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