Publicatieblad
van de Europese Unie

NL
L-serie

2025/2574

23.12.2025

UITVOERINGSBESLUIT (EU) 2025/2574 VAN DE COMMISSIE

van 19 december 2025

tot wijziging van Uitvoeringsbesluit (EU) 2021/1772 van de Commissie overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad betreffende de passende bescherming van persoonsgegevens door het Verenigd Koninkrijk

(Kennisgeving geschied onder nummer C(2025) 8771)

(Voor de EER relevante tekst)

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

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

Overwegende hetgeen volgt:

1. INLEIDING

(1) In Uitvoeringsbesluit (EU) 2021/1772 van de Commissie ([2]) is geconcludeerd dat het Verenigd Koninkrijk voor de toepassing van artikel 45 van Verordening (EU) 2016/679 een passend beschermingsniveau waarborgt voor persoonsgegevens die binnen het toepassingsgebied van die verordening vanuit de Europese Unie naar het Verenigd Koninkrijk worden doorgegeven ([3]).

(2) Bij de vaststelling van Uitvoeringsbesluit (EU) 2021/1772 heeft de Commissie er rekening mee gehouden dat het Verenigd Koninkrijk na het einde van de overgangsperiode waarin 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 ([4]) voorziet, en nadat de overgangsbepaling uit hoofde 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 ([5]), niet langer van toepassing is, een nieuwe gegevensbeschermingsregeling zou vaststellen, toepassen en handhaven ten opzichte van de regeling die van kracht was toen het land gebonden was door het Unierecht.

(3) Aangezien dit kan hebben geleid tot wijzigingen van het in Uitvoeringsbesluit (EU) 2021/1772 beoordeelde gegevensbeschermingskader of andere relevante ontwikkelingen, werd het passend geacht te bepalen dat dat besluit van toepassing zou zijn voor een periode van vier jaar vanaf de inwerkingtreding ervan. Uitvoeringsbesluit (EU) 2021/1772 zou derhalve verstrijken op 27 juni 2025, tenzij het wordt verlengd volgens de in artikel 93, lid 2, van Verordening (EU) 2016/679 bedoelde procedure.

([1]) PB L 119 van 4.5.2016, blz. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj.

([2]) Uitvoeringsbesluit van de Commissie (EU) 2021/1772 van 28 juni 2021 overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad betreffende de passende bescherming van persoonsgegevens door het Verenigd Koninkrijk (PB L 360 van 11.10.2021, blz. 1, ELI: http://data.europa.eu/eli/dec_impl/2021/1772/oj).

([3]) Zie artikel 1, lid 1, van Uitvoeringsbesluit (EU) 2021/1772. Overeenkomstig artikel 1, lid 2, van dat besluit heeft het besluitgeen betrekking op persoonsgegevens die worden doorgegeven ten behoeve van immigratiecontrole van het Verenigd Koninkrijk of die anderszins vallen onder de vrijstelling voor bepaalde rechten van betrokkenen met het oog op de handhaving van een doeltreffende immigratiecontrole overeenkomstig paragraaf 4, punt 1, van bijlage 2 bij de UK DataProtection Act 2018.

([4]) PB C 384I van 12.11.2019, blz. 1.

([5]) PB L 149 van 30.4.2021, blz. 10, ELI: http://data.europa.eu/eli/agree_internation/2021/689(1)/oj.

(4) Om een besluit te nemen over een mogelijke verlenging van Uitvoeringsbesluit (EU) 2021/1772 moet de Commissie beoordelen of de conclusie dat het Verenigd Koninkrijk een passend beschermingsniveau waarborgt, feitelijk en juridisch gerechtvaardigd blijft in het licht van de ontwikkelingen die zich sinds de vaststelling van Uitvoeringsbesluit (EU) 2021/1772 hebben voorgedaan met betrekking tot de in artikel 45, lid 2, van Verordening (EU) 2016/679 genoemde elementen.

(5) Met name op 23 oktober 2024 heeft de Britse regering de Data (Use and Access) Bill ([6]) ingediend bij het Britse parlement, waarin wijzigingen worden voorgesteld op de Britse General Data Protection Regulation (UK GDPR) en de Data Protection Act 2018 (DPA 2018), die wordt beoordeeld in Uitvoeringsbesluit (EU) 2021/1772. De Commissie heeft op 24 juni 2025 Uitvoeringsbesluit (EU) 2025/1226 ([7]) goedgekeurd, waarmee de geldigheidsduur van Uitvoeringsbesluit (EU) 2021/1772 met zes maanden tot 27 december 2025 wordt verlengd. Dankzij deze tijdelijke technische verlenging kon de Commissie haar beoordeling van het passende beschermingsniveau voor persoonsgegevens dat het Verenigd Koninkrijk biedt, afronden op basis van een stabiel rechtskader, d.w.z. na de afronding van het desbetreffende wetgevingsproces. ([8]).

(6) Sinds de vaststelling van Uitvoeringsbesluit (EU) 2021/1772 heeft de Commissie de relevante ontwikkelingen in het Verenigd Koninkrijk voortdurend gemonitord ([9]). Overeenkomstig overweging 281 van Uitvoeringsbesluit (EU) 2021/1772 is bijzondere aandacht besteed aan de toepassing in de praktijk van de Britse voorschriften betreffende de doorgifte van persoonsgegevens naar derde landen, en aan het effect dat die kan hebben op het niveau van de bescherming van gegevens die in het kader van Uitvoeringsbesluit (EU) 2021/1772 worden doorgegeven, aan de doeltreffendheid van de uitoefening van individuele rechten, met inbegrip van relevante ontwikkelingen in de rechtspraktijk met betrekking tot de uitzonderingen op of de beperkingen van die rechten (met name het recht in verband met de instandhouding van een doeltreffende controle van de immigratie), alsook naleving van de beperkingen en waarborgen met betrekking tot overheidstoegang. Ontwikkelingen in de jurisprudentie en het toezicht door het bureau van de Information Commissioner (ICO) en andere onafhankelijke instanties zullen onder andere als basis dienen voor de monitoring door de Commissie.

(7) Op basis van de beoordeling van deze ontwikkelingen, met inbegrip van de wijzigingen in de UK GDPR en de DPA 2018 die zijn ingevoerd bij de Data (Use and Access) Act, concludeert de Commissie dat het Verenigd Koninkrijk nog steeds een passend beschermingsniveau waarborgt voor persoonsgegevens die binnen het toepassingsgebied van Verordening (EU) 2016/679 worden doorgegeven van de Europese Unie aan het Verenigd Koninkrijk.

(8) De Commissie concludeert ook dat, in het licht van de wijzigingen in de relevante bepalingen van het Britse recht ([10]), de uitsluiting van persoonsgegevens die worden doorgegeven voor controle van de immigratie door het Verenigd Koninkrijk of die anderszins vallen binnen de omvang van de vrijstelling van bepaalde rechten van de betrokkene met het oog op instandhouding van doeltreffende controle van de immigratie (de "uitzondering voor immigratie") overeenkomstig paragraaf 4, punt 1, van bijlage 2 bij de UK Data Protection Act, van het toepassingsgebied van Uitvoeringsbesluit (EU) 2021/1772 niet langer gerechtvaardigd is, zoals uiteengezet in overweging 37 van dit besluit.

([6]) Beschikbaar via de volgende link: https://bills.parliament.uk/bills/3825/news.

([7]) Uitvoeringsbesluit (EU) 2025/1226 van de Commissie van 24 juni 2025 tot wijziging van Uitvoeringsbesluit (EU) 2021/1772 van de Commissie overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad betreffende de passende bescherming van persoonsgegevens door het Verenigd Koninkrijk (PB L, 2025/1226, 26.6.2025, ELI: http://data.europa.eu/eli/dec_impl/2025/1226/oj).

([8]) De Data (Use and Access) Act kreeg op 19 juni 2025 koninklijke goedkeuring.

([9]) Artikel 45, lid 4, van Verordening (EU) 2016/679.

([10]) In mei 2021 had het Hof van Beroep van Engeland en Wales geoordeeld dat de uitzondering voor immigratie zoals die destijds was geformuleerd in paragraaf 4, punt 1, van bijlage 2 bij de UK Data Protection Act onverenigbaar was met de Britse wetgeving, aangezien de wetgevende maatregel geen specifieke bepalingen bevatte waarin de waarborgen van artikel 23, lid 2, van de UK GDPR waren opgenomen. Met het oog op de naleving van het arrest heeft de Britse regering de uitzondering voor immigratie herzien met de goedkeuring van de Data Protection Act 2018 (Amendment of Schedule 2 Exemptions) Regulations 2022. De herziene uitzondering werd echter opnieuw aangevochten op grond van het feit dat deze niet voldeed aan alle vereisten van artikel 23, lid 2, van de UK GDPR. In een arrest van 11 december 2023 heeft het Britse Hof van Beroep de herziene uitzondering voor immigratie opnieuw onverenigbaar verklaard met artikel 23, lid 2, van de UK GDPR. Met het oog op naleving heeft de Britse regering vervolgens de Data Protection Act 2018 (Amendment of Schedule 2 Exemptions) Regulations 2024 aangenomen, die op 8 maart 2024 in werking is getreden.

2. RELEVANTE ONTWIKKELINGEN BETREFFENDE DE VOORSCHRIJFTEN DIE VAN TOEPASSING ZIJN OP DE VERWERKING VAN PERSOONSGEGEVENS

2.1. Het kader voor gegevensbescherming van het Verenigd Koninkrijk

(9) Ten tijde van de vaststelling van Uitvoeringsbesluit (EU) 2021/1772 bestond het rechtskader voor de bescherming van persoonsgegevens in het Verenigd Koninkrijk uit:

— de UK GDPR ([11]), zoals opgenomen in het recht van het Verenigd Koninkrijk bij de European Union (Withdrawal) Act 2018 ([12]) en gewijzigd bij de Data Protection, Privacy and Electronic Communications (Amendments etc.) Exit) Regulations 2019 (DPPEC Regulations) ([13]),

— de DPA 2018 ([14]), zoals gewijzigd bij de DPPEC Regulations.

(10) Hoewel deze twee rechtshandelingen, die nauw aansloten bij de overeenkomstige regels die binnen de Europese Unie van toepassing zijn, nog steeds de wetgeving inzake gegevensbescherming van het Verenigd Koninkrijk vormen, zijn zij sindsdien onderworpen aan beperkte wijzigingen, wat duidelijk maakt dat het Verenigd Koninkrijk niet langer onderworpen is aan het recht van de Europese Unie.

(11) Ten eerste werd in de Retained EU Law (Revocation and Reform) Act 2023 (REUL Act) ([15]) verduidelijkt dat de algemene beginselen van het Unierecht na eind 2023 niet langer deel uitmaakten van de nationale wetgeving van het Verenigd Koninkrijk ([16]). Bovendien hoeven Britse rechters het ongewijzigde "gelijkgestelde recht", voorheen "overgenomen Unierecht" genoemd, niet meer uit te leggen overeenkomstig de algemene beginselen van het Unierecht, maar moet dit recht in overeenstemming met de nationale wetgeving van het Verenigd Koninkrijk worden uitgelegd ([17]). Het ongewijzigde, gelijkgestelde recht moet echter nog steeds door de rechters van het Verenigd Koninkrijk worden uitgelegd in overeenstemming met de relevante jurisprudentie van het Europees Hof van Justitie die vóór het einde van de overgangsperiode ([18]) is uitgesproken, zoals ook vermeld in overweging 13 van Uitvoeringsbesluit (EU) 2021/1772. De DPA 2018 is gewijzigd bij de Data (Use and Access) Act om het effect van de REUL Act op de wetgeving inzake de gegevensbescherming van het Verenigd Koninkrijk te verduidelijken. Zo is in artikel 183A, lid 1, van de DPA 2018 als algemene regel bepaald dat elke nieuwe wetgeving (aangenomen op of na 20 augustus 2025) waarmee nieuwe verplichtingen of bevoegdheden voor de verwerking van persoonsgegevens worden ingevoerd, geacht wordt onderworpen te zijn aan de wetgeving inzake gegevensbescherming van het Verenigd Koninkrijk. Dit betekent dat het gegevensbeschermingskader van het Verenigd

([11]) General Data Protection Regulation, beschikbaar via de volgende link: https://www.legislation.gov.uk/eur/2016/679/contents.

([12]) European Union (Withdrawal) Act 2018, beschikbaar via de volgende link: In https://www.legislation.gov.uk/ukpga/2018/16/contents werd de wetgeving van de Unie die aan het einde van de overgangsperiode rechtstreeks toepasselijk was in het Verenigd Koninkrijk, opgenomen in de wetgeving van het Verenigd Koninkrijk. Dit "overgenomen Unierecht" omvatte Verordening (EU) 2016/679 in haar geheel, met inbegrip van de overwegingen hiervan (zie de toelichting bij de European Union (Withdrawal) Act 2018, paragraaf 83, beschikbaar via de volgende link: https://www.legislation.gov.uk/ukpga/2018/16/pdfs/ukpgaen_20180016_en.pdf). Overeenkomstig deze wet moet het ongewijzigde, gehandhaafde Unierecht door de rechters van het Verenigd Koninkrijk worden uitgelegd overeenstemming met de desbetreffende jurisprudentie van het Europees Hof van Justitie en de algemene beginselen van het Unierecht, zoals deze wetgeving direct vóór het einde van de overgangsperiode van kracht is (respectievelijk de "gehandhaafde jurisprudentie van de EU" en de "gehandhaafde algemene beginselen van het Unierecht").

([13]) The 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, zoals gewijzigd bij de DPPEC Regulations 2020, beschikbaar via de volgende link: https://www.legislation.gov.uk/ukdsi/2020/9780348213522. Bij de DPPEC Regulations wordt Verordening (EU) 2016/679, zoals ingevoerd in het Britse recht bij de European Union (Withdrawal) Act 2018, de DPA 2018 en overige wetgeving inzake gegevensbescherming, gewijzigd om aan te sluiten op de binnenlandse context.

([14]) Data Protection Act 2018, beschikbaar via de volgende link: https://www.legislation.gov.uk/ukpga/2018/12/contents. Vóór de terugtrekking van het Verenigd Koninkrijk uit de Europese Unie en tijdens de overgangsperiode bevatte de DPA 2018 nationale regels, voor zover toegestaan door Verordening (EU) 2016/679, waarin de toepassing van de regels van Verordening (EU) 2016/679 werd gespecificeerd en beperkt, en Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad (PB L 119, 4.5.2016, blz. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj), werd omgezet.

([15]) Beschikbaar via de volgende link: https://www.legislation.gov.uk/ukpga/2023/28.

([16]) Artikel 5 van de European Union (Withdrawal) Act 2018, zoals gewijzigd bij de REUL Act.

([17]) Artikel 5, lid A2, van de European Union (Withdrawal) Act 2018, zoals gewijzigd bij de REUL Act.

([18]) Artikel 6, leden 3 en 7, van de European Union (Withdrawal) Act 2018, zoals gewijzigd bij de REUL Act.

Koninkrijk nog steeds voorrang heeft op andere wetgeving. Overeenkomstig artikel 183A, lid 2, punt b), van de DPA 2018 kan deze veronderstelling buiten toepassing worden gelaten indien het Britse parlement daar uitdrukkelijk in wetgeving toe besluit, waarbij de parlementaire soevereiniteit behouden blijft. Bovendien wordt in artikel 186, lid 2A, van de DPA 2018 verduidelijkt dat de beperkingen van de rechten van betrokkenen die in artikel 186, lid 3, van de DPA 2018 worden genoemd, niet worden opgeheven door artikel 186, lid 1, van de DPA 2018, waarin wordt bepaald dat wetten die de openbaarmaking van informatie verbieden of beperken, geen voorrang hebben boven bepaalde rechten inzake gegevensbescherming. Dit zorgt er bijvoorbeeld voor dat beperkingen van de rechten van betrokkenen in de DPA 2018 zelf niet onder de algemene "voorrang inzake gegevensbescherming" in artikel 186, lid 1, van de DPA 2018 vallen.

(12) Ten tweede is sinds de vaststelling van Uitvoeringsbesluit (EU) 2021/1772 de wetgeving inzake gegevensbescherming van het Verenigd Koninkrijk gewijzigd middels de Data Protection (Fundamental Rights and Freedoms) Amendment Regulations 2023 ([19]). In deze Regulations worden verwijzingen naar grondrechten of fundamentele vrijheden in de UK GDPR en de DPA 2018 (die voorheen waren gedefinieerd als verwijzingen naar de grondrechten en fundamentele vrijheden van de EU ([20])) gedefinieerd als verwijzingen naar rechten uit hoofde van het Europees Verdrag tot bescherming van de rechten van de mens, die in het Verenigd Koninkrijk krachtens de Human Rights Act 1998 ([21]) in nationaal recht zijn omgezet. Bij de Human Rights Act 1998 worden de rechten van het Europees Verdrag voor de rechten van de mens opgenomen in het recht van het Verenigd Koninkrijk. De Human Rights Act verleent alle personen de grondrechten en fundamentele vrijheden van de artikelen 2 tot en met 12 en 14 van het Europees Verdrag voor de rechten van de mens, de artikelen 1, 2 en 3 van het eerste protocol en artikel 1 van het dertiende protocol bij dit verdrag, gelezen in samenhang met de artikelen 16, 17 en 18 van dat verdrag. Dit omvat het recht op eerbiediging van het privéleven en van het familie- en gezinsleven (en het recht op gegevensbescherming als onderdeel van dat recht) en het recht op een eerlijk proces ([22]).

(13) Ten slotte zijn de UK GDPR en de DPA 2018 het voorwerp geweest van gerichte hervormingen die zijn vastgelegd in deel vijf en deel zes van de Data (Use and Access) Act. Hoewel het toepassingsgebied van de Data (Use and Access) Act veel verder gaat dan de bescherming van persoonsgegevens, voorziet deze wet in beperkte wijzigingen van verschillende aspecten van de gegevensbeschermingsregeling, zoals onder meer de regels inzake gegevensverwerking voor wetenschappelijk onderzoek, de rechtsgrondslagen voor gegevensverwerking, de regels met betrekking tot het doelbindingsbeginsel en de voorwaarden voor geautomatiseerde besluitvorming. Daarnaast worden met de Data (Use and Access) Act wijzigingen aangebracht in de governancestructuur van het ICO. Zodra deze maatregelen zijn uitgevoerd, wordt het ICO vervangen door een nieuwe entiteit, namelijk de Information Commission. De rol en functies van de toezichthouder als onafhankelijke toezichthoudende autoriteit voor gegevensbescherming in het Verenigd Koninkrijk blijven ongewijzigd. De Act voorziet ook in nieuwe handhavingsbevoegdheden voor de toezichthouder.

(14) In dit besluit worden de ontwikkelingen op het gebied van wetgeving, regelgeving en andere ontwikkelingen beoordeeld die relevant zijn voor de conclusie over het door het Verenigd Koninkrijk gegarandeerde beschermingsniveau, zoals vastgelegd in Uitvoeringsbesluit (EU) 2021/1772. De beoordeling in Uitvoeringsbesluit (EU) 2021/1772 blijft geldig voor die aspecten van het gegevensbeschermingskader van het Verenigd Koninkrijk die sinds de vaststelling van Uitvoeringsbesluit (EU) 2021/1772 niet zijn gewijzigd of zijn beïnvloed door andere ontwikkelingen.

(15) De wetgevende, regelgevende en andere relevante ontwikkelingen worden in de volgende punten uitvoerig geanalyseerd op basis van de adequaatheidsnorm, volgens welke de Commissie moet bepalen of het derde land in kwestie een beschermingsniveau waarborgt dat "in feite overeenkomt" met het niveau dat in de Europese Unie wordt verzekerd ([23]). Zoals het Hof van Justitie van de Europese Unie heeft verklaard, is hiervoor niet noodzakelijk dat hetzelfde beschermingsniveau wordt geboden ([24]). Met name mogen de middelen die het derde land in kwestie voor de bescherming van de persoonsgegevens tot zijn beschikking heeft, anders zijn dan de middelen die binnen de Europese Unie worden ingezet, zolang zij in de praktijk doeltreffend genoeg blijken om een passend beschermingsniveau te bieden ([25]). 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 de rechten inzake gegevensbescherming, de doeltreffende toepassing en afdwingbaarheid daarvan en het toezicht dat wordt uitgeoefend ([26]).

([19]) Beschikbaar via de volgende link: https://www.gov.uk/government/publications/the-data-protection-fundamental-rights-and-freedoms-amendment-regulations-2023.

([20]) De grondrechten en fundamentele vrijheden van de EU waren in het Britse recht behouden gebleven via artikel 4 van de European Union (Withdrawal) Act 2018, die eind 2023 werd ingetrokken bij de REUL Act.

([21]) Artikel 2, lid 3, van de Data Protection (Fundamental Rights and Freedoms) Amendment Regulations 2023.

([22]) Artikelen 6, 8, 10 en 13 EVRM (zie ook bijlage 1 bij de Human Rights Act 1998).

([23]) Overweging 104 van Verordening (EU) 2016/679.

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

([25]) *Schrems I*, punt 74.

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

2.1.1. *Definities*

(16) De basisbegrippen inzake gegevensbescherming die overeenkomen met de terminologie van Verordening (EU) 2016/679 blijven van toepassing in de gegevensbeschermingsregeling van het Verenigd Koninkrijk. Deze begrippen zijn beoordeeld in overweging 23 van Uitvoeringsbesluit (EU) 2021/1772.

(17) Hoewel de Data (Use and Access) Act het overgrote deel van de definities ongewijzigd laat, zijn er in artikel 4, paragrafen 2, 3, 4 en 5 van de UK GDPR specifieke definities geïntroduceerd met betrekking tot de verwerking van persoonsgegevens voor wetenschappelijke, historische en statistische doeleinden. In paragraaf 2 wordt "verwerking voor wetenschappelijke doeleinden" gedefinieerd als de verwerking van persoonsgegevens voor onderzoeksdoeleinden die redelijkerwijs als wetenschappelijk kunnen worden beschouwd. Dergelijk onderzoek kan met publieke of private middelen worden gefinancierd en kan als commerciële of niet-commerciële activiteit worden uitgevoerd. In overeenstemming met de inhoud van overweging 159 van Verordening (EU) 2016/679 bevat paragraaf 3 een niet-uitputtende lijst van voorbeelden van onderzoeksactiviteiten die worden geacht wetenschappelijke doeleinden na te jagen, waaronder technische ontwikkeling, demonstratie, fundamenteel onderzoek en toegepast onderzoek. In paragraaf 4 wordt verduidelijkt dat "historisch onderzoek" ook genealogisch onderzoek omvat, dat ook als historisch doel wordt erkend in overweging 160 van Verordening (EU) 2016/679. Ten slotte wordt in paragraaf 5 verwerking voor statistische doeleinden gedefinieerd als de verwerking van gegevens voor statistische enquêtes of voor het produceren van statistische resultaten, waarbij de gegevens zodanig worden geaggregeerd dat zij geen persoonsgegevens meer vormen. Bovendien mogen de verwerkte gegevens of de daaruit voortvloeiende informatie niet worden gebruikt om besluiten te nemen of maatregelen te treffen die gericht zijn tegen een individu. Deze definitie sluit aan bij het begrip statistische doeleinden zoals uiteengezet in overweging 162 van Verordening (EU) 2016/679.

(18) Concluderend kan worden gesteld dat de wijzigingen in artikel 4 van de UK GDPR weliswaar specifieke definities van gegevensverwerking voor wetenschappelijke, historische en statistische doeleinden toevoegen, maar dat deze definities in overeenstemming zijn met de letter en de geest van Verordening (EU) 2016/679, zoals blijkt uit de bovengenoemde overwegingen 159, 160 en 162.

(19) Door de toevoeging van paragraaf 6 aan artikel 4 van de UK GDPR is met de Data (Use and Access) Act ook een specifiek kader vastgesteld voor het verkrijgen van toestemming van de betrokkene voor de verwerking van persoonsgegevens voor wetenschappelijke doeleinden. Net als in overweging 33 van Verordening (EU) 2016/679, waarin wordt erkend dat op het gebied van wetenschappelijk onderzoek niet altijd toestemming kan worden verkregen voor een specifiek verwerkingsdoel, maakt de nieuwe bepaling bredere vormen van toestemming mogelijk door toe te staan dat betrokkenen geldige toestemming kunnen geven, zelfs wanneer de exacte doeleinden van het onderzoek op het moment van de gegevensverzameling niet volledig kunnen worden geïdentificeerd, mits het vragen van toestemming in overeenstemming is met algemeen erkende ethische normen die relevant zijn voor het specifieke onderzoeksgebied. In ieder geval moeten betrokkenen de mogelijkheid hebben om, waar mogelijk, alleen voor specifieke onderdelen van het onderzoek toestemming te geven voor de verwerking van persoonsgegevens.

(20) Ten slotte zijn in de Data (Use and Access) Act de waarborgen die voorheen waren opgenomen in artikel 89 van de UK GDPR en in artikel 19 van de DPA 2018 voor gegevensverwerking ten behoeve van archivering in het algemeen belang en voor wetenschappelijk, historisch en statistisch onderzoek, verder uitgewerkt in een nieuw hoofdstuk 8A van de UK GDPR ([27]). Deze waarborgen zijn vergelijkbaar met die van artikel 89 van Verordening (EU) 2016/679 en omvatten de verplichting om technische en organisatorische maatregelen te nemen om de naleving van het beginsel van gegevensminimalisatie te waarborgen.

2.2. **Waarborgen, rechten en verplichtingen**

2.2.1. *Rechtmatigheid en behoorlijkheid van de verwerking*

(21) Volgens het gegevensbeschermingskader van het Verenigd Koninkrijk moeten gegevens op een rechtmatige, behoorlijke en legitieme manier worden verwerkt, zoals beoordeeld in de overwegingen 24 tot en met 26 van Uitvoeringsbesluit (EU) 2021/1772.

([27]) Artikelen 84A tot en met 84D van de UK GDPR, zoals ingevoerd door artikel 86 van de Data (Use and Access) Act.

(22) De beginselen van rechtmatigheid, behoorlijkheid en de gronden voor de rechtmatige verwerking blijven gewaarborgd in het recht van het Verenigd Koninkrijk door middel van artikel 5, lid 1, punt a), en artikel 6, lid 1, van de UK GDPR, zoals beoordeeld in Uitvoeringsbesluit (EU) 2021/1772. Hoewel deze bepalingen grotendeels identiek ([28]) blijven aan de respectieve bepalingen in Verordening (EU) 2016/679, wordt met de Data (Use and Access) Act voor het eerst artikel 6, lid 1, van de UK GDPR gewijzigd door de invoering van een aanvullende rechtsgrond voor de verwerking van persoonsgegevens op grond van artikel 6, lid 1, punt ea) ([29]). Volgens die bepaling is de verwerking rechtmatig indien en voor zover deze "noodzakelijk is voor de behartiging van een erkend gerechtvaardigd belang". In tegenstelling tot de rechtsgrond van gerechtvaardigd belang overeenkomstig artikel 6, lid 1, punt f), van de UK GDPR, vereist de nieuw ingevoerde rechtsgrond van erkend gerechtvaardigd belang geen afweging per geval van het gerechtvaardigde belang van de verwerkingsverantwoordelijke tegen het belang of de grondrechten en vrijheden van de betrokkene, waarmee meer rechtszekerheid wordt geboden aan verwerkingsverantwoordelijken die geen overheidsinstantie zijn. In het nieuw ingevoegde artikel 6, lid 5, van de UK GDPR wordt bepaald dat verwerking alleen noodzakelijk is voor de behartiging van een erkend gerechtvaardigd belang indien aan een voorwaarde in bijlage 1 ([30]) wordt voldaan, waarin vervolgens situaties worden opgesomd waarin verwerking noodzakelijk wordt geacht voor de behartiging van een erkend gerechtvaardigd belang, bijvoorbeeld wanneer deze plaatsvindt naar aanleiding van een verzoek van een overheidsinstantie die de gegevens nodig heeft voor de uitvoering van een taak van algemeen belang met een rechtsgrondslag die voldoet aan artikel 6, lid 3, van de UK GDPR, wanneer de verwerking noodzakelijk is om de nationale veiligheid te waarborgen, de openbare veiligheid te beschermen of voor defensiedoeleinden, om te reageren op een noodsituatie, om misdrijven op te sporen, te onderzoeken of te voorkomen of om kwetsbare personen te beschermen ([31]).

(23) Hoewel de Data (Use and Access) Act daarmee de lijst van rechtsgronden voor de verwerking van persoonsgegevens waarover de verwerkingsverantwoordelijke beschikt, uitbreidt, geldt voor de nieuw ingevoerde rechtsgrond van erkend gerechtvaardigd belang een aantal belangrijke beperkingen. Ten eerste zijn de erkende gerechtvaardigde belangen beperkt tot specifieke situaties die uitputtend in de wet worden opgesomd. Ten tweede kunnen overheidsinstanties zich bij de uitvoering van hun taken niet op deze rechtsgrond beroepen ([32]). Ten derde betreft het alleen gebieden waar er een duidelijk algemeen belang is bij de verwerkingsactiviteit (overeenkomstig de voorwaarden uiteengezet in bijlage 1), d.w.z. waar de verwerking dient voor de in artikel 23 van de UK GDPR (dat overeenkomt met artikel 23 van Verordening (EU) 2016/679) genoemde doeleinden en dus niet voor commerciële doeleinden kan worden gebruikt. Ten vierde, hoewel de Data (Use and Access) Act de Secretary of State het recht geeft om de lijst in bijlage 1 te wijzigen door middel van een Regulation ([33]), mag de Secretary of State een dergelijke Regulation alleen vaststellen na overleg met het ICO ([34]) en een erkend gerechtvaardigd belang alleen aan die lijst toevoegen wanneer die verwerking opnieuw noodzakelijk is om een doel van algemeen belang te waarborgen dat is opgenomen in artikel 23, lid 1, punten c) tot en met j), van de UK GDPR ([35]). Tot slot, zoals ook bevestigd in de

([28]) Ter verduidelijking: met de Data (Use and Access) Act wordt in artikel 6 van de UK GDPR ook een nieuw lid ingevoegd met voorbeelden van soorten verwerking die kunnen worden beschouwd als noodzakelijk voor de behartiging van gerechtvaardigde belangen in de zin van artikel 6, lid 1, punt f), van de UK GDPR. Deze voorbeelden (direct marketing, doorgifte van gegevens binnen een groep voor administratieve doeleinden en de beveiliging van netwerken en informatiesystemen) worden ook genoemd in de overwegingen 47 en 48 van Verordening (EU) 2016/679 als situaties waarin de verwerking zou worden beschouwd als zijnde in het gerechtvaardigde belang van de verwerkingsverantwoordelijke.

([29]) Artikel 70, lid 2, punt b), van de Data (Use and Access) Act. Bij artikel 70, lid 5, van de Data (Use and Access) Act is het recht om bezwaar te maken in artikel 21 van de UK GDPR uitgebreid naar het nieuwe artikel 6, lid 1, punt ea), van de UK GDPR.

([30]) Artikel 70, lid 4, van de Data (Use and Access) Act.

([31]) Zij bijlage 4 bij de Data (Use and Access) Act. Volgens de Britse autoriteiten zijn er verschillende situaties waarin niet-overheidsinstanties persoonsgegevens moeten verwerken om criminaliteit te voorkomen of op te sporen, bv. wanneer een bedrijf merkt dat er pogingen worden ondernomen om zijn computersystemen op onwettige wijze te hacken, of wanneer een bank of financiële instelling merkt dat er pogingen worden ondernomen om op frauduleuze wijze een rekening te openen. De verwerking van persoonsgegevens door een niet-overheidsinstantie kan bijvoorbeeld noodzakelijk zijn om de nationale veiligheid of defensie te waarborgen wanneer een commerciële organisatie vermoedt dat de onlineactiviteit van een klant wijst op betrokkenheid bij terroristische activiteiten. Het ICO werkt aan specifieke richtsnoeren op dit gebied, met inbegrip van een definitie van de relevante begrippen. Het verwijst bijvoorbeeld naar "nationale veiligheid", waarmee waarschijnlijk de veiligheid en het welzijn van het Verenigd Koninkrijk als geheel, zijn bevolking, zijn instellingen en zijn regeringssysteem worden bedoeld. Raadpleeg de ontwerprichtsnoeren van het ICO inzake erkend gerechtvaardigd belang, zoals gepubliceerd voor openbare raadpleging, beschikbaar via de volgende link: https://ico.org.uk/for-organisations/recognised-legitimate-interest-guidance/.

([32]) Artikel 6, lid 1, laatste alinea, zoals gewijzigd bij artikel 70, lid 2, punt c), van de Data (Use and Access) Act.

([33]) Alvorens regelingen vast te stellen, moet de Secretary of State rekening houden met de gevolgen van eventuele wijzigingen voor de belangen en fundamentele rechten en vrijheden van betrokkenen en met het feit dat kinderen (voor zover van toepassing) specifieke bescherming verdienen met betrekking tot hun persoonsgegevens. De regelingen moeten worden vastgesteld bij wettelijk instrument en zijn onderworpen aan de bekrachtigingsprocedure, wat betekent dat zij actief moeten worden goedgekeurd door het Britse parlement. Artikel 70, lid 4, alinea 8, van de Data (Use and Access) Act.

([34]) Artikel 182, lid 2, van de DPA 2018.

([35]) Artikel 70, lid 4, alinea 9, van de Data (Use and Access) Act.

richtsnoeren van het ICO ([36]), moeten verwerkingsverantwoordelijken die zich baseren op een erkend gerechtvaardigd belang als rechtsgrondslag, voldoen aan alle andere vereisten van de UK GDPR, waaronder de garantie dat de verwerking noodzakelijk en evenredig is om het gerechtvaardigde belang te verwezenlijken.

(24) Ten tweede wordt met de Data (Use and Access) Act verduidelijkt dat in artikel 6, lid 3, artikel 9, lid 2, punt g), en artikel 10, lid 1, van de UK GDPR, die overeenkomen met de respectieve bepalingen van Verordening (EU) 2016/679, de verwerking van persoonsgegevens, bijzondere categorieën van persoonsgegevens en persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten ter naleving van een wettelijke verplichting of voor de uitvoering van een taak van algemeen belang, haar grondslag niet alleen in de nationale wetgeving, maar ook in het relevante internationale recht kan hebben ([37]). Het relevante internationale recht wordt vervolgens beperkt door het nieuw ingevoerde artikel 9A van de UK GDPR, in combinatie met bijlage A1, tot één enkele overeenkomst, namelijk de overeenkomst tussen de regering van het Verenigd Koninkrijk van Groot-Brittannië en Noord-Ierland en de regering van de Verenigde Staten van Amerika inzake de toegang tot elektronische gegevens ten behoeve van de bestrijding van zware criminaliteit, ondertekend op 3 oktober 2019 (de UK-US Agreement) ([38]). De waarborgen die in die overeenkomst worden geboden, zijn beoordeeld in de overwegingen 153 tot en met 155 van Uitvoeringsbesluit (EU) 2021/1772 en de uitvoering ervan wordt geanalyseerd in de overwegingen 87 tot en met 93 van dit besluit.

2.2.2. *Verwerking van bijzondere categorieën van persoonsgegevens*

(25) Het kader voor gegevensbescherming van het Verenigd Koninkrijk blijft specifieke waarborgen bieden wanneer het om bijzondere categorieën gegevens gaat, zoals beoordeeld in de overwegingen 27 tot en met 42 van Uitvoeringsbesluit (EU) 2021/1772.

(26) Zowel de definitie van bijzondere categorieën van persoonsgegevens als de specifieke regels die van toepassing zijn op de verwerking van deze categorieën gegevens in de UK GDPR en in de DPA 2018 blijven van kracht. Tegelijkertijd verleent de Data (Use and Access) Act de Secretary of State nieuwe regelgevende bevoegdheden om, indien nodig, speciale categorieën gegevens toe te voegen, de voorwaarden voor het gebruik ervan aan te passen en nieuwe definities toe te voegen ([39]). Het is van belang dat het de Secretary of State op grond van deze bevoegdheid niet is toegestaan om bestaande bijzondere categorieën van gegevens te verwijderen of te wijzigen, of de voorwaarden voor de verwerking van deze categorieën te wijzigen ([40]). De nieuw ingevoerde regelgevende bevoegdheid stelt de regering dus alleen in staat om nieuwe categorieën gevoelige gegevens toe te voegen en de voorwaarden voor de verwerking van deze categorieën vast te stellen, zodat de regering waar nodig kan inspelen op toekomstige technologische en maatschappelijke ontwikkelingen.

(27) Deze wijzigingen hebben derhalve geen invloed op het beschermingsniveau voor bijzondere categorieën persoonsgegevens dat in feite overeenkomt met de bescherming binnen de EU in Uitvoeringsbesluit (EU) 2021/1772.

([36]) Raadpleeg de ICO-richtsnoeren over gerechtvaardigd belang, beschikbaar via de volgende link: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/legitimate-interests/?q=appropriate+policy.

([37]) Artikel 72 van de Data (Use and Access) Act.

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

([39]) Artikel 74 van de Data (Use and Access) Act. Dergelijke regelingen zijn onderworpen aan de bekrachtigingsprocedure, wat betekent dat zij actief moeten worden goedgekeurd door het Britse parlement.

([40]) Zie het nieuwe artikel 11A, lid 1, punt b), en lid 2, van de UK GDPR, evenals de toelichting bij de Data (Use and Access) Bill, paragraaf 571, beschikbaar via de volgende link: https://publications.parliament.uk/pa/bills/cbill/59-01/0179/en/240179en.pdf.

2.2.3. *Doelbinding*

(28) Volgens de gegevensbeschermingsregeling van het Verenigd Koninkrijk moeten gegevens nog steeds voor een specifiek doel worden verwerkt en mogen zij vervolgens alleen worden gebruikt voor zover dit niet onverenigbaar is met het oorspronkelijke doel van de verwerking, zoals beoordeeld in de overwegingen 43 tot en met 48 van Uitvoeringsbesluit (EU) 2021/1772.

(29) Ten eerste brengt de Data (Use and Access) Act enkele gerichte wijzigingen aan in het doelbindingsbeginsel zoals vastgelegd in artikel 5, lid 1, punt b), van de UK GDPR. Met deze wijzigingen wordt de toepassing van dit beginsel verduidelijkt zonder dat de inhoud ervan wordt gewijzigd. In artikel 71, leden 1, 2 en 3, van de Data (Use and Access) Act is bepaald dat het doelbindingsbeginsel van toepassing is wanneer gegevens worden verzameld bij de betrokkene of anderszins, dat het alleen van toepassing is wanneer persoonsgegevens verder worden verwerkt door of namens dezelfde verwerkingsverantwoordelijke (d.w.z. dat het niet van toepassing is wanneer er een verandering van verwerkingsverantwoordelijke plaatsvindt) en dat verwerking niet rechtmatig is louter op grond van het feit dat deze verenigbaar is met de doeleinden waarvoor de persoonsgegevens zijn verzameld.

(30) Ten tweede worden in de Data (Use and Access) Act de regels voor de verdere verwerking van persoonsgegevens verduidelijkt door deze te hergroeperen in het nieuw toegevoegde artikel 8A van de UK GDPR, waarin de volledige regeling voor de verdere verwerking van persoonsgegevens wordt uiteengezet. In artikel 8A, lid 2, van de UK GDPR worden de elementen opgesomd waarmee rekening moet worden gehouden bij het bepalen of een nieuw verwerkingsdoel verenigbaar is met het oorspronkelijke doel. Deze elementen waren voordien opgenomen in artikel 6, lid 4, van de UK GDPR, dat overeenkomt met artikel 6, lid 4, van Verordening (EU) 2016/679 ([41]). In artikel 8A, lid 3, van de UK GDPR worden in één bepaling de situaties gebundeld waarin de verwerking van persoonsgegevens voor een nieuw doel als verenigbaar met het oorspronkelijke doel moet worden beschouwd. Het heeft betrekking op situaties waarin de betrokkene instemt met de verwerking van persoonsgegevens voor het nieuwe doel of waarin de verwerking noodzakelijk is om een in artikel 23, lid 1, genoemd doel ([42]) te verwezenlijken, wanneer de verwerking plaatsvindt met het oog op wetenschappelijk of historisch onderzoek, archivering in het algemeen belang of statistische doeleinden ([43]). Ten slotte wordt in de Data (Use and Access) Act verduidelijkt dat elke verwerking die wordt uitgevoerd om ervoor te zorgen dat de verwerking voldoet aan de gegevensbeschermingsbeginselen van artikel 5, lid 1, van de UK GDPR of om aan te tonen dat dit het geval is, als verenigbaar met het oorspronkelijke doel wordt beschouwd. De bovengenoemde situaties komen nog steeds overeen met wat ook in Verordening (EU) 2016/679 als verenigbare verdere verwerking wordt beschouwd.

(31) Ten derde worden met de Data (Use and Access) Act in artikel 8A, lid 3, punt d), van de UK GDPR ook nieuwe aanvullende situaties ingevoerd waarin de verdere verwerking van persoonsgegevens voor een nieuw doel als verenigbaar met het oorspronkelijke doel wordt beschouwd. Deze situaties worden opgesomd in bijlage 2 bij de UK GDPR ([44]) en omvatten bijvoorbeeld gevallen waarin de verwerking plaatsvindt naar aanleiding van een verzoek van een overheidsinstantie die de gegevens nodig heeft voor de uitvoering van een taak van algemeen belang met een rechtsgrondslag die voldoet aan artikel 6, lid 3, van de UK GDPR, wanneer de verwerking noodzakelijk is om de openbare veiligheid te beschermen, om te reageren op een noodsituatie, om misdrijven op te sporen, te onderzoeken of te voorkomen, de vitale belangen van de betrokkene en anderen te beschermen, kwetsbare personen te beschermen, voor belastingdoeleinden of indien dit noodzakelijk is om te voldoen aan een wettelijke verplichting ([45]).

(32) Hoewel met de Data (Use and Access) Act derhalve de lijst van situaties wordt uitgebreid waarin verdere verwerking voor een ander doel als verenigbaar met het oorspronkelijke verwerkingsdoel wordt beschouwd, geldt voor deze uitbreiding een aantal belangrijke beperkingen. Ten eerste is deze beperkt tot specifieke situaties die uitputtend in de wet zijn opgenomen. Ten tweede betreft deze alleen gebieden waar er een duidelijk algemeen belang is bij de verwerkingsactiviteit, d.w.z. waar de verdere verwerking dient voor de in artikel 23 van de UK GDPR (die overeenkomt met artikel 23 van

([41]) Net als in Verordening (EU) 2016/679 omvatten deze elementen elk verband tussen het oorspronkelijke en het nieuwe doel, de context waarin de persoonsgegevens zijn verzameld, met inbegrip van het verband tussen de betrokkene en de verwerkingsverantwoordelijke, de aard van de verwerking en of deze bijzondere categorieën van gegevens omvat, de mogelijke gevolgen van de voorgenomen verwerking voor de betrokkene en het bestaan van passende waarborgen.

([42]) Zie ook artikel 6, lid 4, van Verordening (EU) 2016/679.

([43]) Overweging 50 van Verordening (EU) 2016/679.

([44]) Bijlage 2 wordt in de UK GDPR geïntroduceerd middels bijlage 5 bij de Data (Use and Access) Act, zie artikel 71, lid 6, van die rechtshandeling.

([45]) Zij bijlage 5 bij de Data (Use and Access) Act.

Verordening (EU) 2016/679) genoemde doeleinden. Zij kan dus niet worden gebruikt voor commerciële doeleinden. Ten derde, hoewel de Data (Use and Access) Act de Secretary of State het recht geeft om de lijst in bijlage 2 te wijzigen door middel van een Regulation ([46]), mag de Secretary of State alleen soorten verwerkingen aan die lijst toevoegen wanneer die verwerkingen opnieuw noodzakelijk zijn om een doel van algemeen belang te waarborgen dat is opgenomen in artikel 23, lid 1, punten c) tot en met j), van de UK GDPR ([47]). Ten vierde, wanneer de verzameling van persoonsgegevens door de verwerkingsverantwoordelijke gebaseerd is op de toestemming van de betrokkene, wordt verwerking voor een nieuw doeleinde in de in bijlage 2 genoemde situaties alleen als verenigbaar met het oorspronkelijke doeleinde beschouwd indien redelijkerwijs niet van de verwerkingsverantwoordelijke kan worden verwacht dat hij nieuwe toestemming van de betrokkene verkrijgt ([48]).

2.2.4. *Individuele rechten*

(33) Binnen het kader van het Verenigd Koninkrijk voor de bescherming van persoonsgegevens behouden betrokkenen dezelfde individuele rechten als onder Verordening (EU) 2016/679, zonder significante wijzigingen ([49]), die kunnen worden afgedwongen bij de verwerkingsverantwoordelijke of de verwerker, met name het recht op toegang tot gegevens, het recht om bezwaar te maken tegen de verwerking en het recht om gegevens te laten corrigeren en wissen, zoals beoordeeld in de overwegingen 51 tot en met 54 van Uitvoeringsbesluit (EU) 2021/1772.

(34) Ten eerste worden in de Data (Use and Access) Act bepaalde modaliteiten verduidelijkt waaronder deze rechten kunnen worden uitgeoefend. Enerzijds worden door een wijziging van artikel 12 en de invoering van een nieuw artikel 12A van de UK GDPR ([50]) de termijnen bepaald waarbinnen verwerkingsverantwoordelijken moeten reageren op verzoeken van betrokkenen. Meer bepaald wordt in artikel 12 van de UK GDPR een wijziging aangebracht waardoor de verwerkingsverantwoordelijke niet langer verplicht is om "binnen een maand na ontvangst van het verzoek" informatie te verstrekken over de maatregelen die zijn genomen (of over de redenen waarom geen maatregelen zijn genomen) naar aanleiding van een verzoek van een betrokkene overeenkomstig de artikelen 15 tot en met 22 van de UK GDPR, maar veeleer "vóór het einde van de toepasselijke termijn". De toepasselijke termijn wordt nader omschreven in het nieuw ingevoerde artikel 12A van de UK GDPR als een periode van één maand, te rekenen vanaf het relevante tijdstip, namelijk het tijdstip waarop de verwerkingsverantwoordelijke het verzoek ontvangt, het tijdstip waarop de verwerkingsverantwoordelijke de gevraagde informatie ontvangt in verband met een verzoek op grond van artikel 12, lid 6, van de UK GDPR, of wanneer een vergoeding die in verband met het verzoek op grond van artikel 12, lid 5, van de UK GDPR in rekening is gebracht, is betaald, afhankelijk van welke datum het laatst valt ([51]). Voorts biedt artikel 12A, lid 3, de verwerkingsverantwoordelijke de mogelijkheid om de toepasselijke termijn met nog eens twee maanden te verlengen wanneer dat nodig is vanwege de complexiteit van de verzoeken van de betrokkene of vanwege het aantal van dergelijke verzoeken. Anderzijds, en uitsluitend met betrekking tot het recht op toegang tot informatie en persoonsgegevens, wordt met de Data (Use and Access) Act artikel 15 van de UK GDPR gewijzigd, om de verduidelijking op te nemen die is ontwikkeld op basis van bestaande nationale jurisprudentie — waarbij wordt voortgebouwd op het evenredigheidsbeginsel uit het Unierecht — waarbij wordt verduidelijkt dat verwerkingsverantwoordelijken alleen redelijke en evenredige zoekopdrachten hoeven uit te voeren naar de gevraagde informatie en persoonsgegevens ([52]). Verwacht wordt dat de nieuwe bepaling wordt uitgelegd in overeenstemming met de bestaande jurisprudentie, waarin is bepaald: "[…] *bij de afweging van de evenredigheid wordt het einddoel van de zoekopdracht afgewogen, namelijk het potentiële voordeel dat het verstrekken van de informatie de betrokkene kan opleveren, tegenover de middelen waarmee die informatie wordt verkregen. In elk afzonderlijk geval moet worden beoordeeld of het vinden en verstrekken van de informatie onevenredig veel moeite kost in verhouding tot de voordelen die dit voor de betrokkene kan opleveren*" ([53]).

([46]) Artikel 8A, lid 5, van de UK GDPR, zoals ingevoerd door artikel 71, lid 1, van de Data (Use and Access) Act.

([47]) Artikel 8A, lid 6, van de UK GDPR, zoals ingevoerd door artikel 71, lid 1, van de Data (Use and Access) Act.

([48]) Artikel 8A, lid 4, punt b), van de UK GDPR, zoals ingevoerd door artikel 71, lid 1, van de Data (Use and Access) Act.

([49]) Met artikel 31 van de Victims and Prisoners Act 2024 (VAP Act) is een aanvullende grond toegevoegd aan het recht op verwijdering zoals vastgelegd in artikel 17 van de UK GDPR, waarbij betrokkenen het recht krijgen om verwerkingsverantwoordelijken te verzoeken hun persoonsgegevens te verwijderen wanneer deze zijn verwerkt naar aanleiding van een ongegronde beschuldiging van de betrokkene door een kwaadwillende persoon. Een persoon wordt als "kwaadwillig" beschouwd als die is veroordeeld voor een strafbaar feit zoals bedoeld in artikel 31, lid 3, van de VAP Act (zoals intimidatie) of als er een antistalkingbevel tegen is uitgevaardigd. De VAP Act is beschikbaar via de volgende link: https://www.legislation.gov.uk/ukpga/2024/21/contents. Bovendien wordt in artikel 77 van de Data (Use and Access) Act het recht op informatie zoals bepaald in artikel 13 van de UK GDPR zodanig gewijzigd dat de verwerkingsverantwoordelijke niet langer verplicht is om de betrokkene te informeren over de verdere verwerking van zijn persoonsgegevens voor een nieuw doel indien dat doel wetenschappelijk of historisch onderzoek of archivering in het algemeen belang of statistische doeleinden betreft, de verwerking wordt uitgevoerd overeenkomstig de specifieke waarborgen die zijn vastgelegd in het nieuwe artikel 84B van de UK GDPR, en het verstrekken van de informatie onmogelijk of onevenredig zou zijn.

([50]) Artikel 76 van de Data (Use and Access) Act.

([51]) Artikel 12A, leden 1 en 2, van de UK GDPR, zoals ingevoerd door artikel 76 van de Data (Use and Access) Act.

([52]) Artikel 15, lid 1A, van de UK GDPR, zoals ingevoerd door artikel 78 van de Data (Use and Access) Act.

([53]) *Dawson-Dammer/Taylor Wessing LLP* [2017] EWCA Civ 74.

(35) Hoewel de termijnen voor het beantwoorden van verzoeken van betrokkenen en de specifieke verplichtingen voor verwerkingsverantwoordelijken met betrekking tot het recht van inzage aan meer gedetailleerde regels zijn onderworpen, blijft het Britse systeem ervoor zorgen dat verzoeken van betrokkenen moeten worden behandeld binnen een redelijke termijn, die op basis van objectieve factoren wordt vastgesteld. Bovendien zijn de materiële verplichtingen van de verwerkingsverantwoordelijke bij het beantwoorden van verzoeken om toegang gebaseerd op vastgestelde wettelijke normen waarin ook rekening wordt gehouden met de belangen van de betrokkene. Tot slot is in de huidige ICO-richtsnoeren reeds bepaald dat een verwerkingsverantwoordelijke niet verplicht is om zoekopdrachten uit te voeren die onredelijk of onevenredig zouden zijn ten opzichte van het belang van het verlenen van toegang tot de informatie ([54]).

(36) De beperkingen van deze individuele rechten zoals vastgelegd in de DPA 2018 en passend binnen het kader van artikel 23 van de UK GDPR, evenals de beperkingen en waarborgen die de toepassing van deze beperkingen omkaderen, blijven van kracht in het Britse kader ([55]), zoals uitvoerig beschreven in de overwegingen 55 tot en met 67 van Uitvoeringsbesluit (EU) 2021/1772.

(37) Met betrekking tot de beperking voor persoonsgegevens die worden verwerkt met het oog op het handhaven van een doeltreffende immigratiecontrole of het onderzoeken of opsporen van activiteiten die de handhaving van een doeltreffende immigratiecontrole zouden ondermijnen, voor zover de toepassing van die bepalingen waarschijnlijk afbreuk zou doen aan een van die zaken (de uitzondering voor immigratie) ([56]), heeft de Britse regering paragraaf 4 van bijlage 2 bij de DPA 2018 gewijzigd door middel van de Data Protection Act 2018 (Amendment of Schedule 2 Exemptions) Regulations 2022 ([57]) en de Data Protection Act 2018 (Amendment of Schedule 2 Exemptions) Regulations 2024 ([58]), die een aanvulling vormen op de Regulations van 2022 ([59]). De wijzigingen zorgen ervoor dat de waarborgen voor de toepassing van de uitzondering voor immigratie die vereist zijn op grond van artikel 23, lid 2, van de UK GDPRG, worden opgenomen in paragrafen 4A en 4B van bijlage 2 bij de DPA 2018. Meer bepaald wordt vereist dat i) de uitzondering voor immigratie uitsluitend per geval moet worden ingeroepen, afzonderlijk voor elk van de relevante bepalingen van de UK GDPR en telkens opnieuw wanneer de Secretary of State overweegt om een van de relevante bepalingen van de UK GDPR niet toe te passen of de toepassing ervan te beperken ([60]), ii) bij de toepassing van de uitzondering voor immigratie rekening wordt gehouden met de rechten en vrijheden en mogelijke kwetsbaarheden van de betrokkene ([61]), iii) de Secretary of State een register bijhoudt over het gebruik van de uitzondering voor immigratie en de betrokkene informeert over het gebruik ervan (behalve in specifieke omstandigheden waarin de informatie afbreuk zou doen aan het doel van de uitzondering) ([62]) en iv) wordt verduidelijkt dat het gebruik van de uitzondering voor immigratie beperkt is tot de verwerking van persoonsgegevens door de Secretary of State ([63]), d.w.z., in de praktijk, door het ministerie van Binnenlandse Zaken voor zijn taken die relevant zijn voor paragraaf 4, lid 1, van bijlage 2 bij de DPA 2018. Daarnaast wordt ook uitgelegd dat er een afweging moet worden gemaakt om te bepalen of de uitoefening van de rechten van de betrokkene de effectieve immigratiecontrole kan schaden en of het noodzakelijk en evenredig is om die rechten als gevolg daarvan te beperken.

([54]) Beschikbaar via de volgende link: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/how-do-we-find-and-retrieve-the-relevant-information/.

([55]) In artikel 88, lid 2, van de Data (Use and Access) Act wordt een kleine wijziging aangebracht in artikel 26, lid 2, punt f), van de DPA 2018 (uitzondering inzake nationale veiligheid en defensie), waarbij wordt verduidelijkt dat het recht om een klacht in te dienen bij de Commissioner overeenkomstig artikel 77 van de UK GDPR geen deel uitmaakt van de bepalingen waarvan de toepassing kan worden beperkt om redenen van nationale veiligheid of defensie.

([56]) Bij de vaststelling van Uitvoeringsbesluit (EU) 2021/1772 waren de geldigheid en interpretatie van de uitzondering voor immigratie onder het recht van het Verenigd Koninkrijk nog niet geregeld, na een uitspraak van het Hof van Beroep van Engeland en Wales van 26 mei 2021 waarin werd geoordeeld dat de uitzondering voor immigratie, zoals die op dat moment in de DPA 2018 was opgenomen, onverenigbaar was met het recht van het Verenigd Koninkrijk, aangezien deze geen specifieke bepalingen bevatte waarin de waarborgen van artikel 23, lid 2, van de UK GDPR, die een weerspiegeling zijn van artikel 23, lid 2, van Verordening (EU) 2016/679, waren opgenomen. Om die reden werden persoonsgegevens die met het oog op immigratiecontrole in het Verenigd Koninkrijk werden doorgegeven of die anderszins onder de uitzondering voor immigratie vallen, uitgesloten van het toepassingsgebied van Uitvoeringsbesluit (EU) 2021/1772.

([57]) De Regulations zijn op 31 januari 2022 in werking getreden en zijn beschikbaar via de volgende link: https://www.legislation.gov.uk/uksi/2022/76/contents/made.

([58]) De Regulations zijn op 8 maart 2024 in werking getreden en zijn beschikbaar via de volgende link: https://www.legislation.gov.uk/uksi/2024/342/contents/made.

([59]) De uitzondering voor immigratie zoals herzien door de Regulations van 2022 werd opnieuw aangevochten door middel van een rechterlijke toetsing, op grond van het feit dat deze nog niet voldeed aan alle vereisten van artikel 23, lid 2, van de UK GDPR. Het Britse Hof van Beroep oordeelde in december 2023 dat dit onverenigbaar was met de vereisten van artikel 23, lid 2, van de UK GDPR. Als gevolg van dat arrest vormen de Regulations van 2024 een aanvulling op de Regulations van 2022 en worden verdere wijzigingen aangebracht in de uitzondering voor immigratie.

([60]) Paragraaf 4A, punt 2, van bijlage 2 bij de DPA 2018.

([61]) Paragraaf 4AB, punten 3 en 4, van bijlage 2 bij de DPA 2018. Het bureau van de Information Commissioner werd geraadpleegd over het ontwerp van de Regulations van 2024 en verklaarde publiekelijk tevreden te zijn met de regeling. De brief die naar aanleiding van de raadpleging is gepubliceerd en waarin het standpunt wordt bevestigd, is beschikbaar via de volgende link: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/02/ico-responds-to-home-office-s-draft-regulations-to-the-immigration-exemption/.

([62]) Paragraaf 4B, punten 1 en 2, van bijlage 2 bij de DPA 2018.

([63]) Paragraaf 4, punt 1, van bijlage 2 bij de DPA 2018.

(38) Bovendien heeft het ICO van het Verenigd Koninkrijk uitvoerige richtsnoeren gegeven voor het gebruik van deze specifieke beperking ([64]). In de richtsnoeren wordt met name vermeld: "U mag de uitzondering voor immigratie niet toepassen als een algemene uitzondering om […] rechten voor alle gegevens die u in uw bezit hebt, te beperken. Het toepassingsgebied van de uitzondering is beperkt tot die rechten waarvan de uitoefening ten aanzien van de bewaarde gegevens afbreuk zou doen aan de vastgestelde immigratiedoeleinden. […]. Daarom dient de verwerkingsverantwoordelijke zich in eerste instantie zo veel mogelijk te houden aan de vereisten van Verordening (EU) 2016/679 en de DPA. […] De nadeligheidstoets heeft een hoge drempel en u mag de uitzondering niet zonder meer toepassen. […] U moet overwegen of de toepassing van de uitzondering een evenredige reactie is op het verzoek om gegevensbescherming van de betrokkene. U kunt van mening zijn dat er een dringende maatschappelijke noodzaak bestaat om de uitzondering voor immigratie toe te passen, maar u moet ook afwegen of dit zwaarder weegt dan uw verplichtingen jegens personen op grond van Verordening (EU) 2016/679. Zij hebben rechten met betrekking tot hun persoonsgegevens, die u onder alle omstandigheden in acht dient te nemen, met name het recht op inzage. Het is daarom in elk geval van belang dat u overweegt of de rechten inzake gegevensbescherming van de betrokkene zwaarder wegen dan het vastgestelde risico van nadeel. Uw toepassing van de uitzondering dient in verhouding te staan tot de omstandigheden en u dient elk geval zorgvuldig te overwegen en te documenteren.".

(39) Over het algemeen is de immigratiebeperking waarin paragraaf 4 van bijlage 2 bij de DPA 2018 voorziet, zoals herzien door de Britse regering in 2022 en 2024 en zoals uitgelegd door de jurisprudentie ([65]) en de richtsnoeren van het ICO, onderworpen aan een aantal strikte voorwaarden die de toepassing ervan kaderen en die sterk lijken op de voorwaarden die zijn vastgelegd in het Unierecht, met name artikel 23 van Verordening (EU) 2016/679, voor de beperking van rechten inzake gegevensbescherming en verplichtingen voor belangrijke doelstellingen van algemeen belang, zoals de controle op immigratie.

2.2.5. *Beperkingen op verdere doorgifte*

(40) Het beschermingsniveau dat wordt geboden aan persoonsgegevens die worden doorgegeven vanuit de Europese Unie naar verwerkingsverantwoordelijken of verwerkers in het Verenigd Koninkrijk, mag niet worden ondermijnd door verdere doorgifte van dergelijke gegevens aan ontvangers in een derde land. De regeling inzake internationale doorgifte van persoonsgegevens vanuit het Verenigd Koninkrijk sluit nog steeds nauw aan bij de regels van hoofdstuk V van Verordening (EU) 2016/679, zoals beoordeeld in de overwegingen 74 tot en met 82 van Uitvoeringsbesluit (EU)2021/1772.

(41) Hoewel met de Data (Use and Access) Act een wijziging is aangebracht in hoofdstuk 5 van de UK GDPR inzake de doorgifte van persoonsgegevens aan derde landen of internationale organisaties, blijft de kernvereiste gehandhaafd dat persoonsgegevens alleen aan een derde land of internationale organisatie mogen worden doorgegeven wanneer de doorgifte is gebaseerd op i) regelingen die de doorgifte goedkeuren (nieuwe terminologie voor wat voorheen "adequaatheidsregelingen" werd genoemd), ii) passende waarborgen, of iii) een afwijking voor specifieke situaties. Deze algemene beginselen voor gegevensdoorgifte zijn terug te vinden in het nieuwe artikel 44A, dat artikel 44 van de UK GDPR ([66]) vervangt, waarin ook wordt bepaald dat doorgifte van persoonsgegevens naar een derde land of internationale organisatie alleen is toegestaan indien de doorgifte plaatsvindt in overeenstemming met de andere bepalingen van de UK GDPR.

(42) Wat specifiek de voorschriften voor het goedkeuren van een doorgifte betreft, is in artikel 45A, lid 2, van de UK GDPR bepaald dat de Secretary of State alleen dergelijke voorschriften mag vaststellen indien hij of zij van mening is dat aan de gegevensbeschermingstoets is voldaan. Dit betekent dat de in artikel 45A, lid 3, van de UK GDPR ingevoerde mogelijkheid voor de Secretary of State om bij het vaststellen van dergelijke voorschriften rekening te houden met de wenselijkheid om gegevensstromen te vergemakkelijken, altijd afhankelijk is van de voorwaarde dat aan de gegevensbeschermingstoets is voldaan. De wettelijke norm waaraan de gegevensbeschermingstoets moet voldoen, is vastgelegd in het nieuwe artikel 45B, lid 1, van de UK GDPR, waarin is bepaald dat het beschermingsniveau voor betrokkenen in ontvangende landen of internationale organisaties niet wezenlijk lager mag zijn dan het niveau dat voor betrokkenen is vastgelegd in de relevante wetgeving inzake gegevensbescherming van het Verenigd Koninkrijk. In artikel 45B, lid 2 van de UK GDPR wordt vervolgens een niet-uitputtende lijst gegeven van elementen waarmee rekening moet worden gehouden bij de beoordeling of aan die toets is voldaan, zoals eerbiediging van de rechtsstaat en de mensenrechten, het bestaan en de bevoegdheden van een gegevensbeschermingsautoriteit, de regelingen voor gerechtelijke of buitengerechtelijke verhaalmogelijkheden, de regels inzake de doorgifte van persoonsgegevens vanuit het land of door de organisatie naar andere landen of internationale

([64]) Beschikbaar via de volgende link: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/immigration-exemption-a-guide/.

([65]) *Open Rights Group & Anor, R (On the Application Of)/Secretary of State for the Home Department & Anor* [2019] EWHC 2562 (Admin), punten 40 en 41.

([66]) Artikel 85 van en bijlage 7 bij de Data (Use and Access) Act.

organisaties, de desbetreffende internationale verplichtingen van het land of de organisatie en de grondwet, tradities en cultuur van het land of de organisatie. Bij het herformuleren van de lijst van relevante elementen zoals bepaald in het voormalige artikel 45 van de UK GDPR, behoudt het nieuwe artikel 45B, lid 2, de kernelementen van die lijst en blijft het dus dicht bij wat is bepaald in hoofdstuk V van Verordening (EU) 2016/679. Bovendien hebben de autoriteiten van het Verenigd Koninkrijk bevestigd dat de Secretary of State rekening houdt met elementen die niet in artikel 45B, lid 2, zijn opgenomen, zoals de wetten en praktijken in een derde land met betrekking tot de wijze waarop overheidsinstanties toegang krijgen tot persoonsgegevens ten behoeve van de nationale veiligheid of rechtshandhaving, voor zover deze van invloed zijn op de algemene beschermingsnorm. Daarnaast zijn de autoriteiten van het Verenigd Koninkrijk van mening dat relevante jurisprudentie in het derde land een essentieel onderdeel is van de beoordeling van de kwesties die niet-limitatief zijn opgesomd in artikel 45B, lid 2, van de UK GDPR.

(43) Voorschriften voor het goedkeuren van een doorgifte blijven onderworpen aan de "algemene" procedurele vereisten van artikel 182 van de DPA 2018, zoals uiteengezet in overweging 77 van Uitvoeringsbesluit (EU) 2021/1772. In het kader van deze procedure moet de Secretary of State de Information Commissioner raadplegen wanneer hij voorstelt om Britse adequaatheidsbepalingen vast te stellen ([67]). Zodra deze bepalingen zijn vastgesteld door de Secretary of State, worden zij voorgelegd aan het parlement volgens de zogeheten negative resolution procedure, waarbij beide kamers van het parlement de bepalingen kunnen bestuderen en binnen veertig dagen een motie kunnen aannemen om de bepalingen nietig te verklaren ([68]).

(44) Met betrekking tot passende waarborgen wordt in de nieuwe paragraaf 46, lid 1A, van de UK GDPR bepaald dat dergelijke doorgiften alleen mogen plaatsvinden indien relevante waarborgen worden geboden in de instrumenten die beschikbaar zijn overeenkomstig artikel 46, leden 2 en 3 ([69]), van de UK GDPR en indien de verwerkingsverantwoordelijke, de verwerker of de toepasselijke overheidsinstanties, op redelijke en evenredige wijze handelend, van mening zijn dat aan de gegevensbeschermingstoets is voldaan. In de nieuw ingevoegde paragrafen 6 en 7 wordt verduidelijkt dat aan de gegevensbeschermingstoets is voldaan indien, dankzij de vereiste waarborgen, het beschermingsniveau voor betrokkenen na de doorgifte niet wezenlijk lager is dan het niveau dat geldt krachtens de relevante Britse wetgeving inzake gegevensbescherming, d.w.z. dat, net als in het geval van Verordening (EU) 2016/679, dezelfde wettelijke normen gelden voor zowel regelingen waarbij een doorgifte wordt goedgekeurd als passende waarborgen. Volgens dezelfde paragraaf wordt wat redelijk en evenredig is, bepaald aan de hand van alle omstandigheden of waarschijnlijke omstandigheden van de doorgifte of het type doorgifte, met inbegrip van de aard en de omvang van de doorgegeven persoonsgegevens.

(45) Wat afwijkingen voor specifieke situaties betreft, worden in artikel 49 van de UK GDPR een aantal technische wijzigingen aangebracht met betrekking tot de voorwaarden waaronder afwijkingen voor specifieke situaties kunnen worden toegepast, waarmee de bepaling in overeenstemming wordt gebracht met wijzigingen in andere bepalingen, maar die geen invloed hebben op het niveau van bescherming van persoonsgegevens in het Verenigd Koninkrijk. Daarnaast wordt een nieuwe paragraaf 4A ingevoegd om het effect van artikel 18, lid 1, van de DPA 2018 weer te geven, waarbij de Secretary of State de bevoegdheid wordt verleend om via regelgeving de omstandigheden te specificeren waarin gegevensdoorgifte noodzakelijk wordt geacht om redenen van algemeen belang. Tot slot wordt in een nieuw artikel 49A het effect van artikel 18, lid 2, van de DPA 2018 overgenomen, waarmee de Secretary of State in staat wordt gesteld om via regelgeving beperkingen op te leggen aan gegevensoverdrachten die niet zijn goedgekeurd op grond van artikel 45A (overdrachten die zijn goedgekeurd door regelingen) en wanneer dit noodzakelijk wordt geacht om redenen van zwaarwegend algemeen belang.

(46) Wat de uitvoering van de internationale regels voor doorgifte van gegevens door het Verenigd Koninkrijk betreft, hebben zich sinds de vaststelling van Uitvoeringsbesluit (EU) 2021/1772 verschillende ontwikkelingen voorgedaan.

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

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

([69]) De instrumenten voor overdracht die beschikbaar zijn overeenkomstig artikel 46, leden 2 en 3, van de UK GDPR zijn juridisch bindende en afdwingbare instrumenten tussen overheidsinstanties of -organen, bindende bedrijfsvoorschriften overeenkomstig artikel 47 van de UK GDPR, standaardbepalingen inzake gegevensbescherming die zijn vastgelegd in regelingen van de Secretary of State of in een document van de Information Commission, een goedgekeurde gedragscode en een goedgekeurd certificeringsmechanisme.

(47) Wat de regelingen voor de goedkeuring van doorgiften betreft, zijn tot dusver twee nieuwe regelingen aangenomen, die een afspiegeling zijn van de adequaatheidsbesluiten die ook binnen de Unie van kracht zijn, namelijk voor doorgiften naar de Republiek Korea en voor doorgiften naar commerciële entiteiten die zich hebben aangesloten bij de Britse uitbreiding van het EU-VS-gegevensbeschermingskader. De adequaatheidsregelingen voor de Republiek Korea ([70]) zijn op 19 december 2022 in werking getreden en maken de doorgifte van persoonsgegevens van het Verenigd Koninkrijk naar de Republiek Korea mogelijk. De Britse uitbreiding van het EU-VS-gegevensbeschermingskader, waarvoor de relevante regelingen ([71]) op 12 oktober 2023 in werking zijn getreden, maakt het vrije verkeer van persoonsgegevens naar gecertificeerde Amerikaanse organisaties mogelijk.

(48) Wat de passende waarborgen betreft, heeft het Verenigd Koninkrijk zijn eigen standaardcontractbepalingen inzake gegevensbescherming gepubliceerd, namelijk de International Data Transfer Agreement (IDTA) ([72]) en een addendum bij de standaardcontractbepalingen van de EU, die beide in maart 2022 in werking zijn getreden. De IDTA biedt een specifiek mechanisme voor het Verenigd Koninkrijk om passende waarborgen te bieden voor de doorgifte van persoonsgegevens en vertoont verschillende overeenkomsten met de standaardcontractbepalingen van de EU. Dankzij het addendum, uitgebracht door het ICO, kunnen verwerkingsverantwoordelijken en verwerkers in het Verenigd Koninkrijk voor internationale doorgiften vertrouwen op de standaardcontractbepalingen van de EU in het kader van de UK GDPR. Het ICO heeft ook een Transfer Risk Assessment Tool (instrument voor het beoordelen van overdrachtsrisico's) uitgebracht om Britse organisaties te helpen bij het evalueren van de risico's die gepaard gaan met internationale doorgiften.

(49) Het Verenigd Koninkrijk heeft ook het goedkeuringsproces voor bindende bedrijfsvoorschriften gestroomlijnd door middel van nieuwe richtsnoeren en nieuwe opties voor de goedkeuring van bindende bedrijfsvoorschriften. In juli 2022 publiceerde het ICO richtsnoeren en referentietabellen ter verduidelijking van de Britse aanpak van bindende bedrijfsvoorschriften na de Brexit, en in december 2023 werd een addendum bij de bindende bedrijfsvoorschriften van de EU gepubliceerd om ervoor te zorgen dat bindende bedrijfsvoorschriften die onder het EU-kader zijn goedgekeurd, ook in het Verenigd Koninkrijk afdwingbaar zijn ([73]).

(50) Uiteindelijk werd het Verenigd Koninkrijk in juli 2023 geassocieerd lid van het Global Cross-Border Privacy Rules (CBPR) Forum ([74]). Belangrijk is dat dit lidmaatschap niet inhoudt dat de doorgifte van gegevens van het Verenigd Koninkrijk naar andere leden van het CBPR-forum wordt vergemakkelijkt. Het Verenigd Koninkrijk heeft verduidelijkt dat elke doorgifte van persoonsgegevens vanuit het Verenigd Koninkrijk naar derde landen of internationale organisaties moet voldoen aan de voorwaarden die zijn vastgelegd in de Britse wetgeving, zoals hierboven beschreven, met name de gegevensbeschermingstoets, waarbij de geboden beschermingsnormen "niet wezenlijk lager" mogen zijn dan die van de UK GDPR.

(51) Zoals de Commissie al heeft toegelicht, bieden CBPR's geen voldoende bescherming van persoonsgegevens uit de EU. Het forum voorziet met name niet in afdwingbare individuele rechten ([75]). Het is daarom van bijzonder belang dat, zelfs nu het Verenigd Koninkrijk geassocieerd lid is van het Global CBPR Forum, CBPR geen geldig doorgiftemechanisme kan vormen onder de Britse wetgeving inzake gegevensbescherming. Als dat zou veranderen, zou dit het beschermingsniveau ondermijnen dat momenteel wordt gegarandeerd voor persoonsgegevens die van de EU naar het Verenigd Koninkrijk worden doorgegeven. De Commissie zal de verdere ontwikkelingen op dit gebied dan ook nauwlettend blijven volgen.

([70]) Beschikbaar via de volgende link: https://www.legislation.gov.uk/uksi/2022/1213/made.

([71]) Beschikbaar via de volgende link: https://www.legislation.gov.uk/uksi/2023/1028/made.

([72]) Beschikbaar via de volgende link: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/.

([73]) Het ICO heeft na de Brexit een aanzienlijk aantal Britse aanvragen voor bindende bedrijfsvoorschriften ontvangen. Veel goedgekeurde bindende bedrijfsvoorschriften konden niet meer worden gebruikt, aangezien alleen bindende bedrijfsvoorschriften waarbij het ICO bij het goedkeuringsproces betrokken was geweest, na de Brexit nog konden worden gebruikt, maar de houders van die bindende bedrijfsvoorschriften moesten bij het ICO bijgewerkte documentatie indienen die voldeed aan de UK GDPR.

([74]) Het CBPR-forum bestaat uit de Verenigde Staten van Amerika, Canada, Japan, de Republiek Korea, de Filipijnen, Singapore, Taiwan en Australië, terwijl Mauritius, het Dubai International Financial Centre en Bermuda net als het Verenigd Koninkrijk geassocieerde leden zijn.

([75]) Zie bijvoorbeeld de vergelijkende analyse van de gegevensbeschermingsautoriteiten van de G-7 over de kernelementen van het AVG-certificeringssysteem en het CBPR-systeem, waaruit "aanzienlijke verschillen" tussen de systemen naar voren kwamen, onder meer op het gebied van "afdwingbaarheid en rechtsmiddelen, regels inzake onafhankelijk toezicht en toegang door de overheid". Beschikbaar via de volgende link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10063165.
Zie overweging 79 van Uitvoeringsbesluit van de Commissie (EU) 2019/419 van 23 januari 2019 overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad over de passende bescherming van persoonsgegevens door Japan krachtens de Wet bescherming persoonsinformatie (PB L 76, 19.3.2019, blz. 1, ELI: http://data.europa.eu/eli/dec_impl/2019/419/oj).
Zie ook advies 02/2014 van de Artikel 29-werkgroep over een referentie voor vereisten voor bindende bedrijfsvoorschriften, ingediend bij de nationale gegevensbeschermingsautoriteiten in de EU en grensoverschrijdende privacyregels, ingediend bij de verantwoordingsplichtgemachtigden ("Accountability Agents") van APEC-CBPR, 6 maart 2014.

2.2.6. *Geautomatiseerde besluitvorming*

(52) Hoewel verschillende elementen van de regels inzake geautomatiseerde besluitvorming die in overweging 54 van Uitvoeringsbesluit (EU) 2021/1772 worden beoordeeld, worden gehandhaafd, zijn met de Data (Use and Access) Act enkele aspecten van deze regels gewijzigd.

(53) Ten eerste stelt het nieuw ingevoerde artikel 22B van de UK GDPR een algemeen verbod in op de verwerking van bijzondere categorieën persoonsgegevens (zoals omschreven in artikel 9, lid 1, van de UK GDPR) voor besluiten die uitsluitend op geautomatiseerde verwerking zijn gebaseerd en die juridische of vergelijkbare gevolgen hebben voor de betrokkene. Er worden echter drie uitzonderingen op dit verbod genoemd: de betrokkene heeft uitdrukkelijk toestemming gegeven voor een dergelijke verwerking; het besluit is noodzakelijk voor het aangaan of uitvoeren van een overeenkomst tussen de verwerkingsverantwoordelijke en de betrokkene, of de verwerking is vereist of toegestaan door de wet. Voor de laatste twee uitzonderingen moet de geautomatiseerde verwerking noodzakelijk zijn om redenen van zwaarwegend algemeen belang ([76]). Het algemene verbod geldt niet voor belangrijke besluiten op basis van geautomatiseerde verwerking van niet-bijzondere categorieën gegevens.

(54) Daarnaast wordt in het nieuwe artikel 22A van de UK GDPR de definitie van een besluit dat "uitsluitend op geautomatiseerde verwerking is gebaseerd" verduidelijkt door te bepalen dat een dergelijk besluit een besluit is waarbij geen sprake is van zinvolle menselijke betrokkenheid bij het besluitvormingsproces. Het is van belang dat verwerkingsverantwoordelijken moeten beoordelen in hoeverre profilering bijdraagt aan een besluit om te bepalen of menselijke betrokkenheid zinvol is geweest. In artikel 22A van de UK GDPR wordt ook verduidelijkt dat een "doorslaggevend besluit" een besluit is dat rechtsgevolgen of vergelijkbare belangrijke gevolgen heeft voor een betrokkene ([77]).

(55) Ten tweede wordt in het nieuw ingevoerde artikel 22C van de UK GDPR bepaald dat verwerkingsverantwoordelijken maatregelen moeten invoeren om passende waarborgen te bieden voor ieder belangrijk besluit dat geheel of gedeeltelijk op persoonsgegevens en uitsluitend op geautomatiseerde verwerking (met inbegrip van niet-bijzondere categorieën van persoonsgegevens) is gebaseerd. Deze waarborgen moeten onder meer inhouden dat de betrokkene informatie krijgt over het besluitvormingsproces, dat de betrokkene de mogelijkheid krijgt om het besluit aan te vechten en bezwaar te maken en dat de betrokkene menselijke tussenkomst kan verkrijgen in het besluitvormingsproces ([78]).

(56) Ten slotte verleent het nieuw geïntroduceerde artikel 22D van de UK GDPR de Secretary of State de bevoegdheid om secundaire wetgeving op te stellen waarin wordt beschreven wat wel en wat geen betekenisvolle menselijke betrokkenheid is, en welk besluit al dan niet wordt beschouwd als een besluit met vergelijkbare aanzienlijke gevolgen voor betrokkenen. Het stelt de Secretary of State ook in staat secundaire wetgeving op te stellen om i) nieuwe waarborgen toe te voegen; ii) aanvullende eisen op te leggen ter aanvulling van de bestaande waarborgen, en iii) maatregelen te omschrijven die niet aan de waarborgen voldoen ([79]). Het is van belang dat de Secretary of State alvorens regelingen vast te stellen overeenkomstig artikel 22D van de UK GDPR het ICO raadpleegt ([80]), dat de regelingen geen wijziging mogen inhouden van artikel 22C van de UK GDPR ([81]) en dat de regelingen onderworpen zijn aan de bekrachtigingsprocedure ([82]), wat betekent dat ze door beide kamers van het Britse parlement moeten worden goedgekeurd voordat zij kunnen worden vastgesteld.

(57) Hoewel met de Data (Use and Access) Act het kader voor geautomatiseerde besluitvorming is gewijzigd, is het belangrijk op te merken dat geautomatiseerde besluitvorming binnen het Britse rechtskader onderworpen blijft aan de belangrijkste waarborgen die het recht op menselijke tussenkomst vereisen in alle gevallen van belangrijke besluiten die uitsluitend op geautomatiseerde verwerking zijn gebaseerd, d.w.z. op basis van de verwerking van gevoelige en niet-gevoelige persoonsgegevens ([83]). Bovendien is het, zoals de Commissie in eerdere adequaatheidsbesluiten heeft opgemerkt ([84]), onwaarschijnlijk dat de specifieke regels inzake geautomatiseerde besluitvorming in

([76]) Artikel 22B van de UK GDPR, zoals ingevoerd door artikel 80, lid 1, van de Data (Use and Access) Act.
([77]) Artikel 22A van de UK GDPR, zoals ingevoerd door artikel 80, lid 1, van de Data (Use and Access) Act.
([78]) Artikel 22C van de UK GDPR, zoals ingevoerd door artikel 80, lid 1, van de Data (Use and Access) Act.
([79]) Artikel 22D van de UK GDPR, zoals ingevoerd door artikel 80, lid 1, van de Data (Use and Access) Act. Alle regelingen die op grond van deze bevoegdheden worden vastgesteld, zijn onderworpen aan de bekrachtigingsprocedure, waarmee parlementair toezicht wordt gewaarborgd. De vereisten van artikel 22C kunnen niet worden gewijzigd door de regelingen.
([80]) Artikel 182, lid 2, van de DPA 2018.
([81]) Artikel 22D, lid 4, van de UK GDPR.
([82]) Artikel 22D, lid 5, van de UK GDPR.
([83]) Artikel 22C, lid 2, van de UK GDPR, zoals ingevoerd door artikel 80, lid 1, van de Data (Use and Access) Act.
([84]) Zie bijvoorbeeld overweging 94 van Uitvoeringsbesluit van de Commissie (EU) 2019/419 overweging 81 van Uitvoeringsbesluit (EU) 2022/254 van de Commissie van 17 december 2021 overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad over de passende bescherming van persoonsgegevens door de Republiek Korea krachtens de Wet bescherming persoonsinformatie (PB L 44, 24.2.2022, blz. 1, ELI: http://data.europa.eu/eli/dec_impl/2022/254/oj).

de UK GDPR van invloed zullen zijn op het beschermingsniveau van persoonsgegevens die van de Unie naar het Verenigd Koninkrijk worden doorgegeven. Wat betreft de persoonsgegevens die in de Europese Unie zijn verzameld, wordt echter elk besluit dat is gebaseerd op geautomatiseerde verwerking, doorgaans genomen door de verwerkingsverantwoordelijke in de Unie (die een directe relatie met de betrokkene heeft) en is daarom onderworpen aan de regels van Verordening (EU) 2016/679.

2.3. **Toezicht en handhaving**

2.3.1. *Onafhankelijk toezicht*

(58) In het Verenigd Koninkrijk wordt het toezicht op en de handhaving van de naleving van het kader voor gegevensbescherming nog steeds uitgevoerd door een onafhankelijke toezichthoudende autoriteit voor gegevensbescherming, zoals geanalyseerd in de overwegingen 85 tot en met 91 van Uitvoeringsbesluit (EU) 2021/1772. Met de Data (Use and Access) Act wordt de governancestructuur van deze autoriteit hervormd door de oprichting van een rechtspersoon, de Information Commission, die de plaats inneemt van het ICO, dat als een enkele instantie was gestructureerd.

(59) Meer in het bijzonder wordt met de governancemaatregelen van de Data (Use and Access) Act, zodra deze zijn ingevoerd, het bureau van de Information Commissioner afgeschaft en worden de taken, het personeel en de eigendommen van het ICO overgedragen aan de nieuwe instantie, de Information Commission. De Information Commission bestaat uit uitvoerende en niet-uitvoerende leden ([85]). De Act voorziet ook in de mogelijkheid dat de Information Commissioner de functie vervult van voorzitter van de Information Commission, die een van de niet-uitvoerende leden is ([86]). In de Data (Use and Access) Act is verder bepaald dat, voor zover dit passend is als gevolg van de overdracht van taken, verwijzingen naar de Information Commissioner in alle wetten of andere documenten (ongeacht wanneer deze zijn aangenomen of opgesteld) moeten worden beschouwd als verwijzingen naar de Information Commission. Voor de uitvoering van haar taken kan de Commissie comités oprichten en taken delegeren aan een lid, een werknemer of een comité van de Commissie ([87]), en kan zij regelingen treffen om haar procedure en de procedure van de comités te regelen, onder meer met betrekking tot het quorum en het nemen van besluiten met meerderheid van stemmen. Deze procedures moeten openbaar worden gemaakt ([88]).

(60) Het is van belang dat de onafhankelijkheid van de Information Commission onderworpen is aan dezelfde waarborgen, onder meer met betrekking tot de regels voor het benoemen en ontslaan van de voorzitter, als die welke zijn beoordeeld in de overwegingen 87 tot en met 90 van Uitvoeringsbesluit (EU) 2021/1772 ([89]). Soortgelijke bescherming geldt voor de andere niet-uitvoerende leden van de Information Commission. Met name wordt de voorzitter van de Information Commission benoemd door Zijne Majesteit op aanbeveling van de Secretary of State. Hij/zij wordt geselecteerd op basis van verdienste en een eerlijk en algemeen vergelijkend onderzoek ([90]). De overige niet-uitvoerende leden worden na overleg met de voorzitter door de Secretary of State benoemd. Kandidaten kunnen alleen worden aanbevolen voor benoeming of worden benoemd indien zij zijn geselecteerd op basis van verdienste en een eerlijk en algemeen vergelijkend onderzoek en indien de Secretary of State ervan overtuigd is dat zij geen belangenconflict hebben ([91]). De uitvoerende leden zijn werknemers van de Information Commission die werkzaam zijn onder de voorwaarden die zijn vastgesteld door de niet-uitvoerende leden ([92]). De algemeen directeur wordt benoemd door de voorzitter en andere niet-uitvoerende leden, na overleg met de Secretary of State. Ook voor de benoeming van uitvoerende leden geldt een selectie op basis van verdiensten en een eerlijk en algemeen vergelijkend onderzoek ([93]).

(61) De voorzitter kan alleen door Zijne Majesteit uit zijn functie worden ontheven op verzoek van beide kamers van het parlement en alleen als de Secretary of State aan die kamer een rapport heeft voorgelegd waarin hij verklaart ervan overtuigd te zijn dat de voorzitter zich schuldig heeft gemaakt aan ernstig wangedrag, een belangenconflict heeft,

([85]) Paragraaf 3, punt 1 van bijlage 12A bij de DPA 2018.
([86]) Artikelen 117, 118, 119 en 120, samen met bijlage 14 bij de Data (Use and Access).
([87]) Paragrafen 13 en 14 van bijlage 12A bij de DPA 2018.
([88]) Paragraaf 16 van bijlage 12A bij de DPA 2018.
([89]) Artikel 52 van de UK GDPR, evenals bijlage 12A van de DPA 2018, zoals geïntroduceerd bij artikel 114A van de Data (Use and Access) Bill.
([90]) Paragraaf 5, punt 1, en paragraaf 3, punt 2, van bijlage 12A bij de DPA 2018.
([91]) Paragraaf 3, punt 2, en paragrafen 5 en 6 van bijlage 12A bij de DPA 2018.
([92]) Paragraaf 11 van bijlage 12A bij de DPA 2018.
([93]) Paragraaf 5, punt 2, van bijlage 12A bij de DPA 2018.

niet heeft voldaan aan specifieke informatievereisten met betrekking tot mogelijke belangenconflicten, of niet in staat, ongeschikt of onwillig is om de taken van de voorzitter uit te voeren ([94]). Niet-uitvoerende leden kunnen alleen door de Secretary of State uit hun ambt worden ontheven indien hij/zij ervan overtuigd is dat aan de specifieke voorwaarden van de wetgeving is voldaan. Het gaat onder meer om belangenconflicten, ernstig wangedrag of het niet in staat, niet bereid of ongeschikt zijn om hun taken uit te voeren. Wat de aanvullende waarborgen betreft, is de Secretary of State verplicht het daartoe strekkende besluit openbaar te maken en het lid een motivering voor de verwijdering te geven ([95]).

(62) De belangrijkste taak van de Information Commission is nog steeds de monitoring en handhaving van het gegevensbeschermingskader in het Verenigd Koninkrijk "ter bescherming van de grondrechten en vrijheden" van personen ([96]). Wat de taak van de Information Commission betreft om een passend niveau van bescherming van persoonsgegevens te waarborgen, wordt in de Data (Use and Access) Act specifiek bepaald dat de Information Commission rekening moet houden met de belangen van betrokkenen, verwerkingsverantwoordelijken en anderen, met zaken van algemeen belang en dat zij het vertrouwen van het publiek in de verwerking van persoonsgegevens moet bevorderen ([97]). Deze doelstellingen worden ook genoemd in overweging 7 van Verordening (EU) 2016/679.

(63) Bovendien is in de Data (Use and Access) Act bepaald dat de Information Commission bij de uitvoering van haar taken uit hoofde van de wetgeving inzake gegevensbescherming rekening moet houden met de bevordering van innovatie en concurrentie, het belang van de preventie, het onderzoek, de opsporing en de vervolging van strafbare feiten, de noodzaak om de openbare veiligheid en de nationale veiligheid te waarborgen, en de specifieke behoeften in verband met de bescherming van kinderen ([98]). In de EU-wetgeving inzake gegevensbescherming wordt ook erkend dat er een evenwicht moet worden gevonden tussen de bescherming van persoonsgegevens en verschillende andere grondrechten en doelstellingen, zoals economische en sociale vooruitgang, veiligheid en rechtvaardigheid en de vrijheid van ondernemerschap ([99]).

2.3.2. *Handhaving, met inbegrip van sancties*

(64) De bevoegdheden en taken van de Information Commission komen nog steeds overeen met die van de toezichthoudende autoriteiten voor gegevensbescherming van de lidstaten overeenkomstig de relevante artikelen van Verordening (EU) 2016/679 ([100]), zoals beoordeeld in de overwegingen 91 tot en met 95 van Uitvoeringsbesluit (EU) 2021/1772.

(65) Met de Data (Use and Access) Act zijn bepaalde verduidelijkingen aangebracht met betrekking tot de uitoefening van sommige van deze bevoegdheden.

(66) Enerzijds kan de Commissie op grond van de Data (Use and Access) Act specifieke "documenten" en "informatie" opvragen wanneer zij gebruikmaakt van haar bevoegdheid om een informatienota uit te vaardigen ([101]). Anderzijds worden met de Data (Use and Access) Act twee nieuwe onderzoeksbevoegdheden voor de Information Commission geïntroduceerd: een nieuwe bevoegdheid om een rapport te eisen ([102]) en een nieuwe bevoegdheid om "interviewoproepen" te versturen aan verwerkingsverantwoordelijken in geval van een vermoedelijke inbreuk op de UK GDPR of de DPA 2018 ([103]).

([94]) Paragraaf 7, punt 6, en paragraaf 7 van bijlage 12A bij de DPA 2018.
([95]) Paragraaf 9, punten 7, 8 en 9 van bijlage 12A bij de DPA 2018.
([96]) Artikel 51 van de UK GDPR.
([97]) Artikel 91 van de Data (Use and Access) Act, tot invoering van artikel 120A van de DPA 2018.
([98]) Artikel 91 van de Data (Use and Access) Act, tot invoering van artikel 120B van de DPA 2018. Met de Data (Use and Access) Act wordt bovendien een nieuw artikel 120C toegevoegd aan de DPA 2018, waarin de Information Commission wordt verplicht een strategie op te stellen en te publiceren waarin onder meer wordt aangegeven hoe zij de bovengenoemde kwesties zal beoordelen en hoe zij bij de uitoefening van haar regelgevende taken rekening zal gehouden met de bevordering van economische groei.
([99]) Zie met name overwegingen 2 en 4, evenals artikel 23, van Verordening (EU) 2016/679.
([100]) Artikelen 57 en 58 van de UK GDPR.
([101]) Artikel 97 van de Data (Use and Access) Act, tot wijziging van artikel 142 van de DPA 2018. De overwegingen met betrekking tot de impact van technologie en de rol van gegevensbescherming bij het creëren van vertrouwen in de digitale economie maken deel uit van de activiteiten van gegevensbeschermingsautoriteiten in zowel het Verenigd Koninkrijk als de EU. Zie bijvoorbeeld het jaarverslag 2024 van het Europees Comité voor gegevensbescherming, blz. 12: "Het EDPB is een dynamisch en collegiaal orgaan dat een cruciale rol speelt bij het waarborgen van een consistente toepassing van de wetgeving inzake gegevensbescherming in heel Europa. Vanuit mijn positie als vicevoorzitter zie ik het als een beschermer van de privacyrechten van personen, die op vakkundige wijze een evenwicht weet te vinden tussen de behoeften van innovatie en economische groei.".
([102]) Artikel 98 van de Data (Use and Access) Act, tot wijziging van artikel 146 van de DPA 2018.
([103]) Artikel 100 van de Data (Use and Access) Act, tot invoering van artikel 148A van de DPA 2018.

(67) Wat de uitoefening van deze bevoegdheden door de Information Commission betreft, heeft de Information Commissioner sinds de inwerkingtreding van Uitvoeringsbesluit (EU) 2021/1772 ongeveer 40 000 klachten van betrokkenen per jaar behandeld, wat vergelijkbaar is met het aantal klachten dat werd behandeld toen het Verenigd Koninkrijk nog deel uitmaakte van de Unie en Verordening (EU) 2016/679 toepaste ([104]). Het ICO heeft ook ambtshalve onderzoeken uitgevoerd naar een breed spectrum van sectorale en nalevingskwesties, waaronder de rechten van betrokkenen ([105]).

(68) Wat de handhavingsmaatregelen betreft, heeft de Commissioner sinds de inwerkingtreding van Uitvoeringsbesluit (EU) 2021/1772 120 berispingen, 32 informatieberichten, 3 beoordelingsberichten, 12 handhavingsberichten, 2 waarschuwingen en 12 boeten opgelegd ([106]). Dit omvatte enkele aanzienlijke financiële sancties die op grond van de UK GDPR en de DPA 2018 werden opgelegd. Zo heeft de Information Commissioner in april 2023 een boete van 12,7 miljoen GBP opgelegd aan een socialemediaplatform wegens misbruik van gegevens van kinderen ([107]). In maart 2025 kreeg een softwarebedrijf een boete van 3,07 miljoen GBP opgelegd voor beveiligingsfouten waardoor de persoonlijke gegevens van meer dan 70 000 mensen in gevaar kwamen ([108]). Zeer recent, in juni 2025, heeft de Information Commissioner een genetisch testbedrijf een boete van 2,31 miljoen GBP opgelegd omdat het na een grootschalige cyberaanval in 2023 geen passende veiligheidsmaatregelen had genomen om de persoonsgegevens van Britse gebruikers te beschermen ([109]).

(69) Sinds de goedkeuring van Uitvoeringsbesluit (EU) 2021/1772 heeft het bureau van de Information Commissioner ook een aanzienlijk aantal richtsnoeren, adviezen en andere leidraden opgesteld en gepubliceerd, waarin de toepassing van de gegevensbeschermingsregels op belangrijke gebieden wordt verduidelijkt, zoals gezichtsherkenning, eerlijkheid in kunstmatige intelligentie, gegevens van kinderen, direct marketing, videobewaking, het recht op toegang, transparantie in de gezondheidszorg en sociale zorg enz. voor verschillende doelgroepen, waaronder kleine en middelgrote ondernemingen, specifieke entiteiten zoals scholen, kinderdagverblijven of kleine overheidsinstanties, maar ook voor bedrijven in het algemeen, het grote publiek of betrokkenen ([110]).

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

3.1. Algemeen rechtskader

(70) Het Verenigd Koninkrijk blijft lid van de Raad van Europa, blijft zich houden aan het Europees Verdrag voor de Rechten van de Mens en blijft onderworpen aan de jurisdictie van het Europees Hof voor de Rechten van de Mens. Het blijft derhalve onderworpen aan de verplichtingen die zijn vastgelegd in het internationaal recht, zoals beschreven in de overwegingen 116 tot en met 119 van Uitvoeringsbesluit (EU) 2021/1772, die het kader vormen voor de toegang van de overheid tot persoonsgegevens op basis van beginselen, waarborgen en individuele rechten die identiek zijn aan die welke gelden voor de 27 lidstaten die partij zijn bij het EVRM en die grotendeels worden weerspiegeld in de relevante jurisprudentie van het Hof van Justitie van de Europese Unie.

(71) Specifieke waarborgen en rechten inzake gegevensbescherming blijven gegarandeerd door de DPA 2018 wanneer gegevens worden verwerkt door de overheidsinstanties van het Verenigd Koninkrijk, met inbegrip van rechtshandhavingsinstanties en nationale veiligheidsdiensten, zoals geanalyseerd in de overwegingen 121 tot en met 132 van Uitvoeringsbesluit (EU) 2021/1772. Met de Data (Use and Access) Act zijn slechts beperkte en gerichte wijzigingen aangebracht in die delen van de DPA 2018 die de regels bevatten voor de verwerking van persoonsgegevens in het kader van strafrechthandhaving (deel 3 van de DPA 2018) en nationale veiligheid (deel 4 van de DPA 2018).

([104]) Jaarverslagen van de Information Commissioner voor 2021-2022, 2022-2023 en 2023-2024. Zie ook Uitvoeringsbesluit (EU) 2021/1772, overweging 96.
([105]) Jaarverslag 2023-2024 van de Information Commissioner, blz. 41.
([106]) Jaarverslagen van de Information Commissioner voor 2021-2022, 2022-2023 en 2023-2024.
([107]) Meer informatie over deze en andere handhavingsmaatregelen is te vinden op de website van het ICO, via de volgende link: https://ico.org.uk/action-weve-taken/enforcement/
([108]) Meer informatie is beschikbaar via de volgende link: https://ico.org.uk/action-weve-taken/enforcement/2025/03/advanced-computer-software-group-limited/.
([109]) Meer informatie is beschikbaar via de volgende link: https://ico.org.uk/action-weve-taken/enforcement/2025/06/23andme/.
([110]) Beschikbaar via de volgende link: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/.

(72) Wat betreft de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de uitvoering van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid, blijft deel 3 van de DPA 2018 voorzien in beginselen, rechten en verplichtingen die vergelijkbaar zijn met die welke zijn vastgelegd in Richtlijn (EU) 2016/680 ([111]).

(73) Meer bepaald heeft de Commissie op dezelfde datum als dit besluit een besluit vastgesteld op grond van artikel 36, lid 3, van Richtlijn (EU) 2016/680, waarin wordt bepaald dat de gegevensbeschermingsregeling die van toepassing is op de verwerking door de Britse strafrechtelijke rechtshandhavingsinstanties met het oog op de handhaving van het strafrecht, een beschermingsniveau blijft waarborgen dat in feite overeenkomt met het niveau dat door Richtlijn (EU) 2016/680 wordt gewaarborgd.

(74) Met de Data (Use and Access) Act zijn bestaande vrijstellingen in deel 3 van de DPA 2018, die bevoegde autoriteiten kunnen toepassen ten behoeve van de nationale veiligheid, gewijzigd en geconsolideerd. Met de vrijstelling inzake nationale veiligheid kunnen bevoegde autoriteiten bepaalde bepalingen van deel 3 van de DPA 2018 buiten toepassing laten indien vrijstelling van die bepaling vereist is om de nationale veiligheid te waarborgen ([112]). Hiermee worden de vrijstellingen inzake nationale veiligheid voor de verwerking van persoonsgegevens onder de UK GDPR (zoals bepaald in artikel 26 van de DPA 2018) en onder deel 4 van de DPA 2018 (zoals bepaald in artikel 110 van de DPA 2018) weerspiegeld.

(75) De vrijstelling inzake nationale veiligheid is onderworpen aan dezelfde beperkingen en waarborgen als de vrijstellingen uit hoofde van de UK GDPR en deel 4 van de DPA 2018, zoals geanalyseerd in de overwegingen 64-67 en 126 van Uitvoeringsbesluit (EU) 2021/1772. De vrijstelling kan met name alleen worden toegepast indien en voor zover dit noodzakelijk is om de nationale veiligheid te waarborgen. Het is geen algemene vrijstelling en moet door de verwerkingsverantwoordelijke per geval worden overwogen en ingeroepen ([113]). Een toepassing van de vrijstelling moet bovendien in overeenstemming zijn met de mensenrechtennormen (geschraagd door de Human Rights Act 1998 en het Europees Verdrag tot bescherming van de rechten van de mens), volgens welke elke aantasting van het recht op privacy in een democratische samenleving noodzakelijk en evenredig moet zijn ([114]). Dit wordt ook bevestigd in de ICO-richtsnoeren over de toepassing van vrijstellingen inzake nationale veiligheid ([115]).

(76) Bovendien kan op basis van de wijzigingen die zijn ingevoerd door de Data (Use and Access) Act ([116]) een specifieke verwerkingsactiviteit door autoriteiten die bevoegd zijn voor strafrechthandhaving ook worden geregeld door de bepalingen van deel 4 van de DPA 2018, wat normaal gesproken alleen van toepassing is op de verwerking van gegevens door nationale veiligheidsdiensten.

([111]) Bij artikel 69 van de Data (Use and Access) Act worden de definitie van toestemming en de voorwaarden voor het beroep op toestemming opgenomen, zoals bepaald in artikel 4, lid 11, en artikel 7 van de UK GDPR (die een afspiegeling zijn van de overeenkomstige bepalingen in Verordening (EU) 2016/679), als nieuwe artikelen 33, lid 1A, en 40A in de DPA 2018, waardoor het begrip toestemming en de voorwaarden voor het beroep op toestemming worden verduidelijkt wanneer deze worden gebruikt als rechtsgrondslag voor de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op strafrechthandhaving. Bovendien wordt in artikel 71, leden 7 en 8, van de Data (Use and Access) Act de formulering van artikel 36, lid 1, van de DPA 2018 enigszins verduidelijkt. Ten slotte worden, in voorkomend geval, wijzigingen in de UK GDPR door de Data (Use and Access) Act, zoals beschreven in deel 2, ook weerspiegeld in deel 3 van de DPA 2018, zie bijvoorbeeld artikel 74, leden 2 tot en met 5, over de verwerking van gevoelige gegevens, artikel 76, leden 4 tot en met 6, over de termijnen voor het beantwoorden van verzoeken van betrokkenen, artikel 78, leden 2 en 3, over het zoeken naar gegevens in verband met verzoeken van betrokkenen en artikel 80, leden 3 tot en met 5, over geautomatiseerde besluitvorming.

([112]) Artikel 78A, lid 1, van de DPA 2018, zoals ingevoerd bij artikel 88, van de Data (Use and Access) Act. Overeenkomstig artikel 78A, leden 2-4, van de DPA 2018 maakt de vrijstelling het mogelijk om geen uitvoering te geven aan de gegevensbeschermingsbeginselen (met uitzondering van het beginsel van rechtmatigheid en de voorwaarden en waarborgen voor de verwerking van gevoelige gegevens), de individuele rechten, de verplichtingen van verwerkingsverantwoordelijken en verwerkers met betrekking tot inbreuken op gegevens, bepaalde delen van de regels inzake internationale gegevensdoorgiften en sommige bevoegdheden van de Information Commissioner om inspecties uit te voeren en handhavingsmaatregelen te nemen.

([113]) Zie *Baker/Secretary of State for the Home Department* [2001] UKIT NSA2 (*"Baker/Secretary of State"*).

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

([115]) Zie de ICO-richtsnoeren over de vrijstelling inzake de nationale veiligheid en defensie, beschikbaar op: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/national-security-and-defence-exemption-a-guide.

([116]) Artikelen 89 tot en met 90 van de Data (Use and Access) Act.

(77) Hoewel de gegevensbeschermingsregeling voor verwerking in het kader van de nationale veiligheid in bepaalde situaties dus ook wordt uitgebreid tot gegevensverwerking door strafrechtelijke autoriteiten, is dit alleen het geval in specifieke omstandigheden en onder strikte voorwaarden en waarborgen, d.w.z. indien i) een bevoegde autoriteit wordt aangemerkt als "gekwalificeerde bevoegde autoriteit" in regelingen van de Secretary of State die parlementaire goedkeuring vereisen ([117]), en ii) de Secretary of State door middel van een kennisgeving een specifieke verwerkingsactiviteit aanwijst die door de gekwalificeerde bevoegde autoriteit wordt uitgevoerd. Belangrijk is dat een dergelijke aanwijzing alleen kan plaatsvinden als de Secretary of State van oordeel is dat de aanwijzing van de verwerkingsactiviteit noodzakelijk is voor het waarborgen van de nationale veiligheid, d.w.z. wanneer een strafrechtelijke handhavingsinstantie optreedt met het oog op de nationale veiligheid en de verwerkingsactiviteit wordt uitgevoerd door de bevoegde autoriteit als gezamenlijke verwerkingsverantwoordelijke met ten minste één inlichtingendienst ([118]). Als extra waarborg moet de Secretary of State de Commissioner raadplegen alvorens een aanwijzingsbericht ([119]) te geven; de tekst van het bericht moet in principe worden gepubliceerd ([120]), en een persoon die rechtstreeks door een aanwijzingsbericht wordt getroffen, kan om rechterlijke toetsing verzoeken ([121]). Deze wijziging heeft dan ook hoofdzakelijk tot doel te verduidelijken dat wanneer de autoriteiten van het Verenigd Koninkrijk bevoegdheden hebben op het gebied van zowel rechtshandhaving als nationale veiligheid, en gegevens verwerken in het kader van hun laatstgenoemde verantwoordelijkheden, de gegevensbeschermingsregeling voor nationale veiligheidsdiensten van toepassing kan zijn.

(78) In deel 4 van de DPA 2018 wordt de gegevensverwerking door de inlichtingendiensten van het Verenigd Koninkrijk geregeld. Het bevat nog steeds de belangrijkste beginselen inzake gegevensbescherming, legt voorwaarden op voor de verwerking van bijzondere categorieën gegevens, voorziet in rechten voor betrokkenen, vereist gegevensbescherming door ontwerp en regelt de doorgifte van persoonsgegevens, zoals beschreven in de overwegingen 125 tot en met 132 van Uitvoeringsbesluit (EU) 2021/1772.

(79) De wijzigingen die door de Data (Use and Access) Act in deze regeling zijn ingevoerd, zijn beperkt. Wat betreft het recht op toegang van de betrokkenen zoals bepaald in artikel 94 van de DPA 2018, wordt met de Data (Use and Access) Act een nieuwe subparagraaf 2A ingevoerd, waarin wordt verduidelijkt dat de betrokkene alleen recht heeft op de relevante informatie voor zover de verwerkingsverantwoordelijke deze kan verstrekken op basis van een redelijk en evenredig onderzoek ([122]). Zoals uiteengezet in overweging 35 kadert deze wijziging het recht van toegang op basis van vastgestelde wettelijke normen, waarbij ook rekening wordt gehouden met de belangen van de betrokkene. Op het gebied van geautomatiseerde besluitvorming blijft het voor verwerkingsverantwoordelijken verboden om een besluit te nemen dat aanzienlijke gevolgen heeft voor een betrokkene en dat uitsluitend is gebaseerd op geautomatiseerde verwerking van persoonsgegevens met betrekking tot de betrokkene, tenzij een dergelijk besluit wettelijk verplicht of toegestaan is, de betrokkene toestemming heeft gegeven voor het nemen van het besluit op die basis of het besluit wordt genomen in het kader van een overeenkomst ([123]); met de Data (Use and Access) Act wordt in deel 4 van de DPA 2018 ([124]) dezelfde definitie van het begrip "besluiten die uitsluitend op geautomatiseerde verwerking zijn gebaseerd" opgenomen als in artikel 22A van de UK GDPR en geanalyseerd in overweging 53 van dit besluit.

3.2. **Relevante ontwikkelingen betreffende toegang van en gebruik door de Britse overheidsdiensten met het oog op strafrechtshandhaving**

(80) In de Britse wet worden nog steeds belangrijke beperkingen opgelegd aan de toegang tot en het gebruik van persoonsgegevens met het oog op strafrechtshandhaving, en worden toezichts- en verhaalsmechanismen op dit gebied geboden, zoals geanalyseerd in de overwegingen 134 tot en met 174 van Uitvoeringsbesluit (EU) 2021/1772.

([117]) Artikel 82, leden A1, 2A en 4, van de DPA 2018, zoals ingevoerd bij artikel 89, lid 2, van de Data (Use and Access) Act.

([118]) Artikel 82A, leden 1 en 2, zoals ingevoerd bij artikel 89, lid 3, van de Data (Use and Access) Act. Als extra waarborg moet de Secretary of State de Commissioner raadplegen alvorens een aanwijzingsbericht te geven; zie het nieuwe artikel 82A, lid 8, van de DPA 2018; de tekst van de kennisgeving moet in principe worden gepubliceerd, zie het nieuwe artikel 82D, lid 1, onder voorbehoud van de uitzonderingen die zijn vastgelegd in het nieuwe artikel 82D, lid 3, van de DPA 2018, en een persoon die rechtstreeks door een aanwijzingsbericht wordt getroffen, kan om rechterlijke toetsing verzoeken, zie het nieuwe artikel 82E van de DPA 2018.

([119]) Artikel 82A, lid 8, van de DPA 2018.

([120]) Artikel 82D, lid 1, met inachtneming van de vrijstellingen in het nieuwe artikel 82D, lid 3, van de DPA 2018.

([121]) Artikel 82E van de DPA 2018.

([122]) Artikel 78, lid 4, van de Data (Use and Access) Act.

([123]) Artikel 96 van de DPA 2018.

([124]) Op grond van het nieuwe artikel 96, lid 4, van de DPA 2018 is een besluit gebaseerd op volledig geautomatiseerde verwerking indien het besluitvormingsproces een persoon geen mogelijkheid biedt om het besluit te aanvaarden, te verwerpen of te beïnvloeden. Zie artikel 80, lid 4, punt c), van de Data (Use and Access) Act.

3.2.1. *Rechtsgrondslag en toepasselijke beperkingen/waarborgen*

(81) Het verzamelen van persoonsgegevens van ondernemers in het Verenigd Koninkrijk met het oog op strafrechtshandhaving blijft toegestaan in de Britse rechtsorde op basis van huiszoekingsbevelen en bevelen tot overlegging, met inachtneming van de voorwaarden en waarborgen die zijn beschreven in de overwegingen 135 tot en met 138 van Uitvoeringsbesluit (EU) 2021/1772.

(82) Met de National Security Act 2023 ([125]), die tot doel heeft bedreigingen voor de nationale veiligheid door spionage, sabotage en personen die voor buitenlandse mogendheden handelen, aan te pakken, zijn daarnaast nieuwe bevoegdheden tot het betreden en doorzoeken van plaatsen en het in beslag nemen van voorwerpen voor de Britse politie ingevoerd, waaronder de mogelijkheid om persoonsgegevens te verkrijgen wanneer er redelijke gronden zijn om te vermoeden dat er materiaal zal worden verkregen dat waarschijnlijk bewijs vormt dat ernstigere overtredingen of buitenlandse dreigingsactiviteiten onder de National Security Act 2023 zijn gepleegd of op het punt staan te worden gepleegd ([126]). Deze bevoegdheden zijn onderworpen aan voorwaarden en waarborgen die vergelijkbaar zijn met die welke in Uitvoeringsbesluit (EU) 2021/1772 zijn geanalyseerd voor de op dat moment bestaande bevoegdheden. Het gebruik ervan moet met name worden toegestaan door middel van een bevelschrift, bevel tot overlegging of een bevel tot uitlegging uitgevaardigd door een onafhankelijke rechterlijke instantie, op verzoek van de politieambtenaar/opsporingsambtenaar ([127]). Er bestaan specifieke beschermingsmaatregelen voor vertrouwelijk materiaal, zoals journalistiek materiaal en zaken die onder het wettelijk verschoningsrecht vallen ([128]). Evenzo moet het uitvaardigen van bevelen tot openbaarmaking ([129]), bevelen tot verstrekking van klantinformatie ([130]) en bevelen tot rekeningcontrole ([131]), die eveneens zijn ingesteld bij de National Security Act 2023, worden goedgekeurd door een rechter op verzoek van een bevoegde ambtenaar, en is het onderworpen aan specifieke voorwaarden en waarborgen, waaronder dat het bevel wordt aangevraagd met betrekking tot een specifieke persoon, met het oog op een onderzoek naar dreigende activiteiten van een vreemde mogendheid, dat het bevel de doeltreffendheid van het onderzoek zal vergroten, en dat het niet wordt gebruikt om informatie te verkrijgen die wettelijk vertrouwelijk is of anderszins is uitgesloten, zoals journalistiek materiaal en bepaalde medische dossiers ([132]).

(83) Zoals beschreven in de overwegingen 139-141 van Uitvoeringsbesluit (EU) 2021/1772, kunnen in het rechtskader van het Verenigd Koninkrijk specifieke rechtshandhavingsinstanties, bijvoorbeeld het National Crime Agency of de Metropolitan Police Service, ook gebruikmaken van gerichte onderzoeksbevoegdheden op grond van de Investigatory Powers Act 2016 (IPA 2016) ([133]) om ernstige misdrijven te voorkomen of op te sporen. De specifieke onderzoeksbevoegdheden waarvan die rechtshandhavingsinstanties gebruik kunnen maken, zijn: gerichte intercepties (deel 2 van de IPA 2016), verkrijging van communicatiegegevens (deel 3 van de IPA 2016) en gerichte materiële interferentie (deel 5 van de IPA 2016). Wanneer de Secretary of State op grond van deel 4 van de IPA 2016 aanzeggingen tot bewaring doet, kunnen wetshandhavingsinstanties ook profiteren van de toegang tot de bewaarde communicatiegegevens via de bevoegdheden tot het verkrijgen van communicatiegegevens op grond van deel 3 van de IPA 2016.

([125]) Beschikbaar via de volgende link: https://www.legislation.gov.uk/ukpga/2023/32/contents/enacted.

([126]) Bijlage 2 bij de National Security Act 2023. Relevante overtredingen op grond van de National Security Act 2023 zijn bijvoorbeeld het verkrijgen of openbaar maken van beschermde informatie (artikel 1), het verkrijgen of openbaar maken van bedrijfsgeheimen (artikel 3), het assisteren van een buitenlandse inlichtingendienst (artikel 4), het plegen van sabotage (artikel 12) of het verrichten van specifiek verboden handelingen voor een vreemde mogendheid met de bedoeling een verstorend effect teweeg te brengen (artikel 13).

([127]) Zie paragraaf 2, lid 1, paragraaf 3, lid 1, paragraaf 4, lid 1, en paragraaf 10, lid 1, van bijlage 2 bij de National Security Act 2023.

([128]) Zie paragraaf 2, lid 4, punt b), paragraaf 3, lid 4, punten b en c), paragraaf 4, lid 4, punt b), en paragraaf 10, lid 1, van bijlage 2 bij de National Security Act 2023.

([129]) Op grond van bevelen tot openbaarmaking krachtens bijlage 3 bij de National Security Act 2023 kan een ambtenaar een persoon dwingen om informatie te verstrekken, documenten over te leggen en/of vragen te beantwoorden die relevant zijn voor een onderzoek naar eigendommen die verband houden met activiteiten die een bedreiging vormen voor de nationale veiligheid, met inbegrip van de verplaatsing of het gebruik van die eigendommen.

([130]) Op grond van bijlage 4 bij de National Security Act 2023 kan een ambtenaar een financiële instelling verzoeken om alle klantgegevens met betrekking tot een bepaalde persoon te verstrekken.

([131]) Op grond van bevelen tot rekeningcontrole krachtens bijlage 5 kan een financiële instelling worden verplicht om de in het bevel gespecificeerde informatie te verstrekken aan een functionaris voor de in het bevel gespecificeerde periode en op de in het bevel gespecificeerde wijze, die niet langer mag zijn dan negentig dagen.

([132]) Bijlage 3, paragraaf 2, lid 1, bijlage 4, paragraaf 1, bijlage 5, paragraaf 1, bij de National Security Act 2023.

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

(84) Sinds de vaststelling van Uitvoeringsbesluit (EU) 2021/1772 voorziet de IPA 2016, samen met de Regulation of Investigatory Powers Act 2000 (RIPA) voor Engeland, Wales en Noord-Ierland en de Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) voor Schotland, in de rechtsgrondslag en de toepasselijke beperkingen en waarborgen voor het gebruik van dergelijke bevoegdheden, zoals beschreven in Uitvoeringsbesluit (EU) 2021/1772. Belangrijk is dat volgens het rechtskader de autoriteiten voor de uitoefening van deze bevoegdheden nog steeds een bevel ([134]) moeten verkrijgen dat is uitgevaardigd door een bevoegde autoriteit ([135]) en goedgekeurd door een onafhankelijke Judicial Commissioner (rechterlijke toezichthouder) ([136]) (de zogenaamde "double-lock"-procedure). De verkrijging van een dergelijk bevel is nog steeds onderworpen aan een noodzakelijkheids- en evenredigheidstoets ([137]).

(85) Tegelijkertijd zijn sinds de goedkeuring van Uitvoeringsbesluit (EU) 2021/1772 bepaalde specifieke elementen van de IPA 2016 gewijzigd door de Investigatory Powers (Amendment) Act 2024, die in april 2024 koninklijke goedkeuring kreeg ([138]). Voor zover deze wijzigingen en andere relevante ontwikkelingen betrekking hebben op de voorwaarden, beperkingen en waarborgen rond het gebruik van de bovengenoemde specifieke onderzoeksbevoegdheden door overheidsinstanties in het Verenigd Koninkrijk met het oog op strafrechthandhaving, zoals beoordeeld in de overwegingen 177 tot en met 215 van Uitvoeringsbesluit (EU) 2021/1772, worden zij in de volgende punten geanalyseerd. Wat betreft de elementen van het kader van het Verenigd Koninkrijk die niet door bovengenoemde wet zijn gewijzigd of door andere relevante ontwikkelingen zijn beïnvloed, blijft de analyse in Uitvoeringsbesluit (EU) 2021/1772 geldig.

(86) Wat het gericht verzamelen en bewaren van communicatiegegevens ([139]) betreft, blijven de voorwaarden en waarborgen voor deze bevoegdheden, zoals beoordeeld in Uitvoeringsbesluit (EU) 2021/1772, van kracht. Met de Investigatory Powers (Amendment) Act 2024 werden de bestaande waarborgen verduidelijkt door in artikel 11 van de IPA 2016 (dat het onrechtmatig verkrijgen van communicatiegegevens van een telecommunicatie-exploitant strafbaar stelt) een lijst op te nemen met voorbeelden van wat onder "wettelijke bevoegdheid" in die bepaling wordt verstaan ([140]). Bovendien werd in de Investigatory Powers (Amendment) Act 2024 de definitie van communicatiegegevens in artikel 261 van de IPA 2016 verder verduidelijkt door expliciet te specificeren dat abonneegegevens als communicatiegegevens worden beschouwd ([141]).

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

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

([136]) De Judicial Commissioners staan de Investigatory Powers Commissioner (toezichthouder voor onderzoeksbevoegdheden, IPC) bij, een onafhankelijk orgaan dat toezicht houdt op het gebruik van onderzoeksbevoegdheden door inlichtingendiensten.

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

([138]) Beschikbaar via de volgende link: https://www.legislation.gov.uk/ukpga/2024/9/contents/2025-04-25.

([139]) De term "communicatiegegevens" heeft betrekking op het "wie", "wanneer", "waar" en "hoe" van een communicatie, maar niet op de inhoud, d.w.z. wat er is gezegd of geschreven. Communicatiegegevens kunnen onder meer bestaan uit het tijdstip en de duur van de communicatie, het nummer of het e-mailadres van de afzender en de ontvanger en soms de locatie van de apparaten vanaf welke de telecommunicatie is uitgegaan; zie artikel 261, lid 5, van de IPA 2016. De IPA 2016 staat de Secretary of State toe om telecommunicatie-exploitanten ertoe te verplichten communicatiegegevens te bewaren voor gerichte toegang door diverse overheidsinstanties, met inbegrip van rechtshandhavingsinstanties en inlichtingendiensten. Deel 4 van de IPA 2016 voorziet in de bewaring van communicatiegegevens, terwijl deel 3 voorziet in de gerichte verkrijging van communicatiegegevens. In de delen 3 en 4 van de IPA 2016 worden ook specifieke beperkingen van de uitoefening van deze bevoegdheden uiteengezet en zijn specifieke waarborgen opgenomen.

([140]) Bijvoorbeeld, wanneer de betrokken persoon de communicatiegegevens verkrijgt in het kader van de uitoefening van een wettelijke bevoegdheid van de betrokken overheidsinstantie of wanneer de communicatiegegevens worden verkregen op grond van een gerechtelijk bevel of een andere gerechtelijke machtiging. Artikel 11, lid 3A, van de IPA 2016, zoals ingevoerd bij artikel 12, lid 3, van de Investigatory Powers (Amendment) Act 2024.

([141]) Artikel 261, leden 5A en 5B, zoals ingevoerd bij artikel 13, lid 3, van de Investigatory Powers (Amendment) Act 2024.

(87) Het uitvaardigen van bevelen tot het bewaren van communicatiegegevens ([142]) is nog steeds onderworpen aan beperkingen en waarborgen, zoals beschreven in de overwegingen 208 en 209 van Uitvoeringsbesluit (EU) 2021/1772, met name vereisten inzake noodzakelijkheid en evenredigheid en goedkeuring door een onafhankelijke Judicial Commissioner. Hoewel met de Investigatory Powers (Amendment) Act 2024 de mogelijkheid werd ingevoerd om dergelijke kennisgevingen te verlengen, is elke verlenging onderworpen aan dezelfde voorwaarden van noodzakelijkheid en evenredigheid en moet deze worden goedgekeurd door de Judicial Commissioner ([143]).

(88) Wat communicatiegegevens betreft, is met de Investigatory Powers (Amendment) Act 2024 ook de definitie van telecommunicatie-exploitant, d.w.z. de mogelijke adressaten van een aanzegging tot bewaring, gewijzigd. Deze definitie omvat nu elke persoon die "een telecommunicatiesysteem beheert of aanbiedt dat i) zich niet (geheel of gedeeltelijk) in het Verenigd Koninkrijk bevindt of vanuit het Verenigd Koninkrijk wordt beheerd en ii) door een andere persoon wordt gebruikt om telecommunicatiediensten aan te bieden of te leveren aan personen in het Verenigd Koninkrijk" ([144]). Belangrijk is dat de gewijzigde definitie steeds een nauwe band met de markt van het Verenigd Koninkrijk vereist. De wijziging verduidelijkt dus dat grote ondernemingen met een complexe bedrijfsstructuur in hun geheel onder de IPA 2016 vallen, zonder dat de reikwijdte van de definitie wordt uitgebreid tot aanbieders van telecommunicatiediensten die niet gericht zijn op personen in het Verenigd Koninkrijk. Dit wordt ook bevestigd door de toelichting bij de Investigatory Powers (Amendment) Act 2024, waarin is uiteengezet dat deze wijziging niet is bedoeld om extra bedrijven onder de werkingssfeer van de relevante bevoegdheden van de IPA 2016 ([145]) te brengen, maar dat zij in wezen een verduidelijkende functie heeft.

(89) Ten slotte werden met de Investigatory Powers (Amendment) Act 2024 enkele gerichte wijzigingen aangebracht in de procedure voor het uitvaardigen van bevelen, onder meer met betrekking tot gerichte interceptie en gerichte apparatuurinterferentie, d.w.z. bevoegdheden die ook door specifieke rechtshandhavingsinstanties in het Verenigd Koninkrijk kunnen worden gebruikt om ernstige misdrijven te voorkomen of op te sporen. De wijzigingen hebben alleen betrekking op de specifieke situatie waarin deze bevoegdheden worden gebruikt om communicatiegegevens of privéinformatie op te vragen over een persoon die lid is van een relevante wetgevende instantie ([146]). Hoewel bevelen met betrekking tot gerichte interceptie en apparatuurinterferentie normaal gesproken kunnen worden uitgevaardigd door de Secretary of State en worden goedgekeurd door een Judicial Commissioner (zie overwegingen 186 tot en met 196 en overwegingen 210 tot en met 215 van Uitvoeringsbesluit (EU) 2021/1772), vereisen de artikelen 26 en 111 van de IPA bovendien goedkeuring door de premier wanneer het bevel betrekking heeft op een lid van het parlement of een andere relevante wetgevende instantie (de zogenaamde "triple-lock"-procedure). Op grond van de Investigatory Powers (Amendment) Act 2024 kan de premier nu vijf Secretaries of State aanwijzen die bevoegd zijn om de bevoegdheid van de premier om deze bevelen goed te keuren uit te oefenen, mits de noodzaak van toestemming dringend is en de premier niet in staat is om toestemming te verlenen vanwege medische ongeschiktheid of gebrek aan toegang tot beveiligde communicatie. Belangrijk is dat de beperkingen en waarborgen met betrekking tot de uitvaardiging van deze bevelen, zoals beschreven in de bovengenoemde overwegingen van Uitvoeringsbesluit (EU) 2021/1772, van kracht blijven.

3.2.2. *Verder gebruik van de verzamelde informatie*

(90) Het delen van gegevens door een rechtshandhavingsinstantie met een andere instantie voor andere doeleinden dan die waarvoor zij oorspronkelijk zijn verzameld (de zogenaamde "verdere doorgifte"), is nog steeds onderworpen aan de voorwaarden die worden geanalyseerd in de overwegingen 142 tot en met 156 van Uitvoeringsbesluit (EU) 2021/1772.

([142]) De uitvaardiging van dergelijke aanzeggingen tot bewaring op grond van de artikelen 87 tot en met 89 van de IPA 2016, moet ervoor zorgen dat telecommunicatie-exploitanten relevante communicatiegegevens, die als zij niet langer vereist zijn voor zakelijke doeleinden, anders zouden worden gewist, maximaal twaalf maanden bewaren. De bewaarde gegevens moeten gedurende de vereiste periode beschikbaar zijn mocht het vervolgens voor een overheidsinstantie nodig zijn om deze te verkrijgen in het kader van een toestemming voor een gerichte verkrijging van communicatiegegevens zoals bedoeld in deel 3 van de IPA 2016.

([143]) Artikel 94A van de IPA 2016, zoals ingevoerd bij artikel 20, lid 4, van de Investigatory Powers (Amendment) Act 2024.

([144]) Artikel 261, lid 10, punt c), van de IPA 2016, zoals gewijzigd bij artikel 19 van de Investigatory Powers (Amendment) Act 2024.

([145]) Toelichting bij de Investigatory Powers (Amendment) Act 2024, punt 359, beschikbaar via de volgende link: https://www.legislation.gov.uk/ukpga/2024/9/pdfs/ukpgaen_20240009_en.pdf.

([146]) Zie de artikelen 26 en 111 van de IPA 2016.

(91) Wat de specifieke situatie van verdere doorgifte van gegevens vanuit het Verenigd Koninkrijk naar de Verenigde Staten betreft, is de "Overeenkomst tussen de regering van het Verenigd Koninkrijk van Groot-Brittannië en Noord-Ierland en de regering van de Verenigde Staten van Amerika inzake de toegang tot elektronische gegevens met het oog op de bestrijding van zware criminaliteit (de UK-US Agreement)" ([147]), die in oktober 2019 is gesloten, in werking getreden en wordt sinds oktober 2022 toegepast. In het kader van de UK-US Agreement kunnen gegevens die vanuit de EU aan dienstverleners in het Verenigd Koninkrijk worden doorgegeven, worden onderworpen aan bevelen tot overlegging van bewijsmateriaal die door bevoegde rechtshandhavingsinstanties in de VS zijn uitgevaardigd en in het Verenigd Koninkrijk van toepassing worden verklaard.

(92) Belangrijk is dat de voorwaarden en waarborgen waaronder dergelijke bevelen kunnen worden uitgevaardigd en uitgevoerd, zoals beoordeeld in overweging 154 van Uitvoeringsbesluit (EU) 2021/1772, van toepassing blijven. Met name gegevens die in het kader van de overeenkomst worden verkregen, genieten een bescherming die gelijkwaardig is aan de specifieke waarborgen die worden geboden door de zogenaamde "raamovereenkomst tussen de EU en de VS" ([148]), die allemaal door middel van verwijzing mutatis mutandis in de UK-US Agreement zijn opgenomen ([149]).

(93) Sinds de vaststelling van Uitvoeringsbesluit (EU) 2021/1772 heeft het Verenigd Koninkrijk verduidelijkt, onder meer via overleg met de desbetreffende partijen in het kader van de uitvoering van de UK-US Agreement, hoe de specifieke waarborgen van de raamovereenkomst, die zijn bedoeld voor samenwerking tussen rechtshandhavingsinstanties, worden aangepast en toegepast op de specifieke doorgiften die onder de overeenkomst tussen het UK-US Agreement vallen. Het Verenigd Koninkrijk heeft met name verklaard dat de bepalingen van de raamovereenkomst die voorzien in een rol voor de relevante bevoegde autoriteit (die niet bestaat in een situatie van directe samenwerking tussen een Britse dienstverlener en een rechtshandhavingsinstantie in de VS) mutatis mutandis worden geïnterpreteerd als een verwijzing naar de aangewezen autoriteit (zoals gedefinieerd in de UK-US Agreement) ([150]) van de relevante partij.

(94) Wat bijvoorbeeld de kennisgeving van een informatiebeveiligingsincident overeenkomstig artikel 10 van de raamovereenkomst tussen de EU en de VS betreft, waarin een kennisgeving aan de bevoegde autoriteit die de gegevens doorgeeft, wordt vereist, heeft het Verenigd Koninkrijk verklaard dat deze bepaling mutatis mutandis wordt toegepast, wat betekent dat de kennisgeving moet worden gedaan aan de aangewezen autoriteit van de partij van waaruit de gegevens zijn doorgegeven.

(95) Met betrekking tot de toestemming van de overdragende bevoegde autoriteit voorafgaand aan elke verdere doorgifte van persoonsgegevens overeenkomstig artikel 7 van de raamovereenkomst, heeft het Verenigd Koninkrijk verklaard dat het deze bepaling mutatis mutandis zal toepassen, wat betekent dat de aangewezen autoriteit van de partij van waaruit de gegevens zijn doorgegeven, toestemming moet verlenen voor elke verdere doorgifte.

(96) Met betrekking tot de verplichtingen uit hoofde van artikel 8 van de raamovereenkomst inzake het handhaven van de kwaliteit en integriteit van informatie, zou een mutatis mutandis interpretatie van de bepaling de aangewezen autoriteit van de partij die de gegevens ontvangt, verantwoordelijk maken voor het onderhouden van contacten met de aanbieder die de gegevens heeft overgedragen in geval van problemen met betrekking tot de kwaliteit en integriteit van de gegevens.

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

([148]) Overeenkomst tussen de Verenigde Staten van Amerika en de Europese Unie over de bescherming van persoonlijke informatie in verband met de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten (PB L 336 van 10.12.2016, blz. 3, ELI: http://data.europa.eu/eli/agree_internation/2016/2220/oj).

([149]) Artikel 9, lid 1, van de overeenkomst.

([150]) Overeenkomstig artikel 1, lid 8, van de UK-US Agreement wordt onder "aangewezen autoriteit" verstaan de overheidsinstantie die voor het Verenigd Koninkrijk is aangewezen door de Secretary of State voor binnenlandse zaken, en voor de Verenigde Staten door de Attorney General.

(97) Wat beroep in rechte betreft, heeft het Verenigd Koninkrijk benadrukt dat bij overdrachten in het kader van de UK-US Agreement altijd de aangewezen autoriteit van elke partij betrokken zal zijn. Wanneer de VS de partij is die gegevens ontvangt van dienstverleners in het Verenigd Koninkrijk, treedt het Amerikaanse ministerie van Justitie op als aangewezen autoriteit. Volgens de interpretatie van het Verenigd Koninkrijk zal bij elk verzoek dat op basis van de UK-US Agreement wordt ingediend, het ministerie van Justitie betrokken zijn als federale autoriteit die is aangewezen op grond van de Amerikaanse Judicial Redress Act, en kan dus overeenkomstig artikel 19 van de raamovereenkomst beroep in rechte worden ingesteld tegen het Amerikaanse ministerie van Justitie. Bovendien heeft het Verenigd Koninkrijk tegenover de diensten van de Commissie bevestigd dat de Judicial Redress Act niet het enige mechanisme is om verhaal te halen. Afhankelijk van de omstandigheden en context van het specifieke geval bieden andere toepasselijke Amerikaanse wetten alternatieve wegen waarlangs beroep in rechte kan worden ingesteld.

3.2.3. *Toezicht en verhaal*

(98) Afhankelijk van de bevoegdheden die de bevoegde autoriteiten gebruiken bij de verwerking van persoonsgegevens voor rechtshandhavingsdoeleinden (hetzij op grond van de DPA 2018, hetzij op grond van de IPA 2016), blijven verschillende instanties toezicht houden op het gebruik van deze bevoegdheden, zoals beoordeeld in de overwegingen 158 tot en met 174 van Uitvoeringsbesluit (EU) 2021/1772, en blijven er rechtsmiddelen beschikbaar op grond van deel 3 van de DPA 2018, de IPA 2016 en de Human Rights Act 1998, zoals geanalyseerd in de overwegingen 250 tot en met 269 van Uitvoeringsbesluit (EU) 2021/1772.

(99) Wat het toezicht op deel 3 van de DPA 2018 betreft, worden de taken en bevoegdheden van de Information Commission geanalyseerd in de overwegingen 158 tot en met 160 en overweging 162 van Uitvoeringsbesluit (EU) 2021/1772, onder voorbehoud van de wijzigingen die zijn aangebracht door de Data (Use and Access) Act, zoals beschreven in de punten 2.3.1 en 2.3.2 van dit besluit.

(100) Wat de uitoefening van deze bevoegdheden betreft, heeft de Information Commissioner sinds de vaststelling van Uitvoeringsbesluit (EU) 2021/1772 talrijke klachten ([151]) in behandeling genomen, verschillende onderzoeken uitgevoerd en handhavingsmaatregelen genomen met betrekking tot de verwerking van gegevens door rechtshandhavingsautoriteiten. Tussen 2021 en 2025 heeft de Information Commissioner onderzoeken uitgevoerd en verschillende politie-instanties berispt wegens verschillende gevallen van niet-naleving van hun verplichtingen op het gebied van gegevensbescherming, bijvoorbeeld bij het reageren op verzoeken om toegang tot gegevens, bij het treffen van beveiligingsmaatregelen voor videobewakingsgegevens, bij het omgaan met gevoelige strafregisters, bij het samenvoegen van gegevens van verschillende personen of bij het verstrekken van persoonsgegevens aan derden ([152]). De Information Commissioner heeft ook richtsnoeren, adviezen en begeleidende documenten uitgevaardigd, bijvoorbeeld over het recht op toegang of over de behandeling van kennelijk ongegronde of buitensporige verzoeken op grond van deel 3 van de DPA 2018 ([153]).

(101) Wat het gebruik van onderzoeksbevoegdheden op grond van de IPA 2016 betreft, blijft onafhankelijk en gerechtelijk toezicht gewaarborgd door de Investigatory Powers Commissioner (IPC), bijgestaan door andere Judicial Commissioners, die gezamenlijk Judicial Commissioners worden genoemd ([154]). Op dit gebied zijn met de Investigatory Powers (Amendments) Act 2024 slechts beperkte en gerichte wijzigingen aangebracht, die geen invloed hebben op de onafhankelijkheid, taken en bevoegdheden van de Judicial Commissioners, maar die gericht zijn op het versterken van de werking in de praktijk van de bestaande toezichtsregeling, met name door de invoering van plaatsvervangende IPC's aan wie de IPC specifieke bevoegdheden kan delegeren wanneer zij niet in staat of beschikbaar zijn om hun taken uit te voeren. Dergelijke plaatsvervangende IPC's moeten Judicial Commissioners zijn en worden benoemd door de IPC ([155]).

([151]) Zo ontving de Information Commission in 2023-24 1 890 klachten op basis van de UK GDPR en/of de DPA 2018 over organisaties binnen de subsectoren "Police Authority", "Police Forces" en "Police Commissioners". Zie ook het jaarverslag en de jaarrekening 2023-24 van de Information Commissioner, beschikbaar via de volgende link: https://ico.org.uk/media2/migrated/4030348/annual-report-2023-24.pdf.

([152]) Meer informatie is beschikbaar via de volgende link: https://ico.org.uk/action-weve-taken/enforcement/?ensector=criminal-justice.

([153]) Beschikbaar via de volgende link: https://ico.org.uk/for-organisations/law-enforcement/the-right-of-access-part-3-of-the-dpa-2018/ en https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/individual-rights/manifestly-unfounded-and-excessive-requests/.

([154]) Zie overweging 250 van Uitvoeringsbesluit (EU) 2021/1772.

([155]) Artikel 227 van de IPA 2016, zoals ingevoerd bij artikel 7 van de Investigatory Powers (Amendment) Act.

3.3. **Relevante ontwikkelingen betreffende toegang van en gebruik door Britse overheidsdiensten ten behoeve van de nationale veiligheid**

(102) Wat de onderzoeksbevoegdheden in verband met de nationale veiligheid betreft, blijft de IPA 2016 het rechtskader voor het gebruik van deze bevoegdheden. Naast de wijzigingen met betrekking tot gerichte onderzoeksbevoegdheden waarop, onder bepaalde voorwaarden, ook bepaalde rechtshandhavingsinstanties een beroep kunnen doen, zoals beschreven in de overwegingen 77 tot en met 85 van dit besluit, zijn met de Investigatory Powers (Amendment) Act 2024 ook wijzigingen aangebracht in een van de bevoegdheden van de IPA 2016 die op grote schaal kunnen worden uitgeoefend.

(103) Meer bepaald heeft de Investigatory Powers (Amendment) Act 2024 in het nieuwe deel 7A van de IPA 2016 een specifieke regeling ingevoerd voor het bewaren en onderzoeken van een specifieke subset van bulkdatasets met persoonsgegevens ([156]), d.w.z. voor die datasets waarvan de personen op wie de persoonsgegevens betrekking hebben, geen of slechts een geringe redelijke verwachting van privacy met betrekking tot de gegevens kunnen hebben ([157]). Of een bulkdataset met persoonsgegevens deel uitmaakt van deze specifieke subset van datasets, wordt bepaald door het hoofd van een inlichtingendienst op basis van alle omstandigheden, met name i) de aard van de gegevens, ii) de mate waarin de gegevens door de betrokken personen openbaar zijn gemaakt of de betrokken personen hebben ingestemd met het openbaar maken van de gegevens, iii) indien de gegevens zijn gepubliceerd, de mate waarin zij zijn gepubliceerd onder redactioneel toezicht of door een persoon die handelt in overeenstemming met professionele normen, iv) indien de gegevens zijn gepubliceerd of anderszins in het publieke domein zijn, de mate waarin de gegevens algemeen bekend zijn en v) de mate waarin de gegevens reeds in het publieke domein zijn gebruikt ([158]).

(104) Belangrijk is dat voor het bewaren en onderzoeken van bulkdatasets met persoonsgegevens die niet onder deze categorie vallen, d.w.z. datasets die gevoeliger zijn en daarom een redelijke verwachting van privacy met zich meebrengen, de in de overwegingen 239 en 240 van Uitvoeringsbesluit (EU) 2021/1772 beoordeelde regeling van kracht blijft, met name de noodzaak van een bevel dat eerst door de Secretary of State en vervolgens door de Judicial Commissioner wordt goedgekeurd, met inachtneming van de vereisten van noodzakelijkheid en evenredigheid van de maatregel, zoals bepaald in deel 7 van de IPA 2016 ([159]).

(105) Deel 7A van de IPA 2016 voorziet in twee soorten toelatingen: individuele toelating en categorietoelating. Het bewaren, of het bewaren en onderzoeken, van elke bulkdataset met persoonsgegevens die op grond van deel 7A wordt bewaard, moet worden goedgekeurd op grond van een van deze toelatingen. Voor beide toelatingen is in principe ([160]) een toelating van het hoofd van de inlichtingendienst (of een persoon die namens hem optreedt) en goedkeuring door een onafhankelijke Judicial Commissioner vereist ([161]). Een individuele toelating wordt verleend door het hoofd van een inlichtingendienst onder de voorwaarden van artikel 226B, lid 4, van de IPA 2016 en na voorafgaande goedkeuring door de Judicial Commissioners. De Judicial Commissioner moet de conclusies van de persoon die de toelating heeft verleend, toetsen aan de vraag of artikel 226A, d.w.z. de vereiste dat er weinig of geen redelijke verwachting van privacy bestaat, van toepassing is op de in de toelating beschreven bulkdataset met persoonsgegevens ([162]).

([156]) De op grond van artikel 200 van de IPA 2016 afgegeven bevelen voor bulkdatasets met persoonsgegevens geven inlichtingendiensten de bevoegdheid om datasets met persoonsgegevens van een aantal personen te bewaren en te onderzoeken, waarbij de aard van de set zodanig is dat de meerderheid van de personen voor de inlichtingendienst niet van belang is en waarschijnlijk ook niet zal worden bij de uitoefening van zijn taken, en die elektronisch worden bewaard door een inlichtingendienst en worden bewaard voor analyse in het kader van de uitoefening van zijn wettelijke taken, zie ook artikel 199 van de IPA 2016.

([157]) Artikel 226A, lid 1, van de IPA 2016, zoals ingevoerd bij artikel 2 van de Investigatory Powers (Amendment) Act 2024.

([158]) Artikel 226A, lid 3, van de IPA 2016, zoals ingevoerd bij artikel 2 van de Investigatory Powers (Amendment) Act 2024.

([159]) Met de Investigatory Powers (Amendment) Act 2024 is artikel 213 van de IPA 2016 gewijzigd, waardoor bevelen voor het verzamelen van bulkdatasets met persoonsgegevens twaalf maanden na de uitvaardiging ervan komen te vervallen. Voorheen moesten dergelijke bevelen om de zes maanden worden verlengd. Zie artikel 3 van de Investigatory Powers (Amendment) Act 2024.

([160]) Een individuele toelating kan alleen zonder voorafgaande rechterlijke goedkeuring worden verleend i) indien de persoon die de individuele toelating verleent van mening is dat de betreffende bulkdataset met persoonsgegevens onder een bestaande categorietoelating valt of ii) in spoedeisende gevallen, zie artikel 226B, lid 6, van de IPA 2016. In het laatste geval moet het besluit om een dringende individuele toelating te verlenen binnen drie werkdagen na de dag van afgifte worden getoetst door een Judicial Commissioner, zie artikel 226BC van de IPA 2016.

([161]) Artikel 226B, lid 1, van de IPA 2016, zoals ingevoerd bij artikel 2 van de Investigatory Powers (Amendment) Act.

([162]) Artikel 226BB, lid 1, punt a), van de IPA 2016, zoals ingevoerd bij artikel 2 van de Investigatory Powers (Amendment) Act 2024.

(106) Met een categorietoelating wordt toestemming verleend voor het bewaren, of het bewaren en onderzoeken, van een categorie van bulkdatasets met persoonsgegevens zoals beschreven in de toelating.

(107) Het besluit om de categorietoelating te verlenen wordt genomen door het hoofd van de inlichtingendienst wanneer deze van mening is dat artikel 226A van toepassing is op alle datasets binnen de categorie en wanneer het besluit om de toelating te verlenen wordt goedgekeurd door een onafhankelijke Judicial Commissioner ([163]). Deze laatste moet nagaan of artikel 226A, d.w.z. de vereiste dat er weinig of geen redelijke verwachting van privacy bestaat, van toepassing is op alle datasets die vallen onder de categorie datasets die in de toelating wordt beschreven ([164]).

(108) Belangrijk is dat bij de goedkeuring van een besluit om een individuele of categorietoelating te verlenen de Judicial Commissioner "dezelfde beginselen moet toepassen als een rechter bij een verzoek om rechterlijke toetsing" ([165]) en deze zaken met voldoende zorgvuldigheid moet behandelen om ervoor te zorgen dat de Judicial Commissioner voldoet aan de verplichtingen die zijn opgelegd in artikel 2 van de IPA 2016 (algemene plichten in verband met de persoonlijke levenssfeer) ([166]). Bovendien is de afgifte van toelatingen onderworpen aan streng toezicht achteraf, met name door middel van jaarlijkse rapportage aan de Secretary of State en de Intelligence and Security Committee van het parlement ([167]) en door middel van regelmatige inspecties van het bureau van de IPC ([168]).

(109) Wat relevante ontwikkelingen op het gebied van toezicht betreft, heeft het bureau van de IPC jaarverslagen voor de jaren 2021, 2022 en 2023 gepubliceerd, die gedetailleerde statistieken en informatie bevatten over het gebruik van onderzoeksbevoegdheden door inlichtingendiensten en rechtshandhavingsinstanties in het Verenigd Koninkrijk ([169]). In de verslagen worden ook de audits en onderzoeken van het Bureau beschreven, evenals de bevindingen daarvan, waarmee wordt bevestigd dat het IPC zijn zeer belangrijke toezichthoudende functie in het kader van de Britse regeling inzake onderzoeksbevoegdheden blijft vervullen. Zo heeft het in 2023 de noodzakelijkheid en evenredigheid van het gebruik van bevoegdheden voor grootschalige interceptie (zoals beoordeeld in de overwegingen 218 tot en met 225 van Uitvoeringsbesluit (EU) 2021/1772) door het Government Communications Headquarters (GCHQ) geëvalueerd, waarbij werd geconcludeerd dat een aanzienlijke meerderheid van de verklaringen met een deugdelijke motivering was onderbouwd, terwijl in sommige gevallen de evenredigheid niet goed tot uiting kwam. Deze bevindingen werden besproken met het GCHQ Compliance Team, dat zich ertoe verbond aanvullende interne bewustmakingstrainingen te organiseren om dit probleem aan te pakken ([170]).

(110) Daarnaast heeft het Investigatory Powers Tribunal een openbaar verslag gepubliceerd over zijn activiteiten en jurisprudentie voor de periode 2021-2023 ([171]). Uit het verslag blijkt dat het aantal zaken dat het Tribunal heeft ontvangen sinds 2017 meer dan verdubbeld is, met meer dan 400 zaken in 2023 ([172]). De meeste klachten waren

([163]) Artikel 226BA van de IPA 2016, zoals ingevoerd bij artikel 2 van de Investigatory Powers (Amendment) Act.

([164]) Artikel 226BB, lid 1, punt b, van de IPA 2016, zoals ingevoerd bij artikel 2 van de Investigatory Powers (Amendment) Act.

([165]) Artikel 226BB, lid 2, punt a), van de IPA 2016, zoals ingevoerd bij artikel 2 van de Investigatory Powers (Amendment) Act 2024.

([166]) Artikel 226BB, lid 2, punt b), van de IPA 2016, zoals ingevoerd bij artikel 2 van de Investigatory Powers (Amendment) Act 2024. Overeenkomstig de algemene taken in verband met de persoonlijke levenssfeer zoals uiteengezet in artikel 2 van de IPA 2016, moet een overheidsinstantie rekening houden met de vraag of a) hetgeen met het bevel, de toelating of aanzegging wordt beoogd, redelijkerwijs ook zou kunnen worden bereikt met andere, minder ingrijpende middelen, b) of een hoger beschermingsniveau in verband met de verkrijging van informatie op grond van het bevel, de toelating of aanzegging moet worden geboden met het oog op het bijzonder gevoelige karakter van die informatie, c) het algemeen belang bij de integriteit en veiligheid van telecommunicatiesystemen en posterijen en d) alle overige aspecten van het algemene belang van de bescherming van de persoonlijke levenssfeer.

([167]) Artikelen 226DA en 226DB van de IPA 2016, zoals ingevoerd bij artikel 2 van de Investigatory Powers (Amendment) Act 2024.

([168]) Zie Jaarverslag 2023 van het Investigatory Powers Commissioner Office, beschikbaar via de volgende link: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/E03270100-HC_603-IPCO-Annual-Report-2023-Web_Accessible.pdf, p.3.

([169]) De jaarverslagen zijn beschikbaar via de volgende link: https://www.ipco.org.uk/publications/annual-reports/.

([170]) Zie paragrafen 6.39 tot en met 6.43 van het jaarverslag 2023, beschikbaar via de volgende link: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/E03270100-HC_603-IPCO-Annual-Report-2023-Web_Accessible.pdf.

([171]) Het Investigatory Powers Tribunal Report 2021-2023, beschikbaar via de volgende link: https://investigatorypowerstribunal.org.uk/wp-content/uploads/2024/11/Investigatory-Powers-Tribunal-Report-2024.pdf.

([172]) Het Investigatory Powers Tribunal Report 2021-2023, blz. 5.

gericht tegen rechtshandhavingsinstanties, op de voet gevolgd door veiligheids- en inlichtingendiensten ([173]). Belangrijk is dat het Tribunal in 2022 en 2023 uitspraken heeft gedaan in zaken die het vóór 2021 had ontvangen, waarin het vaststelde dat overheidsinstanties van het Verenigd Koninkrijk (respectievelijk Police Scotland ([174]), Greater Manchester Police ([175]), Surrey Police ([176]), en MI5 en de minister van Binnenlandse Zaken ([177]) onrechtmatig hadden gehandeld. Wat de rechtsmiddelen betreft, gelastte het Investigatory Powers Tribunal onder meer de vernietiging van onrechtmatig verkregen materiaal en in één geval ook de betaling van 12 000 GBP als billijke genoegdoening voor de vastgestelde inbreuken. In het jaarverslag wordt daarmee bevestigd dat het Investigatory Powers Tribunal zijn belangrijke rol op het gebied van toezicht en rechtsmiddelen met betrekking tot strafrechtelijke handhaving en toegang tot persoonsgegevens in het kader van de nationale veiligheid doeltreffend vervult.

(111) Bovendien worden in het verslag ook belangrijke ontwikkelingen onder de aandacht gebracht, zoals een arrest van het Europees Hof voor de Rechten van de Mens waarin het Hof oordeelde dat personen overal ter wereld een klacht kunnen indienen bij het Investigatory Powers Tribunal met betrekking tot de werking van het Britse regeling voor bulksgewijze onderschepping, indien de betreffende handeling is uitgevoerd door een Britse overheidsinstantie en heeft plaatsgevonden in het Verenigd Koninkrijk ([178]).

4. **CONCLUSIE**

(112) De Commissie is van oordeel dat de UK GDPR en de DPA 2018, zoals gewijzigd bij de Data (Use and Access) Act, een beschermingsniveau blijven bieden voor uit de Europese Unie doorgegeven persoonsgegevens dat in feite overeenkomt met het niveau dat bij Verordening (EU) 2016/679 wordt gegarandeerd.

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

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

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

(116) Deze conclusie is gebaseerd op de relevante interne regeling van het Verenigd Koninkrijk, zoals die zich sinds de vaststelling van Uitvoeringsbesluit (EU) 2021/1772 heeft ontwikkeld, en zijn internationale verplichtingen, in het bijzonder de voortdurende naleving door het Verenigd Koninkrijk van het Europees Verdrag voor de rechten van de mens en de voortdurende onderwerping aan de jurisdictie van het Europees Hof voor de Rechten van de Mens. Voortdurende naleving van dergelijke internationale verplichtingen is derhalve een zeer belangrijk onderdeel van de beoordeling waarop dit besluit is gebaseerd.

([173]) Het Investigatory Powers Tribunal Report 2021-2023, blz. 12.
([174]) Wilson/Police Scotland [2022] UKIPTrib 5.
([175]) Pendlebury/Greater Manchester Police [2023] UKIPTrib 2.
([176]) Hill/Metropolitan Police Service & Independent Office For Police Conduct [2022] UKIPTrib 6.
([177]) Liberty & Privacy International/Security Service and Secretary of State for the Home Department [2023] UKIPTrib 1.
([178]) *Wieder and Guarnieri/UK*, [2023] EHRM 668, zie ook Investigatory Powers Tribunal Report 2021-2023, blz. 6.

5. GEVOLGEN VAN DIT BESLUIT EN MAATREGELEN VAN GEGEVENSBESCHERMINGSAUTORITEITEN

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

(118) Daarom is een krachtens artikel 45, lid 3, van Verordening (EU) 2016/679 vastgesteld adequaatheidsbesluit van de Commissie bindend voor alle organen van de lidstaten waartoe het is gericht, met inbegrip van hun onafhankelijke toezichthoudende autoriteiten. Tijdens de periode waarin Uitvoeringsbesluit (EU) 2021/1772, zoals gewijzigd bij dit besluit, 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.

(119) Er zij aan herinnerd dat, krachtens artikel 58, lid 5, van Verordening (EU) 2016/679 en zoals door het Hof van Justitie uitgelegd in het arrest *Schrems I* ([179]), wanneer een nationale gegevensbeschermingsautoriteit, ook na ontvangst van een klacht, de verenigbaarheid van een adequaatheidsbesluit van de Commissie met de grondrechten van de persoon op privacy en gegevensbescherming in twijfel trekt, het nationale recht moet voorzien in een rechtsmiddel voor die persoon om die grieven aan een nationale rechter voor te leggen die eventueel bij prejudiciële verwijzing het Hof van Justitie om beoordeling moet verzoeken ([180]).

6. MONITORING

(120) Overeenkomstig artikel 45, lid 4, van Verordening (EU) 2016/679 moet de Commissie doorlopend toezicht houden op relevante ontwikkelingen in het Verenigd Koninkrijk om te beoordelen of met het besluit nog altijd een beschermingsniveau wordt gewaarborgd dat in feite overeenkomend is. Dit toezicht is met name belangrijk omdat het Verenigd Koninkrijk een gewijzigde gegevensbeschermingsregeling toepast en handhaaft. Bovendien verleent het gewijzigde gegevensbeschermingskader van het Verenigd Koninkrijk de Secretary of State de bevoegdheid om dit kader nader te specificeren door middel van secundaire wetgeving. In dat verband moet bijzondere aandacht worden besteed aan dergelijke aanvullende specificaties en aan de praktische toepassing van de gewijzigde regels van het Verenigd Koninkrijk inzake de doorgifte van persoonsgegevens aan derde landen; de doeltreffendheid van de uitoefening van individuele rechten, met inbegrip van relevante ontwikkelingen in de wetgeving en de praktijk met betrekking tot de nieuw ingevoerde uitzonderingen op of beperkingen van dergelijke rechten, de werking van het geherstructureerde ICO, onder meer met betrekking tot de behandeling van klachten en de toepassing van corrigerende bevoegdheden, alsmede de naleving van de beperkingen en waarborgen met betrekking tot de toegang van de overheid, in het bijzonder met betrekking tot het nieuw ingevoerde deel 7A van de IPA 2016. Ontwikkelingen in de jurisprudentie en het toezicht door de Information Commissioner en andere onafhankelijke instanties moeten onder andere als basis dienen voor de monitoring door de Commissie.

(121) Om deze controle mogelijk te maken, moeten de Britse autoriteiten de Commissie onverwijld in kennis stellen van wezenlijke wijzigingen van de Britse rechtsorde die gevolgen hebben voor het rechtskader waarop Uitvoeringsbesluit (EU) 2021/1772, zoals gewijzigd bij dit besluit, van toepassing is, alsook van ontwikkelingen in praktijken in verband met de verwerking van persoonsgegevens die in dit Uitvoeringsbesluit (EU) 2021/1772, zoals gewijzigd bij dit besluit, wordt onderzocht, zowel met betrekking tot de verwerking van persoonsgegevens door verwerkingsverantwoordelijken en verwerkers op grond van de UK GDPR, als tot de beperkingen en waarborgen die op de toegang tot persoonsgegevens door overheidsinstanties van toepassing zijn. Dit moet ook gelden voor ontwikkelingen met betrekking tot de in overweging 120 genoemde elementen.

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

([179]) *Schrems I*, punt 65.

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

(123) Wanneer uit de beschikbare informatie, met name informatie die voortvloeit uit het toezicht op Uitvoeringsbesluit (EU) 2021/1772, zoals gewijzigd bij dit besluit, of verstrekt wordt door de autoriteiten in het Verenigd Koninkrijk of in de lidstaten, blijkt dat het door het Verenigd Koninkrijk geboden beschermingsniveau niet langer passend is, moet de Commissie de bevoegde Britse autoriteiten daarvan onverwijld in kennis stellen en verzoeken dat binnen een opgegeven termijn van maximaal drie maanden geschikte maatregelen worden genomen. Indien nodig kan deze periode voor een bepaalde tijd worden verlengd, rekening houdend met de aard van de problematiek en/of de maatregelen die moeten worden genomen. Een dergelijke procedure zou bijvoorbeeld in gang worden gezet in gevallen waarin verdere doorgifte, onder andere op basis van nieuwe adequaatheidsbepalingen die door de Secretary of State worden aangenomen of door het Verenigd Koninkrijk gesloten internationale overeenkomsten, niet langer zou worden uitgevoerd in het kader van waarborgen die de continuïteit van de bescherming garanderen in de zin van artikel 44 van Verordening (EU) 2016/679.

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

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

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

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

(127) Ingevolge artikel 45, lid 3, van Verordening (EU) 2016/679, en in het licht van het feit dat het door het rechtskader van het Verenigd Koninkrijk geboden beschermingsniveau kan veranderen, moet de Commissie na de vaststelling van dit besluit periodiek toetsen of de vaststellingen met betrekking tot de adequaatheid van het door het Verenigd Koninkrijk gewaarborgde beschermingsniveau nog steeds feitelijk en rechtens gerechtvaardigd zijn, rekening houdend met de in artikel 45, lid 2, van Verordening (EU) 2016/679 genoemde elementen. Die toetsingen moeten ten minste om de vier jaar plaatsvinden en moeten betrekking hebben op alle aspecten van de werking van dit besluit, met inbegrip van de werking van de relevante toezichts- en handhavingsmechanismen.

(128) Om de toetsing uit te voeren, moet de Commissie bijeenkomen met relevante vertegenwoordigers van de Britse autoriteiten, waaronder de Information Commission. Aan die bijeenkomst moet kunnen worden deelgenomen door vertegenwoordigers van de leden van het Europees Comité voor gegevensbescherming. In het kader van de toetsing moet de Commissie het Verenigd Koninkrijk verzoeken uitvoerige informatie te verstrekken over alle aspecten die relevant zijn voor de vaststelling van adequaatheid. De Commissie moet ook uitleg vragen over alle door haar ontvangen informatie die relevant is voor dit besluit, waaronder informatie van het Europees Comité voor gegevensbescherming, afzonderlijke gegevensbeschermingsautoriteiten of maatschappelijke groeperingen, openbare documenten, berichten in de media en alle andere beschikbare informatiebronnen.

(129) Op basis van de toetsing moet de Commissie een openbaar verslag opstellen dat bij het Europees Parlement en de Raad moet worden ingediend.

(130) De Commissie moet er ook rekening mee houden dat het gegevensbeschermingskader dat in dit besluit en in Uitvoeringsbesluit (EU) 2021/1772 wordt beoordeeld, zich verder kan ontwikkelen.

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

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

8. **SLOTOVERWEGINGEN**

(133) Het Europees Comité voor gegevensbescherming heeft zijn advies bekendgemaakt ([181]), waarmee bij het opstellen van dit besluit rekening is gehouden.

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

(135) Uitvoeringsbesluit (EU) 2021/1772 moet daarom dienovereenkomstig worden gewijzigd,

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

Artikel 1

Artikel 1, lid 2, van Uitvoeringsbesluit (EU) 2021/1772 wordt ingetrokken.

Artikel 2

Artikel 4 van Uitvoeringsbesluit (EU) 2021/1772 wordt vervangen door:

"*Artikel 4*

Dit besluit verstrijkt op 27 december 2031, tenzij het wordt verlengd volgens de in artikel 93, lid 2, van Verordening (EU) 2016/679 bedoelde procedure.".

Artikel 3

Dit besluit is gericht tot de lidstaten.

Gedaan te Brussel, 19 december 2025.

Voor de Commissie
Michael MCGRATH
Lid van de Commissie

([181]) Advies 26/2025 inzake het ontwerp van uitvoeringsbesluit van de Europese Commissie, tot wijziging van Verordening (EU) 2016/679 betreffende adequate bescherming van persoonsgegevens, beschikbaar via de volgende link: https://www.edpb.europa.eu/system/files/2025-10/edpb_opinion_202526_united_kingdom_adequacy_gdpr_en.pdf.