Europeiska unionens
officiella tidning

SV
L-serien

2025/2574

23.12.2025

KOMMISSIONENS GENOMFÖRANDEBESLUT (EU) 2025/2574

av den 19 december 2025

om ändring av kommissionens genomförandebeslut (EU) 2021/1772 i enlighet med Europaparlamentets och rådets förordning (EU) 2016/679 om adekvat skydd av personuppgifter i Förenade kungariket

[delgivet med nr C(2025) 8771]

(Text av betydelse för EES)

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DETTA BESLUT

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) ([1]), särskilt artikel 45.3, och

av följande skäl:

1. INLEDNING

(1) I kommissionens genomförandebeslut (EU) 2021/1772 ([2]) dras slutsatsen att Förenade kungariket, vid tillämpningen av artikel 45 i förordning (EU) 2016/679, säkerställer en adekvat skyddsnivå för personuppgifter som inom tillämpningsområdet för den förordningen överförs från Europeiska unionen till Förenande kungariket ([3]).

(2) När kommissionen antog genomförandebeslut (EU) 2021/1772 beaktade den att Förenade kungariket – efter utgången av den övergångsperiod som föreskrivs i avtalet om Förenade konungariket Storbritannien och Nordirlands utträde ur Europeiska unionen och Europeiska atomenergigemenskapen ([4]) och utgången av interimsbestämmelsen enligt artikel 782 i avtalet om handel och samarbete mellan Europeiska unionen och Europeiska atomenergigemenskapen, å ena sidan, och Förenade konungariket Storbritannien och Nordirland, å andra sidan ([5]) – skulle anta, tillämpa och genomföra ett nytt system för uppgiftsskydd som skiljer sig från det som gällde när landet var bundet av unionsrätten.

(3) Eftersom detta skulle medföra ändringar i den dataskyddsram som utvärderades i genomförandebeslut (EU) 2021/1772 eller annan relevant utveckling, bedömdes det lämpligt att föreskriva att beslutet skulle gälla för en period på fyra år från och med ikraftträdandet. Genomförandebeslut (EU) 2021/1772 skulle därför upphöra att gälla den 27 juni 2025, såvida det inte förlängdes i enlighet med det förfarande som avses i artikel 93.2 i förordning (EU) 2016/679.

([1]) EUT L 119, 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj.
([2]) Kommissionens genomförandebeslut (EU) 2021/1772 av den 28 juni 2021 i enlighet med Europaparlamentets och rådets förordning (EU) 2016/679 om adekvat skydd av personuppgifter i Förenade kungariket (EUT L 360, 11.10.2021, s. 1, ELI: http://data.europa.eu/eli/dec_impl/2021/1772/oj).
([3]) Se artikel 1.1 i genomförandebeslut (EU) 2021/1772. Enligt artikel 1.2 i det beslutet omfattar inte beslutet personuppgifter som överförs för Förenade kungarikets invandringskontroll eller som på annat sätt omfattas av undantaget från vissa registrerades rättigheter i fråga om upprätthållandet av en effektiv invandringskontroll enligt artikel 4.1 i tillägg 2 till Förenade kungarikets 2018 års dataskyddslag.
([4]) EUT C 384 I, 12.11.2019, s. 1.
([5]) EUT L 149, 30.4.2021, s. 10, ELI: http://data.europa.eu/eli/agree_internation/2021/689(1)/oj.

(4) För att fatta ett beslut om en eventuell förlängning av genomförandebeslut (EU) 2021/1772 måste kommissionen bedöma om slutsatsen att Förenade kungariket säkerställer en adekvat skyddsnivå fortsatt är sakligt och rättsligt motiverad mot bakgrund av den utveckling som ägt rum sedan genomförandebeslut (EU) 2021/1772 antogs med hänsyn till de element som anges i artikel 45.2 i förordning (EU) 2016/679.

(5) Den 23 oktober 2024 lade Förenade kungarikets regering fram lagförslaget Data (Use and Access) Act ([6]) för parlamentet, med förslag om ändringar av Förenade kungarikets allmänna dataskyddsförordning (den brittiska dataskyddsförordningen)och *UK Data Protection Act 2018* (2018 års dataskyddslag), vilka bedöms i genomförandebeslut (EU) 2021/1772. Den 24 juni 2025 antog kommissionen genomförandebeslut (EU) 2025/1226 ([7]), varigenom giltighetstiden för genomförandebeslut (EU) 2021/1772 förlängdes med sex månader till och med den 27 december 2025. Denna tidsbegränsade tekniska förlängning gjorde det möjligt för kommissionen att slutföra sin bedömning av huruvida Förenade kungariket tillhandahåller en adekvat skyddsnivå för personuppgifter på grundval av en stabil rättslig ram, dvs. efter det att den relevanta lagstiftningsprocessen hade avslutats ([8]).

(6) Sedan antagandet av genomförandebeslut (EU) 2021/1772 har kommissionen fortlöpande övervakat den relevanta utvecklingen i Förenade kungariket ([9]). I enlighet med skäl 281 i genomförandebeslut (EU) 2021/1772 har särskild uppmärksamhet ägnats åt den praktiska tillämpningen av Förenade kungarikets regler om överföring av personuppgifter till tredjeländer och de verkningar som sådana överföringar kan ha på skyddsnivån för uppgifter som överförs enligt genomförandebeslut (EU) 2021/1772, på ändamålsenligheten när det gäller utövandet av individuella rättigheter, inklusive eventuell relevant utveckling av lag och praxis för undantag från eller begränsningar av sådana rättigheter (särskilt avseende upprätthållandet av en ändamålsenlig invandringskontroll), samt efterlevnaden av begränsningar och skyddsåtgärder i samband med regeringens tillgång till personuppgifter. Bland annat har utvecklingen av rättspraxis och den tillsyn som utövas av kontoret för *Information Commissioner* (ICO) och andra oberoende organ legat till grund för kommissionens övervakning.

(7) På grundval av bedömningen av dessa förändringar, inklusive de ändringar i den brittiska dataskyddsförordningen och 2018 års dataskyddslag som infördes genom *Data (Use and Access) Act*, drar kommissionen slutsatsen att Förenade kungariket fortsätter att säkerställa en adekvat skyddsnivå för personuppgifter som överförs från Europeiska unionen till Förenade kungariket inom tillämpningsområdet för förordning (EU) 2016/679.

(8) Kommissionen drar även slutsatsen att det, mot bakgrund av ändringarna i relevanta bestämmelser i Förenade kungarikets lagstiftning ([10]), inte längre är motiverat att undanta personuppgifter som överförts för användning i Förenade kungarikets invandringskontroll eller som på annat sätt omfattas av undantaget från vissa registrerades rättigheter i fråga om upprätthållandet av en effektiv invandringskontroll (*invandringsundantaget*) enligt artikel 4.1 i tillägg 2 till den brittiska dataskyddslagen från tillämpningsområdet för genomförandebeslut (EU) 2021/1772, vilket förklaras i skäl 37 i detta beslut.

([6]) Finns på följande länk: https://bills.parliament.uk/bills/3825/news.

([7]) Kommissionens genomförandebeslut (EU) 2025/1226 av den 24 juni 2025 om ändring av kommissionens genomförandebeslut (EU) 2021/1772 i enlighet med Europaparlamentets och rådets förordning (EU) 2016/679 om adekvat skydd av personuppgifter i Förenade kungariket (EUT L, 2025/1226, 26.6.2025, ELI: http://data.europa.eu/eli/dec_impl/2025/1226/oj).

([8]) *Data (Use and Access) Act* erhöll kunglig sanktion den 19 juni 2025.

([9]) Artikel 45.4 i förordning (EU) 2016/679.

([10]) I maj 2021 fann appellationsdomstolen för England och Wales att invandringsundantaget såsom det formulerades vid den tidpunkten i artikel 4.1 i tillägg 2 till den brittiska dataskyddslagen var oförenligt med Förenade kungarikets lagstiftning, eftersom lagstiftningsåtgärden saknade specifika bestämmelser om de skyddsåtgärder som anges i artikel 23.2 i den brittiska dataskyddsförordningen. För att följa domen ändrade den brittiska regeringen invandringsundantaget genom att anta *The Data Protection Act 2018 (Amendment of Schedule 2 Exemptions) Regulations 2022*. Det ändrade undantaget ifrågasattes dock på nytt, med hänvisning till att det inte uppfyllde samtliga krav i artikel 23.2 i den brittiska dataskyddsförordningen. I en dom av den 11 december 2023 förklarade appellationsdomstolen på nytt att det ändrade invandringsundantaget är oförenligt med artikel 23.2 i den brittiska dataskyddsförordningen. För att uppfylla kraven antog den brittiska regeringen *The Data Protection Act 2018 (Amendment of Schedule 2 Exemptions) Regulations 2024*, som trädde i kraft den 8 mars 2024.

2. RELEVANT UTVECKLING AVSEENDE REGLER FÖR BEHANDLING AV PERSONUPPGIFTER

2.1 Förenade kungarikets dataskyddsram

(9) När genomförandebeslut (EU) 2021/1772 antogs bestod den rättsliga ramen för skydd av personuppgifter i Förenade kungariket av

— den brittiska dataskyddsförordningen ([11]), införlivad i Förenade kungarikets lagstiftning enligt *European Union (Withdrawal) Act 2018* ([12]) och ändrad genom 2019 års förordningar om dataskydd, integritet och elektronisk kommunikation (ändringar osv.) *(EU Exit) Regulations 2019* (DPPEC-förordningarna) ([13]),

— 2018 års dataskyddslag ([14]), i dess lydelse enligt de brittiska DPPEC-förordningarna.

(10) Även om dessa två lagar, som nära återspeglade motsvarande regler inom Europeiska unionen, fortfarande utgör grunden för Förenade kungarikets dataskyddslagstiftning, har de sedan dess genomgått begränsade ändringar, vilket återspeglar att Förenade kungariket inte längre omfattas av EU-rätten.

(11) För det första klargjordes genom *Retained EU Law (Revocation and Reform) Act 2023* ([15]) att de allmänna principerna i EU-rätten inte längre omfattades av Förenade kungarikets nationella lagstiftning efter utgången av 2023 ([16]). Därtill behöver inte längre domstolarna i Förenade kungariket tolka oförändrat ”införlivad lagstiftning”, som tidigare kallades ”bibehållen EU-lagstiftning”, i enlighet med de allmänna principerna i EU-rätten, utan sådan lagstiftning ska i stället tolkas på ett sätt som är förenligt med den brittiska lagstiftningen ([17]). Oförändrat införlivad lagstiftning måste dock av de relevanta brittiska domstolarna fortfarande tolkas i enlighet med relevant rättspraxis från Europeiska unionens domstol som har utfärdats före utgången av övergångsperioden ([18]), vilket även nämns i skäl 13 i genomförandebeslut (EU) 2021/1772. 2018 års dataskyddslag har ändrats genom *Data (Use and Access) Act* för att klargöra hur *Retained EU Law (Revocation and Reform) Act 2023* påverkar Förenade kungarikets dataskyddslagstiftning. I avsnitt 183A.1 i 2018 års dataskyddslag föreskrivs till exempel som en allmän regel att all ny lagstiftning (som antogs den 20 augusti 2025 eller senare) som inför nya skyldigheter eller befogenheter att behandla personuppgifter antas omfattas av Förenade kungarikets dataskyddslagstiftning. Detta innebär att Förenade kungarikets dataskyddsram fortsätter att åsidosätta annan lagstiftning. Enligt avsnitt 183A.2 b i 2018 års

([11]) Den allmänna dataskyddsförordningen, finns på följande länk: https://www.legislation.gov.uk/eur/2016/679/contents.

([12]) *European Union Withdrawal Act 2018*, som finns på följande länk: https://www.legislation.gov.uk/ukpga/2018/16/contents,, införlivade unionens lagstiftning som var direkt tillämplig i Förenade kungariket vid övergångsperiodens utgång i Förenade kungarikets lagstiftning. Denna så kallade bibehållna EU-lagstiftning omfattade förordning (EU) 2016/679 i dess helhet, inklusive skälen (se de förklarande anmärkningarna till *European Union (Withdrawal) Act 2018*, punkt 83, som finns på följande länk: https://www.legislation.gov.uk/ukpga/2018/16/pdfs/ukpgaen_20180016_en.pdf). I enlighet med den lagen måste den oförändrat bibehållna EU-lagstiftningen tolkas av domstolarna i Förenade kungariket i enlighet med relevant rättspraxis från Europeiska unionens domstol och allmänna principer i unionsrätten eftersom de har verkan omedelbart före övergångsperiodens utgång (*bibehållen EU-rättspraxis* respektive *bibehållen allmän EU-rättspraxis*).

([13]) 2019 års förordningar om dataskydd, integritet och elektronisk kommunikation (ändringar etc.) (*EU Exit*), som finns på https://www.legislation.gov.uk/uksi/2019/419/contents/made, i dess lydelse enligt DPPEC-förordningarna, som finns på https://www.legislation.gov.uk/ukdsi/2020/9780348213522. Genom DPPEC-förordningarna ändras förordning (EU) 2016/679 så som den införlivats i Förenade kungarikets lagstiftning genom *European Union (Withdrawal) Act 2018*, dataskyddslagen från 2018 och annan dataskyddslagstiftning för att passa det inhemska sammanhanget.

([14]) Dataskyddslagen från 2018, finns på följande länk: https://www.legislation.gov.uk/ukpga/2018/12/contents. Före Förenade kungarikets utträde ur Europeiska unionen och under övergångsperioden föreskrev dataskyddslagen från 2018 nationella bestämmelser, när så var tillåtet enligt förordning (EU) 2016/679, som preciserade och begränsade tillämpningen av bestämmelserna i förordning (EU) 2016/679 och införlivade Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (EUT L 119, 4.5.2016, s. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj).

([15]) Finns på följande länk: https://www.legislation.gov.uk/ukpga/2023/28.

([16]) Avsnitt 5 i *European Union (Withdrawal) Act 2018*, i dess lydelse enligt *Retained EU Law (Revocation and Reform) Act 2023*.

([17]) Avsnitt 5.A2 i *European Union (Withdrawal) Act 2018*, i dess lydelse enligt *Retained EU Law (Revocation and Reform) Act 2023*.

([18]) Avsnitt 6.3 och 6.7 i *European Union (Withdrawal) Act 2018*, i dess lydelse enligt *Retained EU Law (Revocation and Reform) Act 2023*.

dataskyddslag kan man bortse från detta antagande om Förenade kungarikets parlament medvetet beslutar att göra detta uttryckligen i lagstiftningen och bevarar parlamentets suveränitet. I avsnitt 186.2A i 2018 års dataskyddslag klargörs dessutom att de begränsningar av registrerades rättigheter som anges i avsnitt 186.3 i 2018 års dataskyddslag inte åsidosätts genom avsnitt 186.1 i 2018 års dataskyddslag, där det föreskrivs att rättsakter som förbjuder eller begränsar utlämnandet av information inte åsidosätter vissa dataskyddsrättigheter. Detta säkerställer till exempel att de begränsningar av registrerades rättigheter som anges i 2018 års dataskyddslag inte själva omfattas av det allmänna åsidosättandet av uppgiftsskydd i avsnitt 186.1 i 2018 års dataskyddslag.

(12) För det andra har den brittiska dataskyddslagstiftningen sedan antagandet av genomförandebeslut (EU) 2021/1772 ändrats genom *The Data Protection (Fundamental Rights and Freedoms) Amendment Regulations 2023* ([19]). I denna förordning definieras hänvisningar till grundläggande rättigheter eller friheter i den brittiska dataskyddsförordningen och 2018 års dataskyddslag (som tidigare avsåg EU:s grundläggande rättigheter och friheter ([20])) som hänvisningar till rättigheter enligt Europeiska konventionen om de mänskliga rättigheterna, vilka har införlivats i Förenade kungarikets nationella rätt genom Human Rights Act 1998 ([21]). Genom *Human Rights Act 1998* införlivas rättigheterna i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna i Förenade kungarikets lagstiftning. *Human Rights Act* ger varje enskild de grundläggande rättigheter och friheter som föreskrivs i artiklarna 2–12 och 14 i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, artiklarna 1, 2 och 3 i dess första protokoll och artikel 1 i dess trettonde protokoll, jämförda med artiklarna 16, 17 och 18 i den konventionen. Detta inbegriper rätten till respekt för privatlivet och familjelivet (och rätten till skydd av personuppgifter som en del av denna rätt) och rätten till en rättvis rättegång ([22]).

(13) Slutligen har den brittiska dataskyddsförordningen och 2018 års dataskyddslag varit föremål för riktade reformer enligt delarna fem och sex i *Data (Use and Access) Act*. Även om *Data (Use and Access) Act* har ett tillämpningsområde som sträcker sig långt bortom skyddet av personuppgifter innehåller den begränsade ändringar av flera delar av systemet för uppgiftsskydd, t.ex. reglerna om databehandling för vetenskaplig forskning, de rättsliga grunderna för databehandling, reglerna om principen om ändamålsbegränsning och villkoren för automatiserat beslutsfattande. Dessutom ändrar *Data (Use and Access) Act* ICO:s styrningsstruktur. När dessa åtgärder väl har genomförts kommer ICO att ersättas av en ny enhet, närmare bestämt *Information Commission*. Tillsynsmyndighetens roll och funktioner som oberoende tillsynsmyndighet för dataskydd i Förenade kungariket kommer att förbli oförändrade. Genom lagen införs också nya verkställighetsbefogenheter för tillsynsmyndigheten.

(14) I detta beslut bedöms lagstiftningsmässiga, regleringsmässiga och andra utvecklingsmässiga tendenser som har betydelse för den slutsats om skyddsnivån i Förenade kungariket som drogs i genomförandebeslut (EU) 2021/1772. Bedömningen i genomförandebeslut (EU) 2021/1772 gäller fortfarande för de delar av Förenade kungarikets dataskyddsram som inte har ändrats eller påverkats av andra utvecklingar sedan genomförandebeslutet antogs.

(15) Den rättsliga, regleringsmässiga och på annat sätt relevanta utvecklingen analyseras i detalj i följande avsnitt utifrån standarden för adekvat skyddsnivå, enligt vilken kommissionen måste avgöra om tredjelandet i fråga garanterar en skyddsnivå som ”i huvudsak motsvarar” den som säkerställs i unionen ([23]). Såsom klargjorts av Europeiska unionens domstol kräver detta inte att en identisk skyddsnivå uppnås ([24]). I synnerhet kan de medel som tredjelandet i fråga har till sitt förfogande för att skydda personuppgifter skilja sig från dem som används i EU förutsatt att de i praktiken visar sig vara effektiva för att säkerställa en adekvat skyddsnivå ([25]). Standarden för en adekvat skyddsnivå kräver därför inte att unionens regler kopieras till punkt och pricka. Det handlar snarare om huruvida det utländska rättsliga systemet som helhet, genom innehållet i rätten till dataskydd och dess faktiska genomförande, övervakning och verkställighet, uppnår den skyddsnivå som krävs ([26]).

([19]) Finns på följande länk: https://www.gov.uk/government/publications/the-data-protection-fundamental-rights-and-freedoms-amendment-regulations-2023.

([20]) EU:s grundläggande rättigheter och friheter hade bibehållits i den brittiska lagstiftningen genom avsnitt 4 i *European Union (Withdrawal) Act 2018*, som upphävdes i slutet av 2023 genom *Retained EU Law (Revocation and Reform) Act 2023*.

([21]) Avsnitt 2.3 i *The Data Protection (Fundamental Rights and Freedoms) Amendment Regulations 2023*.

([22]) Artiklarna 6, 8, 10 och 13 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (se även tillägg 1 till *Human Rights Act 1998*).

([23]) Skäl 104 i förordning (EU) 2016/679.

([24]) Mål C-362/14, Schrems, ECLI:EU:C:2015:650, punkt 73.

([25]) Se föregående fotnot, punkt 74.

([26]) Se meddelande från kommissionen till Europaparlamentet och rådet, *Utbyte och skydd av personuppgifter i en globaliserad värld*, COM(2017) 7 final, 10.1.2017, avsnitt 3.1, s. 6–7, som finns på följande länk: https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:52017DC0007&from=SV.

2.1.1 *Definitioner*

(16) Grundläggande dataskyddsbegrepp som återspeglar terminologin i förordning (EU) 2016/679 fortsätter att gälla i Förenade kungarikets system för uppgiftsskydd. Dessa begrepp har bedömts i skäl 23 i genomförandebeslut (EU) 2021/1772.

(17) Även om *Data (Use and Access) Act* lämnar en övervägande majoritet av definitionerna oförändrade, har det genom den införts specifika definitioner som rör behandlingen av personuppgifter för vetenskapliga, historiska och statistiska ändamål i artikel 4.2, 4.3, 4.4 och 4.5 i den brittiska dataskyddsförordningen. I punkt 2 definieras *behandling för vetenskapliga ändamål* som behandling av personuppgifter som utförs för forskning som rimligen kan beskrivas som vetenskaplig. Denna forskning kan vara offentligt eller privat finansierad och kan bedrivas som en kommersiell eller icke-kommersiell verksamhet. I linje med innehållet i skäl 159 i förordning (EU) 2016/679 innehåller punkt 3 en icke uttömmande förteckning med exempel på forskningsverksamhet som anses syfta till vetenskapliga ändamål, inklusive teknisk utveckling, demonstration, grundforskning och tillämpad forskning. I punkt 4 klargörs att ”historisk forskning” inbegriper genealogisk forskning, vilket också erkänns som ett historiskt ändamål i skäl 160 i förordning (EU) 2016/679. Slutligen definieras i punkt 5 behandling för statistiska ändamål som behandling av data för statistiska undersökningar eller för att ta fram statistiska resultat, där uppgifterna är aggregerade i sådan utsträckning att de inte längre utgör personuppgifter. Dessutom får de behandlade uppgifterna eller den framtagna informationen inte användas för att fatta beslut eller vidta åtgärder riktade mot någon enskild person. Denna definition överensstämmer med den tolkning av statistiska ändamål som anges i skäl 162 i förordning (EU) 2016/679.

(18) Sammanfattningsvis innehåller ändringarna av artikel 4 i den brittiska dataskyddsförordningen specifika definitioner av databehandling för vetenskapliga, historiska och statistiska ändamål, men dessa definitioner är förenliga med bokstaven och andemeningen i förordning (EU) 2016/679, vilket återspeglas i de ovannämnda skälen 159, 160 och 162.

(19) Genom att lägga till punkt 6 i artikel 4 i den brittiska dataskyddsförordningen har *Data (Use and Access) Act* även inrättat en särskild ram för att inhämta samtycke från den registrerade vid behandling av personuppgifter för vetenskapliga ändamål. I mycket liknande ordalag som i skäl 33 i förordning (EU) 2016/679, där det erkänns att samtycke inte alltid kan inhämtas för ett specifikt behandlingsändamål inom vetenskaplig forskning, tillåter den nya bestämmelsen bredare former av samtycke. Den möjliggör att den registrerade kan ge giltigt samtycke även när de exakta forskningsändamålen inte kan fastställas vid tidpunkten för datainsamlingen, förutsatt att begäran om samtycke följer allmänt erkända etiska normer som är relevanta för det aktuella forskningsområdet. Under alla omständigheter måste de registrerade ha möjlighet att samtycka till behandling av personuppgifter endast för vissa delar av forskningen, om möjligt.

(20) Slutligen har *Data (Use and Access) Act* ytterligare preciserat de skyddsåtgärder som tidigare fanns i artikel 89 i den brittiska dataskyddsförordningen och avsnitt 19 i 2018 års dataskyddslag, för databehandling för arkivändamål i allmänhetens intresse samt för vetenskapliga, historiska och statistiska forskningsändamål, i ett nytt kapitel 8A i den brittiska dataskyddsförordningen ([27]). Dessa skyddsåtgärder liknar dem som krävs enligt artikel 89 i förordning (EU) 2016/679 och innefattar bland annat krav på tekniska och organisatoriska åtgärder för att säkerställa respekten för principen om uppgiftsminimering.

2.2 **Skyddsåtgärder, rättigheter och skyldigheter**

2.2.1 *Laglig och korrekt behandling*

(21) Förenade kungarikets dataskyddsram fortsätter att kräva att uppgifter behandlas på ett lagligt, rättvist och legitimt sätt, enligt bedömningen i skälen 24–26 i genomförandebeslut (EU) 2021/1772.

([27]) Artiklarna 84A–84D i den brittiska dataskyddsförordningen, som infördes genom avsnitt 86 i *Data (Use and Access) Act*.

(22) Principerna om laglighet och rättvisa samt grunderna för laglig behandling fortsätter att garanteras i Förenade kungarikets lagstiftning genom artiklarna 5.1 a och 6.1 i den brittiska dataskyddsförordningen, enligt bedömningen i genomförandebeslut (EU) 2021/1772. Även om dessa bestämmelser till stor del förblir identiska ([28]) med motsvarande bestämmelser i förordning (EU) 2016/679, ändrar *Data (Use and Access) Act* först artikel 6.1 i den brittiska dataskyddsförordningen genom att införa en ytterligare laglig grund för behandling av personuppgifter enligt artikel 6.1 ea ([29]). Enligt den bestämmelsen ska behandlingen vara laglig om och i den utsträckning som den *är nödvändig för att tillgodose ett erkänt berättigat intresse*. Till skillnad från den rättsliga grunden ”berättigat intresse” enligt artikel 6.1 f i den brittiska dataskyddsförordningen, kräver den nya grunden ”erkänt berättigat intresse” inte en individuell avvägning mellan den personuppgiftsansvariges intressen och den registrerades intressen eller grundläggande rättigheter och friheter, vilket är avsett att ge icke-offentliga personuppgiftsansvariga större rättssäkerhet. I den nya artikel 6.5 i den brittiska dataskyddsförordningen anges att behandling är nödvändig för ändamål som rör ett erkänt berättigat intresse endast om den uppfyller ett villkor i bilaga 1 ([30]). Bilagan innehåller en uppräkning av situationer där behandling anses nödvändig för ändamål som rör ett erkänt berättigat intresse, till exempel när den sker som svar på en begäran från en offentlig myndighet som behöver uppgifterna för att utföra en uppgift i allmänhetens intresse med rättslig grund enligt artikel 6.3 i den brittiska dataskyddsförordningen, när behandlingen är nödvändig för att skydda nationell säkerhet, allmän säkerhet eller för försvarsändamål, för att hantera en nödsituation, för att upptäcka, utreda eller förebygga brott, eller för att skydda sårbara individer ([31]).

(23) Även om *Data (Use and Access) Act* därmed utökar den personuppgiftsansvariges möjligheter att åberopa rättsliga grunder för behandling av personuppgifter, omfattas den nya grunden ”erkänt berättigat intresse” av flera viktiga begränsningar. För det första är de erkända berättigade intressena begränsade till specifika situationer som förtecknas i detalj i lagen. För det andra kan de offentliga myndigheterna inte åberopa denna rättsliga grund för att utföra sina uppgifter ([32]). För det tredje gäller den endast områden där det finns ett tydligt allmänintresse i behandlingen (enligt villkoren i bilaga 1), det vill säga där behandlingen tjänar de syften som anges i artikel 23 i den brittiska dataskyddsförordningen (motsvarande artikel 23 i förordning (EU) 2016/679), och kan därför inte åberopas för kommersiella ändamål. För det fjärde ger *Data (Use and Access) Act* den ansvariga ministern (*Secretary of State*) befogenhet att genom förordning ([33]) ändra listan i bilaga 1. Ministern får dock endast införa en sådan

([28]) I syfte att förtydliga införs i artikel 6 i den brittiska dataskyddsförordningen även en ny punkt i *Data (Use and Access) Act* som innehåller exempel på typer av behandling som kan anses nödvändiga för ändamål av legitimt intresse i den mening som avses i artikel 6.1 f i den brittiska dataskyddsförordningen. Dessa exempel (direkt marknadsföring, gruppintern överföring av uppgifter för administrativa ändamål och säkerhet i nätverk och informationssystem) nämns också i skälen 47 och 48 i förordning (EU) 2016/679 som situationer där behandling skulle anses ligga i den personuppgiftsansvariges legitima intresse.

([29]) Avsnitt 70.2 b i *Data (Use and Access) Act*. Avsnitt 70.5 i *Data (Use and Access) Act* har utvidgat rätten att invända enligt artikel 21 i den brittiska dataskyddsförordningen till den nya artikel 6.1 ea i den brittiska dataskyddsförordningen.

([30]) Avsnitt 70.4 i *Data (Use and Access) Act*.

([31]) Se tillägg 4 till *Data (Use and Access) Act*. Enligt de brittiska myndigheterna kan exempel på situationer där icke-offentliga organ kan behöva behandla personuppgifter för att förebygga eller upptäcka brott vara ett företag som får kännedom om att någon olagligen försöker hacka dess datorsystem eller en bank eller ett finansinstitut som får kännedom om bedrägliga försök att öppna ett konto. Behandling av personuppgifter som utförs av ett icke-offentligt organ kan till exempel vara nödvändig för att skydda den nationella säkerheten eller det nationella försvaret om en kommersiell organisation misstänker att en kunds onlineaktivitet tyder på inblandning i terroristverksamhet. ICO arbetar med specifik vägledning i denna fråga, inklusive en definition av relevanta begrepp. Det handlar till exempel om att ”nationell säkerhet” sannolikt kommer att omfatta säkerheten och välbefinnandet för hela Förenade kungariket, dess befolkning, institutioner och regeringssystem. Se utkastet till ICO:s vägledning om erkänt berättigat intresse, som offentliggjorts för offentligt samråd, som finns på följande länk: https://ico.org.uk/for-organisations/recognised-legitimate-interest-guidance/.

([32]) Artikel 6.1 sista stycket, i dess lydelse enligt avsnitt 70.2 c i *Data (Use and Access) Act*.

([33]) Innan den ansvariga ministern utfärdar förordningar ska hänsyn tas till hur eventuella förändringar påverkar de registrerades intressen samt grundläggande rättigheter och friheter, och till att barn (när det är relevant) förtjänar särskilt skydd av sina personuppgifter. Förordningarna ska utfärdas som lagstadgade instrument och är föremål för ett positivt resolutionsförfarande, vilket innebär att de aktivt måste godkännas i det brittiska parlamentet. Avsnitt 70.4 stycke 8 i *Data (Use and Access) Act*.

förordning efter samråd med ICO ([34]) och lägga till ett erkänt berättigat intresse endast om behandlingen är nödvändig för att skydda ett mål av allmänt intresse enligt artikel 23.1 c–j i den brittiska dataskyddsförordningen ([35]). Slutligen, vilket också bekräftas av ICO:s vägledning ([36]), måste personuppgiftsansvariga som förlitar sig på ett erkänt berättigat intresse som rättslig grund uppfylla alla andra krav i Förenade kungarikets dataskyddsförordning, inbegripet att säkerställa att behandlingen är nödvändig och proportionerlig för att uppnå det berättigade intresset.

(24) För det andra klargörs genom *Data (Use and Access) Act* bestämmelserna i artiklarna 6.3, 9.2 g och 10.1 i den brittiska dataskyddsförordningen, som motsvarar respektive bestämmelser i förordning (EU) 2016/679, nämligen att grunden för behandling av personuppgifter, särskilda kategorier av personuppgifter och personuppgifter om brott och fällande domar, när sådan behandling sker för att uppfylla en rättslig förpliktelse eller för att utföra en uppgift i allmänhetens intresse, inte bara kan ha stöd i nationell rätt, utan även i relevant internationell rätt ([37]). Relevant internationell rätt begränsas därefter, genom den nya artikel 9A i den brittiska dataskyddsförordningen tillsammans med tillägg A1, till ett enda avtal – nämligen avtalet mellan Förenade konungariket Storbritannien, Nordirlands regering och Amerikas förenta staters regering om tillgång till elektroniska uppgifter för bekämpning av grov brottslighet, undertecknat den 3 oktober 2019 (*avtalet mellan Förenade kungariket och Förenta staterna*) ([38]). De skyddsåtgärder som föreskrivs i det avtalet har bedömts i skälen 153–155 i genomförandebeslut (EU) 2021/1772 och deras genomförande analyseras i skälen 87–93 i det här beslutet.

2.2.2 *Behandling av särskilda kategorier av personuppgifter*

(25) Förenade kungarikets dataskyddsram fortsätter att tillhandahålla särskilda skyddsåtgärder vid behandling av särskilda kategorier av uppgifter, vilket har bedömts i skälen 27–42 i genomförandebeslut (EU) 2021/1772.

(26) Både definitionen av särskilda kategorier av personuppgifter och de särskilda regler som gäller för behandlingen av dessa kategorier av uppgifter i den brittiska dataskyddsförordningen och 2018 års dataskyddslag kvarstår. Samtidigt ger *Data (Use and Access) Act* nya befogenheter till den ansvariga ministern att genom förordning lägga till särskilda kategorier av uppgifter, anpassa villkoren för deras användning samt införa nya definitioner, om så krävs ([39]). Viktigt är att ministern inte ges befogenhet att ta bort eller ändra befintliga särskilda kategorier av uppgifter eller att ändra villkoren för behandlingen av dessa kategorier ([40]). Den nya regleringsmakten ger således endast regeringen möjlighet att lägga till nya kategorier av känsliga uppgifter och att fastställa villkoren för behandlingen av dessa kategorier, vilket är avsett att ge regeringen möjlighet att reagera på den framtida tekniska och samhälleliga utvecklingen vid behov.

(27) Därför påverkar inte dessa ändringar skyddsnivån för särskilda kategorier av personuppgifter, som i huvudsak anses vara ekvivalent med det skydd som gäller inom EU enligt genomförandebeslut (EU) 2021/1772.

([34]) Avsnitt 182.2 i 2018 års dataskyddslag.

([35]) Avsnitt 70.4 stycke 9 i *Data (Use and Access) Act*.

([36]) Se ICO:s vägledning om berättigade intressen, som finns på följande länk: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/legitimate-interests/?q=appropriate+policy.

([37]) Avsnitt 72 i *Data (Use and Access) Act*.

([38]) Avtal mellan Förenade konungariket Storbritannien, Nordirlands regering och Amerikas förenta staters regering om tillgång till elektroniska uppgifter för bekämpning av grov brottslighet, finns på följande länk: 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]) Avsnitt 74 i *Data (Use and Access) Act*. Sådana förordningar är föremål för ett positivt resolutionsförfarande, vilket innebär att de kräver ett aktivt godkännande från det brittiska parlamentet.

([40]) Se den nya artikel 11A.1 b och 11A.2 i den brittiska dataskyddsförordningen samt de förklarande anmärkningarna till *Data (Use and Access) Act*, punkt 571, som finns på följande länk: https://publications.parliament.uk/pa/bills/cbill/59-01/0179/en/240179en.pdf.

2.2.3 *Ändamålsbegränsning*

(28) Förenade kungarikets system för skydd av personuppgifter kräver fortsatt att uppgifter behandlas för ett specifikt ändamål och därefter endast används i den utsträckning det inte strider mot det ursprungliga ändamålet med behandlingen, vilket har bedömts i skälen 43–48 i genomförandebeslut (EU) 2021/1772.

(29) För det första görs genom *Data (Use and Access) Act* några få riktade ändringar av principen om ändamålsbegränsning enligt artikel 5.1 b i den brittiska dataskyddsförordningen. Dessa ändringar klargör tillämpningen av denna princip utan att ändra dess innehåll. I avsnitt 71.1, 71.2 och 71.3 i *Data (Use and Access) Act* specificeras att principen om ändamålsbegränsning gäller när uppgifter samlas in från den registrerade eller på annat sätt, att den endast gäller när personuppgifter vidarebehandlas av eller för samma personuppgiftsansvarige (dvs. att den inte gäller vid byte av personuppgiftsansvarig), och att behandling inte är laglig enbart på grund av att den är förenlig med det ändamål för vilket personuppgifterna samlades in.

(30) För det andra klargörs i *Data (Use and Access) Act* reglerna för ytterligare behandling av personuppgifter genom att de samlas i den nya artikel 8A i den brittiska dataskyddsförordningen, där det fullständiga regelverket för ytterligare behandling av personuppgifter fastställs. Artikel 8A.2 i den brittiska dataskyddsförordningen förtecknar de faktorer som ska beaktas när man avgör om ett nytt behandlingsändamål är förenligt med det ursprungliga ändamålet. Dessa faktorer förtecknades tidigare i artikel 6.4 i den brittiska dataskyddsförordningen, vilket motsvarar artikel 6.4 i förordning (EU) 2016/679 ([41]). Artikel 8A.3 i den brittiska dataskyddsförordningen samlar i en enda bestämmelse de situationer där behandling av personuppgifter för ett nytt ändamål ska behandlas som förenlig med det ursprungliga ändamålet. Den avser situationer där den registrerade samtycker till behandlingen av personuppgifter för det nya ändamålet, eller där behandling är nödvändig för att skydda ett mål som anges i artikel 23.1 ([42]), där behandlingen utförs för vetenskapliga eller historiska forskningsändamål, för arkivändamål av allmänt intresse eller för statistiska ändamål ([43]). Slutligen klargörs i *Data (Use and Access) Act* att all behandling som utförs för att säkerställa att behandlingen är förenlig med dataskyddsprinciperna i artikel 5.1 i den brittiska dataskyddsförordningen eller som visar att den är det anses vara förenlig med det ursprungliga ändamålet. De ovan nämnda situationerna motsvarar fortsatt vad som även i förordning (EU) 2016/679 anses utgöra förenlig ytterligare behandling.

(31) För det tredje införs genom *Data (Use and Access) Act* även i artikel 8A.3 d i den brittiska dataskyddsförordningen nya situationer där ytterligare behandling av personuppgifter för ett nytt ändamål anses vara förenlig med det ursprungliga ändamålet. Dessa situationer anges i bilaga 2 till den brittiska dataskyddsförordningen ([44]) och omfattar exempelvis fall där behandling sker som svar på en begäran från en offentlig myndighet som behöver uppgifterna för att utföra en uppgift av allmänt intresse, med rättslig grund i enlighet med artikel 6.3 i den brittiska dataskyddsförordningen, samt där behandling är nödvändig för att skydda den allmänna säkerheten, reagera på en nödsituation, upptäcka, utreda eller förebygga brott, skydda den registrerades och andras vitala intressen, skydda sårbara personer, av skatteskäl eller, om det är nödvändigt för att uppfylla en rättslig skyldighet ([45]).

(32) Även om *Data (Use and Access) Act* därmed utökar förteckningen över situationer där ytterligare behandling för ett annat ändamål anses vara förenlig med det ursprungliga behandlingsändamålet, omfattas denna utökning av viktiga begränsningar. För det första är den begränsad till specifika situationer som förtecknas uttömmande i lagen. För det andra gäller den endast områden där det finns ett tydligt allmänintresse i behandlingen, det vill säga där den ytterligare behandlingen tjänar de syften som anges i artikel 23 i den brittiska dataskyddsförordningen

([41]) Liksom i förordning (EU) 2016/679 omfattar dessa faktorer kopplingar mellan det ursprungliga och det nya ändamålet, inom vilket sammanhang personuppgifterna samlades in, inklusive förhållandet mellan den registrerade och den personuppgiftsansvarige, behandlingens karaktär och huruvida den omfattar särskilda kategorier av uppgifter, de möjliga konsekvenserna av den avsedda behandlingen för den registrerade samt förekomsten av lämpliga skyddsåtgärder.

([42]) Se även artikel 6.4 i förordning (EU) 2016/679.

([43]) Skäl 50 i förordning (EU) 2016/679.

([44]) Bilaga 2 införs i den brittiska dataskyddsförordningen genom tillägg 5 till *Data (Use and Access) Act*, se avsnitt 71.6 i den lagen.

([45]) Se tillägg 5 till *Data (Use and Access) Act*.

(motsvarande artikel 23 i förordning (EU) 2016/679). Den kan därmed inte användas för kommersiella ändamål. För det tredje ger *Data (Use and Access) Act* den ansvariga ministern befogenhet att genom förordning ([46]) ändra förteckningen i bilaga 2. Ministern får dock endast lägga till typer av behandling om behandlingen är nödvändig för att skydda ett mål av allmänt intresse enligt artikel 23.1 c–j i den brittiska dataskyddsförordningen ([47]). För det fjärde gäller att när insamlingen av personuppgifter av den personuppgiftsansvarige baseras på den registrerades samtycke, anses behandling för ett nytt ändamål i de situationer som anges i bilaga 2 endast vara förenlig med det ursprungliga ändamålet om den personuppgiftsansvarige inte med rimlighet kan förväntas inhämta nytt samtycke från den registrerade ([48]).

2.2.4 *Individuella rättigheter*

(33) Inom Förenade kungarikets ram för skydd av personuppgifter fortsätter den registrerade att ha samma individuella rättigheter som enligt förordning (EU) 2016/679, utan några väsentliga förändringar ([49]), vilka kan göras gällande gentemot den personuppgiftsansvarige eller personuppgiftsbiträdet. Detta inkluderar särskilt rätten till tillgång till uppgifter, rätten att göra invändningar mot behandlingen samt rätten att få uppgifter rättade och raderade, vilket har bedömts i skälen 51–54 i genomförandebeslut (EU) 2021/1772.

(34) För det första klargörs i *Data (Use and Access) Act* vissa villkor för hur dessa rättigheter kan utövas. Å ena sidan preciseras, genom en ändring av artikel 12 och införandet av en ny artikel 12a i den brittiska dataskyddsförordningen ([50]) de tidsfrister inom vilka personuppgiftsansvariga måste besvara den registrerades begäran. Mer specifikt ändras artikel 12 i den brittiska dataskyddsförordningen så att den personuppgiftsansvarige inte längre är skyldig att lämna information om vidtagna åtgärder (eller skälen till att inga åtgärder har vidtagits) som svar på en begäran från den registrerade enligt artiklarna 15–22 i den brittiska dataskyddsförordningen *inom en månad från mottagandet av begäran*, utan i stället *före utgången av den tillämpliga tidsperioden*. Den tillämpliga tidsperioden definieras vidare i den nya artikel 12a i den brittiska dataskyddsförordningen som en period om en månad, räknat från den relevanta tidpunkten, vilken är den tidpunkt då den personuppgiftsansvarige mottar begäran, mottar eventuell information som efterfrågats i samband med en begäran enligt artikel 12.6 i den brittiska dataskyddsförordningen, eller när en avgift som har tagits ut i samband med begäran enligt artikel 12.5 i den brittiska dataskyddsförordningen har betalats, beroende på vilken av dessa tidpunkter som infaller sist ([51]). Enligt artikel 12A.3 är det dessutom möjligt för den personuppgiftsansvarige att förlänga den tillämpliga tidsperioden med ytterligare två månader om det är nödvändigt på grund av komplexiteten i den registrerades begäran eller antalet sådana begäranden. Vad gäller enbart rätten till tillgång till information och personuppgifter, ändras å andra sidan artikel 15 i den brittiska dataskyddsförordningen genom *Data (Use and Access) Act* för att införliva det förtydligande som har utarbetats inom ramen för befintlig nationell rättspraxis – på grundval av principen om proportionalitet inom ramen för EU-lagstiftningen – varvid det klargörs att personuppgiftsansvariga endast behöver göra rimliga och proportionella sökningar efter information och begärda personuppgifter ([52]). Den nya bestämmelsen förväntas tolkas i linje med befintlig rättspraxis, enligt vilken ”[…] det som vägs upp i proportionalitetsbedömningen är slutföremålet för sökningen, nämligen den potentiella fördel som tillhandahållandet av informationen kan medföra för den registrerade, i förhållande till hur denna information erhålls. Det kommer att behöva utvärderas i varje enskilt fall huruvida oproportionerliga insatser kommer att behöva göras för att hitta och tillhandahålla information i förhållande till de fördelar som kan medföras för den registrerade” ([53]).

([46]) Artikel 8A.5 i den brittiska dataskyddsförordningen, som infördes genom avsnitt 71.1 i *Data (Use and Access) Act*.
([47]) Artikel 8A.6 i den brittiska dataskyddsförordningen, som infördes genom avsnitt 71.1 i *Data (Use and Access) Act*.
([48]) Artikel 8A.4 b i den brittiska dataskyddsförordningen, som infördes genom avsnitt 71.1 i *Data (Use and Access) Act*.
([49]) Avsnitt 31 i *Victims and Prisoners Act 2024* införde ytterligare en grund för rätten till radering enligt artikel 17 i den brittiska dataskyddsförordningen, vilket ger registrerade rätt att begära att personuppgiftsansvariga raderar deras personuppgifter när de har behandlats till följd av en obefogad anklagelse mot den registrerade från en illvillig person. En person anses vara ”illvillig” om han eller hon har dömts för ett brott som anges i avsnitt 31.3 i *Victims and Prisoners Act 2024* (t.ex. trakasserier) eller är föremål för ett skyddsföreläggande mot stalkning. *Victims and Prisoners Act 2024* finns på följande länk: https://www.legislation.gov.uk/ukpga/2024/21/contents. Dessutom ändras rätten till information enligt artikel 13 i den brittiska dataskyddsförordningen genom avsnitt 77 i *Data (Use and Access) Act* på så sätt att den personuppgiftsansvarige inte längre är skyldig att informera den registrerade om ytterligare behandling av dennes personuppgifter för ett nytt ändamål, om detta ändamål är vetenskaplig eller historisk forskning, arkivering i allmänhetens intresse eller statistiska ändamål, behandlingen sker i enlighet med de särskilda skyddsåtgärder som anges i den nya artikel 84B i den brittiska dataskyddsförordningen och om det vore omöjligt eller oproportionellt att lämna sådan information.
([50]) Avsnitt 76 i *Data (Use and Access) Act*.
([51]) Artikel 12A.1 och 12A.2 i den brittiska dataskyddsförordningen, som infördes genom avsnitt 76 i *Data (Use and Access) Act*.
([52]) Artikel 15.1A i den brittiska dataskyddsförordningen, som infördes genom avsnitt 78 i *Data (Use and Access) Act*.
([53]) *Dawson-Damer v Taylor Wessing LLP* [2017] EWCA Civ 74.

(35) Därför gäller att även om tidsfristerna för att besvara begäranden från de registrerade och de särskilda skyldigheterna för personuppgiftsansvariga i fråga om rätten till tillgång numera omfattas av mer detaljerade regler, säkerställer det brittiska systemet fortsatt att registrerades begäranden måste hanteras inom skäliga tidsramar, fastställda utifrån objektiva faktorer. Vidare är den personuppgiftsansvariges materiella skyldigheter vid besvarande av en begäran om tillgång utformade utifrån vedertagna rättsliga standarder som även beaktar den registrerades intressen. Slutligen fastställs det redan i ICO:s nuvarande vägledning att en personuppgiftsansvarig inte behöver genomföra sökningar som skulle vara orimliga eller oproportionella i förhållande till vikten av att ge tillgång till informationen ([54]).

(36) De inskränkningar i de individuella rättigheterna enligt 2018 års dataskyddslag, som omfattas av artikel 23 i den brittiska dataskyddsförordningen, liksom de begränsningar och skyddsåtgärder som reglerar tillämpningen av dessa inskränkningar, är fortsatt en del av Förenade kungarikets ram ([55]), vilket beskrivs i detalj i skälen 55–67 i genomförandebeslut (EU) 2021/1772.

(37) När det särskilt gäller begränsningen avseende personuppgifter som behandlas i syfte att upprätthålla en effektiv invandringskontroll, eller för att utreda eller upptäcka verksamhet som skulle kunna undergräva en sådan kontroll, i den mån tillämpningen av relevanta bestämmelser sannolikt skulle motverka dessa ändamål (*invandringsundantaget*) ([56]), har den brittiska regeringen ändrat punkt 4 i bilaga 2 till 2018 års dataskyddslag genom *The Data Protection Act 2018 (Amendment of Schedule 2 Exemptions) Regulations 2022* ([57]) och *The Data Protection Act 2018 (Amendment of Schedule 2 Exemptions) Regulations 2024* ([58]), som kompletterar ändringsakten från 2022 ([59]). Genom ändringarna införs i punkt 4A och 4B i tillägg 2 till 2018 års dataskyddslag de skyddsåtgärder för utövandet av invandringsundantaget som krävs enligt artikel 23.2 i den brittiska dataskyddsförordningen. Närmare bestämt föreskrivs i ändringarna att i) invandringsundantaget ska endast tillämpas från fall till fall, separat i förhållande till varje relevant bestämmelse i den brittiska dataskyddsförordningen och på nytt vid varje tillfälle då ministern överväger att åsidosätta eller begränsa tillämpningen av någon sådan bestämmelse ([60]), ii) den registrerades rättigheter, friheter och eventuella sårbarheter ska beaktas vid tillämpningen av undantaget ([61]), iii) ministern ska föra register över användningen av invandringsundantaget och informera den registrerade om att det har använts (utom i specifika fall där sådan information skulle motverka syftet med undantaget) ([62]), iv) användningen av invandringsundantaget är begränsad till behandling av personuppgifter som utförs av ministern ([63]), vilket i praktiken innebär inrikesministeriet (*Home Office*), för dess funktioner som är relevanta för punkt 4.1 i tillägg 2 till 2018 års dataskyddslag. Därutöver förtydligas även den avvägning som måste göras vid bedömningen av om utövandet av de registrerades rättigheter sannolikt skulle motverka en effektiv invandringskontroll samt om det är nödvändigt och proportionellt att inskränka sådana rättigheter till följd av detta.

([54]) Finns på följande länk: 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]) Avsnitt 88.2 i *Data (Use and Access) Act* innebär en mindre ändring av avsnitt 26.2 f i 2018 års dataskyddslag (undantag avseende nationell säkerhet och nationellt försvar), genom att det klargörs att rätten att inge klagomål till *Commissioner* enligt artikel 77 i den brittiska dataskyddsförordningen inte omfattas av de bestämmelser vars tillämpning kan begränsas av nationella säkerhets- eller försvarsändamål.

([56]) När genomförandebeslut (EU) 2021/1772 antogs hade giltigheten och tolkningen av invandringsundantaget enligt brittisk rätt ännu inte fastställts, till följd av ett beslut av appellationsdomstolen för England och Wales av den 26 maj 2021. Domstolen fann att invandringsundantaget i 2018 års dataskyddslag vid den tidpunkten stred mot brittisk rätt, eftersom det saknade specifika bestämmelser om de skyddsåtgärder som anges i artikel 23.2 i den brittiska dataskyddsförordningen, vilket motsvarar artikel 23.2 i förordning (EU) 2016/679. Av denna anledning undantogs personuppgifter om överförts för ändamål kopplade till invandringskontroll i Förenade kungariket, eller som på annat sätt omfattas av invandringsundantaget, från tillämpningsområdet för genomförandebeslut (EU) 2021/1772.

([57]) Lagen trädde i kraft den 31 januari 2022 och finns tillgänglig på följande länk: https://www.legislation.gov.uk/uksi/2022/76/contents/made.

([58]) Lagen trädde i kraft den 8 mars 2024 och finns tillgänglig på följande länk: https://www.legislation.gov.uk/uksi/2024/342/contents/made.

([59]) Invandringsundantaget, i dess reviderade form enligt ändringsakten från 2022, ifrågasattes återigen genom rättslig prövning, med hänvisning till att det fortfarande inte uppfyllde samtliga krav enligt artikel 23.2 i den brittiska dataskyddsförordningen. Appellationsdomstolen fann i december 2023 att undantaget var oförenligt med kraven i artikel 23.2 i den brittiska dataskyddsförordningen. Till följd av denna dom kompletterar ändringsakten från 2024 ändringsakten från 2022 och innebär ytterligare ändringar av invandringsundantaget.

([60]) Punkt 4A.2 i tillägg 2 till 2018 års dataskyddslag.

([61]) Punkt 4AB.3 och 4 i tillägg 2 till 2018 års dataskyddslag. ICO rådfrågades om utkasten till 2024 års förordningar och uttalade offentligt att de inte hade några invändningar mot förordningarna. Den skrivelse som offentliggjordes som svar på samrådet och som bekräftar dess åsikt finns på följande länk: 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]) Punkt 4B.1 och 2 i tillägg 2 till 2018 års dataskyddslag.

([63]) Punkt 4.1 i tillägg 2 till 2018 års dataskyddslag.

(38) Dessutom har ICO utfärdat detaljerad vägledning om användningen av denna specifika begränsning ([64]). I vägledningen anges särskilt följande: *Invandringsundantaget bör inte tillämpas som ett generellt undantag för att begränsa […] rättigheter för alla behandlade uppgifter. Undantagets tillämpningsområde är begränsat till sådana rättigheter som, om de utövades i förhållande till de aktuella uppgifterna, skulle påverka de angivna invandringsändamålen.* […]. *Den personuppgiftsansvarige bör därför i första hand utgå från att i största möjliga utsträckning uppfylla kraven i förordning (EU) 2016/679 och dataskyddslagen.* […] *Prövningen av menlig inverkan har en hög tröskel och undantaget bör inte tillämpas generellt.* […] *Det måste övervägas om tillämpningen av undantaget utgör ett proportionellt svar på personens begäran om dataskydd. Man kan anse att det finns ett trängande socialt behov av att tillämpa invandringsundantaget, men man måste samtidigt ta hänsyn till om detta väger tyngre än skyldigheterna gentemot enskilda personer enligt förordning (EU) 2016/679. De har rättigheter över sina personuppgifter som måste beaktas i alla situationer, särskilt rätten till tillgång. Det är därför viktigt att man i varje enskilt fall överväger om den enskildes dataskyddsrättigheter väger tyngre än den identifierade risken för menlig inverkan. Tillämpningen av undantaget måste stå i proportion till omständigheterna och man måste noga överväga och dokumentera varje enskilt fall.*

(39) Sammantaget är den invandringsbegränsning som anges i punkt 4 i tillägg 2 till 2018 års dataskyddslag, som reviderades av den brittiska regeringen 2022 och 2024 och tolkas utifrån rättspraxis ([65]) och ICO:s vägledning, föremål för ett antal strikta villkor som reglerar dess tillämpning. Dessa villkor är mycket liknande de som anges i unionsrätten, särskilt artikel 23 i förordning (EU) 2016/679, avseende dataskyddsrättigheter och skyldigheter för viktiga mål av allmänt intresse, såsom invandringskontroll.

2.2.5 *Begränsningar av vidare överföringar*

(40) Den skyddsnivå som ges för personuppgifter som överförs från Europeiska unionen till personuppgiftsansvariga eller personuppgiftsbiträden i Förenade kungariket undergrävs fortfarande inte av vidare överföring av sådana uppgifter till mottagare i ett tredjeland. Ordningen för internationella överföringar av personuppgifter från Förenade kungariket ligger fortsatt mycket nära de regler som anges i kapitel V i förordning (EU) 2016/679, såsom bedömts i skälen 74–82 i genomförandebeslut (EU) 2021/1772.

(41) Även om kapitel 5 i den brittiska dataskyddsförordningen om överföring av personuppgifter till tredjeländer eller internationella organisationer ändrades genom *Data (Use and Access) Act*, kvarstår det grundläggande kravet att personuppgifter endast får överföras om överföringen grundas på i) föreskrifter som godkänner överföringen (ny terminologi för det som tidigare kallades ”föreskrifter om adekvat skyddsnivå”), ii) lämpliga skyddsåtgärder eller iii) ett undantag för specifika situationer. Dessa allmänna principer för dataöverföring återspeglas i den nya artikel 44a, som ersätter artikel 44 i den brittiska dataskyddsförordningen ([66]), där det också anges att överföring av personuppgifter till ett tredjeland eller en internationell organisation endast är tillåten om den sker i enlighet med övriga bestämmelser i den brittiska dataskyddsförordningen.

(42) När det gäller de förordningar som godkänner en överföring anges i artikel 45A.2 i den brittiska dataskyddsförordningen att ministern endast får utfärda sådana förordningar om han eller hon anser att dataskyddstestet är godkänt. Detta innebär att ministerns möjlighet som införs genom artikel 45A.3 i den brittiska dataskyddsförordningen att ta hänsyn till hur önskvärt det är att underlätta dataflöden vid utfärdandet av sådana förordningar alltid omfattas av villkoret att dataskyddstestet ska vara godkänt. Den rättsliga standarden för det dataskyddstest som ska godkännas fastställs i den nya artikeln 45B.1 i den brittiska dataskyddsförordningen, enligt vilken skyddsnivån för de registrerade i mottagarländerna eller inom internationella organisationer inte får vara väsentligt lägre än den nivå som föreskrivs för registrerade enligt relevant brittisk dataskyddslagstiftning. Artikel 45B.2 i den brittiska dataskyddsförordningen innehåller därefter en icke uttömmande förteckning över faktorer som ska beaktas vid bedömningen av om dataskyddstestet är uppfyllt. Exempel på sådana faktorer är respekten för rättsstatsprincipen och de mänskliga rättigheterna, förekomsten av en dataskyddsmyndighet och dess befogenheter, arrangemangen för rättslig eller icke-rättslig prövning, regler för överföring av personuppgifter från landet eller av

([64]) Finns på följande länk: 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) v Secretary of State for the Home Department & Anor* [2019] EWHC 2562 (Admin), punkterna 40 och 41.

([66]) Avsnitt 85 och tillägg 7 till *Data (Use and Access) Act*.

organisationen till andra länder eller internationella organisationer, landets eller organisationens relevanta internationella skyldigheter samt landets eller organisationens författning, traditioner och kultur. Genom att omformulera förteckningen över relevanta faktorer i den tidigare artikel 45 i den brittiska dataskyddsförordningen behåller den nya artikel 45B.2 de centrala faktorerna i förteckningen och ligger därmed fortsatt nära bestämmelserna i kapitel V i förordning (EU) 2016/679. Dessutom har de brittiska myndigheterna bekräftat att ministern kommer att beakta element som inte anges i artikel 45B.2, såsom lagar och praxis i ett tredjeland om hur offentliga myndigheter får tillgång till personuppgifter för ändamål såsom nationell säkerhet eller brottsbekämpning, i den mån de påverkar den övergripande skyddsstandarden. Dessutom anser de brittiska myndigheterna att relevant rättspraxis i tredjelandet kommer att vara en viktig del när det gäller de frågor som anges i dem icke uttömmande förteckningen i artikel 45B.2 i den brittiska dataskyddsförordningen.

(43) Förordningar om godkännande av en överföring omfattas fortfarande av de ”allmänna” förfarandekraven i avsnitt 182 i 2018 års dataskyddslag, i enlighet med skäl 77 i genomförandebeslut (EU) 2021/1772. Enligt detta förfarande måste den ansvarige ministern samråda med *Information Commissioner* vid förslag om antagande av brittiska förordningar om adekvat skyddsnivå ([67]). När dessa förordningar har antagits av ministern läggs de fram inför parlamentet. De omfattas då av förfarandet för ”att rösta emot förordningen” (*negative resolution*), enligt vilket båda kamrarna kan granska förordningarna och kan anta ett förslag om att ogiltigförklara dessa inom en 40-dagarsperiod ([68]).

(44) När det gäller lämpliga skyddsåtgärder anges i den nya artikel 46.1A i den brittiska dataskyddsförordningen att sådana överföringar endast får ske om relevanta skyddsåtgärder tillhandahålls genom de instrument som anges i artikel 46.2 och 46.3 ([69]) i den brittiska dataskyddsförordningen och om den personuppgiftsansvarige, personuppgiftsbiträdet eller tillämpliga offentliga organ, som agerar rimligt och proportionellt, bedömer att dataskyddstestet är uppfyllt. I de nya punkter 6 och 7 klargörs att dataskyddstestet anses vara uppfyllt om skyddsnivån för de registrerade, till följd av de nödvändiga skyddsåtgärderna, inte är väsentligt lägre efter överföringen än den nivå som gäller enligt relevant brittisk dataskyddslagstiftning. Det innebär att, precis som i förordning (EU) 2016/679, samma rättsliga standard gäller för både föreskrifter som godkänner en överföring och för lämpliga skyddsåtgärder. Enligt samma punkt ska vad som är rimligt och proportionellt bedömas med hänsyn till samtliga omständigheter, eller sannolika omständigheter, kring överföringen eller typen av överföring, inklusive personuppgifternas art och omfattning.

(45) Vad gäller undantag för särskilda situationer i artikel 49 i den brittiska dataskyddsförordningen, som reglerar villkoren för när sådana undantag kan tillämpas, har ett antal tekniska ändringar införts. Dessa anpassar bestämmelsen till ändringar i andra bestämmelser, men påverkar inte skyddsnivån för personuppgifter i Förenade kungariket. Dessutom införs en ny punkt 4A för att reproducera effekterna i avsnitt 18.1 i 2018 års dataskyddslag som ger ministern befogenhet att genom förordningar ange de omständigheter under vilka överföringar av uppgifter kan anses nödvändiga av skäl som rör allmänintresset. Slutligen reproducerar en ny artikel 49A de effekter i avsnitt 18.2 i 2018 års dataskyddslag som ger ministern möjlighet att genom förordningar införa begränsningar för uppgiftsöverföringar om dessa inte är godkända enligt artikel 45A (överföringar som godkänts genom förordningar) och när det anses nödvändigt av skäl som rör ett viktigt allmänintresse.

(46) När det gäller genomförandet av Förenade kungarikets regler för internationella överföringar har det skett flera förändringar sedan antagandet av genomförandebeslut (EU) 2021/1772.

([67]) Se samförståndsavtalet mellan ministern för *Department for Digital, Culture, Media and Sport* (ministeriet för digitala frågor, kultur, mediefrågor och idrott) och kontoret för *Information Commissioner* om det senares roll i samband med Förenade kungarikets nya bedömningar av adekvat skyddsnivå, finns på följande länk: https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments.

([68]) Om en sådan omröstning antas kommer förordningarna i slutändan att upphöra att ha någon ytterligare rättslig verkan.

([69]) Det överföringsinstrument som är tillgängligt enligt artikel 46.2 och 46.3 i den brittiska dataskyddsförordningen utgörs av rättsligt bindande och verkställbara instrument mellan offentliga myndigheter eller organ, bindande företagsregler i enlighet med artikel 47 i den brittiska dataskyddsförordningen, standardiserade dataskyddsklausuler som fastställts genom föreskrifter utfärdade av ministern eller i ett dokument utfärdat av *Information Commission*, en godkänd uppförandekod samt en godkänd certifieringsmekanism.

(47) När det gäller förordningar som godkänner överföringar har hittills två nya förordningar antagits, som speglar beslut om adekvat skyddsnivå som gäller även inom unionen, dvs. för överföringar till Sydkorea och för överföringar till kommersiella aktörer som har anslutit sig till Förenade kungarikets utvidgning av ramen för dataskydd mellan EU och Förenta staterna. Bestämmelserna om adekvat skyddsnivå för Republiken Korea ([70]) trädde i kraft den 19 december 2022 och möjliggör överföring av personuppgifter från Förenade kungariket till Republiken Korea. Förenade kungarikets utvidgning av ramen för dataskydd mellan EU och Förenta staterna, för vilken de relevanta förordningarna ([71]) trädde i kraft den 12 oktober 2023, möjliggör ett fritt flöde av personuppgifter till certifierade amerikanska organisationer.

(48) När det gäller lämpliga skyddsåtgärder har Förenade kungariket offentliggjort sina egna standardavtalsklausuler om dataskydd, *International Data Transfer Agreement* (IDTA) ([72]) och ett tillägg till EU:s standardavtalsklausuler, vilka bägge trädde i kraft i mars 2022. *International Data Transfer Agreement* utgör en mekanism som är specifik för Förenade kungariket; den syftar till att säkerställa lämpliga skyddsåtgärder vid överföring av personuppgifter och har flera likheter med EU:s standardavtalsklausuler. Tillägget, som utfärdats av ICO, gör det möjligt för personuppgiftsansvariga och personuppgiftsbiträden i Förenade kungariket att åberopa EU:s standardavtalsklausuler enligt den brittiska dataskyddsförordningen vid internationella överföringar. ICO har också tagit fram ett verktyg för riskbedömning av överföringar för att stödja brittiska organisationer i utvärderingen av riskerna i samband med internationella överföringar.

(49) Förenade kungariket har också förenklat godkännandeförfarandet för bindande företagsregler genom nya riktlinjer och nya möjligheter att godkänna bindande företagsregler. I juli 2022 offentliggjorde ICO vägledning och referenstabeller för att förklara Förenade kungarikets syn på bindande företagsregler efter brexit, och i december 2023 offentliggjordes ett tillägg till EU:s bindande företagsregler för att säkerställa att bindande företagsregler som godkänts enligt EU:s regelverk också är verkställbara i Förenade kungariket ([73]).

(50) I juli 2023 blev Förenade kungariket slutligen medlem i det globala forumet för gränsöverskridande integritetsskyddsregler (*Global CBPR Forum*) ([74]). Det är viktigt att påpeka att detta medlemskap inte innebär någon förenkling av uppgiftsöverföringar från Förenade kungariket till andra medlemmar i forumet. Förenade kungariket har klargjort att varje överföring av personuppgifter från Förenade kungariket till tredjeländer eller internationella organisationer måste uppfylla de villkor som fastställs i brittisk rätt, såsom beskrivits ovan, i synnerhet dataskyddstestet, som kräver att skyddsnivån inte får vara ”väsentligt lägre” än den som fastställs i den brittiska dataskyddsförordningen.

(51) Som kommissionen redan har förklarat säkerställer de gränsöverskridande integritetsskyddsreglerna inte en tillräcklig skyddsnivå för personuppgifter med ursprung i EU. Det föreskriver i synnerhet inte verkställbara individuella rättigheter ([75]). Det är därför särskilt viktigt att Global CBPR Forum, även om Förenade kungariket är medlem i forumet, inte kan utgöra en giltig överföringsmekanism enligt brittisk dataskyddslagstiftning. Om detta skulle förändras skulle det undergräva den skyddsnivå som för närvarande garanteras för personuppgifter som överförs från EU till Förenade kungariket. Kommissionen kommer därför att fortsätta att noggrant följa den fortsatta utvecklingen i detta avseende.

([70]) Finns på följande länk: https://www.legislation.gov.uk/uksi/2022/1213/made.

([71]) Finns på följande länk: https://www.legislation.gov.uk/uksi/2023/1028/made.

([72]) Finns på följande länk: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/.

([73]) ICO mottog ett stort antal ansökningar från Förenade kungariket om bindande företagsregler efter brexit. Många godkända bindande företagsregler kunde inte längre användas, eftersom endast bindande företagsregler där ICO hade varit involverad i förfarandet för godkännande kunde fortsätta att användas efter brexit. Dessa innehavare var dock skyldiga att tillhandahålla uppdaterad dokumentation som uppfyller kraven enligt den brittiska dataskyddsförordningen.

([74]) Global CBPR Forum består av Förenta staterna, Kanada, Japan, Sydkorea, Filippinerna, Singapore, Taiwan och Australien. Mauritius, Dubai International Financial Centre och Bermuda är associerade medlemmar, liksom Förenade kungariket.

([75]) Se till exempel den jämförande analys som har genomförts av G7-ländernas dataskyddsmyndigheter av de centrala delarna i dataskyddsförordningens certifieringssystem och systemet för gränsöverskridande integritetsskyddsregler, som visade på ”betydande skillnader” mellan systemen, bland annat med avseende på verkställbarhet och rättslig prövning, regler om oberoende tillsyn och statlig tillgång. Finns på följande länk: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10063165.
Se skäl 79 i kommissionens genomförandebeslut (EU) 2019/419 av den 23 januari 2019 enligt Europaparlamentets och rådets förordning (EU) 2016/679 om Japans adekvata skyddsnivå för personuppgifter enligt lagen om skydd av personuppgifter (EUT L 76, 19.3.2019, s. 1, ELI: http://data.europa.eu/eli/dec_impl/2019/419/oj.
Se även artikel 29-arbetsgruppens yttrande 2/2014 om en referens för kraven för bindande företagsregler som lämnas till de nationella dataskyddsmyndigheterna i EU och gränsöverskridande regler om skydd av den personliga integriteten till ansvarsskyldighetsombuden inom Apecsystemet, den 6 mars 2014.

2.2.6 *Automatiserat beslutsfattande*

(52) Medan flera av reglerna om automatiserat beslutsfattande, som bedöms i skäl 54 i genomförandebeslut (EU) 2021/1772, har behållits, har vissa aspekter av dessa regler ändrats genom *Data (Use and Access) Act*.

(53) För det första inför den nya artikel 22B i den brittiska dataskyddsförordningen ett allmänt förbud mot att behandla särskilda kategorier av personuppgifter (enligt artikel 9.1 i den brittiska dataskyddsförordningen) för beslut som uteslutande baseras på automatiserad behandling som har rättsliga eller liknande väsentliga effekter för den registrerade. Den redogör dock för tre undantag från detta förbud: Den registrerade har lämnat uttryckligt samtycke till sådan behandling. Beslutet är nödvändigt för att ingå eller fullgöra ett avtal mellan den personuppgiftsansvarige och den registrerade. Behandlingen krävs eller är tillåten enligt lag. För de två senare undantagen måste den automatiserade behandlingen vara nödvändig av skäl som rör ett betydande allmänintresse ([76]). Det allmänna förbudet gäller inte viktiga beslut som grundar sig på automatiserad behandling av icke-särskilda kategorier av uppgifter.

(54) Dessutom preciseras i den nya artikel 22A i den brittiska dataskyddsförordningen definitionen av ett beslut som ”uteslutande baseras på automatiserad behandling” genom att det anges att ett sådant beslut är ett där det inte finns någon väsentlig mänsklig medverkan i beslutsprocessen. Det är viktigt att personuppgiftsansvariga ska bedöma i vilken utsträckning profilering bidrar till ett beslut för att avgöra om den mänskliga medverkan har varit väsentlig. I artikel 22A i den brittiska dataskyddsförordningen klargörs också att ett ”viktigt beslut” är ett beslut som medför rättsliga konsekvenser eller liknande väsentliga effekter för den registrerade ([77]).

(55) För det andra föreskrivs i den nyligen införda artikel 22C i den brittiska dataskyddsförordningen att personuppgiftsansvariga ska genomföra åtgärder för att tillhandahålla relevanta skyddsåtgärder för alla viktiga beslut som helt eller delvis grundas på personuppgifter och enbart baseras på automatiserad behandling (inbegripet icke-särskilda kategorier av personuppgifter). Dessa skyddsåtgärder ska bland annat innefatta att informera den registrerade om beslutsprocessen, möjliggöra för den registrerade att bestrida beslutet och framföra synpunkter samt säkerställa att den registrerade kan få mänsklig medverkan i beslutsprocessen ([78]).

(56) Slutligen ger den nyligen införda artikel 22D i den brittiska dataskyddsförordningen ministern befogenhet att utfärda sekundärlagstiftning för att beskriva vad som utgör, och vad som inte utgör, väsentlig mänsklig medverkan och vilka beslut som har, och inte ska, anses ha liknande väsentliga effekter för registrerade. Det gör det också möjligt för ministern att införa sekundärlagstiftning för att i) lägga till nya skyddsåtgärder, ii) införa krav som kompletterar de befintliga skyddsåtgärderna, och iii) fastställa åtgärder som inte uppfyller skyddsåtgärderna ([79]). Innan förordningar antas i enlighet med artikel 22D i den brittiska dataskyddsförordningen ska ministern samråda med ICO ([80]), förordningarna får inte ändra artikel 22C i den brittiska dataskyddsförordningen ([81]) och förordningarna är föremål för ett positivt resolutionsförfarande ([82]), vilket innebär att de måste godkännas av båda kamrarna i Förenade kungarikets parlament innan de kan genomföras.

(57) Även om *Data (Use and Access) Act* har ändrat ramen för automatiserat beslutsfattande är det viktigt att notera att beslut enligt Förenade kungarikets rättsliga ram fortsatt omfattas av de viktigaste skyddsåtgärderna, vilka innebär rätten till mänsklig medverkan i samtliga fall av viktiga beslut som grundas enbart på automatiserad behandling, dvs. vid behandling av både känsliga och icke-känsliga personuppgifter ([83]). Dessutom, som kommissionen har

([76]) Artikel 22B i den brittiska dataskyddsförordningen, som infördes genom avsnitt 80.1 i *Data (Use and Access) Act*.
([77]) Artikel 22A i den brittiska dataskyddsförordningen, som infördes genom avsnitt 80.1 i *Data (Use and Access) Act*.
([78]) Artikel 22A i den brittiska dataskyddsförordningen, som infördes genom avsnitt 80.1 i *Data (Use and Access) Act*.
([79]) Artikel 22D i den brittiska dataskyddsförordningen, som infördes genom avsnitt 80.1 i *Data (Use and Access) Act*. Alla förordningar som utarbetas inom ramen för dessa befogenheter är föremål för ett positivt resolutionsförfarande, vilket garanterar parlamentarisk tillsyn. Förordningarna kan inte ändra kraven i artikel 22C.
([80]) Avsnitt 182.2 i 2018 års dataskyddslag.
([81]) Artikel 22D.4 i den brittiska dataskyddsförordningen.
([82]) Artikel 22D.5 i den brittiska dataskyddsförordningen.
([83]) Artikel 22C.2 i den brittiska dataskyddsförordningen, som infördes genom avsnitt 80.1 i *Data (Use and Access) Act*.

påpekat i tidigare beslut om adekvat skyddsnivå ([84]), är det osannolikt att de särskilda reglerna om automatiserat beslutsfattande i den brittiska dataskyddsförordningen påverkar skyddsnivån för personuppgifter som överförs från unionen till Förenade kungariket. Vad gäller personuppgifter som samlats in i unionen kommer de beslut som bygger på automatisk insamling normalt att fattas av den personuppgiftsansvarige i unionen (som har en direkt förbindelse med berörd registrerad) och omfattas därför av bestämmelserna i förordning (EU) 2016/679.

2.3 **Tillsyn och efterlevnad**

2.3.1 *Oberoende tillsyn*

(58) I Förenade kungariket utövas tillsynen över och verkställigheten av efterlevnaden av dataskyddsramen fortsatt av en oberoende tillsynsmyndighet för dataskydd, såsom analyseras i skälen 85–91 i genomförandebeslut (EU) 2021/1772. Genom *Data (Use and Access) Act* reformeras styrningsstrukturen för denna myndighet genom att det inrättas en juridisk person, *Information Commission*, som kommer att ersätta ICO, som var organiserad som en separat juridisk person bestående av en enda person.

(59) Närmare bestämt kommer de styrningsåtgärder som fastställs i *Data (Use and Access) Act*, när de har genomförts, att avskaffa kontoret för *Information Commissioner* och överföra funktionerna, personalen och egendomen från ICO till det nya organet, *Information Commission*. *Information Commission* består av verkställande och icke-verkställande ledamöter ([85]). I lagen föreskrivs också att *Information Commissioner* ska övergå till att bli ordförande för *Information Commission*, som är en av de icke-verkställande ledamöterna ([86]). I den utsträckning det är lämpligt till följd av överföringen av funktioner, föreskrivs vidare i *Data (Use and Access) Act* att hänvisningar till *Information Commissioner* i all lagstiftning eller andra handlingar (oavsett när de antagits eller upprättats) ska tolkas som hänvisningar till *Information Commission*. För att utföra sina uppgifter får *Information Commission* inrätta kommittéer och delegera uppgifter till en ledamot, en anställd eller en kommitté vid *Information Commission* ([87]) samt vidta åtgärder för att reglera dess förfarande och kommittéernas förfarande, även när det gäller beslutsförhet och beslutsfattande med majoritet. Dessa förfaranden måste offentliggöras ([88]).

(60) Det är viktigt att notera att *Information Commissions* oberoende omfattas av samma skyddsåtgärder – inbegripet reglerna om utnämning och avsättning av ordföranden – som de som bedöms i skälen 87–90 i genomförandebeslut (EU) 2021/1772 ([89]). Liknande skydd gäller för övriga icke verkställande ledamöter av *Information Commission*. I synnerhet utnämns ordföranden för *Information Commission* av Hans Majestät, på rekommendation av ministern. Han eller hon väljs ut på grundval av meriter och rättvis och öppen konkurrens ([90]). Övriga icke verkställande ledamöter utses av ministern efter samråd med ordföranden. Kandidater kan rekommenderas för utseende alternativt utses under föreutsättning att de valts ut på grundval av meriter enligt rättvis och öppen konkurrens och om ministern är övertygad om att de inte belastas av någon intressekonflikt ([91]). De verkställande ledamöterna är anställda vid *Information Commission* på de villkor som fastställs av de icke verkställande ledamöterna ([92]). Den verkställande direktören utses av ordföranden och andra icke verkställande ledamöter efter samråd med ministern. Utnämningen av de verkställande ledamöterna är också föremål för ett urval på grundval av meriter och rättvis och öppen konkurrens ([93]).

(61) Ordföranden får endast avsättas av Hans Majestät efter ett anförande i båda kamrarna i parlamentet, och endast om ministern har överlämnat en rapport till kammaren där det anges att ministern är övertygad om att ordföranden gjort sig skyldig till allvarlig försummelse, har en intressekonflikt, har underlåtit att uppfylla särskilda

([84]) Se t.ex. skäl 94 i genomförandebeslut (EU) 2019/419 och skäl 81 i kommissionens genomförandebeslut (EU) 2022/254 av den 17 december 2021 enligt Europaparlamentets och rådets förordning (EU) 2016/679 om Sydkoreas adekvata skyddsnivå för personuppgifter enligt lagen om skydd av personuppgifter (EUT L 44, 24.2.2022, s. 1, ELI: http://data.europa.eu/eli/dec_impl/2022/254/oj).
([85]) Punkterna 3.1 i tillägg 12A till 2018 års dataskyddslag.
([86]) Avsnitten 117, 118, 119 och 120 tillsammans med tillägg 14 i *Data (Use and Access) Act*.
([87]) Punkterna 13 och 14 i tillägg 12A till 2018 års dataskyddslag.
([88]) Punkt 16 i tillägg 12A till 2018 års dataskyddslag.
([89]) Artikel 52 i den brittiska dataskyddsförordningen samt tillägg 12A till 2018 års dataskyddslag, som infördes genom avsnitt 114A i *Data (Use and Access) Act*.
([90]) Punkterna 5.1 och 3.2 i tillägg 12A till 2018 års dataskyddslag.
([91]) Punkterna 3.2, 3.5 och 3.6 i bilaga 12A till dataskyddslagen från 2018.
([92]) Punkt 11 i tillägg 12A till 2018 års dataskyddslag.
([93]) Punkt 5.2 i tillägg 12A till 2018 års dataskyddslag.

informationskrav avseende potentiella intressekonflikter, eller är oförmögen, olämplig eller ovillig att fullgöra sina uppgifter ([94]). Icke-verkställande ledamöter får endast skiljas från sina uppdrag av ministern om han eller hon är förvissad om att de särskilda villkoren i lagstiftningen är uppfyllda. Dessa omfattar intressekonflikter, allvarlig försummelse eller att man är oförmögen, ovillig eller olämplig att utföra sina uppgifter. När det gäller ytterligare skyddsåtgärder är ministern skyldig att offentliggöra beslutet om att göra detta och ge ledamoten en motivering till att denne skiljs från sitt uppdrag ([95]).

(62) *Information Commission* kommer fortsättningsvis att ha som huvudsaklig uppgift att övervaka och säkerställa efterlevnaden av Förenade kungarikets dataskyddsram *i syfte att skydda enskildas grundläggande rättigheter och friheter* ([96]). När det gäller Information Commissions uppgift att säkerställa en lämplig skyddsnivå för personuppgifter föreskriver *Data (Use and Access) Act* uttryckligen att *Information Commission* ska beakta registrerades, personuppgiftsansvarigas och andras intressen och allmänhetens intresse i stort samt främja allmänhetens förtroende för behandlingen av personuppgifter ([97]). Dessa mål nämns också i skäl 7 i förordning (EU) 2016/679.

(63) I *Data (Use and Access) Act* anges dessutom att *Information Commission* ska beakta främjandet av innovation och konkurrens, vikten av att förebygga, utreda, avslöja och lagföra brott, behovet av att skydda den allmänna säkerheten och den nationella säkerheten samt de särskilda behoven i samband med skyddet av barn när den fullgör sina uppgifter enligt dataskyddslagstiftningen ([98]). EU:s dataskyddslagstiftning erkänner också behovet av att balansera skyddet av personuppgifter med flera andra grundläggande rättigheter och mål, såsom ekonomiska och sociala framsteg, säkerhet och rättvisa och näringsfrihet ([99]).

2.3.2 *Verkställighet, inbegripet påföljder*

(64) *Information Commissions* befogenheter och uppgifter fortsätter att motsvara de befogenheter och uppgifter som tillsynsmyndigheterna för dataskydd har i medlemsstaterna enligt de relevanta artiklarna i förordning (EU) 2016/679 ([100]), såsom bedömts i skälen 91–95 i genomförandebeslut (EU) 2021/1772.

(65) Genom *Data (Use and Access) Act* har det införts vissa förtydliganden avseendet utövandet av några av dessa befogenheter.

(66) Å ena sidan klargör *Data (Use and Access) Act* att *Commission* har rätt att kräva specifika ”dokument” och specifik ”information” när den använder sin befogenhet att utfärda informationsmeddelanden ([101]). Å andra sidan inför *Data (Use and Access) Act* två nya utredningsbefogenheter för *Information Commission*: en ny befogenhet att kräva en rapport ([102]) och en ny befogenhet att utfärda ”förhörsföreläggande” till personuppgiftsansvariga vid misstänkt överträdelse av den brittiska dataskyddsförordningen eller 2018 års dataskyddslag ([103]).

([94]) Punkterna 7.6 och 7 i tillägg 12A till dataskyddslagen från 2018.
([95]) Punkterna 9.6, 9.7, 9.8 och 9.9 i tillägg 12A till 2018 års dataskyddslag.
([96]) Artikel 51 i den brittiska dataskyddsförordningen.
([97]) Avsnitt 91 i *Data (Use and Access) Act*, genom vilken avsnitt 120A i 2018 års dataskyddslag infördes.
([98]) Avsnitt 91 i *Data (Use and Access) Act*, genom vilken avsnitt 120B i 2018 års dataskyddslag infördes. Genom *Data (Use and Access) Act* införs dessutom ett nytt avsnitt 120C i 2018 års dataskyddslag, som ålägger *Information Commission* att utarbeta och offentliggöra en strategi som bland annat återspeglar hur den ska beakta ovannämnda frågor samt främjandet av ekonomisk tillväxt vid utövandet av sina tillsynsfunktioner.
([99]) Se särskilt skälen 2 och 4 samt artikel 23 i förordning (EU) 2016/679.
([100]) Artiklarna 57 och 58 i den brittiska dataskyddsförordningen.
([101]) Avsnitt 97 i *Data (Use and Access) Act*, genom vilken avsnitt 142 i 2018 års dataskyddslag ändrades. Övervägandena kring teknikens inverkan och dataskyddets roll i att skapa förtroende i den digitala ekonomin utgör en del av dataskyddsmyndigheternas verksamhet både i Förenade kungariket och inom EU. Se t.ex. Europeiska dataskyddsstyrelsens årsrapport 2024, s. 12: *EDPB är ett dynamiskt och samarbetsvilligt organ som spelar en avgörande roll för att säkerställa en konsekvent tillämpning av dataskyddslagstiftningen i hela Europa. Ur mitt perspektiv som vice ordförande ser jag det som en garant för individers rätt till privatliv, som skickligt balanserar behovet av innovation och ekonomisk tillväxt.*
([102]) Avsnitt 98 i *Data (Use and Access) Act*, genom vilken avsnitt 146 i 2018 års dataskyddslag ändrades.
([103]) Avsnitt 100 i *Data (Use and Access) Act*, genom vilken avsnitt 148A i 2018 års dataskyddslag infördes.

(67) När det gäller utövandet av dessa befogenheter av *Information Commission* har myndigheten, sedan ikraftträdandet av genomförandebeslut (EU) 2021/1772, hanterat omkring 40 000 klagomål från registrerade per år, vilket motsvarar antalet klagomål som hanterades när Förenade kungariket fortfarande var en del av unionen och tillämpade förordning (EU) 2016/679 ([104]). ICO har även genomfört undersökningar på eget initiativ som omfattar ett brett spektrum av sektorsspecifika och efterlevnadsrelaterade frågor, inklusive registrerades rättigheter ([105]).

(68) När det gäller verkställighetsåtgärder har *Commissioner*, sedan genomförandebeslut (EU) 2021/1772 trädde i kraft, utfärdat 120 reprimander, 32 informationsföreläggande, 3 bedömningspåföljdsföreläggande, 12 verkställighetsföreläggande, 2 varningar och 12 administrativa påföljdsföreläggande ([106]). Detta inbegriper flera betydande sanktionsavgifter som utdömts enligt den brittiska dataskyddsförordningen och 2018 års dataskyddslag. Exempelvis utfärdade *Information Commissioner* i april 2023 böter på 12,7 miljoner pund till en social medieplattform för otillbörlig behandling av uppgifter om barn ([107]). I mars 2025 ålades ett mjukvaruföretag böter på 3,07 miljoner pund för brister i säkerheten som utsatte fler än 70 000 personers personuppgifter för risk ([108]). Så sent som i juni 2025 ålade *Information Commissioner* ett företag för genetiska tester böter på 2,31 miljoner pund för underlåtenhet att vidta lämpliga säkerhetsåtgärder för att skydda brittiska användares personuppgifter, till följd av en omfattande cyberattack 2023 ([109]).

(69) Sedan antagandet av genomförandebeslut (EU) 2021/1772 har ICO också utarbetat och offentliggjort ett stort antal riktlinjer, yttranden och andra vägledningsdokument, där man klargör tillämpningen av dataskyddsregler inom viktiga områden, såsom ansiktsigenkänning, rättvisa i artificiell intelligens, barns uppgifter, direkt marknadsföring, videoövervakning, rätten till tillgång, transparens inom hälso- och sjukvård samt social omsorg osv. Dessa riktar sig till olika målgrupper, inbegripet små och medelstora företag, specifika aktörer såsom skolor, förskolor eller mindre offentliga myndigheter samt näringslivet i stort, allmänheten eller registrerade ([110]).

3. RELEVANT UTVECKLING NÄR DET GÄLLER TILLGÅNG TILL OCH ANVÄNDNING AV PERSONUPPGIFTER SOM ÖVERFÖRS FRÅN EUROPEISKA UNIONEN AV MYNDIGHETER I FÖRENADE KUNGARIKET

3.1 Allmän rättslig ram

(70) Förenade kungariket är fortsatt medlem av Europarådet, liksom landet fortfarande är anslutet till Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna och omfattas av Europadomstolens jurisdiktion. Landet är därför fortsatt bundet av de skyldigheter som följer av internationell rätt, såsom beskrivs i skälen 116–119 i genomförandebeslut (EU) 2021/1772, vilka utgör ramen för dess system för statlig tillgång till personuppgifter och bygger på principer, skyddsåtgärder och individuella rättigheter som är identiska med dem som gäller för de 27 medlemsstaterna som parter i Europakonventionen och som i stor utsträckning återspeglas i relevant rättspraxis från Europeiska unionens domstol.

(71) Specifika dataskyddsgarantier och dataskyddsrättigheter garanteras fortfarande av 2018 års dataskyddslag vid uppgiftsbehandling som utförs av Förenade kungarikets offentliga myndigheter, inbegripet brottsbekämpande myndigheter och nationella säkerhetsmyndigheter, såsom analyseras i skälen 121–132 i genomförandebeslut (EU) 2021/1772. *Data (Use and Access) Act* har endast medfört begränsade och riktade ändringar av de delar av 2018 års dataskyddslag som reglerar behandlingen av personuppgifter inom ramen för brottsbekämpning (del 3 i 2018 års dataskyddslag) och nationell säkerhet (del 4 i 2018 års dataskyddslag).

([104]) *Information Commissioners* årsrapporter 2021–2022, 2022–2023 och 2023–2024. Se även skäl 96 i genomförandebeslut (EU) 2021/1772.
([105]) *Information Commissioners* årsrapport 2023–2024, s. 41.
([106]) *Information Commissioners* årsrapporter 2021–2022, 2022–2023 och 2023–2024.
([107]) Mer information om dessa och fler verkställighetsåtgärder finns på ICO:s webbplats, som finns på följande länk: https://ico.org.uk/action-weve-taken/enforcement/.
([108]) Mer information finns på följande länk: https://ico.org.uk/action-weve-taken/enforcement/2025/03/advanced-computer-software-group-limited/.
([109]) Mer information finns på följande länk: https://ico.org.uk/action-weve-taken/enforcement/2025/06/23andme/.
([110]) Finns på följande länk: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/.

(72) Vad gäller behandling av personuppgifter av behöriga myndigheter i syfte att förebygga, utreda, upptäcka eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive skydd mot och förebyggande av hot mot den allmänna säkerheten, fortsätter del 3 i 2018 års dataskyddslag att fastställa principer, rättigheter och skyldigheter som liknar dem i direktiv (EU) 2016/680 ([111]).

(73) Samma dag som detta beslut [antog] kommissionen ett beslut på grundval av artikel 36.3 i direktiv (EU) 2016/680 där den konstaterade att det system för dataskydd som är tillämpligt på behandling som utförs av brittiska brottsbekämpande myndigheter för brottsbekämpande ändamål säkerställer en skyddsnivå som i allt väsentligt är likvärdig med den som garanteras enligt direktiv (EU) 2016/680.

(74) *Data (Use and Access) Act* har ändrat och konsoliderat de befintliga undantag i del 3 i 2018 års dataskyddslag som är tillgängliga för behöriga myndigheter för ändamål som rör nationell säkerhet. Undantaget för nationell säkerhet gör det möjligt för behöriga myndigheter att inte tillämpa vissa bestämmelser i del 3 i 2018 års dataskyddslag om undantag från den bestämmelsen krävs för att skydda den nationella säkerheten ([112]). Den avspeglar de undantag för nationell säkerhet som föreskrivs för behandling av personuppgifter enligt den brittiska dataskyddsförordningen (enligt avsnitt 26 i 2018 års dataskyddslag) och enligt del 4 i 2018 års dataskyddslag (enligt avsnitt 110 i 2018 års dataskyddslag).

(75) Undantaget för nationell säkerhet omfattas av samma begränsningar och skyddsåtgärder som undantagen enligt den brittiska dataskyddsförordningen och del 4 i 2018 års dataskyddslag, enligt analysen i skälen 64–67 och 126 i genomförandebeslut (EU) 2021/1772. I synnerhet kan undantaget endast tillämpas om och i den mån det krävs för att skydda den nationella säkerheten. Det är inte ett generellt undantag och måste övervägas och åberopas av den personuppgiftsansvarige från fall till fall ([113]). Dessutom måste varje tillämpning av undantaget vara förenlig med människorättsnormer (med stöd av *Human Rights Act 1998* och den europeiska konventionen om de mänskliga rättigheterna) enligt vilken varje ingrepp i rätten till integritet bör vara nödvändigt och proportionerligt i ett demokratiskt samhälle ([114]). Detta bekräftas också i ICO:s vägledning om tillämpningen av undantag avseende nationell säkerhet ([115]).

(76) Med stöd av de ändringar som införts genom *Data (Use and Access) Act* ([116]) kan dessutom en särskild behandling av personuppgifter av behöriga brottsbekämpande myndigheter också regleras av bestämmelserna i del 4 i 2018 års dataskyddslag, som vanligtvis endast tillämpas på behandling av uppgifter av nationella säkerhetsmyndigheter.

([111]) Avsnitt 69 i *Data (Use and Access) Act* inför definitionen av samtycke samt villkoren för att kunna åberopa samtycke, såsom de anges i artiklarna 4.11 och 7 i den brittiska dataskyddsförordningen (vilka speglar motsvarande bestämmelser i förordning (EU) 2016/679), som de nya avsnitten 33.1A och 40A i 2018 års dataskyddslag. Därmed förtydligas begreppet samtycke och villkoren för att kunna åberopa samtycke när det används som rättslig grund för behandling av personuppgifter av behöriga myndigheter för brottsbekämpande ändamål. Dessutom förtydligar avsnitt 71.7 och 71.8 i *Data (Use and Access) Act* ordalydelsen i avsnitt 36.1 i 2018 års dataskyddslag något. Slutligen, där så är tillämpligt, återspeglas ändringarna i den brittiska dataskyddsförordningen genom *Data (Use and Access) Act*, såsom beskrivits i avsnitt 2, även i del 3 i 2018 års dataskyddslag. Detta gäller exempelvis avsnitt 74.2–74.5 om känslig behandling, avsnitt 76.4–76.6 avseende tidsfrister för att svara på registrerades begäranden, avsnitt 78.2 och 78.3 avseende sökningar som svar på registrerades begäranden, och avsnitt 80.3–80.5 om automatiserat beslutsfattande.

([112]) Avsnitt 78A.1 i 2018 års dataskyddslag, som infördes genom avsnitt 88 i *Data (Use and Access) Act*. Enligt avsnitt 78A.2–78A.4 i 2018 års dataskyddslag medger undantaget åsidosättande av principerna om uppgiftsskydd (förutom principen om lagenlighet och villkoren och skyddsåtgärderna för behandling av känsliga uppgifter), de individuella rättigheterna, de personuppgiftsansvarigas och personuppgiftsbiträdens skyldigheter när det gäller dataintrång, vissa delar av reglerna om internationella överföringar av uppgifter och vissa av *Information Commissioners* befogenheter att få tillträde för att utföra inspektioner och vidta verkställighetsåtgärder.

([113]) Se *Baker v Secretary of State for the Home Department* [2001] UKIT NSA2 (*"Baker mot Secretary of State"*).

([114]) Se även *Guriev v Community Safety Development (United Kingdom) Ltd* [2016] EWHC 643 (QB), punkt 45. *Lin v Commissioner of the Police for the Metropolis* [2015] EWHC 2484 (QB), punkt 80.

([115]) Se ICO:s vägledning om undantaget avseende nationell säkerhet och försvar, som finns på följande länk: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/national-security-and-defence-exemption-a-guide.

([116]) Avsnitten 89–90 i *Data (Use and Access) Act*.

(77) Även om dataskyddssystemet för behandling inom nationell säkerhet i vissa situationer även gäller behandling av uppgifter av brottsbekämpande myndigheter, är detta endast tillämpligt under särskilda omständigheter och föremål för strikta villkor och skyddsåtgärder, dvs. om i) en behörig myndighet har angetts som ”kvalificerad behörig myndighet” i föreskrifter som utarbetats av ministern och som kräver parlamentariskt godkännande ([117]), och ii) ministern genom meddelande utser en särskild behandling som utförs av den kvalificerade behöriga myndigheten. Det är viktigt att påpeka att ett sådant utseende endast kan ske om ministern anser att uppgiftsbehandlingen är nödvändigt för att skydda den nationella säkerheten, dvs. när en brottsbekämpande myndighet agerar för ändamål som rör den nationella säkerheten, och uppgiftsbehandlingen utförs av den kvalificerade behöriga myndigheten som gemensam personuppgiftsansvarig tillsammans med minst en underrättelsetjänst ([118]). Som ytterligare skyddsåtgärder måste ministern samråda med *Commissioner* innan ett meddelande om utseende ([119]) utfärdas och texten till meddelandet måste i princip offentliggöras ([120]) och en person som direkt berörs av ett meddelande om utseende kan begära rättslig prövning ([121]). Denna ändring syftar huvudsakligen till att klargöra att när brittiska myndigheter har befogenheter inom både brottsbekämpning och nationell säkerhet och behandlar uppgifter inom ramen för det senare området, kan dataskyddssystemet för nationella säkerhetstjänster gälla.

(78) Del 4 i 2018 års dataskyddslag reglerar brittiska underrättelsetjänsters databehandling. Den fortsätter att fastställa de viktigaste principerna för dataskydd, ställa villkor för behandling av särskilda kategorier av uppgifter, säkerställa registrerades rättigheter, kräva inbyggt dataskydd samt reglera överföringar av personuppgifter, enligt beskrivningen i skälen 125–132 i genomförandebeslut (EU) 2021/1772.

(79) De ändringar av detta system som införs genom *Data (Use and Access) Act* är begränsade. Vad gäller de registrerades rätt till tillgång enligt avsnitt 94 i 2018 års dataskyddslag, införs genom *Data (Use and Access) Act* ett nytt underavsnitt 2A, där det klargörs att den registrerade endast har rätt till relevant information i den mån den personuppgiftsansvarige kan tillhandahålla den på grundval av en rimlig och proportionerlig sökning ([122]). Som förklaras i skäl 35 avgränsar denna ändring rätten till tillgång utifrån vedertagna rättsliga standarder, vilka även beaktar den registrerades intressen. Inom området för automatiserat beslutsfattande är personuppgiftsansvariga fortsatt förbjudna att fatta beslut som i betydande grad påverkar en registrerad och som enbart grundar sig på automatiserad behandling av personuppgifter som rör den registrerade, såvida inte ett sådant beslut är föreskrivet eller tillåtet enligt lag, den registrerade har lämnat samtycke till att beslutet fattas på denna grund, eller beslutet fattas inom ramen för ett avtal ([123]). Genom *Data (Use and Access) Act* införs i del 4 i 2018 års dataskyddslag ([124]) samma definition av begreppet *beslut som enbart grundar sig på automatiserad behandling* som återfinns i artikel 22A i den brittiska dataskyddsförordningen och som analyseras i skäl 53 i detta beslut.

3.2 **Relevant utveckling när det gäller brittiska myndigheters tillgång och användning i brottsbekämpningssyfte**

(80) Förenade kungarikets lagstiftning fortsätter att föreskriva ett antal begränsningar av tillgången till och användningen av personuppgifter i brottsbekämpningssyfte och tillhandahåller tillsyns- och prövningsmekanismer på detta område, såsom analyseras i skälen 134–174 i genomförandebeslut (EU) 2021/1772.

([117]) Avsnitt 82.A1, 82.2A och 82.4 i 2018 års dataskyddslag, som infördes genom avsnitt 89.2 i *Data (Use and Access) Act*.

([118]) Avsnitt 82A.1 och 82A.2, som infördes genom avsnitt 89.3 i *Data (Use and Access) Act*. Som ytterligare skyddsåtgärder måste ministern samråda med *Commissioner* innan ett meddelande om utseende utfärdas, se det nya avsnittet 82A.8 i 2018 års dataskyddslag. Texten i meddelandet måste i princip offentliggöras, se det nya avsnittet 82D.1, med förbehåll för undantagen i det nya avsnittet 82D.3 i 2018 års dataskyddslag. Dessutom kan en person som direkt berörs av ett meddelande om utseende begära rättslig prövning, se det nya avsnittet 82E i 2018 års dataskyddslag.

([119]) Avsnitt 82A.8 i 2018 års dataskyddslag.

([120]) Avsnitt 82D.1, med förbehåll för de undantag som anges i det nya avsnitt 82D.3, i 2018 års dataskyddslag.

([121]) Avsnitt 82E i 2018 års dataskyddslag.

([122]) Avsnitt 78.4 i *Data (Use and Access) Act*.

([123]) Avsnitt 96 i 2018 års dataskyddslag.

([124]) Enligt det nya avsnittet 96.4 i 2018 års dataskyddslag grundar sig ett beslut på helt automatiserad behandling om beslutsprocessen inte innefattar någon möjlighet för en människa att godkänna, avslå eller påverka beslutet. Se avsnitt 80.4 c i *Data (Use and Access) Act*.

3.2.1 *Rättslig grund och tillämpliga begränsningar och skyddsåtgärder*

(81) Insamling av personuppgifter från näringsidkare i Förenade kungariket för brottsbekämpning är fortfarande tillåten i Förenade kungarikets rättsordning på grundval av beslut om husrannsakan och utlämnandeorder, med förbehåll för de villkor och skyddsåtgärder som beskrivs i skälen 135–138 i genomförandebeslut (EU) 2021/1772.

(82) Dessutom har 2023 års lag om nationell säkerhet (*National Security Act 2023*) ([125]), som syftar till att ta itu med hot mot den nationella säkerheten genom spionage, sabotage och personer som agerar för främmande makt, infört nya befogenheter för ingripanden, husrannsakningar och beslagtagningar för polisen i Förenade kungariket, inklusive möjligheten att inhämta personuppgifter, där det finns rimliga skäl att misstänka att material kommer att inhämtas, som sannolikt kommer utgör bevis för att ett av de allvarligare brotten eller aktiviteter som avser hot från främmande makt i 2023 års lag om nationell säkerhet har begåtts eller är på väg att begås ([126]). Dessa befogenheter är föremål för liknande villkor och skyddsåtgärder som de som analyseras i genomförandebeslut (EU) 2021/1772 för de befogenheter som fanns vid den tidpunkten. Särskilt gäller att användningen av dessa befogenheter måste godkännas genom ett beslut om husrannsakan, en utlämnandeorder eller ett förklaringsföreläggande utfärdat av en oberoende rättslig myndighet, på begäran av polis eller förundersökningsledare ([127]). Särskilda skyddsåtgärder finns för konfidentiellt material, såsom journalistiskt material och handlingar som omfattas av rätten till förtrolig kommunikation mellan advokat och klient ([128]). På samma sätt måste utfärdandet av utlämningsorder ([129]), kundinformationsorder ([130]) och kontoövervakningsorder ([131]) som också har skapats genom 2023 års lag om nationell säkerhet, godkännas av en domare på ansökan av en lämplig tjänsteman, och omfattas av särskilda villkor och skyddsåtgärder, bland annat att beslutet söks med avseende på en viss person, i syfte att utreda hot från utländska makter, att ordern kommer att öka utredningens effektivitet och att den inte används för att erhålla information som omfattas av rätten till förtrolig kommunikation mellan advokat och klient eller som på annat sätt är utesluten, såsom journalistiskt material och vissa patientjournaler ([132]).

(83) Såsom beskrivs i skälen 139–141 i genomförandebeslut (EU) 2021/1772 kan enligt den brittiska rättsliga ramen särskilda brottsbekämpande myndigheter, till exempel den nationella brottsbekämpningsmyndigheten (*National Crime Agency*) eller polismyndigheten för Londons storstadsområde (*Metropolitan Police Service*), även använda riktade utredningsbefogenheter enligt 2016 års lag om utredningsbefogenheter ([133]) för att förebygga eller upptäcka allvarliga brott. De specifika utredningsbefogenheter som dessa brottsbekämpande myndigheter kan förlita sig till är riktad avlyssning (del 2 i 2016 års lag om utredningsbefogenheter), inhämtande av kommunikationsuppgifter (del 3 i 2016 års lag om utredningsbefogenheter) och riktat ingrepp i utrustning (del 5 i 2016 års lag om utredningsbefogenheter). Om föreläggandena om lagring lämnas av ministern enligt del 4 i 2016 års lag om utredningsbefogenheter kan brottsbekämpningen också gynnas genom tillgång till lagrade kommunikationsdata genom befogenheter att förvärva kommunikationsdata enligt del 3 i 2016 års lag om utredningsbefogenheter.

([125]) Finns på följande länk: https://www.legislation.gov.uk/ukpga/2023/32/contents/enacted.

([126]) Bilaga 2 till 2023 års lag om nationell säkerhet. Relevanta brott enligt 2023 års lag om nationell säkerhet är till exempel att olovligen erhålla eller lämna ut skyddad information (avsnitt 1), att olovligen erhålla eller lämna ut företagshemligheter (avsnitt 3), att bistå en främmande underrättelsetjänst (avsnitt 4), att utföra sabotage (avsnitt 12) eller att utföra specifika förbjudna handlingar för en främmande makts räkning med avsikt att skapa störande effekter (avsnitt 13).

([127]) Se punkterna 2.1, 3.1, 4.1 och 10.1 i tillägg 2 till 2023 års lag om nationell säkerhet.

([128]) Se punkterna 2.4 b, 3.4 b och c, 4.4 b och c och 10.1 i tillägg 2 till 2023 års lag om nationell säkerhet.

([129]) Genom utlämningsorder enligt bilaga 3 till 2023 års lag om nationell säkerhet kan en tjänsteman lämna en anmodan till en person om att tillhandahålla information, uppvisa handlingar och/eller besvara frågor som är relevanta för en utredning avseende egendom kopplad till hot från främmande makt, inklusive egendomens förflyttning eller användning.

([130]) Genom kundinformationsorder enligt bilaga 4 till 2023 års lag om nationell säkerhet kan en tjänsteman underrätta ett finansinstitut om att begära att det tillhandahåller kundinformation om en viss person.

([131]) Genom kontoövervakningsorder enligt bilaga 5 får ett finansinstitut åläggas att lämna den information som anges i ordern till en tjänsteman under den period och på det sätt som anges i ordern, som inte får överstiga 90 dagar.

([132]) Tillägg 3 punkt 2.1, tillägg 4 punkt 1, tillägg 5 punkt 1 till 2023 års lag om nationell säkerhet.

([133]) 2016 års lag om utredningsbefogenheter (se https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted) ersatte en annan lagstiftning om avlyssning av kommunikation, ingrepp i utrustning och inhämtande av kommunikationsuppgifter, särskilt del I i 2000 års lag om utredningsbefogenheter som innehöll den tidigare allmänna rättsliga ramen för brottsbekämpande och nationella säkerhetsmyndigheters användning av utredningsbefogenheter.

(84) Sedan genomförandebeslut (EU) 2021/1772 antogs fortsätter 2016 års lag om utredningsbefogenheter, tillsammans med 2000 års lag om utredningsbefogenheter för England, Wales och Nordirland och 2000 års lag om utredningsbefogenheter för Skottland att utgöra den rättsliga grunden och att fastställa tillämpliga begränsningar och skyddsåtgärder för användningen av sådana befogenheter, i enlighet med vad som beskrivs i genomförandebeslut (EU) 2021/1772. Det är viktigt att den rättsliga ramen fortsätter att kräva att myndigheterna för att kunna utöva dessa befogenheter måste erhålla ett beslut ([134]) som utfärdats av behörig myndighet ([135]) och som godkänts av en oberoende *Judicial Commissioner* ([136]) (det s.k. double lock-förfarandet). Erhållandet av ett sådant beslut är fortsatt föremål för en nödvändighets- och proportionalitetsprövning ([137]).

(85) Sedan genomförandebeslut (EU) 2021/1772 antogs har samtidigt vissa specifika delar av 2016 års lag om utredningsbefogenheter ändrats genom 2024 års lag om utredningsbefogenheter (ändring) ([138]), som erhöll kunglig sanktion i april 2024. I den mån dessa ändringar och annan relevant utveckling rör villkoren, begränsningarna och skyddsåtgärderna för användningen av ovan nämnda särskilda utredningsbefogenheter av offentliga myndigheter i Förenade kungariket för brottsbekämpande ändamål, enligt bedömningen i skälen 177–215 i genomförandebeslut (EU) 2021/1772, analyseras de i följande punkter. När det gäller de delar av Förenade kungarikets ram som inte har ändrats genom den ovan nämnda lagen eller påverkats av annan relevant utveckling, är den analys som genomfördes i genomförandebeslut (EU) 2021/1772 fortfarande giltig.

(86) När det gäller riktat inhämtande och lagring av kommunikationsuppgifter ([139]) kvarstår de villkor och skyddsåtgärder som styr dessa befogenheter, enligt bedömningen i genomförandebeslut (EU) 2021/1772. I 2024 års lag om utredningsbefogenheter (ändring) förtydligas de befintliga skyddsåtgärderna genom att i avsnitt 11 i 2016 års lag om utredningsbefogenheter (som kriminaliserar olaglig inhämtning av kommunikationsuppgifter från en teleoperatör) införa en förteckning över exempel på vad som anses omfattas av begreppet *laglig auktoritet* i den bestämmelsen ([140]). Dessutom förtydligas ytterligare definitionen av kommunikationsuppgifter i avsnitt 261 i 2016 års lag om utredningsbefogenheter genom 2024 års lag om utredningsbefogenheter (ändring) genom att det uttryckligen anges att abonnentuppgifter omfattas av begreppet kommunikationsuppgifter ([141]).

([134]) I del 2 kapitel 2 i 2016 års lag om utredningsbefogenheter föreskrivs ett begränsat antal fall där ingripanden kan verkställas utan beslut. Detta består av följande: avlyssning med avsändarens eller mottagarens samtycke, avlyssning för administrativa ändamål eller verkställande ändamål, avlyssning som äger rum på vissa institutioner (fängelser, psykiatriska sjukhus och förvarsanläggningar för immigranter) samt avlyssning som utförs i enlighet med ett relevant internationellt avtal.

([135]) I de flesta fall är den ansvariga ministern den myndighet som utfärdar beslut enligt 2016 års lag om utredningsbefogenheter medan de skotska ministrarna har befogenhet att utfärda beslut om riktad avlyssning, beslut om ömsesidigt bistånd och beslut om riktat ingrepp i utrustning när de personer eller lokaler som det gäller och den utrustning som ingreppet ska ske i är belägna i Skottland (se avsnitten 22 och 103 i 2016 års lag om utredningsbefogenheter). Vid riktat ingrepp i utrustning kan chefer för brottsbekämpande myndigheter (som beskrivs i del 1 och del 2 i bilaga 6 till 2016 års lag om utredningsbefogenheter) utfärda beslutet enligt villkoren i avsnitt 106 i 2016 års lag om utredningsbefogenheter.

([136]) *Judicial Commissioners* bistår *Investigatory Powers Commissioner*, ett oberoende organ som utövar tillsyn över underrättelsetjänsternas användning av utredningsbefogenheter.

([137]) Se särskilt avsnitten 19 och 23 i 2016 års lag om utredningsbefogenheter.

([138]) Finns på följande länk: https://www.legislation.gov.uk/ukpga/2024/9/contents/2025-04-25.

([139]) Termen ”kommunikationsuppgifter” omfattar ”vem”, ”när”, ”var” och ”hur” i en kommunikation men inte innehållet, dvs. vad som sades eller skrevs. Kommunikationsuppgifter kan omfatta tid och varaktighet för kommunikation, avsändarens och mottagarens telefonnummer eller e-postadress och ibland platsen för de enheter från vilka telekommunikationen gjordes, se avsnitt 261.5 i 2016 års lag om utredningsbefogenheter. Enligt 2016 års lag om utredningsbefogenheter får ministern ålägga teleoperatörer att lagra kommunikationsuppgifter för riktad åtkomst för en rad myndigheter, däribland brottsbekämpande myndigheter och underrättelsetjänster. Del 4 i 2016 års lag om utredningsbefogenheter innehåller bestämmelser om lagring av kommunikationsuppgifter, medan del 3 föreskriver riktat inhämtande av kommunikationsuppgifter. I del 3 och del 4 i 2016 års lag om utredningsbefogenheter fastställs också särskilda begränsningar av användningen av dessa befogenheter och särskilda skyddsåtgärder.

([140]) Till exempel när den berörda personen inhämtar kommunikationsuppgifterna med stöd av en lagstadgad befogenhet för den relevanta offentliga myndigheten, eller när kommunikationsuppgifterna inhämtas i enlighet med ett domstolsbeslut eller annat rättsligt tillstånd. Avsnitt 11.3A i 2016 års lag om utredningsbefogenheter, som infördes genom avsnitt 12.3 i 2024 års lag om utredningsbefogenheter (ändring).

([141]) Avsnitt 261.5A och 261.5B, som infördes genom avsnitt 13.3 i 2024 års lag om utredningsbefogenheter (ändring).

(87) Utfärdandet av förelägganden om lagring av kommunikationsuppgifter ([142]) omfattas även fortsatt av begränsningar och skyddsåtgärder, såsom beskrivs i skälen 208 och 209 i genomförandebeslut (EU) 2021/1772, särskilt kraven på nödvändighet och proportionalitet samt godkännande av en oberoende *Judicial Commissioner*. Genom 2024 års lag om utredningsbefogenheter (ändring) infördes möjligheten att förnya sådana förelägganden, men alla förnyelser omfattas av samma villkor avseende nödvändighet och proportionalitet och godkännande av *Judicial Commissioner* ([143]).

(88) När det gäller kommunikationsuppgifter ändrades genom 2024 års lag om utredningsbefogenheter (ändring) även definitionen av en teleoperatör, dvs. de som kan omfattas av ett föreläggande om lagring. Denna definition omfattar nu alla personer som ”kontrollerar eller tillhandahåller ett telekommunikationssystem som i) inte (helt eller delvis) är beläget i eller kontrolleras av Förenade kungariket och ii) används av en annan person för att erbjuda eller tillhandahålla en telekommunikationstjänst till personer i Förenade kungariket” ([144]). Den ändrade definitionen kräver fortfarande alltid en nära koppling till den brittiska marknaden. I ändringen klargörs därför att stora företag med komplexa företagsstrukturer i sin helhet omfattas av 2016 års lag om utredningsbefogenheter utan att definitionen utvidgas till att omfatta leverantörer av telekommunikationstjänster som inte riktar sig till personer i Förenade kungariket.. Detta bekräftas också av de förklarande anmärkningarna till 2024 års lag om utredningsbefogenheter (ändring) (*Investigatory Powers (Amendment) Act 2024*) som föreskriver att ändringen inte syftar till att utöka tillämpningsområdet för de relevanta befogenheterna enligt 2016 års lag om utredningsbefogenheter ([145]) till fler företag, utan har i huvudsak en klargörande funktion.

(89) Slutligen infördes genom 2024 års lag om utredningsbefogenheter (ändring) vissa riktade ändringar av förfarandet för utfärdande av beslut, bland annat när det gäller riktad avlyssning och riktat ingrepp i utrustning, dvs. befogenheter som även kan användas av särskilda brottsbekämpande myndigheter i Förenade kungariket för att förebygga eller upptäcka allvarliga brott. Ändringarna gäller endast den specifika situation där dessa befogenheter används för att erhålla meddelanden från eller privat information om en person som är ledamot av en relevant lagstiftande församling ([146]). Även om beslut avseende riktad avlyssning och riktat ingrepp i utrustning normalt kan utfärdas av den ansvariga ministern och godkänns av en domare (se skälen 186–196 och 210–215 i genomförandebeslut (EU) 2021/1772), kräver avsnitten 26 och 111 i lagen om utredningsbefogenheter dessutom godkännande av premiärministern när beslutet gäller en parlamentsledamot eller en annan relevant lagstiftande församling (det s.k. triple-lock-förfarandet). Enligt 2024 års lag om utredningsbefogenheter (ändring) får nu premiärministern utse fem ansvariga ministrar som bemyndigas att utöva premiärministerns befogenhet att godkänna dessa beslut, förutsatt att behovet av godkännande är brådskande och att premiärministern inte kan godkänna besluten på grund av medicinsk oförmåga eller bristande tillgång till säker kommunikation. Det är viktigt att de begränsningar och skyddsåtgärder som gäller för utfärdandet av dessa beslut, såsom beskrivs i ovannämnda skäl i genomförandebeslut (EU) 2021/1772, kvarstår.

3.2.2 *Vidare användning av de insamlade uppgifterna*

(90) En brottsbekämpande myndighets delning av uppgifter med en annan myndighet för andra ändamål än de för vilka de ursprungligen samlades in (s.k. vidare delning) omfattas fortfarande av de villkor som analyseras i skälen 142–156 i genomförandebeslut (EU) 2021/1772.

([142]) Utfärdandet av sådana förelägganden om lagring enligt avsnitten 87–89 i 2016 års lag om utredningsbefogenheter syftar till att säkerställa att teleoperatörer, dock för en period på högst tolv månader, lagrar relevanta kommunikationsuppgifter som annars skulle raderas när de inte längre behövs för affärsändamål. De lagrade uppgifterna ska förbli tillgängliga under den tid som krävs om det senare skulle bli nödvändigt för en myndighet att inhämta dem inom ramen för ett tillstånd för riktat inhämtande av kommunikationsuppgifter enligt del 3 i 2016 års lag om utredningsbefogenheter.

([143]) Avsnitt 94A i 2016 års lag om utredningsbefogenheter, som infördes genom avsnitt 20.4 i 2024 års lag om utredningsbefogenheter (ändring).

([144]) Avsnitt 261.10 c i 2016 års lag om utredningsbefogenheter, som infördes genom avsnitt 19 i 2024 års lag om utredningsbefogenheter (ändring).

([145]) Förklarande anmärkningar till 2024 års lag om utredningsbefogenheter (ändring), punkt 359, finns på följande länk: https://www.legislation.gov.uk/ukpga/2024/9/pdfs/ukpgaen_20240009_en.pdf.

([146]) Se avsnitten 26 och 111 i 2016 års lag om utredningsbefogenheter.

(91) När det gäller den särskilda situationen med vidareöverföringar från Förenade kungariket till Förenta staterna har avtalet mellan Förenade konungariket Storbritannien, Nordirlands regering och Amerikas förenta staters regering om tillgång till elektroniska uppgifter för bekämpning av grov brottslighet (*avtalet mellan Förenade kungariket och Förenta staterna*) ([147]), som ingicks i oktober 2019, trätt i kraft och tillämpats sedan oktober 2022. Enligt avtalet mellan Förenade kungariket och Förenta staterna skulle uppgifter som överförs från EU till tjänsteleverantörer i Förenade kungariket kunna bli föremål för förelägganden om framläggande av elektroniska bevis som utfärdats av behöriga amerikanska brottsbekämpande myndigheter och gjorts tillämpliga i Förenade kungariket.

(92) Det är viktigt att de villkor och skyddsåtgärder enligt vilka sådana förelägganden kan utfärdas och verkställas, såsom bedömts i skäl 154 i genomförandebeslut (EU) 2021/1772, fortsatt är tillämpliga. Särskilt gäller att uppgifter som inhämtas enligt avtalet åtnjuter ett skydd som är likvärdigt med de särskilda skyddsåtgärder som föreskrivs i det så kallade paraplyavtalet mellan EU och Förenta staterna ([148]), vilka samtliga har införlivats i avtalet mellan Förenade kungariket och Förenta staterna genom hänvisning i tillämpliga delar ([149]).

(93) Sedan antagandet av genomförandebeslut (EU) 2021/1772 har Förenade kungariket förklarat att landet, bland annat genom samarbete med de berörda parterna i samband med genomförandet av avtalet mellan Förenade kungariket och Förenta staterna, har klargjort hur de särskilda skyddsåtgärder i paraplyavtalet som utformats för samarbete mellan brottsbekämpande myndigheter har anpassats och tillämpats på de specifika överföringar som omfattas av avtalet mellan Förenade kungariket och Förenta staterna. Förenade kungariket har särskilt förklarat att de bestämmelser i paraplyavtalet som föreskriver en roll för den berörda behöriga myndigheten (vilket inte är fallet vid direkt samarbete mellan en tjänsteleverantör i Förenade kungariket och en brottsbekämpande myndighet i Förenta staterna) i tillämpliga delar tolkas som en hänvisning till den utsedda myndigheten (enligt definitionen i avtalet mellan Förenade kungariket och Förenta staterna) ([150]) för den berörda parten.

(94) Till exempel har Förenade kungariket förklarat att, när det gäller anmälan av informationssäkerhetsincidenter enligt artikel 10 i paraplyavtalet mellan EU och Förenta staterna, som kräver att en anmälan görs till den överförande behöriga myndigheten, ska denna bestämmelse tillämpas i tillämpliga delar, så att anmälan i stället ska göras till den utsedda myndigheten hos den part från vilken uppgifterna har överförts.

(95) När det gäller kravet på tillstånd från den överförande behöriga myndigheten före vidareöverföring av personuppgifter enligt artikel 7 i paraplyavtalet har Förenade kungariket klargjort att denna bestämmelse ska tillämpas i tillämpliga delar, så att det är den utsedda myndigheten hos den part från vilken uppgifterna överfördes som måste godkänna vidareöverföring.

(96) När det gäller skyldigheterna enligt artikel 8 i paraplyavtalet om att säkerställa kvalitet och integritet i informationen, skulle en motsvarande tolkning av bestämmelsen innebära att den utsedda myndigheten hos den part som tar emot uppgifterna ansvarar för att samordna med den leverantör som har överfört uppgifterna vid eventuella problem med uppgifternas kvalitet och integritet.

([147]) Avtal mellan Förenade konungariket Storbritannien, Nordirlands regering och Amerikas förenta staters regering om tillgång till elektroniska uppgifter för bekämpning av grov brottslighet, finns på följande länk: 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]) Avtal mellan Amerikas förenta stater och Europeiska unionen om skydd av personuppgifter i samband med förebyggande, utredning, upptäckt och lagföring av brott (EUT L 336, 10.12.2016, s. 3, ELI: http://data.europa.eu/eli/agree_internation/2016/2220/oj).

([149]) Artikel 9.1 i avtalet.

([150]) I enlighet med artikel 1.8 i avtalet mellan Förenade kungariket och Förenta staterna avser ”utsedd myndighet” det statliga organ som, för Förenade kungarikets del, utses av inrikesministern (*Secretary of State for the Home Department*), och för Förenta staternas del, av justitieministern (*Attorney General*).

(97) När det gäller rättslig prövning har Förenade kungariket understrukit att överföringar enligt avtalet mellan Förenade kungariket och Förenta staterna alltid kommer att involvera den utsedda myndigheten hos varje part. När Förenta staterna är den part som mottar uppgifter från tjänsteleverantörer i Förenade kungariket ska Förenta staternas justitiedepartement fungera som den utsedda myndigheten. Enligt Förenade kungarikets tolkning ska därför justitiedepartementet vara involverat i varje begäran som utfärdas med stöd av avtalet mellan Förenade kungariket och Förenta staterna, som är en federal myndighet som utsetts enligt den amerikanska lagen om rättslig prövning. Därmed kan rättslig prövning utövas mot justitiedepartementet i enlighet med artikel 19 i paraplyavtalet. Dessutom har Förenade kungariket bekräftat för kommissionens avdelningar att lagen om rättslig prövning inte är den enda mekanismen för att söka rättslig prövning. Beroende på omständigheterna och kontexten i det enskilda fallet finns andra tillämpliga amerikanska lagar som erbjuder alternativa vägar för att söka rättslig prövning.

3.2.3 *Tillsyn och prövningsmöjligheter*

(98) Beroende på vilka befogenheter som används av de behöriga myndigheterna vid behandling av personuppgifter för brottsbekämpande ändamål (enligt antingen 2018 års dataskyddslag eller 2016 års lag om utredningsbefogenheter), fortsätter olika organ att utöva tillsyn över användningen av dessa befogenheter, såsom bedömts i skälen 158–174 i genomförandebeslut (EU) 2021/1772. Möjligheter till prövning finns även fortsatt tillgängliga enligt del 3 i 2018 års dataskyddslag, enligt 2016 års lag om utredningsbefogenheter och *Human Rights Act 1998*, i enlighet med analysen i skälen 250–269 i genomförandebeslut (EU) 2021/1772.

(99) När det gäller tillsynen över del 3 i 2018 års dataskyddslag analyseras *Information Commissions* uppgifter och befogenheter i skälen 158–160 och 162 i genomförandebeslut (EU) 2021/1772, med förbehåll för de ändringar som införs genom *Data (Use and Access) Act* och som beskrivs i avsnitten 2.3.1 och 2.3.2 i detta beslut.

(100) Vad gäller tillämpningen av dessa befogenheter har *Information Commissioner* sedan genomförandebeslut (EU) 2021/1772 antogs hanterat ett stort antal klagomål ([151]) samt genomfört flera utredningar och vidtagit verkställighetsåtgärder i fråga om brottsbekämpande myndigheters behandling av uppgifter. Mellan 2021 och 2025 genomförde *Information Commissioner* utredningar och utfärdade reprimander mot olika polisorgan för bristande efterlevnad av sina dataskyddsskyldigheter, exempelvis vid besvarande av begäranden om tillgång till uppgifter, vid införande av säkerhetsåtgärder för videoövervakningsuppgifter, vid behandling av känsliga uppgifter i brottsregister, vid sammanslagning av uppgifter om olika enskilda personer eller vid utlämnande av personuppgifter till tredje part ([152]). *Information Commissioner* utfärdade även riktlinjer, yttranden och vägledningsdokument, exempelvis om rätten till tillgång eller om hantering av uppenbart ogrundade eller orimliga begäranden enligt del 3 i 2018 års dataskyddslag ([153]).

(101) När det gäller användningen av utredningsbefogenheter inom ramen för 2016 års lag om utredningsbefogenheter, säkerställs fortsatt oberoende och rättslig tillsyn av *Investigatory Powers Commissioner*, med bistånd av andra *Judicial Commissioners*, som tillsammans kallas *Judicial Commissioners* ([154]). Inom detta område har *Investigatory Powers (Amendments) Act 2024* endast medfört begränsade och riktade ändringar, som inte påverkar *Judicial Commissioners* oberoende, uppgifter och befogenheter, utan syftar till att stärka det befintliga tillsynssystemets praktiska funktion, särskilt genom införandet av ställföreträdande *Investigatory Powers Commissioners* till vilka *Investigatory Powers Commissioner* kan delegera särskilda befogenheter när de inte kan eller är tillgängliga för att utföra sina uppgifter. Sådana ställföreträdande *Investigatory Powers Commissioners* måste vara *Judicial Commissioners* och utses av *Investigatory Powers Commissioner* ([155]).

([151]) Till exempel tog *Information Commissioner* under 2023–2024 emot 1 890 klagomål med stöd av den allmänna dataskyddsförordningen och/eller dataskyddslagen från 2018 avseende organisationer inom undersektorerna ”Police Authority”, ”Police Forces” och ”Police Commissioners”. Se även *Information Commissioner's Annual Report and Financial Statements 2023/24*, som finns på följande länk: https://ico.org.uk/media2/migrated/4030348/annual-report-2023-24.pdf.

([152]) Mer information finns på följande länk: https://ico.org.uk/action-weve-taken/enforcement/?ensector=criminal-justice.

([153]) Finns på följande länk: https://ico.org.uk/for-organisations/law-enforcement/the-right-of-access-part-3-of-the-dpa-2018/ and https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/individual-rights/manifestly-unfounded-and-excessive-requests/.

([154]) Se skäl 250 i genomförandebeslut (EU) 2021/1772.

([155]) Avsnitt 227 i 2016 års lag om utredningsbefogenheter, som infördes genom avsnitt 7 i lagen om utredningsbefogenheter (ändring).

3.3 Relevant utveckling när det gäller brittiska myndigheters tillgång och användning för ändamål som rör den nationella säkerheten

(102) När det gäller utredningsbefogenheter som utövas inom ramen för nationell säkerhet fortsätter 2016 års lag om utredningsbefogenheter att utgöra den rättsliga ramen för utövandet av dessa befogenheter. Utöver de ändringar som rör riktade utredningsbefogenheter, vilka – under vissa särskilda villkor – även kan utnyttjas av vissa brottsbekämpande myndigheter, såsom beskrivs i skälen 77–85 i detta beslut, har 2024 års lag om utredningsbefogenheter (ändring) även medfört ändringar av en av de befogenheter enligt 2016 års lag om utredningsbefogenheter som kan utövas för massutredning.

(103) Mer specifikt har det genom 2024 års lag om utredningsbefogenheter (ändring) införts ett särskilt system i den nya del 7A i 2016 års lag om utredningsbefogenheter, avseende lagring och granskning av en specifik kategori av massdataset av personuppgifter ([156]), det vill säga sådana uppgifter där de registrerade personerna antingen inte kan ha, eller endast kan ha en låg, rimlig förväntan på integritet förhållande till uppgifterna ([157]). Huruvida ett massdataset av personuppgifter ingår i detta specifika dataset ska avgöras av chefen för en underrättelsetjänst utifrån samtliga omständigheter, särskilt i) uppgifternas karaktär, ii) i vilken utsträckning uppgifterna har offentliggjorts av enskilda personer eller med dessa enskilda personers samtycke, iii) om uppgifterna har offentliggjorts, i vilken mån detta har skett under redaktionell kontroll eller av en person som agerat i enlighet med yrkesetiska normer, iv) om uppgifterna har offentliggjorts eller på annat sätt är offentligt tillgängliga, i vilken utsträckning dessa uppgifter är allmänt kända, samt v) i vilken utsträckning uppgifterna redan har använts i det offentliga rummet ([158]).

(104) Det är viktigt att notera att för lagring och granskning av massdataset av personuppgifter som inte omfattas av denna kategori, dvs. de som är känsligare och därför innebär att integritet rimligen kan förväntas, kvarstår det system som analyseras i skälen 239 och 240 i genomförandebeslut (EU) 2021/1772. I synnerhet gäller fortsatt kravet på ett beslut som först måste godkännas av den ansvariga ministern och därefter av en *Judicial Commissioner*. Detta sker under förutsättning att åtgärden uppfyller kraven på nödvändighet och proportionalitet, i enlighet med bestämmelserna i del 7 i 2016 års lag om utredningsbefogenheter ([159]).

(105) I del 7A i 2016 års lag om utredningsbefogenheter föreskrivs två typer av tillstånd: individuellt tillstånd och kategoritillstånd. Lagring eller lagring och granskning av alla massdataset av personuppgifter som innehas enligt del 7A måste tillåtas enligt något av dessa tillstånd. Båda tillstånden kräver i princip ([160]) tillstånd av chefen för underrättelsetjänsten (eller en person som agerar på dennes vägnar) och godkännande av en oberoende *Judicial Commissioner* ([161]). Ett individuellt tillstånd beviljas av chefen för en underrättelsetjänst på de villkor som anges i avsnitt 226B.4 i 2016 års lag om utredningsbefogenheter, och efter förhandsgodkännande av de som är *Judicial Commissioners*. *Judicial Commissioner* måste granska slutsatserna från den person som beviljade tillståndet med avseende på huruvida avsnitt 226A, dvs. att det finns låga eller inga rimliga förväntningar med avseende på integritetskrav, gäller för det massdataset av personuppgifter som beskrivs i tillståndet ([162]).

([156]) Beslut om massdataset av personuppgifter, som utfärdas enligt artikel 200 i 2016 års lag om utredningsbefogenheter, ger underrättelsetjänster rätt att lagra och granska dataset som innehåller personuppgifter om flera individer, där flertalet av dessa personer inte är – och sannolikt inte heller kommer att bli – av intresse för underrättelsetjänsten i dess verksamhetsutövning. Uppgifterna lagras elektroniskt av en underrättelsetjänst och innehas för analys inom ramen för dess lagstadgade uppdrag. Se även artikel 199 i 2016 års lag om utredningsbefogenheter.

([157]) Avsnitt 226A.1 i 2016 års lag om utredningsbefogenheter, som infördes genom avsnitt 2 i 2024 års lag om utredningsbefogenheter (ändring).

([158]) Avsnitt 226A.3 i 2016 års lag om utredningsbefogenheter, som infördes genom avsnitt 2 i 2024 års lag om utredningsbefogenheter (ändring).

([159]) Genom 2024 års lag om utredningsbefogenheter (ändring) har avsnitt 213 i 2016 års lag om utredningsbefogenheter ändrats så att beslut om massdataset av personuppgifter upphör att gälla tolv månader efter det att de utfärdades. Tidigare behövde sådana beslut förnyas var sjätte månad. Se avsnitt 3 i 2024 års lag om utredningsbefogenheter (ändring).

([160]) Ett individuellt tillstånd får endast beviljas utan föregående rättsligt godkännande i) om den person som beviljar det individuella tillståndet anser att massdatasetet av personuppgifter i fråga omfattas av ett befintligt kategoritillstånd eller ii) i brådskande fall, se avsnitt 226B.6 i 2016 års lag om utredningsbefogenheter. I det senare fallet måste beslutet att bevilja ett brådskande individuellt tillstånd ses över av en *Judicial Commissioner* tre arbetsdagar efter utfärdandedagen, se avsnitt 226BC i 2016 års lag om utredningsbefogenheter.

([161]) Avsnitt 226B.1 i 2016 års lag om utredningsbefogenheter, som infördes genom avsnitt 2 i lagen om utredningsbefogenheter (ändring).

([162]) Avsnitt 226BB.1 a i 2016 års lag om utredningsbefogenheter, som infördes genom avsnitt 2 i 2024 års lag om utredningsbefogenheter (ändring).

(106) Ett kategoritillstånd medger lagring eller lagring och undersökning av en kategori av massdataset av personuppgifter som beskrivs i tillståndet.

(107) Beslutet att bevilja kategoritillstånd fattas av chefen för underrättelsetjänsten om denne anser att avsnitt 226A är tillämpligt på alla dataset inom kategorin och om beslutet att bevilja tillstånd godkänns av en oberoende *Judicial Commissioner* ([163]). Den senare måste huruvida avsnitt 226A, dvs. att det finns låga eller inga rimliga förväntningar med avseende på integritetskrav, gäller för alla dataset som omfattas av den kategori av dataset som beskrivs i tillståndet ([164]).

(108) Det är viktigt att påpeka att *Judicial Commissioner*, när denne godkänner ett beslut om att bevilja ett individuellt tillstånd eller ett kategoritillstånd, måste ”tillämpa samma principer som en domstol skulle tillämpa på en ansökan om rättslig prövning” ([165]) och beakta ärendet med tillräcklig noggrannhet för att säkerställa att de skyldigheter som föreskrivs i avsnitt 2 i 2016 års lag om utredningsbefogenheter (allmänna skyldigheter i fråga om integritet) ([166]) är uppfyllda. Dessutom är utfärdandet av tillstånd underkastat strikt efterhandstillsyn, särskilt genom årlig rapportering till ministern och parlamentets underrättelse- och säkerhetsutskott ([167]), samt genom regelbundna inspektioner av *Investigatory Powers Commissioner's Office* ([168]).

(109) När det gäller relevant utveckling avseende tillsyn, har *Investigatory Powers Commissioner's Office* publicerat årliga rapporter för åren 2021, 2022 och 2023 med detaljerad statistik och information om underrättelsetjänsters och brottsbekämpande myndigheters användning av utredningsbefogenheter i Förenade kungariket ([169]). Rapporterna redogör även för kontorets granskningar och utredningar samt deras resultat, och bekräftar att Investigatory Powers Commissioner fortsatt fullgör sin mycket viktiga tillsynsfunktion inom ramen för Förenade kungarikets system för utredningsbefogenheter. Till exempel granskade Investigatory Powers Commissioner under 2023 nödvändighets- och proportionalitetsbedömningarna för användningen av befogenheter för massavlyssning (såsom analyserats i skälen 218–225 i genomförandebeslut (EU) 2021/1772) av *Government Communications Headquarters*. Man drog slutsatsen att en betydande majoritet av motiveringarna var välgrundade, medan proportionalitetsaspekten i vissa fall inte var tillräckligt tydligt uttryckt. Dessa resultat diskuterades med enheten för efterlevnad vid *Government Communications Headquarters*, som åtog sig att beställa ytterligare internutbildning i syfte att öka medvetenheten och åtgärda denna brist ([170]).

(110) Domstolen för utredningsbefogenheter (*Investigatory Powers Tribunal*) utfärdade dessutom en offentlig rapport om sin verksamhet och rättspraxis för perioden 2021–2023 ([171]). Rapporten visar att antalet mål som tas emot av domstolen har mer än fördubblats sedan 2017, och att mer än 400 mål togs emot 2023 ([172]). De flesta klagomål

([163]) Avsnitt 226BA i 2016 års lag om utredningsbefogenheter, som infördes genom avsnitt 2 i lagen om utredningsbefogenheter (ändring).

([164]) Avsnitt 226BB.1 b i 2016 års lag om utredningsbefogenheter, som infördes genom avsnitt 2 i lagen om utredningsbefogenheter (ändring).

([165]) Avsnitt 226BB.2 a i 2016 års lag om utredningsbefogenheter, som infördes genom avsnitt 2 i 2024 års lag om utredningsbefogenheter (ändring).

([166]) Avsnitt 226BB.2 b i 2016 års lag om utredningsbefogenheter, som infördes genom avsnitt 2 i 2024 års lag om utredningsbefogenheter (ändring). I enlighet med de allmänna skyldigheter i fråga om integritet som anges i avsnitt 2 i 2016 års lag om utredningsbefogenheter ska en offentligt myndighet ta hänsyn till a) om det som avses med beslutet, tillståndet eller föreläggandet rimligen skulle kunna uppnås med andra mindre inkräktande medel, b) huruvida den skyddsnivå som ska tillämpas i samband med inhämtande av information enligt beslutet, tillståndet eller föreläggandet är högre på grund av den särskilda känsligheten för denna information, c) det allmänna intresset för integritet och säkerhet i fråga om telekommunikationssystem och andra posttjänster och d) alla andra aspekter av allmänt intresse när det gäller skyddet av integriteten.

([167]) Avsnitt 226DA och 226DB i 2016 års lag om utredningsbefogenheter, som infördes genom avsnitt 2 i 2024 års lag om utredningsbefogenheter (ändring).

([168]) Se Investigatory Powers Commissioners årsrapport från 2023, finns på följande länk: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/E03270100-HC_603-IPCO-Annual-Report-2023-Web_Accessible.pdf, s. 3.

([169]) Årsrapporterna finns på följande länk: https://www.ipco.org.uk/publications/annual-reports/.

([170]) Se punkterna 6.39–6.43 i årsrapporten 2023, som finns på följande länk: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/E03270100-HC_603-IPCO-Annual-Report-2023-Web_Accessible.pdf.

([171]) *The Investigatory Powers Tribunal Report 2021–2023*, som finns på https://investigatorypowerstribunal.org.uk/wp-content/uploads/2024/11/Investigatory-Powers-Tribunal-Report-2024.pdf.

([172]) The Investigatory Powers Tribunal Report 2021–2023, s. 5.

riktades mot brottsbekämpande myndigheter, tätt följt av säkerhets- och underrättelsemyndigheter ([173]). Det är viktigt att notera att domstolen 2022 och 2023 avkunnade domar i mål som den hade tagit emot före 2021, där den konstaterade att Förenade kungarikets offentliga myndigheter (Skottlands polismyndighet [*Police Scotland*] ([174]), polismyndigheten för Manchesters storstadsområde [*Greater Manchester Police*] ([175]), Surreys polismyndighet [*Surrey Police*] ([176]) och MI5 och inrikesministern [*Home Secretary*] ([177]) hade agerat olagligt. När det gäller rättsmedel beordrade domstolen bl.a. att allt material som erhållits olagligen skulle förstöras, och i ett fall även att 12 000 pund skulle betalas ut som en rättvis kompensation för de konstaterade överträdelserna. Årsrapporten bekräftar således att domstolen på ett effektivt sätt uppfyller sin viktiga funktion när det gäller att garantera tillsyn och prövning på området tillgång till personuppgifter inom ramen för brottsbekämpning och nationell säkerhet.

(111) Dessutom belyser rapporten också viktig utveckling, t.ex. en dom från Europeiska domstolen för de mänskliga rättigheterna i vilken domstolen slog fast att enskilda personer var som helst i världen kan begära att talan väcks vid *Investigatory Powers Tribunal* i fråga om tillämpningen av Förenade kungarikets system för massavlyssning om verksamheten i fråga utfördes av ett brittiskt offentligt organ och ägde rum i Förenade kungariket ([178]).

4. **SLUTSATS**

(112) Kommissionen anser att den brittiska dataskyddsförordningen och 2018 års dataskyddslag, i dess lydelse enligt *Data (Use and Access) Act* fortsätter att säkerställa en skyddsnivå för personuppgifter som överförs från Europeiska unionen som i allt väsentligt motsvarar den som garanteras genom förordning (EU) 2016/679.

(113) Kommissionen anser dessutom att tillsynsmekanismerna och möjligheterna till prövning enligt brittisk rätt sammantaget gör det möjligt att upptäcka och bestraffa överträdelser i praktiken och erbjuda den registrerade rättsmedel för att få tillgång till personuppgifter som rör honom eller henne och, i slutändan, rättelse eller radering av sådana uppgifter.

(114) På grundval av tillgänglig information om Förenade kungarikets rättsordning anser kommissionen slutligen att varje ingrepp i de grundläggande rättigheterna för de personer vars personuppgifter överförs från Europeiska unionen till Förenade kungariket av brittiska myndigheter för ändamål av allmänt intresse, särskilt brottsbekämpning och nationell säkerhet, kommer att begränsas till vad som är absolut nödvändigt för att uppnå det legitima målet i fråga och att det finns ett effektivt rättsligt skydd mot sådana intrång.

(115) Mot bakgrund av slutsatserna i detta beslut bör det därför beslutas att Förenade kungariket fortsätter att säkerställa en adekvat skyddsnivå i den mening som avses i artikel 45 i förordning (EU) 2016/679, tolkad mot bakgrund av Europeiska unionens stadga om de grundläggande rättigheterna.

(116) Denna slutsats grundar sig på både Förenade kungarikets relevanta inhemska system, eftersom det har utvecklats sedan genomförandebeslut (EU) 2021/1772 antogs, och dess internationella åtaganden, som särskilt innebär att Förenade kungarikets fortsatt är anslutet till den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna och fortsatt omfattas av jurisdiktionen för Europeiska domstolen för de mänskliga rättigheterna. Fortsatt efterlevnad av sådana internationella förpliktelser är därför ett särskilt viktigt inslag i den bedömning som ligger till grund för detta beslut.

([173]) *The Investigatory Powers Tribunal Report 2021–2023, s. 12.*
([174]) Wilson v Police Scotland [2022] UKIPTrib 5.
([175]) Pendlebury v Greater Manchester Police [2023] UKIPTrib 2.
([176]) Hill v Metropolitan Police Service & Independent Office For Police Conduct [2022] UKIPTrib 6.
([177]) Liberty & Privacy International v Security Service and Secretary of State for the Home Department [2023] UKIPTrib 1.
([178]) *Wieder and Guarnieri v UK*, [2023] Europeiska domstolen för de mänskliga rättigheterna 668, se även *Investigatory Powers Tribunal Report 2021–2023, s. 6*.

5. EFFEKTERNA AV DETTA BESLUT OCH DATASKYDDSMYNDIGHETERNAS ÅTGÄRDER

(117) Medlemsstaterna och deras organ är skyldiga att vidta de åtgärder som är nödvändiga för att följa unionsinstitutionernas rättsakter, eftersom dessa antas vara lagenliga och följaktligen har rättsverkningar fram till dess att de löper ut, återkallas, ogiltigförklaras inom ramen för en talan om ogiltigförklaring eller förklaras ogiltiga till följd av en begäran om förhandsavgörande eller en invändning om rättsstridighet.

(118) Ett beslut om adekvat skyddsnivå som antas av kommissionen enligt artikel 45.3 i förordning (EU) 2016/679 är följaktligen bindande för alla organ i medlemsstaterna som det riktar sig till, också för deras oberoende tillsynsmyndigheter. Under tillämpningsperioden för genomförandebeslut (EU) 2021/1772, i dess lydelse enligt detta beslut, får överföringar från en personuppgiftsansvarig eller ett personuppgiftsbiträde i Europeiska unionen till personuppgiftsansvariga eller personuppgiftsbiträden i Förenade kungariket ske utan ytterligare tillstånd.

(119) Det bör erinras om att enligt artikel 58.5 i förordning (EU) 2016/679, och i enlighet med vad domstolen förklarade i domen i målet *Schrems I* ([179]), ska en nationell dataskyddsmyndighet, även vid klagomål, ifrågasätta huruvida ett kommissionsbeslut om adekvat skyddsnivå är förenligt med den enskildas grundläggande rätt till integritet och skydd av personuppgifter och därför måste den nationella lagstiftningen innehålla ett rättsmedel för att framföra dessa invändningar till en nationell domstol som kan vara skyldig att begära ett förhandsavgörande från Europeiska unionens domstol ([180]).

6. ÖVERVAKNING

(120) Enligt artikel 45.4 i förordning (EU) 2016/679 ska kommissionen fortlöpande övervaka relevant utveckling i Förenade kungariket för att bedöma om det fortfarande säkerställer en väsentligen likvärdig skyddsnivå. Sådan övervakning är särskilt viktig eftersom Förenade kungariket kommer att tillämpa och upprätthålla ett ändrat dataskyddssystem. Dessutom ger Förenade kungarikets ändrade dataskyddsram ministern befogenhet att ytterligare specificera denna ram genom sekundärlagstiftning. I detta avseende bör särskild uppmärksamhet ägnas åt sådana ytterligare specifikationer samt tillämpningen i praktiken av Förenade kungarikets ändrade regler om överföring av personuppgifter till tredjeländer, effektiviteten när det gäller utövandet av individuella rättigheter, inbegripet all relevant utveckling med avseende på lagstiftning och praxis när det gäller de nyligen införda undantagen eller begränsningarna av sådana rättigheter, ICO:s omstrukturerade funktion, inbegripet med avseende på hanteringen av klagomål och tillämpningen av korrigerande befogenheter, samt efterlevnaden av begränsningarna och skyddsåtgärderna när det gäller statlig tillgång, särskilt när det gäller den nyligen införda del 7A i 2016 års lag om utredningsbefogenheter. Bland annat bör utveckling av rättspraxis och ICO:s och andra oberoende organs tillsyn ligga till grund för kommissionens övervakning.

(121) För att underlätta denna övervakning bör de brittiska myndigheterna omgående informera kommissionen om alla väsentliga ändringar av den brittiska rättsordningen som påverkar den rättsliga ram som är föremål för genomförandebeslut (EU) 2021/1772, i dess lydelse enligt detta beslut, liksom om eventuella förändringar av praxis i samband med behandling av personuppgifter som bedöms i genomförandebeslut (EU) 2021/1772, i dess lydelse enligt detta beslut, både vad gäller personuppgiftsansvarigas och personuppgiftsbiträdens behandling av personuppgifter enligt den brittiska dataskyddsförordningen och de begränsningar och skyddsåtgärder som är tillämpliga på myndigheters tillgång till personuppgifter. Detta bör omfatta utveckling gällande de faktorer som nämns i skäl 120.

(122) För att kommissionen ska kunna utföra sin övervakningsfunktion på ett effektivt sätt bör medlemsstaterna dessutom informera kommissionen om alla relevanta åtgärder som vidtas av de nationella dataskyddsmyndigheterna, särskilt när det gäller förfrågningar eller klagomål från registrerade i EU om överföring av personuppgifter från unionen till personuppgiftsansvariga eller personuppgiftsbiträden i Förenade kungariket. Kommissionen bör också informeras om eventuella indikationer på att de åtgärder som vidtas av brittiska myndigheter med ansvar för att förebygga, utreda, avslöja eller lagföra brott eller för nationell säkerhet, inbegripet eventuella tillsynsorgan, inte säkerställer den skyddsnivå som krävs.

([179]) Se föregående fotnot, punkt 65.

([180]) *Schrems I*, punkt 65: ”Det ankommer härvidlag på den nationella lagstiftaren att föreskriva rättsmedel som gör det möjligt för den nationella tillsynsmyndigheten att vid nationella domstolar göra gällande de invändningar som den anser att det finns fog för, så att nationella domstolar, för det fall att de delar myndighetens tvivel angående kommissionsbeslutets giltighet, kan hänskjuta en begäran om förhandsavgörande för att granska detta besluts giltighet.”

(123) Om tillgänglig information, särskilt information från övervakningen av genomförandebeslut (EU) 2021/1772, i dess lydelse enligt detta beslut, eller från Förenade kungarikets eller medlemsstaternas myndigheter, visar att den skyddsnivå som Förenade kungariket erbjuder kanske inte längre är adekvat, bör kommissionen omgående informera de behöriga myndigheterna i Förenade kungariket om detta och begära att lämpliga åtgärder vidtas inom en angiven tidsram, som inte får överskrida tre månader. Med hänsyn tagen till problemets art och/eller de åtgärder som krävs får denna period vid behov förlängas med en angiven tidsperiod. Ett sådant förfarande skulle till exempel inledas i fall där vidare överföringar, även på grundval av de nya bestämmelser om adekvat skyddsnivå som antas av den ansvariga ministern eller enligt internationella avtal som ingås av Förenade kungariket, inte längre utförs enligt skyddsåtgärder som säkerställer ett fortsatt skydd i den mening som avses i artikel 44 i förordning (EU) 2016/679.

(124) Om de behöriga brittiska myndigheterna vid utgången av den angivna tidsfristen underlåter att vidta dessa åtgärder eller på annat tillfredsställande sätt visar att detta beslut fortfarande bygger på en adekvat skyddsnivå, kommer kommissionen att inleda det förfarande som avses i artikel 93.2 i förordning (EU) 2016/679 i syfte att helt eller delvis tillfälligt upphäva eller upphäva detta beslut.

(125) Alternativt kommer kommissionen att inleda detta förfarande i syfte att ändra beslutet, särskilt genom att underställa överföringar av uppgifter ytterligare villkor eller genom att begränsa räckvidden för slutsatsen om adekvat skyddsnivå endast till uppgiftsöverföringar för vilka en adekvat skyddsnivå fortfarande säkerställs.

(126) Vid vederbörligen motiverade och tvingande skäl till skyndsamhet kommer kommissionen att utnyttja möjligheten att, i enlighet med det förfarande som avses i artikel 93.3 i förordning (EU) 2016/679, anta genomförandeakter med omedelbar verkan som upphäver, återkallar eller ändrar beslutet.

7. ÖVERSYN, GILTIGHETSTID OCH FÖRLÄNGNING AV DETTA BESLUT

(127) Vid tillämpningen av artikel 45.3 i förordning (EU) 2016/679, och med tanke på att skyddsnivån i Förenade kungarikets rättsliga ram kan bli föremål för ändringar, bör kommissionen, efter antagandet av detta beslut, regelbundet se över huruvida konstaterandena om den adekvata skyddsnivå som säkerställs av Förenade kungariket fortfarande är sakligt och rättsligt motiverade, med beaktande av de element som anges i artikel 45.2 i förordning (EU) 2016/679. Sådana utvärderingar bör äga rum minst vart fjärde år och bör omfatta alla aspekter av hur detta beslut fungerar, däribland hur de relevanta tillsyns- och verkställighetsmekanismerna fungerar.

(128) För att genomföra översynen bör kommissionen träffa relevanta företrädare för de brittiska myndigheterna, inklusive *Information Commission*. Deltagande i mötet bör vara öppet för företrädare för ledamöterna i Europeiska dataskyddsstyrelsen. I samband med översynen bör kommissionen begära att UK förser den med omfattande information om samtliga aspekter av relevans för konstaterandet om adekvat skyddsnivå. Kommissionen bör också begära klargöranden om de uppgifter som inkommit till den och som är relevanta för detta beslut, däribland från Europeiska dataskyddsstyrelsen, enskilda dataskyddsmyndigheter, grupper i det civila samhället, offentliga rapporter eller medierapporter eller andra tillgängliga informationskällor.

(129) På grundval av översynen ska kommissionen utarbeta en offentlig rapport som ska överlämnas till Europaparlamentet och rådet.

(130) Kommissionen måste också ta hänsyn till att den dataskyddsram som bedöms i detta beslut och i genomförandebeslut (EU) 2021/1772 kan komma att utvecklas ytterligare.

(131) Det är därför lämpligt att föreskriva att detta beslut ska tillämpas under en period av sex år från och med dess ikraftträdande.

(132) Om framför allt information från övervakningen av detta beslut visar att slutsatserna om den skyddsnivå som säkerställs i Förenade kungariket fortfarande är sakligt och rättsligt motiverade, bör kommissionen senast sex månader innan detta beslut upphör att gälla inleda förfarandet för att ändra detta beslut genom att i princip förlänga dess tidsmässiga tillämpningsområde med ytterligare fyra år. En eventuell sådan genomförandeakt som ändrar detta beslut ska antas i överensstämmelse med det förfarande som nämns i artikel 93.2 i förordning (EU) 2016/679.

8. **SLUTLIGA ÖVERVÄGANDEN**

(133) Europeiska dataskyddsstyrelsen har offentliggjort ett yttrande ([181]), vilket har beaktats vid utarbetandet av detta beslut.

(134) De åtgärder som föreskrivs i detta beslut är förenliga med yttrandet från den kommitté som inrättats i enlighet med artikel 93 i förordning (EU) 2016/679.

(135) Genomförandebeslut (EU) 2021/1772 bör därför ändras i enlighet med detta.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Artikel 1.2 i genomförandebeslut (EU) 2021/1772 ska upphöra att gälla.

Artikel 2

Artikel 4 i genomförandebeslut (EU) 2021/1772 ska ersättas med följande:

”*Artikel 4*

Detta beslut ska upphöra att gälla den 27 december 2031, såvida det inte förlängs i enlighet med det förfarande som avses i artikel 93.2 i förordning (EU) 2016/679.”

Artikel 3

Detta beslut riktar sig till medlemsstaterna.

Utfärdat i Bryssel den 19 december 2025.

På kommissionens vägnar
Michael MCGRATH
Ledamot av kommissionen

([181]) Yttrande 26/2025 om Europeiska kommissionens utkast till genomförandebeslut i enlighet med förordning (EU) 2016/679 om adekvat skydd av personuppgifter i Förenade kungariket, som finns på https://www.edpb.europa.eu/system/files/2025-10/edpb_opinion_202526_united_kingdom_adequacy_gdpr_en.pdf.