Als alternatief zal de Commissie deze procedure inleiden met het oog op een wijziging van dit besluit, met name door voor gegevensdoorgiften aanvullende voorwaarden te stellen of door de reikwijdte van de vaststelling van adequaatheid te beperken tot gegevensdoorgiften waarvoor een adequaat beschermingsniveau gewaarborgd blijft.

(171) De Commissie zal om naar behoren gerechtvaardigde dwingende urgente redenen gebruikmaken van de mogelijkheid om, overeenkomstig de in artikel 58, lid 3, van Richtlijn (EU) 2016/680 bedoelde procedure, onmiddellijk toepasselijke uitvoeringshandelingen tot schorsing, intrekking of wijziging van het besluit vast te stellen.

6. GELDIGHEIDSDUUR EN VERLENGING VAN DIT BESLUIT

(172) Er moet rekening worden gehouden met het feit dat het Verenigd Koninkrijk, zodra de in het Terugtrekkingsakkoord vastgelegde overgangsperiode is verstreken en de tijdelijke bepaling op grond van artikel 782 van de Handels- en samenwerkingsovereenkomst tussen de EU en het Verenigd Koninkrijk niet langer van toepassing is, een nieuwe gegevensbeschermingsregeling zal beheren, toepassen en handhaven ten opzichte van de regeling die gold toen het Verenigd Koninkrijk nog gebonden was door het Unierecht. Dit kan met name amendementen of wijzigingen van het in dit besluit beoordeelde gegevensbeschermingskader en andere relevante ontwikkelingen met zich meebrengen.

(173) Daarom is het passend te bepalen dat dit besluit van toepassing zal zijn gedurende een periode van vier jaar vanaf de inwerkingtreding ervan.

(174) Indien uit bepaalde uit het toezicht op dit besluit voortvloeiende informatie blijkt dat de bevindingen in verband met de adequaatheid van het in het Verenigd Koninkrijk geboden beschermingsniveau nog steeds feitelijk en juridisch gerechtvaardigd zijn, moet de Commissie uiterlijk zes maanden voordat dit besluit niet meer van toepassing zal zijn, de procedure inleiden tot wijziging van dit besluit door verlenging van de toepassingsduur ervan, in beginsel met een bijkomende periode van vier jaar. Elke uitvoeringshandeling tot wijziging van dit besluit moet worden vastgesteld overeenkomstig de in artikel 58, lid 2, van Richtlijn (EU) 2016/680 bedoelde procedure.

7. **SLOTOVERWEGINGEN**

(175) Het Europees Comité voor gegevensbescherming heeft zijn advies ([271]) gepubliceerd, waarmee bij het opstellen van dit besluit rekening is gehouden.

(176) De in dit besluit vervatte maatregelen zijn in overeenstemming met het advies van het bij artikel 58 van Richtlijn (EU) 2016/680 ingestelde comité.

(177) Overeenkomstig artikel 6 bis van Protocol nr. 21 betreffende de positie van het Verenigd Koninkrijk en Ierland ten aanzien van de ruimte van vrijheid, veiligheid en recht, dat gehecht is aan het Verdrag betreffende de Europese Unie (VEU) en het Verdrag betreffende de werking van de Europese Unie (VWEU), is Ierland niet gebonden door de in Richtlijn (EU) 2016/680 vastgestelde regels, en bijgevolg dit uitvoeringsbesluit, in verband met de verwerking van persoonsgegevens door de lidstaten bij de uitvoering van activiteiten onder het toepassingsgebied van de hoofdstukken 4 en 5 van titel V van het derde deel VWEU, wanneer Ierland niet gebonden is door de regels betreffende de vormen van justitiële samenwerking in strafzaken of van politiële samenwerking in het kader waarvan de op grond van artikel 16 VWEU vastgestelde bepalingen moeten worden nageleefd. Uit hoofde van Uitvoeringsbesluit (EU) 2020/1745 van de Raad ([272]) moet Richtlijn (EU) 2016/680 bovendien vanaf 1 januari 2021 voorlopig in werking worden gesteld en toegepast in Ierland. Ierland is derhalve gebonden door dit uitvoeringsbesluit, onder dezelfde voorwaarden die gelden voor de toepassing van Richtlijn (EU) 2016/680 in Ierland zoals uiteengezet in Uitvoeringsbesluit (EU) 2020/1745, met betrekking tot de bepalingen van het Schengenacquis waaraan het deelneemt.

(178) Overeenkomstig de artikelen 2 en 2 bis van Protocol nr. 22 betreffende de positie van Denemarken, dat gehecht is aan het VEU en het VWEU, is Denemarken niet gebonden door de in Richtlijn (EU) 2016/680 vastgestelde regels, en derhalve dit uitvoeringsbesluit, noch aan de toepassing ervan in verband met de verwerking van persoonsgegevens door de lidstaten bij de uitvoering van activiteiten onder het toepassingsgebied van de hoofdstukken 4 en 5 van titel V van het derde deel VWEU. Aangezien Richtlijn (EU) 2016/680 echter voortbouwt op het Schengenacquis, heeft Denemarken, overeenkomstig artikel 4 van bedoeld protocol, op 26 oktober 2016 kennis gegeven van zijn besluit om Richtlijn (EU) 2016/680 uit te voeren. Denemarken is daarom krachtens internationaal recht verplicht dit uitvoeringsbesluit uit te voeren.

(179) Wat IJsland en Noorwegen betreft, houdt dit uitvoeringsbesluit een ontwikkeling in van de bepalingen van het Schengenacquis als bedoeld in de Overeenkomst tussen de Raad van de Europese Unie, de Republiek IJsland en het Koninkrijk Noorwegen inzake de wijze waarop deze twee staten worden betrokken bij de uitvoering, de toepassing en de ontwikkeling van het Schengenacquis ([273]).

(180) Wat Zwitserland betreft, houdt dit uitvoeringsbesluit een ontwikkeling in van de bepalingen van het Schengenacquis als bedoeld in de Overeenkomst tussen de Europese Unie, de Europese Gemeenschap en de Zwitserse Bondsstaat inzake de wijze waarop Zwitserland wordt betrokken bij de uitvoering, de toepassing en de ontwikkeling van het Schengenacquis ([274]).

(181) Wat Liechtenstein betreft, houdt dit uitvoeringsbesluit een ontwikkeling in van de bepalingen van het Schengenacquis als bedoeld in het Protocol tussen de Europese Unie, de Europese Gemeenschap, de Zwitserse Bondsstaat en het Vorstendom Liechtenstein betreffende de toetreding van het Vorstendom Liechtenstein tot de Overeenkomst tussen de Europese Unie, de Europese Gemeenschap en de Zwitserse Bondsstaat inzake de wijze waarop Zwitserland wordt betrokken bij de uitvoering, de toepassing en de ontwikkeling van het Schengenacquis ([275]),

---

([271]) Advies 15/2021 inzake het ontwerp van uitvoeringsbesluit van de Europese Commissie overeenkomstig Richtlijn (EU) 2016/680 betreffende de adequate bescherming van persoonsgegevens in het Verenigd Koninkrijk, beschikbaar via de volgende link: https://edpb.europa.eu/our-work-tools/our-documents/opinion-led/opinion-152021-regarding-european-commission-draft_en.

([272]) Uitvoeringsbesluit (EU) 2020/1745 van de Raad van 18 november 2020 betreffende de inwerkingstelling van de bepalingen van het Schengenacquis inzake gegevensbescherming en de voorlopige inwerkingstelling van sommige bepalingen van het Schengenacquis in Ierland (PB L 393 van 23.11.2020, blz. 3).

([273]) PB L 176 van 10.7.1999, blz. 36.

([274]) PB L 53 van 27.2.2008, blz. 52.

([275]) PB L 160 van 18.6.2011, blz. 21.

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

Artikel 1

Voor de toepassing van artikel 36 van Richtlijn (EU) 2016/680 waarborgt het Verenigd Koninkrijk een adequaat beschermingsniveau voor persoonsgegevens die vanuit de Europese Unie worden doorgegeven aan overheidsinstanties in het Verenigd Koninkrijk die verantwoordelijk zijn voor de preventie, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen.

Artikel 2

Wanneer de bevoegde toezichthoudende autoriteiten in de lidstaten, met het oog op de bescherming van personen in verband met de verwerking van hun persoonsgegevens, hun bevoegdheden uit hoofde van artikel 47 van Richtlijn (EU) 2016/680 uitoefenen met betrekking tot gegevensdoorgiften naar overheidsinstanties in het Verenigd Koninkrijk binnen de werkingssfeer van artikel 1, stelt de betrokken lidstaat de Commissie daarvan onverwijld in kennis.

Artikel 3

1. De Commissie houdt voortdurend toezicht op de toepassing van het rechtskader waarop dit besluit is gebaseerd, met inbegrip van de voorwaarden waaronder verdere doorgiften plaatsvinden en individuele rechten worden uitgeoefend, teneinde te beoordelen of het Verenigd Koninkrijk een passend beschermingsniveau in de zin van artikel 1 blijft waarborgen.

2. De lidstaten en de Commissie stellen elkaar in kennis van gevallen waarin de Information Commissioner of enige andere bevoegde autoriteit van het Verenigd Koninkrijk niet garandeert dat het rechtskader waarop dit besluit is gebaseerd wordt geëerbiedigd.

3. De lidstaten en de Commissie stellen elkaar in kennis van eventuele aanwijzingen dat inmenging van de overheidsinstanties van het Verenigd Koninkrijk in het recht van personen op de bescherming van hun persoonsgegevens verder gaat dan hetgeen strikt noodzakelijk is, of dat er geen doeltreffende rechtsbescherming tegen dergelijke inmenging bestaat.

4. Wanneer de Commissie over aanwijzingen beschikt dat het adequate beschermingsniveau niet langer wordt gewaarborgd, stelt de Commissie de bevoegde autoriteiten van het Verenigd Koninkrijk daarvan in kennis en kan zij dit besluit schorsen, intrekken of wijzigen.

5. De Commissie kan dit besluit schorsen, intrekken of wijzigen indien zij door een gebrek aan medewerking van de regering van het Verenigd Koninkrijk niet kan bepalen of de bevinding in artikel 1 in het gedrang komt.

Artikel 4

Dit besluit verstrijkt op 27 juni 2025, tenzij het wordt verlengd volgens de in artikel 58, lid 2, van Richtlijn (EU) 2016/680 bedoelde procedure.

Artikel 5

Dit besluit is gericht tot de lidstaten.

Gedaan te Brussel, 28 juni 2021.

Voor de Commissie
Didier REYNDERS
Lid van de Commissie

UITVOERINGSBESLUIT (EU) 2021/1774 VAN DE RAAD

van 5 oktober 2021

tot wijziging van Uitvoeringsbesluit (EU) 2018/1493 waarbij Hongarije wordt gemachtigd een bijzondere maatregel toe te passen die afwijkt van artikel 26, lid 1, punt a), en de artikelen 168 en 168 bis van Richtlijn 2006/112/EG betreffende het gemeenschappelijke stelsel van belasting over de toegevoegde waarde

DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Richtlijn 2006/112/EG van de Raad van 28 november 2006 betreffende het gemeenschappelijke stelsel van belasting over de toegevoegde waarde ([1]), en met name artikel 395, lid 1, eerste alinea,

Gezien het voorstel van de Europese Commissie,

Overwegende hetgeen volgt:

(1) Bij Uitvoeringsbesluit (EU) 2018/1493 van de Raad ([2]) werd Hongarije gemachtigd om, tot en met 31 december 2021, een bijzondere maatregel toe te passen, enerzijds bestaande uit de beperking tot 50 % van het recht op aftrek van de belasting over de toegevoegde waarde (btw) ter zake van de uitgaven voor personenauto's die niet uitsluitend voor bedrijfsdoeleinden worden gebruikt, in afwijking van de artikelen 168 en 168 bis van Richtlijn 2006/112/EG, en anderzijds voor het niet-aanmerken van niet-zakelijk gebruik van een tot het bedrijf van een belastingplichtige behorende personenauto als een dienst onder bezwarende titel, wanneer het recht op aftrek voor dit voertuig krachtens artikel 1 van dat uitvoeringsbesluit, in afwijking van artikel 26, lid 1, punt a), van die richtlijn ("de bijzondere maatregel") is beperkt.

(2) Bij brief, ingekomen bij de Commissie op 25 februari 2021, heeft Hongarije verzocht om de bijzondere maatregel te mogen blijven toepassen ("het verzoek om verlenging").

(3) Op grond van artikel 395, lid 2, tweede alinea, van Richtlijn 2006/112/EG heeft de Commissie de overige lidstaten bij brief van 7 april 2021 van het verzoek om verlenging in kennis gesteld. Bij brief van 8 april 2021 heeft de Commissie Hongarije ervan in kennis gesteld dat zij over alle gegevens beschikte die zij nodig achtte voor de beoordeling van het verzoek om verlenging.

(4) Op grond van artikel 5 van Uitvoeringsbesluit (EU) 2018/1493 heeft Hongarije de Commissie, samen met het verzoek om verlenging, een verslag met daarin ook een evaluatie van het percentage van de aftrekbeperking voorgelegd. Op basis van actuele gegevens, te weten ervaringen met belastingcontroles en statistische gegevens over het privégebruik van personenauto's, bevestigt Hongarije in het verzoek om verlenging dat de beperking van 50 % nog altijd gerechtvaardigd en passend is. Bovendien heeft de bijzondere maatregel, doordat daarmee de inning van de btw wordt vereenvoudigd, de administratieve lasten voor bedrijven en belastingautoriteiten bovendien effectief verlaagd. Tegelijkertijd wordt belastingfraude door onjuiste administratie voorkomen. Hongarije moet derhalve worden gemachtigd de bijzondere maatregel te blijven toepassen.

([1]) PB L 347 van 11.12.2006, blz. 1.

([2]) Uitvoeringsbesluit (EU) 2018/1493 van de Raad van 2 oktober 2018 waarbij Hongarije wordt gemachtigd een bijzondere maatregel toe te passen die afwijkt van artikel 26, lid 1, onder a), en de artikelen 168 en 168 bis van Richtlijn 2006/112/EG betreffende het gemeenschappelijke stelsel van belasting over de toegevoegde waarde (PB L 252 van 8.10.2018, blz. 44).

(5) De verlenging van de bijzondere maatregel moet in de tijd worden beperkt, zodat de effectiviteit ervan en de toepasselijkheid van het tarief kunnen worden geëvalueerd. Hongarije moet derhalve worden gemachtigd de bijzondere maatregel gedurende een beperkte periode te blijven toepassen, meer bepaald tot en met 31 december 2024.

(6) Indien Hongarije een verlenging van de machtiging na 2024 nodig acht, moet het de Commissie uiterlijk 31 maart 2024, samen met het verzoek om verlenging, een verslag voorleggen met daarin ook een evaluatie van het toegepaste percentage.

(7) De bijzondere maatregel zal geen noemenswaardige invloed hebben op de totale belastingopbrengst in het stadium van het eindverbruik en geen negatieve gevolgen hebben voor de eigen middelen van de Unie uit de btw.

(8) Uitvoeringsbesluit (EU) 2018/1493 moet daarom dienovereenkomstig worden gewijzigd,

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

Artikel 1

Artikel 5 van Uitvoeringsbesluit (EU) 2018/1493 wordt vervangen door:

"*Artikel 5*

Dit besluit is van toepassing met ingang van 1 januari 2019 tot en met 31 december 2024.

Een verzoek om verlenging van de bij dit besluit verleende machtiging wordt uiterlijk op 31 maart 2024 aan de Commissie voorgelegd, samen met een verslag met daarin ook een evaluatie van het in artikel 1 vastgestelde percentage.".

Artikel 2

Dit besluit wordt van kracht op de datum van kennisgeving.

Artikel 3

Dit besluit is gericht tot Hongarije.

Gedaan te Luxemburg, 5 oktober 2021.

Voor de Raad
De voorzitter
A. ŠIRCELJ

UITVOERINGSBESLUIT (EU) 2021/1775 VAN DE RAAD

van 5 oktober 2021

tot wijziging van Uitvoeringsbesluit (EU) 2018/789 waarbij Hongarije wordt gemachtigd een bijzondere maatregel in te voeren die afwijkt van artikel 193 van Richtlijn 2006/112/EG betreffende het gemeenschappelijke stelsel van belasting over de toegevoegde waarde

DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Richtlijn 2006/112/EG van de Raad van 28 november 2006 betreffende het gemeenschappelijke stelsel van belasting over de toegevoegde waarde ([1]), en met name artikel 395, lid 1, eerste alinea,

Gezien het voorstel van de Europese Commissie,

Overwegende hetgeen volgt:

(1) In artikel 193 van Richtlijn 2006/112/EG is bepaald dat de belastingplichtige die op belastbare wijze goederen levert of diensten verricht, in de regel ook de persoon is die tot voldoening van de btw is gehouden.

(2) Bij Uitvoeringsbesluit (EU) 2018/789 van de Raad ([2]), is Hongarije gemachtigd tot invoering van een maatregel die afwijkt van artikel 193 van Richtlijn 2006/112/EG, wat betreft de tot voldoening van de btw gehouden persoon wanneer bepaalde prestaties worden verricht door een belastingplichtige die in liquidatie is of in een andere procedure waarbij officieel zijn staat van insolventie is vastgesteld ("de bijzondere maatregel").

(3) Bij brief, ingekomen bij de Commissie op 18 februari 2021, heeft Hongarije bij de Commissie een verzoek ingediend om de machtiging tot toepassing van de bijzondere maatregel te verlengen tot en met 31 december 2026 ("het verzoek"). Hongarije heeft tegelijk met het verzoek een verslag ingediend, waarin het onder meer een evaluatie van de speciale maatregel heeft opgenomen.

(4) Op grond van artikel 395, lid 2, tweede alinea, van Richtlijn 2006/112/EG heeft de Commissie het verzoek bij brief van 7 april 2021 aan de andere lidstaten toegezonden. Bij brief van 8 april 2021 heeft de Commissie Hongarije meegedeeld dat zij over alle benodigde gegevens beschikte voor de beoordeling van het verzoek.

(5) Hongarije voert aan dat belastingplichtigen die zich in staat van liquidatie bevinden of aan een insolventieprocedure onderworpen zijn, vaak de verschuldigde btw niet afdragen. Tegelijkertijd is de koper een belastingplichtige met recht op aftrek die nog altijd de btw in mindering kan brengen; dit heeft negatieve gevolgen voor de begroting en de liquidatie wordt zo gefinancierd. Hongarije heeft ook fraude geconstateerd waarbij bedrijven in staat van liquidatie fictieve facturen uitreiken aan actieve bedrijven, waardoor de belasting die deze bedrijven moeten betalen, fors daalt zonder dat er een garantie is dat de uitreiker van de factuur de verschuldigde btw betaalt.

(6) Overeenkomstig artikel 199, lid 1, punt g), van Richtlijn 2006/112/EG kunnen de lidstaten bepalen dat de btw moet worden voldaan door de belastingplichtige aan wie onroerend goed wordt geleverd dat in een openbare verkoop op grond van een executoriale titel door de executieschuldenaar is verkocht ("de verleggingsgregeling"). De speciale maatregel stelt Hongarije in staat de verleggingsregeling ook toe te passen op andere leveringen door belastingplichtigen die aan insolventieprocedures onderworpen zijn, namelijk de levering van kapitaalgoederen en de levering van andere goederen en diensten met een normale waarde van meer dan 100 000 HUF.

([1]) PB L 347 van 11.12.2006, blz. 1.

([2]) Uitvoeringsbesluit (EU) 2018/789 van de Raad van 25 mei 2018 waarbij Hongarije wordt gemachtigd een bijzondere maatregel toe te passen die afwijkt van artikel 193 van Richtlijn 2006/112/EG betreffende het gemeenschappelijke stelsel van belasting over de toegevoegde waarde (PB L 134 van 31.5.2018, blz. 10).

(7) Op basis van door Hongarije verstrekte informatie heeft de toepassing van de verleggingsregeling op dat soort transacties de belastinginning daadwerkelijk vereenvoudigd en belastingontduiking voorkomen. De uitvoering van de bijzondere maatregel heeft de inkomstenderving voor de overheid beperkt en heeft extra begrotingsinkomsten gegenereerd. Bovendien kunnen de economische gevolgen van de COVID-19-pandemie in de nabije toekomst tot een sterke toename van het aantal liquidaties leiden, wat de noodzaak om de bijzondere maatregel te verlengen onderstreept.

(8) De verzochte afwijking moet in de tijd worden beperkt, maar de belastingdienst ook de tijd geven om in de periode totdat de bijzondere maatregel is verstreken andere, klassieke maatregelen te nemen om het probleem aan te pakken en de verliezen voor de overheidsbegroting te verminderen, met name verliezen die verband houden met frauduleuze praktijken, zodat een verdere verlenging van de bijzondere maatregel overbodig wordt. Een derogatie op grond waarvan de verleggingsregeling kan worden gebruikt, wordt slechts bij uitzondering verleend voor specifieke frauduleuze gebieden en moet als een laatste redmiddel worden gezien. De machtiging mag daarom slechts tot en met 31 december 2024 worden verlengd.

(9) De bijzondere maatregel zal geen negatieve gevolgen hebben voor de eigen middelen van de Unie uit de btw.

(10) Uitvoeringsbesluit (EU) 2018/789 moet daarom dienovereenkomstig worden gewijzigd,

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

Artikel 1

In artikel 2 van Uitvoeringsbesluit (EU) 2018/789 wordt de tweede alinea vervangen door:

"Dit besluit verstrijkt op 31 december 2024.".

Artikel 2

Dit besluit wordt van kracht op de datum van kennisgeving.

Artikel 3

Dit besluit is gericht tot Hongarije.

Gedaan te Luxemburg, 5 oktober 2021.

Voor de Raad
De voorzitter
A. ŠIRCELJ

UITVOERINGSBESLUIT (EU) 2021/1776 VAN DE RAAD

van 5 oktober 2021

tot wijziging van Beschikking 2009/791/EG waarbij de Bondsrepubliek Duitsland wordt gemachtigd een maatregel te blijven toepassen die afwijkt van artikel 168 van Richtlijn 2006/112/EG betreffende het gemeenschappelijke stelsel van belasting over de toegevoegde waarde

DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Richtlijn 2006/112/EG van de Raad van 28 november 2006 betreffende het gemeenschappelijke stelsel van belasting over de toegevoegde waarde ([1]), en met name artikel 395, lid 1, eerste alinea,

Gezien het voorstel van de Europese Commissie,

Overwegende hetgeen volgt:

(1) De artikelen 168 en 168 bis van Richtlijn 2006/112/EG betreffen het recht op aftrek van een belastingplichtige ter zake van de belasting over de toegevoegde waarde (btw) op goederen en diensten die hij ten behoeve van zijn belaste activiteiten heeft ontvangen. Aan de Bondsrepubliek Duitsland ("Duitsland") is een afwijkende maatregel verleend die ertoe strekte de btw op goederen en diensten van het recht op aftrek uit te sluiten wanneer die goederen en diensten voor meer dan 90 % voor de privédoeleinden van de belastingplichtige of diens werknemers, dan wel in het algemeen, voor andere dan bedrijfsdoeleinden of niet-economische activiteiten worden gebruikt.

(2) Initieel werd Duitsland op grond van Beschikking 2000/186/EG van de Raad ([2]) gemachtigd om maatregelen in te voeren die afwijken van de artikelen 6 en 17 van Richtlijn 77/388/EEG van de Raad ([3]), en deze toe te passen tot en met 31 december 2002. Nadien werd Duitsland op grond van Beschikking 2003/354/EG van de Raad ([4]) gemachtigd om tot en met 30 juni 2004 een maatregel toe te passen die afwijkt van artikel 17 van Richtlijn 77/388/EEG. Die machtiging werd bij Beschikking 2004/817/EG van de Raad ([5]) verlengd tot en met 31 december 2009.

(3) Bij Beschikking 2009/791/EG van de Raad ([6]) werd Duitsland gemachtigd om een maatregel te blijven toepassen die afwijkt van artikel 168 van Richtlijn 2006/112/EG. Na opeenvolgende verlengingen zal die machtiging aflopen op 31 december 2021.

(4) Bij Richtlijn 2009/162/EU van de Raad ([7]) is in Richtlijn 2006/112/EG artikel 168 bis ingevoegd, teneinde de aftrek te beperken naar evenredigheid van het werkelijke zakelijke gebruik en aldus beter het beginsel toe te passen dat het recht op aftrek pas ontstaat voor zover de goederen en diensten in kwestie voor de bedrijfsactiviteiten van de belastingplichtige worden gebruikt. Artikel 1 van Beschikking 2009/791/EG is gewijzigd om er een verwijzing naar artikel 168 bis van Richtlijn 2006/112/EG in op te nemen. Daarom moet in de titel van Beschikking 2009/791/EG ook naar artikel 168 bis van Richtlijn 2006/112/EG worden verwezen.

([1]) PB L 347 van 11.12.2006, blz. 1.

([2]) Beschikking 2000/186/EG van de Raad van 28 februari 2000 waarbij de Bondsrepubliek Duitsland wordt gemachtigd af te wijken van de artikelen 6 en 17 van de Zesde Richtlijn 77/388/EEG betreffende de harmonisatie van de wetgevingen der lidstaten inzake omzetbelasting — Gemeenschappelijk stelsel van belasting over de toegevoegde waarde: uniforme grondslag (PB L 59 van 4.3.2000, blz. 12).

([3]) Zesde Richtlijn 77/388/EEG van de Raad van 17 mei 1977 betreffende de harmonisatie van de wetgevingen der lidstaten inzake omzetbelasting — Gemeenschappelijk stelsel van belasting over de toegevoegde waarde: uniforme grondslag (PB L 145 van 13.6.1977, blz. 1).

([4]) Beschikking 2003/354/EG van de Raad van 13 mei 2003 waarbij Duitsland wordt gemachtigd een maatregel toe te passen in afwijking van artikel 17 van Zesde Richtlijn 77/388/EEG betreffende de harmonisatie van de wetgevingen der lidstaten inzake omzetbelasting (PB L 123 van 17.5.2003, blz. 47).

([5]) Beschikking 2004/817/EG van de Raad van 19 november 2004 waarbij Duitsland wordt gemachtigd een maatregel toe te passen in afwijking van artikel 17 van de Zesde Richtlijn 77/388/EEG betreffende de harmonisatie van de wetgevingen der lidstaten inzake omzetbelasting (PB L 357 van 2.12.2004, blz. 33).

([6]) Beschikking 2009/791/EG van de Raad van 20 oktober 2009 waarbij de Bondsrepubliek Duitsland wordt gemachtigd een maatregel te blijven toepassen die afwijkt van artikel 168 van Richtlijn 2006/112/EG betreffende het gemeenschappelijke stelsel van belasting over de toegevoegde waarde (PB L 283 van 30.10.2009, blz. 55).

([7]) Richtlijn 2009/162/EU van de Raad van 22 december 2009 tot wijziging van enkele bepalingen van Richtlijn 2006/112/EG betreffende het gemeenschappelijke stelsel van belasting over de toegevoegde waarde (PB L 10 van 15.1.2010, blz. 14).

(5) Bij brief, ingekomen bij de Commissie op 19 februari 2021, heeft Duitsland de Commissie verzocht om verlenging van de machtiging ("het verzoek") om een maatregel te mogen blijven toepassen die afwijkt van de artikelen 168 en 168 bis van Richtlijn 2006/112/EG, teneinde de btw op goederen en diensten die door een belastingplichtige voor meer dan 90 % worden gebruikt voor privédoeleinden of voor andere dan bedrijfsdoeleinden, daaronder begrepen niet-economische activiteiten, volledig van het recht op aftrek uit te sluiten ("de bijzondere maatregel"). Bij het verzoek ging een verslag over de toepassing van de bijzondere maatregel, dat ook een evaluatie omvatte van de procentuele opsplitsing ter zake van het recht op aftrek van de btw, zoals vereist krachtens artikel 2 van Beschikking 2009/791/EG.

(6) Op grond van artikel 395, lid 2, tweede alinea, van Richtlijn 2006/112/EG heeft de Commissie het verzoek aan de overige lidstaten doen toekomen bij brief van 17 maart 2021. Bij brief van 18 maart 2021 heeft de Commissie Duitsland meegedeeld dat zij over alle gegevens beschikte die zij nodig achtte voor de beoordeling van het verzoek.

(7) Volgens Duitsland is de bijzondere maatregel zeer doeltreffend gebleken om de inning van de btw te vereenvoudigen en belastingontduiking en -ontwijking te voorkomen. De bijzondere maatregel verlicht de administratieve lasten voor zowel de bedrijven als de belastingdiensten omdat er nadien geen controle meer moet worden uitgeoefend op het gebruik van de goederen of diensten die bij de aanschaf ervan van het recht op aftrek werden uitgesloten. Duitsland moet derhalve worden gemachtigd de bijzondere maatregel gedurende een nieuwe beperkte periode te blijven toepassen, meer bepaald tot en met 31 december 2024.

(8) Indien Duitsland een verlenging na 2024 nodig acht, moet het de Commissie uiterlijk op 31 maart 2024, samen met het daartoe strekkende verzoek, een verslag over de toepassing van de bijzondere maatregel voorleggen met daarin ook een evaluatie van de procentuele opsplitsing.

(9) De bijzondere maatregel zal geen negatieve gevolgen hebben voor de eigen middelen van de Unie uit de btw.

(10) Beschikking 2009/791/EG moet daarom dienovereenkomstig worden gewijzigd,

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

Artikel 1

Beschikking 2009/791/EG wordt als volgt gewijzigd:

1) De titel wordt vervangen door:

"Beschikking 2009/791/EG van de Raad van 20 oktober 2009 waarbij de Bondsrepubliek Duitsland wordt gemachtigd een maatregel te blijven toepassen die afwijkt van de artikelen 168 en 168 bis van Richtlijn 2006/112/EG betreffende het gemeenschappelijke stelsel van belasting over de toegevoegde waarde".

2) Artikel 2 wordt vervangen door:

"Artikel 2

Deze beschikking vervalt op 31 december 2024.

Een verzoek om verlenging van de in deze beschikking vervatte afwijkende maatregel wordt uiterlijk op 31 maart 2024 bij de Commissie ingediend.

Bij een dergelijk verzoek wordt een verslag over de toepassing van deze maatregel gevoegd, dat ook een evaluatie omvat van de op basis van deze beschikking gehanteerde procentuele opsplitsing ter zake van het recht op aftrek van de btw.".

Artikel 2

Dit besluit wordt van kracht op de datum van kennisgeving.

Artikel 3

Dit besluit is gericht tot de Bondsrepubliek Duitsland.

Gedaan te Luxemburg, 5 oktober 2021.

Voor de Raad
De voorzitter
A. ŠIRCELJ

UITVOERINGSBESLUIT (EU) 2021/1777 VAN DE RAAD

van 5 oktober 2021

tot machtiging van Italië om een verlaagd belastingtarief toe te passen op gasolie voor verwarmingsdoeleinden en op elektriciteit die op het grondgebied van de gemeente Campione d'Italia worden geleverd

DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Richtlijn 2003/96/EG van de Raad van 27 oktober 2003 tot herstructurering van de communautaire regeling voor de belasting van energieproducten en elektriciteit ([1]), en met name artikel 19,

Gezien het voorstel van de Europese Commissie,

Overwegende hetgeen volgt:

(1) Bij brief van 7 augustus 2020 heeft Italië verzocht om machtiging, voor de periode 1 januari 2021 tot en met 31 december 2026, tot toepassing van een verlaagd belastingtarief op gasolie voor verwarmingsdoeleinden en op elektriciteit die op het grondgebied van de gemeente Campione d'Italia worden geleverd, krachtens artikel 19 van Richtlijn 2003/96/EG. De Italiaanse autoriteiten hebben aanvullende informatie en nadere toelichtingen bij hun verzoek verstrekt op 19 januari 2021.

(2) De gemeente Campione d'Italia is een exclave van Italië in Zwitserland met een zeer kleine oppervlakte en een gering aantal inwoners. Het gebied is bergachtig, wat de verstedelijking, de vestiging van industrie en meer algemeen de toegankelijkheid beperkt. Gezien de geografische ligging van de gemeente, het ontbreken van toegang tot het aardgasnet en de strenge klimatologische omstandigheden, zijn de kosten voor de levering van energieproducten aan Campione d'Italia hoog, ongeacht of de energie uit Zwitserland of uit Italië afkomstig is. Bovendien zorgde de toetreding van Campione d'Italia tot het douanegebied van de Unie op 1 januari 2020 voor een stijging van de kosten van energieproducten voor huishoudens en bedrijven. Daarnaast heeft Campione d'Italia te kampen met een ernstige economische crisis, die verergerd is door de COVID-19-pandemie.

(3) Om de hoge energiekosten in Campione d'Italia te beperken, dient de belasting op bepaalde energieproducten te worden verlaagd.

(4) De gevraagde maatregel is door de Commissie aan een evaluatie onderworpen waaruit is gebleken dat hij de mededinging niet verstoort noch de goede werking van de interne markt belemmert, en wordt niet onverenigbaar geacht met het Uniebeleid op het gebied van milieu, energie en vervoer. De verlaagde belasting voor zowel gasolie als elektriciteit blijft gelijk aan of hoger dan de in Richtlijn 2003/96/EG vastgestelde minimumbelastingniveaus en compenseert ten dele de gestegen energiekosten in de gemeente Campione d'Italia. De belastingverlaging wordt niet gecombineerd met andere vormen van belastingverlaging.

(5) Italië moet derhalve worden gemachtigd verlaagde belastingtarieven toe te passen op gasolie voor verwarmingsdoeleinden en op elektriciteit die op het grondgebied van de gemeente Campione d'Italia worden geleverd.

(6) Teneinde ervoor te zorgen dat de door deze afwijkingsmaatregel nagestreefde doelstellingen worden bereikt, met name het voorkomen van verstorende gevolgen van de huidige economische, sociale en geografische omstandigheden van Campione d'Italia en het waarborgen van een gelijk speelveld door het beperken van de hoge energiekosten, is het passend dat dit besluit van toepassing is met ingang van 1 januari 2021. Door in de toepassing met ingang van een datum vóór de inwerkingtreding van de afwijkingsmaatregel te voorzien, wordt het gewettigd vertrouwen van marktdeelnemers en particulieren geëerbiedigd, aangezien de afwijkingsmaatregel geen inbreuk maakt op hun rechten en verplichtingen.

([1]) PB L 283 van 31.10.2003, blz. 51.

(7) Overeenkomstig artikel 19, lid 2, van Richtlijn 2003/96/EG verleende machtigingen dienen strikt beperkt in de tijd te zijn. Om ervoor te zorgen dat de gemeente Campione d'Italia voldoende zekerheid krijgt, moet de machtiging worden verleend voor een periode van zes jaar. Om evenwel toekomstige algemene ontwikkelingen van het bestaande juridische kader niet te ondergraven, is het passend te bepalen dat deze machtiging, mocht de Raad op basis van artikel 113 van het Verdrag betreffende de werking van de Europese Unie een gewijzigde algemene regeling voor de belasting van energieproducten invoeren waaraan deze machtiging niet zou zijn aangepast, zou vervallen op de dag waarop die algemene regeling van toepassing wordt.

(8) Dit besluit laat de toepassing van de Unieregels betreffende staatssteun onverlet,

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

Artikel 1

Italië wordt gemachtigd een verlaagd belastingtarief toe te passen op gasolie voor verwarmingsdoeleinden en op elektriciteit die op het grondgebied van de gemeente Campione d'Italia worden geleverd, mits de in de artikelen 9 en 10 van Richtlijn 2003/96/EG bedoelde minimumbelastingniveaus in acht worden genomen.

Artikel 2

Dit besluit is van toepassing van 1 januari 2021 tot en met 31 december 2026.

Mocht de Raad evenwel op grond van artikel 113 of enige andere relevante bepaling van het Verdrag betreffende de werking van de Europese Unie een gewijzigde algemene regeling voor de belasting van energieproducten invoeren waaraan de in artikel 1 van dit besluit verleende machtiging niet zou zijn aangepast, dan vervalt dit besluit op de dag waarop die algemene regeling van toepassing wordt.

Artikel 3

Dit besluit is gericht tot de Italiaanse Republiek.

Gedaan te Luxemburg, 5 oktober 2021.

Voor de Raad
De voorzitter
A. ŠIRCELJ

UITVOERINGSBESLUIT (EU) 2021/1778 VAN DE RAAD

van 5 oktober 2021

waarbij de Bondsrepubliek Duitsland wordt gemachtigd een bijzondere maatregel toe te passen die afwijkt van artikel 193 van Richtlijn 2006/112/EG betreffende het gemeenschappelijke stelsel van belasting over de toegevoegde waarde

DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Richtlijn 2006/112/EG van de Raad van 28 november 2006 betreffende het gemeenschappelijke stelsel van belasting over de toegevoegde waarde ([1]), en met name artikel 395, lid 1, eerste alinea,

Gezien het voorstel van de Europese Commissie,

Overwegende hetgeen volgt:

(1) In artikel 193 van Richtlijn 2006/112/EG is bepaald dat de belastingplichtige die goederen levert of diensten verricht, in de regel ook de persoon is die tot voldoening van de btw is gehouden.

(2) Bij brief, ingekomen bij de Commissie op 15 maart 2021, heeft de Bondsrepubliek Duitsland ("Duitsland") bij de Commissie een verzoek ingediend om machtiging tot toepassing van een bijzondere maatregel die afwijkt van artikel 193 van Richtlijn 2006/112/EG wat betreft de tot voldoening van de btw gehouden persoon in het geval van overdracht van emissierechten die in een nationaal handelssysteem worden verhandeld in het kader van de wet op de brandstofemissierechtenhandel (*Gesetz über einen nationalen Zertifikatehandel für Brennstoffemissionen* — de "BEHG") van 12 december 2019 ("het verzoek").

(3) Op grond van artikel 395, lid 2, tweede alinea, van Richtlijn 2006/112/EG heeft de Commissie het verzoek bij brief van 7 april 2021 aan de andere lidstaten toegezonden en bij brief van 8 april 2021 heeft zij Duitsland meegedeeld dat ze over alle gegevens beschikte die zij nodig achtte voor de beoordeling van het verzoek.

(4) Artikel 199 bis, lid 1, punten a) en b), van Richtlijn 2006/112/EG staat de lidstaten toe om belastingplichtigen aan wie broeikasgasemissierechten als omschreven in artikel 3 van Richtlijn 2003/87/EG van het Europees Parlement en de Raad ([2]), alsook andere eenheden die door exploitanten kunnen worden gebruikt om aan die richtlijn te voldoen, worden overgedragen, als de tot voldoening van de btw gehouden persoon aan te wijzen ("de verleggingsregeling"). Deze bepalingen zijn bij Richtlijn 2010/23/EU van de Raad ([3]) opgenomen in Richtlijn 2006/112/EG ten behoeve van de strijd tegen de btw-fraude. De toepassing van de verleggingsregeling voor de handel in broeikasgasemissierechten overeenkomstig artikel 199 bis, lid 1, punten a) en b), van Richtlijn 2006/112/EG is beperkt tot rechten die onder het EU-emissiehandelssysteem ("het EU-ETS") worden verhandeld.

(5) Met de BEHG heeft Duitsland een wettelijk kader voor een nationaal emissiehandelssysteem gecreëerd, dat betrekking heeft op emissies die niet onder het EU-ETS vallen. Daarom biedt artikel 199 bis, lid 1, punten a) en b), van Richtlijn 2006/112/EG geen rechtsgrondslag voor de toepassing van de verleggingsregeling op de handel in het kader van de BEHG.

([1]) PB L 347 van 11.12.2006, blz. 1.

([2]) Richtlijn 2003/87/EG van het Europees Parlement en de Raad van 13 oktober 2003 tot vaststelling van een systeem voor de handel in broeikasgasemissierechten binnen de Unie en tot wijziging van Richtlijn 96/61/EG van de Raad (PB L 275 van 25.10.2003, blz. 32).

([3]) Richtlijn 2010/23/EU van de Raad van 16 maart 2010 tot wijziging van Richtlijn 2006/112/EG betreffende het gemeenschappelijke stelsel van belasting over de toegevoegde waarde, wat betreft een facultatieve en tijdelijke toepassing van de verleggingsregeling voor leveringen van bepaalde fraudegevoelige diensten (PB L 72 van 20.3.2010, blz. 1).

(6) Volgens Duitsland is de handel in emissierechten zeer gevoelig voor btw-fraude. Bij de handel in brandstofemissierechten in het kader van de BEHG kan op dezelfde manier worden gefraudeerd als bij de emissiehandel in het kader van het EU-ETS. Emissierechten kunnen snel, meermaals en vlot worden uitgewisseld. Het is derhalve zeer moeilijk voor de autoriteiten om dergelijke eigendomsoverdrachten na te gaan of, en te garanderen, dat het juiste bedrag aan belastingen wordt geheven. De koper van de rechten, een belastingplichtige met recht op aftrek, kan de voorbelasting aftrekken zonder dat de verkoper de door hem in rekening gebrachte btw afdraagt aan de belastingautoriteiten. Met name wanneer er in de leveringsketen sprake is van "ploffers", die snel verdwijnen of geen activa hebben, kan de ontdoken belasting niet door de autoriteiten worden geïnd, met de daaruit voortvloeiende negatieve gevolgen voor de begroting. Om dit verlies aan overheidsinkomsten te ondervangen, heeft Duitsland om machtiging verzocht om te mogen afwijken van artikel 193 van Richtlijn 2006/112/EG teneinde de verleggingsregeling te mogen invoeren voor de overdracht van emissierechten.

(7) Als de belastingplichtige afnemer in die specifieke gevallen wordt aangewezen als de tot voldoening van de btw gehouden persoon, zal de belastinginning worden vereenvoudigd en belastingontduiking en -ontwijking worden voorkomen. Daarom moet Duitsland worden gemachtigd de verleggingsregeling toe te passen op de overdracht van emissierechten die worden verhandeld in een nationaal handelssysteem in het kader van de BEHG ("de bijzondere maatregel").

(8) De bijzondere maatregel moet in de tijd worden beperkt. Daarom moet Duitsland worden gemachtigd de bijzondere maatregel toe te passen tot en met 31 december 2024.

(9) Gezien het toepassingsgebied en de nieuwheid van de bijzondere maatregel is het zaak het effect ervan te evalueren. Indien Duitsland de bijzondere maatregel dus na 2024 wil verlengen, moet het de Commissie uiterlijk 31 maart 2024 een verslag voorleggen met daarin ook een evaluatie van de bijzondere maatregel samen met het verzoek om verlenging. In dat verslag moet worden beoordeeld welk effect de bijzondere maatregel heeft gesorteerd op de strijd tegen btw-fraude en worden vermeld hoeveel ondernemers en transacties onder de bijzondere maatregel vielen.

(10) De bijzondere maatregel zal geen negatieve gevolgen hebben voor de eigen middelen van de Unie uit de btw,

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

Artikel 1

In afwijking van artikel 193 van Richtlijn 2006/112/EG wordt Bondsrepubliek Duitsland gemachtigd de belastingplichtige aan wie emissierechten worden overgedragen die in een nationaal handelssysteem in het kader van de wet op de brandstofemissierechtenhandel (*Gesetz über einen nationalen Zertifikatehandel für Brennstoffemissionen*) van 12 december 2019 worden verhandeld, aan te wijzen als de tot voldoening van de btw gehouden persoon.

Artikel 2

Dit besluit vervalt op 31 december 2024.

Een verzoek om verlenging van de bijzondere maatregel waarin dit besluit voorziet, moet uiterlijk 31 maart 2024 aan de Commissie worden voorgelegd, samen met een verslag over de toepassing van de maatregel, waarin wordt beoordeeld welk effect deze heeft gesorteerd op de strijd tegen btw-fraude en wordt vermeld hoeveel marktdeelnemers en transacties onder de maatregel vielen.

Artikel 3

Dit besluit wordt van kracht op de datum van kennisgeving.

Artikel 4

Dit besluit is gericht tot de Bondsrepubliek Duitsland.

Gedaan te Luxemburg, 5 oktober 2021.

Voor de Raad
De voorzitter
A. ŠIRCELJ

UITVOERINGSBESLUIT (EU) 2021/1779 VAN DE RAAD

van 5 oktober 2021

tot wijziging van Uitvoeringsbesluit 2009/1013/EU waarbij de Republiek Oostenrijk wordt gemachtigd een maatregel te blijven toepassen die afwijkt van artikel 168 van Richtlijn 2006/112/EG betreffende het gemeenschappelijke stelsel van belasting over de toegevoegde waarde

DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Richtlijn 2006/112/EG van de Raad van 28 november 2006 betreffende het gemeenschappelijke stelsel van belasting over de toegevoegde waarde ([1]), en met name artikel 395, lid 1, eerste alinea,

Gezien het voorstel van de Europese Commissie,

Overwegende hetgeen volgt:

(1) Bij Uitvoeringsbesluit 2009/1013/EU van de Raad ([2]) werd de Republiek Oostenrijk ("Oostenrijk") gemachtigd een bijzondere maatregel toe te passen die afwijkt van Richtlijn 2006/112/EG ("de bijzondere maatregel"). Na opeenvolgende verlengingen zal die machtiging aflopen op 31 december 2021.

(2) Bij Richtlijn 2009/162/EU van de Raad ([3]) is in Richtlijn 2006/112/EG artikel 168 bis ingevoegd, teneinde de aftrek te beperken naar evenredigheid van het werkelijke zakelijke gebruik en aldus beter het beginsel toe te passen dat het recht op aftrek pas ontstaat voor zover de goederen en diensten in kwestie voor de bedrijfsactiviteiten van de belastingplichtige worden gebruikt. Artikel 1 van Uitvoeringsbesluit 2009/1013/EU is gewijzigd om er een verwijzing naar artikel 168 bis van Richtlijn 2006/112/EG in op te nemen. Daarom moet in de titel van Uitvoeringsbesluit 2009/1013/EU ook naar artikel 168 bis van Richtlijn 2006/112/EG worden verwezen.

(3) De bijzondere maatregel wijkt af van de artikelen 168 en 168 bis van Richtlijn 2006/112/EG betreffende het recht op aftrek van een belastingplichtige ter zake van de belasting over de toegevoegde waarde (btw) op goederen en diensten die hij ten behoeve van zijn belaste activiteiten heeft ontvangen. De bijzondere maatregel strekt ertoe de btw op goederen en diensten van het recht op aftrek uit te sluiten wanneer die goederen en diensten voor meer dan 90 % voor de privédoeleinden van de belastingplichtige of diens werknemers, dan wel in het algemeen, voor andere dan bedrijfsdoeleinden of niet-economische activiteiten worden gebruikt.

(4) De bijzondere maatregel strekt ertoe de heffing en de inning van de btw te vereenvoudigen. Er is geen noemenswaardig effect op de in het stadium van het eindverbruik verschuldigde belasting.

(5) Bij brief, ingekomen bij de Commissie op 19 maart 2021, heeft Oostenrijk verzocht de bijzondere maatregel te mogen blijven toepassen (hierna "het verzoek" genoemd).

(6) Op grond van artikel 395, lid 2, tweede alinea, van Richtlijn 2006/112/EG heeft de Commissie de overige lidstaten het verzoek doen toekomen bij brief van 7 april 2021. Bij brief van 8 april 2021 heeft de Commissie Oostenrijk meegedeeld dat zij over alle gegevens beschikte die zij nodig achtte voor de beoordeling van het verzoek.

(7) Volgens Oostenrijk is de bijzondere maatregel zeer doeltreffend gebleken om de inning van de btw te vereenvoudigen en belastingontduiking en -ontwijking te voorkomen. De maatregel verlicht de administratieve lasten voor zowel de bedrijven als de belastingdiensten omdat er nadien geen controle meer moet worden uitgeoefend op het gebruik van de goederen of diensten die bij de aanschaf ervan van het recht op aftrek werden uitgesloten. Oostenrijk moet derhalve worden gemachtigd de bijzondere maatregel gedurende een nieuwe beperkte periode te blijven toepassen, meer bepaald tot en met 31 december 2024.

([1]) PB L 347 van 11.12.2006, blz. 1.

([2]) Uitvoeringsbesluit 2009/1013/EU van de Raad van 22 december 2009 waarbij de Republiek Oostenrijk wordt gemachtigd een maatregel te blijven toepassen die afwijkt van artikel 168 van Richtlijn 2006/112/EG betreffende het gemeenschappelijke stelsel van belasting over de toegevoegde waarde (PB L 348 van 29.12.2009, blz. 21).

([3]) Richtlijn 2009/162/EU van de Raad van 22 december 2009 tot wijziging van enkele bepalingen van Richtlijn 2006/112/EG betreffende het gemeenschappelijke stelsel van belasting over de toegevoegde waarde (PB L 10 van 15.1.2010, blz. 14).

(8) Indien Oostenrijk een verlenging na 2024 nodig acht, moet het de Commissie uiterlijk 31 maart 2024, samen met het daartoe strekkende verzoek, een verslag over de toepassing van de bijzondere maatregel voorleggen met daarin ook een evaluatie van de procentuele opsplitsing.

(9) De bijzondere maatregel zal geen negatieve gevolgen hebben voor de eigen middelen van de Unie uit de btw.

(10) Uitvoeringsbesluit 2009/1013/EU moet daarom dienovereenkomstig worden gewijzigd,

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

Artikel 1

Uitvoeringsbesluit 2009/1013/EU wordt als volgt gewijzigd:

1) De titel wordt vervangen door:

"Uitvoeringsbesluit 2009/1013/EU van de Raad van 22 december 2009 waarbij de Republiek Oostenrijk wordt gemachtigd een maatregel te blijven toepassen die afwijkt van de artikelen 168 en 168 bis van Richtlijn 2006/112/EG betreffende het gemeenschappelijke stelsel van belasting over de toegevoegde waarde".

2) De artikelen 1 en 2 worden vervangen door:

"Artikel 1

In afwijking van de artikelen 168 en 168 bis van Richtlijn 2006/112/EG wordt de Republiek Oostenrijk gemachtigd de belasting over de toegevoegde waarde (btw) op goederen en diensten volledig van het recht op aftrek uit te sluiten, wanneer deze goederen en diensten voor meer dan 90 % voor de privédoeleinden van een belastingplichtige of diens werknemers of, meer in het algemeen, voor andere dan bedrijfsdoeleinden of niet-economische activiteiten worden gebruikt.

Artikel 2

Dit besluit vervalt op 31 december 2024.

Een verzoek om verlenging van de in dit besluit vervatte afwijkende maatregel wordt uiterlijk op 31 maart 2024 bij de Commissie ingediend.

Bij een dergelijk verzoek wordt een verslag over de toepassing van deze maatregel gevoegd, dat ook een evaluatie omvat van de op basis van dit besluit gehanteerde procentuele opsplitsing ter zake van het recht op aftrek van de btw.".

Artikel 2

Dit besluit wordt van kracht op de datum van kennisgeving.

Artikel 3

Dit besluit is gericht tot de Republiek Oostenrijk.

Gedaan te Luxemburg, 5 oktober 2021.

Voor de Raad
De voorzitter
A. ŠIRCELJ

UITVOERINGSBESLUIT (EU) 2021/1780 VAN DE RAAD

van 5 oktober 2021

tot wijziging van Beschikking 2009/790/EG waarbij Polen wordt gemachtigd een maatregel toe te passen die afwijkt van artikel 287 van Richtlijn 2006/112/EG betreffende het gemeenschappelijke stelsel van belasting over de toegevoegde waarde

DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Richtlijn 2006/112/EG van de Raad van 28 november 2006 betreffende het gemeenschappelijke stelsel van belasting over de toegevoegde waarde ([1]), en met name artikel 395, lid 1, eerste alinea,

Gezien het voorstel van de Europese Commissie,

Overwegende hetgeen volgt:

(1) Op grond van artikel 287, punt 14, van Richtlijn 2006/112/EG mag de Republiek Polen ("Polen") vrijstelling van btw verlenen aan belastingplichtigen met een jaaromzet die ten hoogste gelijk is aan de tegenwaarde van 10 000 EUR in de nationale munteenheid tegen de op de dag van zijn toetreding geldende omrekeningskoers.

(2) Op grond van Beschikking 2009/790/EG van de Raad ([2]) is Polen gemachtigd om een bijzondere maatregel in te voeren die afwijkt van artikel 287 van Richtlijn 2006/112/EG, teneinde belastingplichtigen met een jaaromzet van niet meer dan de tegenwaarde van 40 000 EUR in nationale munteenheid van de btw vrij te stellen ("de afwijkende maatregel").

(3) Polen werd bij Uitvoeringsbesluit (EU) 2018/1919 van de Raad ([3]) gemachtigd de afwijkende maatregel toe te passen tot en met 31 december 2021 dan wel de datum van inwerkingtreding van een richtlijn tot wijziging van de bepalingen van de artikelen 281 tot en met 294 van Richtlijn 2006/112/EG, indien deze datum eerder valt.

(4) Bij brief, ingekomen bij de Commissie op 1 maart 2021, heeft Polen bij de Commissie een verzoek ingediend om de afwijkende maatregel te mogen blijven toepassen tot en met 31 december 2024 ("het verzoek").

(5) Op grond van Richtlijn 2006/112/EG, artikel 395, lid 2, tweede alinea, heeft de Commissie de overige lidstaten, behalve Cyprus, bij brief van 25 maart 2021 en Cyprus bij brief van 26 maart 2021 het verzoek doen toekomen. Bij brief van 29 maart 2021 heeft de Commissie Polen meegedeeld dat zij over alle gegevens beschikte die zij nodig achtte voor de beoordeling van het verzoek.

(6) De afwijkende maatregel is in overeenstemming met de doelstellingen van de mededeling van de Commissie van 25 juni 2008 getiteld ""Denk eerst klein" — Een "Small Business Act" voor Europa".

(7) Volgens de door Polen verstrekte gegevens zal de afwijkende maatregel geen noemenswaardige invloed zal hebben op de totale belastingopbrengst in Polen in het stadium van het eindverbruik. Belastingplichtigen zullen nog altijd kunnen kiezen voor het normale btw-stelsel.

(8) Na de inwerkingtreding van Verordening (EU, Euratom) 2021/769 van de Raad ([4]) zal Polen geen compensatieberekening met betrekking tot het overzicht van de eigen btw-middelen voor het begrotingsjaar 2021.

([1]) PB L 347 van 11.12.2006, blz. 1.

([2]) Beschikking 2009/790/EG van de Raad van 20 oktober 2009 waarbij de Republiek Polen wordt gemachtigd een maatregel toe te passen die afwijkt van artikel 287 van Richtlijn 2006/112/EG betreffende het gemeenschappelijke stelsel van belasting over de toegevoegde waarde (PB L 283 van 30.10.2009, blz. 53).

([3]) Uitvoeringsbesluit (EU) 2018/1919 van de Raad van 4 december 2018 tot wijziging van Beschikking 2009/790/EG waarbij Polen wordt gemachtigd een maatregel toe te passen die afwijkt van artikel 287 van Richtlijn 2006/112/EG betreffende het gemeenschappelijke stelsel van belasting over de toegevoegde waarde (PB L 311 van 7.12.2018, blz. 32).

([4]) Verordening (EU, Euratom) 2021/769 van de Raad van 30 april 2021 tot wijziging van Verordening (EEG, Euratom) nr. 1553/89 betreffende de definitieve uniforme regeling voor de inning van de eigen middelen uit de belasting over de toegevoegde waarde (PB L 165 van 11.5.2021, blz. 9).

(9) Gezien het mogelijke positieve effect van de derogatiemaatregel voor de vereenvoudiging van de btw-verplichtingen door de vermindering van de administratieve lasten en kosten voor kleine ondernemingen, moet Polen worden gemachtigd de derogatiemaatregel gedurende een nieuwe periode toe te passen.

(10) Bij Richtlijn (EU) 2020/285 van de Raad ([5]) zijn de artikelen 281 tot en met 294 van Richtlijn 2006/112/EG gewijzigd wat betreft de bijzondere regeling voor kleine ondernemingen, waarbij nieuwe regels voor kleine ondernemingen werden vastgesteld, met inbegrip van de maximumdrempel van de jaaromzet van de lidstaten van 85 000 EUR of de tegenwaarde daarvan in de nationale munteenheid.

(11) De machtiging tot toepassing van de afwijkende maatregel moet in de tijd beperkt worden. De periode moet lang genoeg zijn om te kunnen evalueren of de drempel doeltreffend en passend is. Bovendien moeten de lidstaten op grond van Richtlijn (EU) 2020/285 uiterlijk op 31 december 2024 de nodige wettelijke en bestuursrechtelijke bepalingen vaststellen en bekendmaken om aan artikel 1 van die richtlijn te voldoen en moeten zij deze bepalingen met ingang van 1 januari 2025 toepassen. Het is derhalve passend Polen te machtigen de afwijkende maatregel toe te passen tot en met 31 december 2024.

(12) Beschikking 2009/790/EG moet daarom dienovereenkomstig worden gewijzigd,

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

Artikel 1

Artikel 2 van Beschikking 2009/790/EG wordt vervangen door:

"*Artikel 2*

Deze beschikking is van toepassing van 1 januari 2010 tot en met 31 december 2024.".

Artikel 2

Dit besluit wordt van kracht op de datum van kennisgeving.

Artikel 3

Dit besluit is gericht tot de Republiek Polen.

Gedaan te Luxemburg, 5 oktober 2021.

Voor de Raad
De voorzitter
A. Šircelj

([5]) Richtlijn (EU) 2020/285 van de Raad van 18 februari 2020 tot wijziging van Richtlijn 2006/112/EG betreffende het gemeenschappelijke stelsel van belasting over de toegevoegde waarde wat betreft de bijzondere regeling voor kleine ondernemingen en Verordening (EU) nr. 904/2010 betreffende de administratieve samenwerking en uitwisseling van inlichtingen voor doeleinden van toezicht op de juiste uitvoering van de bijzondere regeling voor kleine ondernemingen (PB L 62 van 2.3.2020, blz. 13).

UITVOERINGSBESLUIT (EU) 2021/1781 VAN DE RAAD

van 7 oktober 2021

tot opschorting van een aantal bepalingen van Verordening (EG) nr. 810/2009 van het Europees Parlement en de Raad ten aanzien van Gambia

DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EG) nr. 810/2009 van het Europees Parlement en de Raad van 13 juli 2009 tot vaststelling van een gemeenschappelijke visumcode (Visumcode) ([1]), en met name artikel 25 bis, lid 5, punt a),

Gezien het voorstel van de Europese Commissie,

Overwegende hetgeen volgt:

(1) Eind februari 2019 besloten de Gambiaanse autoriteiten eenzijdig een moratorium in te stellen op alle operaties op het gebied van gedwongen terugkeer, waardoor doeltreffende terugkeer gedurende het grootste deel van 2019 werd verhinderd. Sinds het moratorium in januari 2020 werd opgeheven, worden de lidstaten geconfronteerd met obstakels die Gambia herhaaldelijk opwerpt met betrekking tot de organisatie en uitvoering van terugkeeroperaties. De wisselende mate van medewerking door Gambia hebben tevens alle fasen van het terugkeerproces belemmerd, óók bij de toepassing van de bestaande goede praktijken en andere operationele afspraken die de Unie en Gambia voorheen waren overeengekomen. Op 6 april 2021 deelden de Gambiaanse autoriteiten mee dat het land tot nader bericht niet in staat is om repatrianten op te nemen en in juni 2021 bevestigden zij dat er tot na de verkiezingen in december een moratorium rust op gedwongen terugkeer of repatriëringen.

(2) Sinds 2019 heeft de Commissie stappen ondernomen om Gambia beter te doen meewerken aan de overname van illegaal verblijvende onderdanen van derde landen. Die stappen omvatten meerdere vergaderingen met de Gambiaanse autoriteiten op zowel technisch als politiek niveau, die ten doel hadden om voor beide partijen aanvaardbare oplossingen te vinden en afspraken te maken over verdere steunprojecten ten gunste van Gambia. Tegelijkertijd hebben vertegenwoordigers van de Commissie en Gambia op hoog niveau overlegd. De overnamekwesties zijn ook aan de orde gesteld met Gambia op andere, door de EDEO georganiseerde vergaderingen.

(3) Gezien de stappen die de Commissie tot dusver heeft ondernomen om de samenwerking en de algemene betrekkingen van de Unie met Gambia te verbeteren, geldt de medewerking die Gambia de Unie verleent op het gebied van overname als onvoldoende en moeten er bijgevolg maatregelen door de Unie worden getroffen.

(4) Derhalve dient de toepassing van een aantal bepalingen van Verordening (EG) nr. 810/2009 tijdelijk te worden opgeschort voor onderdanen van Gambia die krachtens Verordening (EU) 2018/1806 van het Europees Parlement en de Raad ([2]) visumplichtig zijn. Dit moet de Gambiaanse autoriteiten ertoe te bewegen de nodige maatregelen te nemen ter verbetering van de medewerking op het gebied van overname.

(5) De tijdelijk opgeschorte bepalingen zijn vastgesteld in artikel 25 bis, lid 5, punt a), van de Visumcode: opschorting van de mogelijkheid om vrijstelling te verlenen van de eisen inzake de door de in artikel 14, lid 6, bedoelde aanvragers te verstrekken bewijsstukken, opschorting van de algemene behandelingstermijn van vijftien kalenderdagen van artikel 23, lid 1, (wat ook betekent dat de regel inzake de verlenging van deze periode tot ten hoogste 45 kalenderdagen in individuele gevallen niet wordt toegepast), opschorting van de afgifte van meervoudige inreisvisa overeenkomstig artikel 24, leden 2 en 2 quater, en opschorting van de facultatieve vrijstelling van betaling van visumleges voor houders van diplomatieke en dienstpaspoorten overeenkomstig artikel 16, lid 5, punt b).

([1]) PB L 243 van 15.9.2009, blz. 1.

([2]) Verordening (EU) 2018/1806 van het Europees Parlement en de Raad van 14 november 2018 tot vaststelling van de lijst van derde landen waarvan de onderdanen bij overschrijding van de buitengrenzen in het bezit moeten zijn van een visum en de lijst van derde landen waarvan de onderdanen van die plicht zijn vrijgesteld (PB L 303 van 28.11.2018, blz. 39).

(6) Artikel 21, lid 1, van het Verdrag betreffende de werking van de Europese Unie (VWEU) bepaalt dat iedere burger van de Unie het recht heeft vrij op het grondgebied van de lidstaten te reizen en te verblijven, onder voorbehoud van de beperkingen en voorwaarden die bij de Verdragen en de bepalingen ter uitvoering daarvan zijn vastgesteld. Richtlijn 2004/38/EG van het Europees Parlement en de Raad ([3]) geeft invulling aan die beperkingen en voorwaarden. Dit besluit doet geen afbreuk aan de toepassing van die richtlijn, waarbij het recht van vrij verkeer wordt uitgebreid tot familieleden, ongeacht hun nationaliteit, die de burger van de Unie begeleiden of zich bij hem voegen. Dit besluit is derhalve niet van toepassing op familieleden van een burger van de Unie op wie Richtlijn 2004/38/EG van toepassing is of familieleden van een onderdaan van een derde land die een recht van vrij verkeer geniet dat gelijkwaardig is aan dat van de burgers van de Unie op grond van een overeenkomst tussen de Unie en haar lidstaten, enerzijds, en een derde land, anderzijds.

(7) De in dit besluit vervatte maatregelen mogen geen afbreuk doen aan de volkenrechtelijke verplichtingen van de lidstaten als gastlanden van internationale intergouvernementele organisaties of van internationale conferenties die door in de lidstaten gevestigde internationale intergouvernementele organisaties bijeen worden geroepen. De tijdelijke opschorting mag derhalve niet gelden voor onderdanen van Gambia die een visum aanvragen louter omdat de lidstaten dit vereisen om aan hun verplichtingen als gastlanden van dergelijke organisaties of van dergelijke conferenties te voldoen.

(8) Overeenkomstig de artikelen 1 en 2 van Protocol nr. 22 betreffende de positie van Denemarken, gehecht aan het Verdrag betreffende de Europese Unie en het Verdrag betreffende de werking van de Europese Unie, neemt Denemarken niet deel aan de vaststelling van dit besluit en is dit bijgevolg niet bindend voor, noch van toepassing op deze lidstaat. Aangezien dit besluit voortbouwt op het Schengenacquis, beslist Denemarken overeenkomstig artikel 4 van het bovengenoemde protocol binnen een termijn van zes maanden nadat de Raad dit besluit heeft vastgesteld of het dit besluit in zijn nationale wetgeving zal omzetten.

(9) Dit besluit vormt een ontwikkeling van bepalingen van het Schengenacquis waaraan Ierland niet deelneemt, overeenkomstig Besluit 2002/192/EG van de Raad ([4]); Ierland neemt derhalve niet deel aan de vaststelling van dit besluit en is dit niet bindend voor, noch van toepassing op deze lidstaat.

(10) Wat IJsland en Noorwegen betreft, vormt dit besluit een ontwikkeling van bepalingen van het Schengenacquis in de zin van de Overeenkomst tussen de Raad van de Europese Unie en de Republiek IJsland en het Koninkrijk Noorwegen inzake de wijze waarop IJsland en Noorwegen worden betrokken bij de uitvoering, de toepassing en de ontwikkeling van het Schengenacquis ([5]) die vallen onder het gebied bedoeld in artikel 1, punt B, van Besluit 1999/437/EG van de Raad ([6]).

(11) Wat Zwitserland betreft, vormt dit besluit een ontwikkeling van de bepalingen van het Schengenacquis in de zin van de Overeenkomst tussen de Europese Unie, de Europese Gemeenschap en de Zwitserse Bondsstaat inzake de wijze waarop Zwitserland wordt betrokken bij de uitvoering, de toepassing en de ontwikkeling van het Schengenacquis ([7]) die vallen onder het gebied bedoeld in artikel 1, punt B, van Besluit 1999/437/EG, in samenhang met artikel 3 van Besluit 2008/146/EG van de Raad ([8]).

([3]) Richtlijn 2004/38/EG van het Europees Parlement en de Raad van 29 april 2004 betreffende het recht van vrij verkeer en verblijf op het grondgebied van de lidstaten voor de burgers van de Unie en hun familieleden, tot wijziging van Verordening (EEG) nr. 1612/68 en tot intrekking van Richtlijnen 64/221/EEG, 68/360/EEG, 72/194/EEG, 73/148/EEG, 75/34/EEG, 75/35/EEG, 90/364/EEG, 90/365/EEG en 93/96/EEG (PB L 158 van 30.4.2004, blz. 77).

([4]) Besluit 2002/192/EG van de Raad van 28 februari 2002 betreffende het verzoek van Ierland deel te mogen nemen aan bepalingen van het Schengenacquis (PB L 64 van 7.3.2002, blz. 20).

([5]) PB L 176 van 10.7.1999, blz. 36.

([6]) Besluit 1999/437/EG van de Raad van 17 mei 1999 inzake bepaalde toepassingsbepalingen van de door de Raad van de Europese Unie, de Republiek IJsland en het Koninkrijk Noorwegen gesloten overeenkomst inzake de wijze waarop deze twee staten worden betrokken bij de uitvoering, de toepassing en de ontwikkeling van het Schengenacquis (PB L 176 van 10.7.1999, blz. 31).

([7]) PB L 53 van 27.2.2008, blz. 52.

([8]) Besluit 2008/146/EG van de Raad van 28 januari 2008 betreffende de sluiting namens de Europese Gemeenschap van de Overeenkomst tussen de Europese Unie, de Europese Gemeenschap en de Zwitserse Bondsstaat inzake de wijze waarop Zwitserland wordt betrokken bij de uitvoering, de toepassing en de ontwikkeling van het Schengenacquis (PB L 53 van 27.2.2008, blz. 1).

(12) Wat Liechtenstein betreft, vormt dit besluit een ontwikkeling van de bepalingen van het Schengenacquis in de zin van het Protocol tussen de Europese Unie, de Europese Gemeenschap, de Zwitserse Bondsstaat en het Vorstendom Liechtenstein betreffende de toetreding van het Vorstendom Liechtenstein tot de Overeenkomst tussen de Europese Unie, de Europese Gemeenschap en de Zwitserse Bondsstaat inzake de wijze waarop Zwitserland wordt betrokken bij de uitvoering, de toepassing en de ontwikkeling van het Schengenacquis ([9]) die vallen onder het gebied bedoeld in artikel 1, punt B, van Besluit 1999/437/EG, in samenhang met artikel 3 van Besluit 2011/350/EU van de Raad ([10]).

(13) Dit besluit vormt een handeling die op het Schengenacquis voortbouwt of anderszins daarmee verband houdt in de zin van respectievelijk artikel 3, lid 2, van de Toetredingsakte van 2003, artikel 4, lid 2, van de Toetredingsakte van 2005 en artikel 4, lid 2, van de Toetredingsakte van 2011,

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

Artikel 1

Toepassingsgebied

1. Dit besluit is van toepassing op onderdanen van Gambia die op grond van Verordening (EU) 2018/1806 visumplichtig zijn.

2. Het is niet van toepassing op onderdanen van Gambia die uit hoofde van artikel 4 of artikel 6 van Verordening (EU) 2018/1806 van de visumplicht zijn vrijgesteld.

3. Dit besluit is niet van toepassing op onderdanen van Gambia die een visum aanvragen en familielid zijn van een burger van de Unie op wie Richtlijn 2004/38/EG van toepassing is of familieleden van een onderdaan van een derde land die een recht van vrij verkeer geniet dat gelijkwaardig is aan dat van de burgers van de Unie op grond van een overeenkomst tussen de Unie en haar lidstaten, enerzijds, en een derde land, anderzijds.

4. Dit besluit laat de gevallen onverlet waarin de lidstaten gebonden zijn aan een volkenrechtelijke verplichting, en wel:

a) als gastland van een internationale intergouvernementele organisatie;

b) als gastland van een internationale conferentie die wordt bijeengeroepen door of plaatsvindt onder auspiciën van de Verenigde Naties of andere internationale intergouvernementele organisaties waarvoor een lidstaat als gastheer optreedt;

c) uit hoofde van een multilaterale overeenkomst die voorrechten en immuniteiten verleent, of

d) op grond van het Concordaat (Verdrag van Lateranen) van 1929 dat werd gesloten tussen de Heilige Stoel (Vaticaanstad) en Italië, zoals laatstelijk gewijzigd.

Artikel 2

Tijdelijke opschorting van de toepassing van een aantal bepalingen van Verordening (EG) nr. 810/2009

De toepassing van de navolgende bepalingen van Verordening (EG) nr. 810/2009 wordt tijdelijk opgeschort:

a) artikel 14, lid 6;

b) artikel 16, lid 5, punt b);

([9]) PB L 160 van 18.6.2011, blz. 21.

([10]) Besluit 2011/350/EU van de Raad van 7 maart 2011 betreffende de sluiting namens de Europese Unie van het Protocol tussen de Europese Unie, de Europese Gemeenschap, de Zwitserse Bondsstaat en het Vorstendom Liechtenstein betreffende de toetreding van het Vorstendom Liechtenstein tot de Overeenkomst tussen de Europese Unie, de Europese Gemeenschap en de Zwitserse Bondsstaat inzake de wijze waarop Zwitserland wordt betrokken bij de uitvoering, de toepassing en de ontwikkeling van het Schengenacquis betreffende de afschaffing van controles aan de binnengrenzen en het verkeer van personen (PB L 160 van 18.6.2011, blz. 19).

c) artikel 23, lid 1;

d) artikel 24, leden 2 en 2 quater.

Artikel 3

Adressaten

Dit besluit is gericht tot het Koninkrijk België, de Republiek Bulgarije, de Tsjechische Republiek, de Bondsrepubliek Duitsland, de Republiek Estland, de Helleense Republiek, het Koninkrijk Spanje, de Franse Republiek, de Republiek Kroatië, de Italiaanse Republiek, de Republiek Cyprus, de Republiek Letland, de Republiek Litouwen, het Groothertogdom Luxemburg, Hongarije, de Republiek Malta, het Koninkrijk der Nederlanden, de Republiek Oostenrijk, de Republiek Polen, de Portugese Republiek, Roemenië, de Republiek Slovenië, de Slowaakse Republiek, de Republiek Finland en het Koninkrijk Zweden.

Gedaan te Luxemburg, 7 oktober 2021.

Voor de Raad
De voorzitter
M. DIKAUČIČ

AANBEVELINGEN

AANBEVELING (EU) 2021/1782 VAN DE RAAD

van 8 oktober 2021

tot wijziging van Aanbeveling (EU) 2020/912 over de tijdelijke beperking van niet-essentiële reizen naar de EU en de mogelijke opheffing van die beperking

DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 77, lid 2, punten b) en e), en artikel 292, eerste en tweede zin,

Overwegende hetgeen volgt:

(1) Op 30 juni 2020 heeft de Raad een aanbeveling aangenomen over de tijdelijke beperking van niet-essentiële reizen naar de EU en de mogelijke opheffing van die beperking ([1]) ("aanbeveling van de Raad").

(2) Sindsdien heeft de Raad Aanbevelingen (EU) 2020/1052 ([2]), (EU) 2020/1144 ([3]), (EU) 2020/1186 ([4]), (EU) 2020/1551 ([5]), (EU) 2020/2169 ([6]), (EU) 2021/89 ([7]), (EU) 2021/132 ([8]), (EU) 2021/767 ([9]), (EU) 2021/892 ([10]), (EU) 2021/992 ([11]), (EU) 2021/1085 ([12]), (EU) 2021/1170 ([13]), (EU) 2021/1346 ([14]), (EU) 2021/1459 ([15]) en (EU) 2021/1712 ([16]) tot wijziging van Aanbeveling (EU) 2020/912 van de Raad over de tijdelijke beperking van niet-essentiële reizen naar de EU en de mogelijke opheffing van die beperking, aangenomen.

(3) Op 20 mei 2021 heeft de Raad Aanbeveling (EU) 2021/816 tot wijziging van Aanbeveling (EU) 2020/912 van de Raad over de tijdelijke beperking van niet-essentiële reizen naar de EU en de mogelijke opheffing van die beperking aangenomen ([17]), met als doel de criteria te actualiseren die worden gehanteerd om te beoordelen of niet-essentiële reizen vanuit derde landen veilig zijn en moeten worden toegestaan.

(4) De aanbeveling van de Raad strekt ertoe dat de lidstaten de tijdelijke beperking van niet-essentiële reizen naar de EU voor de ingezetenen van de in bijlage I bij de aanbeveling van de Raad genoemde derde landen vanaf 1 juli 2020 geleidelijk en gecoördineerd moeten opheffen. Voorts zou de Raad de lijst van derde landen in bijlage I om de twee weken na nauw overleg met de Commissie en de bevoegde EU-agentschappen en -diensten moeten evalueren — en zo nodig actualiseren — na een algehele beoordeling op basis van de in de aanbeveling van de Raad bedoelde methode, criteria en informatie.

([1]) PB L 208I van 1.7.2020, blz. 1.
([2]) PB L 230 van 17.7.2020, blz. 26.
([3]) PB L 248 van 31.7.2020, blz. 26.
([4]) PB L 261 van 11.8.2020, blz. 83.
([5]) PB L 354 van 26.10.2020, blz. 19.
([6]) PB L 431 van 21.12.2020, blz. 75.
([7]) PB L 33 van 29.1.2021, blz. 1.
([8]) PB L 41 van 4.2.2021, blz. 1.
([9]) PB L 165I van 11.5.2021, blz. 66.
([10]) PB L 198 van 4.6.2021, blz. 1.
([11]) PB L 221 van 21.6.2021, blz. 12.
([12]) PB L 235 van 2.7.2021, blz. 27.
([13]) PB L 255 van 16.7.2021, blz. 3.
([14]) PB L 306 van 31.8.2021, blz. 4.
([15]) PB L 320 van 10.9.2021, blz. 1.
([16]) PB L 341 van 24.9.2021, blz. 1.
([17]) PB L 182 van 21.5.2021, blz. 1.

(5) Sindsdien heeft de Raad in nauw overleg met de Commissie en de bevoegde EU-agentschappen en -diensten besprekingen gehouden over de evaluatie van de lijst van derde landen in bijlage I bij de aanbeveling van de Raad en daarbij de criteria en de methode van de aanbeveling van de Raad (als gewijzigd bij Aanbeveling (EU) 2021/816) gebruikt. Uitkomst van deze besprekingen is dat de lijst van derde landen in bijlage I dient te worden gewijzigd. Bahrein en de Verenigde Arabische Emiraten moeten aan de lijst worden toegevoegd.

(6) Grenstoezicht is niet alleen in het belang van de lidstaat aan de buitengrenzen waarvan het toezicht wordt uitgeoefend, maar ook in het belang van alle lidstaten die de controles aan de binnengrenzen hebben afgeschaft. De lidstaten zouden er daarom voor moeten zorgen dat de maatregelen aan de buitengrenzen worden gecoördineerd om zo de goede werking van het Schengengebied te garanderen. Daartoe zouden de lidstaten vanaf 8 oktober 2021 moeten voortgaan met het gecoördineerd opheffen van de tijdelijke beperking van niet-essentiële reizen naar de EU voor de ingezetenen van de derde landen, de speciale administratieve regio's *en de andere territoriale entiteiten en autoriteiten* die worden genoemd in bijlage I bij de aanbeveling van de Raad, als gewijzigd bij deze aanbeveling.

(7) Overeenkomstig de artikelen 1 en 2 van Protocol nr. 22 betreffende de positie van Denemarken, gehecht aan het Verdrag betreffende de Europese Unie en aan het VWEU, neemt Denemarken niet deel aan de aanneming van deze aanbeveling; deze is bijgevolg niet bindend voor, noch van toepassing op deze lidstaat. Aangezien deze aanbeveling voortbouwt op het Schengenacquis, beslist Denemarken overeenkomstig artikel 4 van het bovengenoemde protocol binnen een termijn van zes maanden nadat de Raad heeft beslist over deze aanbeveling, of het deze zal uitvoeren.

(8) Deze aanbeveling vormt een ontwikkeling van de bepalingen van het Schengenacquis waaraan Ierland niet deelneemt, overeenkomstig Besluit 2002/192/EG van de Raad ([18]). Ierland neemt derhalve niet deel aan de aanneming van deze aanbeveling en deze is niet bindend voor, noch van toepassing op deze lidstaat.

(9) Wat IJsland en Noorwegen betreft, vormt deze aanbeveling een ontwikkeling van de bepalingen van het Schengenacquis in de zin van de Overeenkomst tussen de Raad van de Europese Unie en de Republiek IJsland en het Koninkrijk Noorwegen inzake de wijze waarop IJsland en Noorwegen worden betrokken bij de uitvoering, de toepassing en de ontwikkeling van het Schengenacquis die vallen onder het gebied bedoeld in artikel 1, punt A, van Besluit 1999/437/EG van de Raad ([19]).

(10) Wat Zwitserland betreft, vormt deze aanbeveling een ontwikkeling van de bepalingen van het Schengenacquis in de zin van de Overeenkomst tussen de Europese Unie, de Europese Gemeenschap en de Zwitserse Bondsstaat inzake de wijze waarop Zwitserland wordt betrokken bij de uitvoering, de toepassing en de ontwikkeling van het Schengenacquis die vallen onder het gebied bedoeld in artikel 1, punt A, van Besluit 1999/437/EG van de Raad ([20]), juncto artikel 3 van Besluit 2008/146/EG van de Raad ([21]).

(11) Wat Liechtenstein betreft, vormt deze aanbeveling een ontwikkeling van de bepalingen van het Schengenacquis in de zin van het Protocol tussen de Europese Unie, de Europese Gemeenschap, de Zwitserse Bondsstaat en het Vorstendom Liechtenstein betreffende de toetreding van het Vorstendom Liechtenstein tot de Overeenkomst tussen de Europese Unie, de Europese Gemeenschap en de Zwitserse Bondsstaat inzake de wijze waarop Zwitserland wordt betrokken bij de uitvoering, de toepassing en de ontwikkeling van het Schengenacquis die vallen onder het gebied bedoeld in artikel 1, punt A, van Besluit 1999/437/EG ([22]), juncto artikel 3 van Besluit 2011/350/EU ([23]),

([18]) Besluit 2002/192/EG van de Raad van 28 februari 2002 betreffende het verzoek van Ierland deel te mogen nemen aan bepalingen van het Schengenacquis (PB L 64 van 7.3.2002, blz. 20).
([19]) PB L 176 van 10.7.1999, blz. 31.
([20]) PB L 53 van 27.2.2008, blz. 52.
([21]) Besluit 2008/146/EG van de Raad van 28 januari 2008 betreffende de sluiting namens de Europese Gemeenschap van de Overeenkomst tussen de Europese Unie, de Europese Gemeenschap en de Zwitserse Bondsstaat inzake de wijze waarop Zwitserland wordt betrokken bij de uitvoering, de toepassing en de ontwikkeling van het Schengenacquis (PB L 53 van 27.2.2008, blz. 1).
([22]) PB L 160 van 18.6.2011, blz. 21.
([23]) Besluit 2011/350/EU van de Raad van 7 maart 2011 betreffende de sluiting namens de Europese Unie van het Protocol tussen de Europese Unie, de Europese Gemeenschap, de Zwitserse Bondsstaat en het Vorstendom Liechtenstein betreffende de toetreding van het Vorstendom Liechtenstein tot de Overeenkomst tussen de Europese Unie, de Europese Gemeenschap en de Zwitserse Bondsstaat inzake de wijze waarop Zwitserland wordt betrokken bij de uitvoering, de toepassing en de ontwikkeling van het Schengenacquis betreffende de afschaffing van controles aan de binnengrenzen en het verkeer van personen (PB L 160 van 18.6.2011, blz. 19).

HEEFT DE VOLGENDE AANBEVELING AANGENOMEN:

Aanbeveling (EU) 2020/912 van de Raad, zoals gewijzigd bij de Aanbevelingen (EU) 2020/1052, (EU) 2020/1144, (EU) 2020/1186, (EU) 2020/1551, (EU) 2020/2169, (EU) 2021/89, (EU) 2021/132, (EU) 2021/767, (EU) 2021/816, (EU) 2021/892, (EU) 2021/992, (EU) 2021/1085, (EU) 2021/1170, (EU) 2021/1346, (EU) 2021/1459 en (EU) 2021/1712, over de tijdelijke beperking van niet-essentiële reizen naar de EU en de mogelijke opheffing van die beperking, wordt als volgt gewijzigd:

1) In punt 1 van de aanbeveling van de Raad wordt de eerste alinea vervangen door:

"1. Vanaf 8 oktober 2021 zouden de lidstaten voor de ingezetenen van de in bijlage I genoemde derde landen de tijdelijke beperking van niet-essentiële reizen naar de EU geleidelijk en gecoördineerd moeten opheffen.".

2) Bijlage I bij de aanbeveling wordt vervangen door:

"*BIJLAGE I*

Derde landen, speciale administratieve regio's en andere territoriale entiteiten en autoriteiten waarvan de ingezetenen niet zouden mogen vallen onder de tijdelijke beperking van niet-essentiële reizen naar de EU aan de buitengrenzen:

I. STATEN

1. AUSTRALIË
2. BAHREIN
3. CANADA
4. CHILI
5. JORDANIË
6. KOEWEIT
7. NIEUW-ZEELAND
8. QATAR
9. RWANDA
10. SAUDI-ARABIË
11. SINGAPORE
12. ZUID-KOREA
13. OEKRAÏNE
14. VERENIGDE ARABISCHE EMIRATEN
15. URUGUAY
16. CHINA (*)

II. SPECIALE ADMINISTRATIEVE REGIO'S VAN DE VOLKSREPUBLIEK CHINA

Speciale Administratieve Regio Hongkong

Speciale Administratieve Regio Macau

III. TERRITORIALE ENTITEITEN EN AUTORITEITEN DIE DOOR TEN MINSTE ÉÉN LIDSTAAT NIET ALS STAAT WORDEN ERKEND

Taiwan.

(*) Onder voorbehoud van wederkerigheid."

Gedaan te Luxemburg, op 8 oktober 2021.

Voor de Raad
De voorzitter
M. DIKAUČIČ

ISSN 1977-0758 (elektronische uitgave)
ISSN 1725-2598 (papieren uitgave)

Bureau voor publicaties
van de Europese Unie
L-2985 Luxemburg
LUXEMBURG

NL