

II

(Icke-lagstiftningsakter)

BESLUT

KOMMISSIONENS GENOMFÖRANDEFÖRORDNING (EU) 2021/1772

av den 28 juni 2021

i enlighet med Europaparlamentets och rådets direktiv (EU) 2016/679 om adekvat skydd av personuppgifter i Förenade kungariket*[delgivet med nr C(2021) 4800]***(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 förordning (EU) 2016/679 fastställs regler för överföring av personuppgifter från personuppgiftsansvariga eller personuppgiftsbiträden i Europeiska unionen till tredjeländer och internationella organisationer i den mån sådana överföringar omfattas av förordningens tillämpningsområde. Reglerna om internationella överföringar av uppgifter fastställs i kapitel V i den förordningen, dvs. i artiklarna 44–50. Flödet av personuppgifter till och från länder utanför Europeiska unionen är av avgörande betydelse för det internationella samarbetet och den gränsöverskridande handeln men skyddet av personuppgifter i Europeiska unionen får inte undergrävas av överföringar till tredjeländer ⁽²⁾.
- (2) Enligt artikel 45.3 i förordning (EU) 2016/679 får kommissionen genom en genomförandeakt besluta att ett tredjeland, ett territorium eller en eller flera specificerade sektorer i ett tredjeland eller en internationell organisation säkerställer en adekvat skyddsnivå. Enligt detta villkor får överföring av personuppgifter till ett tredjeland ske utan ytterligare tillstånd enligt artikel 45.1 och skäl 103 i den förordningen.
- (3) Enligt artikel 45.2 i förordning (EU) 2016/679 måste antagandet av ett beslut om adekvat skyddsnivå grundas på en omfattande analys av tredjelandets rättsordning som omfattar både de regler som är tillämpliga på uppgiftsinföraren, begränsningarna och skyddsåtgärderna när det gäller myndigheters tillgång till personuppgifter. I sin bedömning måste kommissionen avgöra om det berörda tredjelandet garanterar en skyddsnivå som "i allt väsentligt är likvärdig" med den som säkerställs inom Europeiska unionen (skäl 104 i förordning (EU) 2016/679). Den standard mot vilken den "väsentliga likvärdigheten" bedöms är den som fastställs i EU-lagstiftningen, särskilt förordning (EU) 2016/679 samt rättspraxis från Europeiska unionens domstol ⁽³⁾. Europeiska dataskyddsstyrelsens referensram för adekvat skyddsnivå är också av betydelse i detta avseende ⁽⁴⁾.

⁽¹⁾ EUT L 119, 4.5.2016, s. 1.⁽²⁾ Se skäl 101 i förordning (EU) 2016/679.⁽³⁾ Se det senaste målet C-311/18, Facebook Ireland och Schrems (Schrems II), ECLI:EU:C:2020:559.⁽⁴⁾ Europeiska dataskyddsstyrelsen, *Adequacy Referential*, WP 254 rev. 01. Finns på följande länk: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

- (4) Enligt EU-domstolen kräver detta inte att en identisk skyddsnivå uppnås ⁽⁵⁾. I synnerhet kan de medel som tredjelandet i fråga har till sitt förfogande för att skydda personuppgifter skilja sig från dem som används i Europeiska unionen förutsatt att de i praktiken visar sig vara effektiva för att säkerställa en adekvat skyddsnivå ⁽⁶⁾. Standarden för en adekvat skyddsnivå kräver därför inte att unionens regler kopieras till punkt och pricka. Det handlar snarare om huruvida det utländska systemet som helhet, genom innehållet i rätten till dataskydd och dess faktiska genomförande, övervakning och verkställighet, uppnår den skyddsnivå som krävs ⁽⁷⁾.
- (5) Kommissionen har noggrant analyserat Förenade kungarikets lagstiftning och praxis. På grundval av konstateranden som utvecklas i skälen 8–270 drar kommissionen slutsatsen att Förenade kungariket säkerställer en adekvat skyddsnivå för personuppgifter som inom tillämpningsområdet för förordning (EU) 2016/679 överförs från Europeiska unionen till Förenade kungariket.
- (6) Denna slutsats rör inte personuppgifter som överförs 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 (*UK Data Protection Act*). Giltigheten och tolkningen av invandringsundantaget enligt brittisk lagstiftning har ännu inte fastställts, på grund av ett beslut från appellationsdomstolen för England och Wales av den 26 maj 2021. Även om appellationsdomstolen har bekräftat att registrerades rättigheter i princip kan begränsas när det gäller invandringskontroll som "en fråga av viktigt allmänintresse" har den slagit fast att invandringsundantaget i sin nuvarande form är oförenligt med brittisk rätt, eftersom lagstiftningsåtgärden saknar specifika bestämmelser som fastställer de skyddsåtgärder som anges i artikel 23.2 i Förenade kungarikets allmänna dataskyddsförordning (den brittiska dataskyddsförordningen) ⁽⁸⁾. Under dessa förhållanden bör överföring av personuppgifter från unionen till Förenade kungariket undantas från detta besluts tillämpningsområde om personuppgifterna i fråga omfattas av invandringsundantaget ⁽⁹⁾. När den brittiska lagstiftningen har gjorts förenlig bör invandringsundantaget och behovet av att upprätthålla begränsningen av detta besluts tillämpningsområde tas upp till förnyad bedömning.
- (7) Detta beslut bör inte påverka den direkta tillämpningen av förordning (EU) 2016/679 på organisationer som är etablerade i Förenade kungariket om villkoren för den förordningens territoriella tillämpningsområde, som fastställs i artikel 3 i den förordningen, är uppfyllda.

2. REGLER FÖR BEHANDLING AV PERSONUPPGIFTER

2.1 Den konstitutionella ramen

- (8) Förenade kungariket är en parlamentarisk demokrati som har en konstitutionell monark som statschef. Det har ett suveränt parlament som är högsta instans för alla andra statliga institutioner, en verkställande makt som är utvald av och ansvarig inför parlamentet och ett oberoende rättsväsende. Den verkställande makten får sitt bemyndigande från sin förmåga att upprätthålla det valda underhusets förtroende och är ansvarig inför båda kamrarna i parlamentet som ansvarar för att granska regeringen samt debattera och stifta lagar.

⁽⁵⁾ Mål C-362/14, Schrems (Schrems I), ECLI:EU:C:2015:650, punkt 73.

⁽⁶⁾ Schrems I, punkt 74.

⁽⁷⁾ 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/EN/TXT/PDF/?uri=CELEX:52017DC0007&from=EN>.

⁽⁸⁾ Appellationsdomstolen (civilrättsligt beslut), *Open Rights Group/Secretary of State for the Home Department and Secretary of State for Digital, Culture, Media and Sport*, [2021] EWCA Civ 800, punkterna 53–56. Appellationsdomstolen upphävde överdomstolens beslut, som tidigare hade bedömt undantaget mot bakgrund av förordning (EU) 2016/679 (särskilt dess artikel 23) och Europeiska unionens stadga om de grundläggande rättigheterna, och slagit fast att undantaget var lagligt (*Open Rights Group & Anor, R (On the Application Of) Secretary of State for the Home Department & Anor* [2019] EWHC 2562).

⁽⁹⁾ Under förutsättning att de tillämpliga villkoren är uppfyllda får överföringar för Förenade kungarikets invandringskontroll utföras enligt de överföringsmekanismer som anges i artiklarna 46–49 i förordning (EU) 2016/679.

- (9) Det brittiska parlamentet har delegerat ansvaret till det skotska parlamentet, det walesiska parlamentet (*Senedd Cymru*) och Nordirlands parlament för att lagstifta om inrikes frågor i Skottland, Wales och Nordirland vilket det brittiska parlamentet inte har förbehållit sig självt. Uppgiftsskydd är en reserverad fråga, dvs. samma lagstiftning gäller i hela landet, medan andra politikområden som är relevanta för detta beslut har delegerats. Till exempel har Skottlands och Nordirlands straffrättsliga system, inklusive polisväsendet, delegerats till det skotska parlamentet respektive Nordirlands parlament. Förenade kungariket har inte någon kodifierad konstitution i form av ett grundläggande konstituerande dokument. Konstitutionella principer har med tiden vuxit fram, särskilt från rättspraxis och konvention. Det konstitutionella värdet av vissa lagar, till exempel *Magna Carta*, *Bill of Rights 1689* och *Human Rights Act 1998*, har erkänts av domstolarna. Enskilda personers grundläggande rättigheter har utvecklats, som en del av konstitutionen, genom common law, dessa stadgar och internationella fördrag, särskilt den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna som Förenade kungariket ratificerade 1951. Förenade kungariket ratificerade även Europarådets konvention om skydd för enskilda personer vid automatisk databehandling av personuppgifter (konvention 108) 1987 ⁽¹⁰⁾.
- (10) 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 ⁽¹¹⁾. Enligt artikel 8 i den konventionen får en myndighet endast ingripa i rätten till privatliv i enlighet med lag om det är nödvändigt i ett demokratiskt samhälle med hänsyn till den nationella säkerheten, den allmänna säkerheten eller landets ekonomiska välbefinnande, för att förebygga oordning eller brott, för att skydda hälsa eller moral eller för att skydda andras fri- och rättigheter.
- (11) I enlighet med *Human Rights Act 1998* måste alla åtgärder som vidtas av myndigheter vara förenliga med en rättighet enligt konventionen ⁽¹²⁾. Dessutom måste primär- och sekundärrätten läsas och genomföras på ett sätt som är förenligt med konventionens rättigheter ⁽¹³⁾.

2.2 Förenade kungarikets dataskyddsram

- (12) Storbritannien lämnade EU den 31 januari 2020. På grundval av avtalet om Förenade konungariket Storbritannien och Nordirlands utträde ur Europeiska unionen och Europeiska atomenergigemenskapen ⁽¹⁴⁾ fortsatte unionsrätten att tillämpas i Förenade kungariket under övergångsperioden till och med den 31 december 2020. Före utträdet och under övergångsperioden bestod den rättsliga ramen för skydd av personuppgifter i Förenade kungariket av relevant EU-lagstiftning (särskilt förordning (EU) 2016/679 och Europaparlamentets och rådets direktiv ⁽¹⁵⁾ (EU) 2016/680) och nationell lagstiftning, särskilt 2018 års dataskyddslag ⁽¹⁶⁾ som innehöll 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 direktiv (EU) 2016/680.

⁽¹⁰⁾ Principerna i konvention 108 införlivades ursprungligen i Förenade kungarikets lagstiftning genom 1984 års dataskyddslag (*Data Protection Act 1984*) som ersattes av 1998 års dataskyddslag (*Data Protection Act 1998*) och därefter i sin tur av 2018 års dataskyddslag (*Data Protection Act 2018*) (enligt den brittiska dataskyddsförordningen). Förenade kungariket undertecknade också 2018 protokollet om ändring av konventionen om skydd för enskilda vid automatisk databehandling av personuppgifter (konvention 108+) och håller för närvarande på att ratificera konventionen.

⁽¹¹⁾ Artiklarna 6 och 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (se även tillägg 1 till *Human Rights Act 1998*).

⁽¹²⁾ Avsnitt 6 i *Human Rights Act 1998*.

⁽¹³⁾ Avsnitt 3 i *Human Rights Act 1998*.

⁽¹⁴⁾ Avtalet om Förenade konungariket Storbritannien och Nordirlands utträde ur Europeiska unionen och Europeiska atomenergigemenskapen 2019/C 384 I/01, XT/21054/2019/INIT, (EUT C 384I, 12.11.2019, s. 1), som finns på följande länk: [https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:12019W/TXT\(02\)&from=SV](https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=SV)

⁽¹⁵⁾ 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), som finns på följande länk: <https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016L0680&from=EN>.

⁽¹⁶⁾ 2018 års dataskyddslag, finns på följande länk: <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>.

- (13) Som en förberedelse inför EU-utträdet antog Förenade kungarikets regering *European Union (Withdrawal) Act 2018* ⁽¹⁷⁾ som införlivar direkt tillämplig unionslagstiftning i Förenade kungarikets lagstiftning ⁽¹⁸⁾. Denna så kallade bibehållna EU-lagstiftning omfattar förordning (EU) 2016/679 i sin helhet (inklusive skälen) ⁽¹⁹⁾. I enlighet med den akten 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) ⁽²⁰⁾.
- (14) Enligt *European Union (Withdrawal) Act 2018* har Förenade kungarikets ministrar befogenhet att införa sekundärlagstiftning genom förordningar, för att göra nödvändiga ändringar av bibehållen EU-lagstiftning till följd av Förenade kungarikets utträde ur Europeiska unionen. Ministrarna utövade denna befogenhet genom 2019 års förordningar om dataskydd, integritet och elektronisk kommunikation (ändringar osv.) (*EU Exit*) (*DPPEC-förordningarna*) ⁽²¹⁾. DPPEC-förordningarna ändrar förordning (EU) 2016/679 så som den införlivats i brittisk lagstiftning genom *European Union (Withdrawal) Act 2018*, 2018 års dataskyddslag och annan dataskyddslagstiftning för att passa det inhemska sammanhanget ⁽²²⁾.
- (15) Den rättsliga ramen för skydd av personuppgifter i Förenade kungariket efter övergångsperiodens utgång består följaktligen av följande:
- *United Kingdom General Data Protection Regulation* (den brittiska dataskyddsförordningen), införlivad i Förenade kungarikets lagstiftning enligt *European Union (Withdrawal) Act 2018* och ändrad genom *DPPEC Regulations* ⁽²³⁾, och
 - 2018 års dataskyddslag ⁽²⁴⁾, ändrad genom de brittiska DPPEC-förordningarna.
- (16) Eftersom den brittiska dataskyddsförordningen bygger på EU-lagstiftningen återspeglar dataskyddsbestämmelserna i Förenade kungariket i många avseenden nära motsvarande regler som är tillämpliga inom Europeiska unionen.
- (17) Utöver de befogenheter som den ansvariga ministern (*Secretary of State*) ges genom *European Union (Withdrawal) Act 2018* ger flera bestämmelser i 2018 års dataskyddslag den ansvariga ministern befogenhet att anta sekundärlagstiftning för att ändra vissa bestämmelser i lagen eller föreskriva kompletterande och ytterligare regler ⁽²⁵⁾. Den

⁽¹⁷⁾ *European Union Withdrawal Act 2018* finns på följande länk: <https://www.legislation.gov.uk/ukpga/2018/16/contents>.

⁽¹⁸⁾ Avsikten med och verkan av *European Union (Withdrawal) Act 2018* är att all direkt unionslagstiftning som införlivades i Förenade kungarikets lagstiftning vid övergångsperiodens utgång införlivas i Förenade kungarikets lagstiftning eftersom den har verkan i unionsrätten omedelbart före övergångsperiodens utgång, se avsnitt 3 i *European Union (Withdrawal) Act 2018*.

⁽¹⁹⁾ I de förklarande anmärkningarna till *European Union (Withdrawal) Act 2018* anges följande: "När lagstiftning omvandlas enligt detta avsnitt är det själva lagtexten som kommer att utgöra en del av den nationella lagstiftningen. Detta kommer att inbegripa den fullständiga texten till alla EU-instrument (inklusive skälen i ingressen)." (Förklarande anmärkningar till *European Union (Withdrawal) Act 2018*, punkt 83, finns på följande länk: https://www.legislation.gov.uk/ukpga/2018/16/pdfs/ukpgaen_20180016_en.pdf). Enligt uppgifter från de brittiska myndigheterna var det inte nödvändigt att ändra dem på samma sätt som artiklarna i förordning (EU) 2016/679 har ändrats genom förordningar om dataskydd, integritet och elektronisk kommunikation (DPPEC-förordningarna) eftersom skälen inte har status som bindande rättsliga bestämmelser.

⁽²⁰⁾ Avsnitt 6 i *European Union (Withdrawal) Act 2018*.

⁽²¹⁾ 2019 års förordningar om dataskydd, integritet och elektronisk kommunikation (ändringar etc.) (*EU Exit*), finns på följande länk: <https://www.legislation.gov.uk/uksi/2019/419/contents/made>, ändrad genom DPPEC Regulations 2020 och finns på följande länk: <https://www.legislation.gov.uk/ukdsi/2020/9780348213522>.

⁽²²⁾ Dessa ändringar av den brittiska dataskyddsförordningen och 2018 års dataskyddslag är för det mesta av teknisk natur, t.ex. strykning av hänvisningar till "medlemsstater" eller anpassning av terminologin, t.ex. ersättande av hänvisningar till förordning (EU) 2016/679 med hänvisningar till den brittiska dataskyddsförordningen. I vissa fall krävdes ändringar för att återspegla bestämmelsernas rent inhemska sammanhang, till exempel när det gäller "vem" antar "förordningar om adekvat skyddsnivå" i enlighet med Förenade kungarikets lagstiftning om dataskydd (se avsnitt 17A i 2018 års dataskyddslag), dvs. den ansvariga ministern i stället för Europeiska kommissionen.

⁽²³⁾ Den allmänna dataskyddsförordningen, *Keeling Schedule*, finns på följande länk: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946117/20201102_-_GDPR_-_MASTER_Keeling_Schedule_with_changes_highlighted_V3.pdf.

⁽²⁴⁾ 2018 års dataskyddslag, *Keeling Schedule*, finns på följande länk: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946100/20201102_-_DPA_-_MASTER_Keeling_Schedule_with_changes_highlighted_V3.pdf.

⁽²⁵⁾ Sådana befogenheter finns till exempel i avsnitt 16 (befogenhet att i specifika, snävt avgränsade situationer göra ytterligare undantag från specifika bestämmelser i den brittiska dataskyddsförordningen), 17A (befogenhet att anta förordningar om adekvat skyddsnivå), 212 och 213 (befogenheter att inleda lagstiftning och vidta övergångsåtgärder) och 211 (befogenhet att göra mindre och följändringar) i 2018 års dataskyddslag.

ansvariga ministern har hittills endast utövat sin befogenhet enligt avsnitt 137 i 2018 års dataskyddslag att anta 2019 års förordningar om skydd av personuppgifter (Avgifter och information) (Ändring) som anger under vilka omständigheter personuppgiftsansvariga är skyldiga att betala en årlig avgift till Förenade kungarikets oberoende dataskyddsmyndighet, *the Information Commissioner*.

- (18) Slutligen ges ytterligare vägledning om Förenade kungarikets dataskyddslagstiftning i de uppförandekoder och andra riktlinjer som antagits av *the Information Commissioner*. Även om vägledningen inte är formellt rättsligt bindande har den tolkningstyngd och visar hur dataskyddslagstiftningen tillämpas och verkställs av *the Commissioner* i praktiken. Enligt avsnitten 121–125 i 2018 års dataskyddslag ska *the Commissioner* utarbeta uppförandekoder för datadelning, direktmarknadsföring, åldersanpassad utformning samt dataskydd och journalistik.
- (19) Den brittiska rättsliga ram som är tillämplig på uppgifter som överförs enligt detta beslut är således mycket lik den som gäller i Europeiska unionen i dess struktur och huvudkomponenter. Detta inbegriper det faktum att en sådan ram inte enbart bygger på skyldigheter som föreskrivs i nationell rätt, som har utformats genom unionsrätten, utan även på skyldigheter som följer av internationell rätt, särskilt genom Förenade kungarikets anslutning till den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna och konvention 108 samt dess överlämnande till Europeiska domstolen för de mänskliga rättigheternas jurisdiktion. Dessa skyldigheter som följer av rättsligt bindande internationella instrument, särskilt när det gäller skydd av personuppgifter, är därför en särskilt viktig del av den rättsliga ram som bedöms i detta beslut.

2.3 Materiellt och territoriellt tillämpningsområde

- (20) I likhet med förordning (EU) 2016/679 är den brittiska dataskyddsförordningen tillämplig på behandling av personuppgifter helt eller delvis på automatisk väg eller på annan behandling om personuppgifterna ingår i ett register⁽²⁶⁾. Definitionerna av "personuppgifter", "den registrerade" och "behandling" i den brittiska dataskyddsförordningen är identiska med definitionerna i förordning (EU) 2016/679⁽²⁷⁾. Dessutom är den brittiska dataskyddsförordningen tillämplig på behandling av manuella ostrukturerade personuppgifter⁽²⁸⁾ som innehas av vissa brittiska myndigheter⁽²⁹⁾ även om brittiska principer och rättigheter som inte är relevanta för sådana personuppgifter inte tillämpas i avsnitten 24 och 25 i 2018 års dataskyddslag. I likhet med vad som föreskrivs i förordning (EU) 2016/679 är den brittiska dataskyddsförordningen inte tillämplig på behandling av personuppgifter som utförs av en enskild person i samband med verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll⁽³⁰⁾.
- (21) Den brittiska dataskyddsförordningen utvidgar tillämpningsområdet till att även omfatta behandling inom ramen för en verksamhet som omedelbart före övergångsperiodens utgång inte omfattades av unionsrättens tillämpningsområde (t.ex. nationell säkerhet)⁽³¹⁾ eller omfattades av kapitel 2 i avdelning 5 i fördraget om Europeiska unionen (verksamhet inom den gemensamma utrikes- och säkerhetspolitiken)⁽³²⁾. På samma sätt som i Europeiska unionens system är den brittiska dataskyddsförordningen inte tillämplig på en behörig myndighets behandling av personuppgifter i syfte att förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga

⁽²⁶⁾ Artiklarna 2.1 och 5 i den brittiska dataskyddsförordningen.

⁽²⁷⁾ Artikel 4.1 och 4.2 i den brittiska dataskyddsförordningen.

⁽²⁸⁾ Manuell ostrukturerad behandling av personuppgifter definieras i artikel 2.5 b som behandling av personuppgifter som inte är automatisk eller strukturerad behandling av personuppgifter.

⁽²⁹⁾ I artikel 2.1a i den brittiska dataskyddsförordningen föreskrivs att förordningen också är tillämplig på manuell ostrukturerad behandling av personuppgifter som innehas av en myndighet som omfattas av lagen informationsfrihet. Med myndighet som omfattas av lagen om informationsfrihet avses alla myndigheter enligt definitionen i *Freedom of Information Act 2000* eller alla skotska myndigheter enligt definitionen i *Freedom of Information (Scotland) Act 2002* (asp 13). Avsnitt 21.5 i 2018 års dataskyddslag.

⁽³⁰⁾ Artikel 2.2 a i den brittiska dataskyddsförordningen.

⁽³¹⁾ Nationell säkerhetsverksamhet omfattas endast av den brittiska dataskyddsförordningens tillämpningsområde i den mån den inte utförs av en behörig myndighet för brottsbekämpande ändamål, då del 3 i 2018 års dataskyddslag är tillämplig eller av en underrättelsetjänst, eller för dess räkning, vars verksamhet inte omfattas av den brittiska dataskyddsförordningen och omfattas av del 4 2018 års dataskyddslag i enlighet med artikel 2.2 c i den brittiska dataskyddsförordningen. Till exempel kan en polisstyrka utföra säkerhetskontroller av en anställd för att säkerställa att han eller hon är pålitlig nog att få tillgång till nationellt säkerhetsmaterial. Trots att polisen är en behörig myndighet för brottsbekämpande ändamål är behandlingen i fråga inte avsedd för brottsbekämpning och den brittiska dataskyddsförordningen skulle vara tillämplig. Se *UK Explanatory Framework for Adequacy Discussions Section H: National Security Data Protection and Investigatory Powers Framework*, s. 8, finns på följande länk: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf.

⁽³²⁾ Artikel 2.1 a och 2.1 b i den brittiska dataskyddsförordningen.

påföljder, inbegripet skydd mot och förebyggande av hot mot den allmänna säkerheten (så kallade brottsbekämpande ändamål) – sådan behandling regleras i stället av del 3 i 2018 års dataskyddslag vilket är fallet för direktiv (EU) 2016/680 enligt EU-rätten – eller behandling av personuppgifter som utförs av underrättelsetjänster (Security Service, Secret Intelligence Service och the Government Communications Headquarters) som omfattas av enligt unionsrätten – eller behandling av personuppgifter som täcks av del 4 i 2018 års dataskyddslag ⁽³³⁾.

- (22) Den brittiska dataskyddsförordningens territoriella tillämpningsområde anges i artikel 3 i den brittiska dataskyddsförordningen ⁽³⁴⁾ och omfattar behandling av personuppgifter (oavsett var de äger rum) i samband med verksamhet vid en personuppgiftsansvarigs eller ett personuppgiftsbiträdes verksamhetsställe i Förenade kungariket samt behandling av personuppgifter om registrerade som befinner sig i Förenade kungariket om behandlingen har samband med erbjudande av varor eller tjänster till sådana registrerade eller övervakning av deras beteende ⁽³⁵⁾. Detta återspeglar tillvägagångssättet i artikel 3 i förordning (EU) 2016/679.

2.4 Definitioner av personuppgifter samt begreppen personuppgiftsansvarig och personuppgiftsbiträde

- (23) Definitionerna av personuppgifter, behandling, personuppgiftsansvarig, personuppgiftsbiträde och definitionen av pseudonymisering i förordning (EU) 2016/679 har behållits i den brittiska dataskyddsförordningen utan väsentliga ändringar ⁽³⁶⁾. Dessutom definieras särskilda kategorier av uppgifter i artikel 9.1 i den brittiska dataskyddsförordningen på samma sätt som i förordning (EU) 2016/679 ("avslöjande av ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter i syfte att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning"). I avsnitt 205 i 2018 års dataskyddslag definieras "biometriska uppgifter" ⁽³⁷⁾, "uppgifter om hälsa" ⁽³⁸⁾ och "genetiska uppgifter" ⁽³⁹⁾.

2.5 Skyddsåtgärder, rättigheter och skyldigheter

2.5.1 Laglig och korrekt behandling

- (24) Personuppgifter bör behandlas på ett lagligt och korrekt sätt.
- (25) Principerna om laglighet, rättvisa och öppenhet samt grunderna för laglig behandling garanteras i Förenade kungarikets lagstiftning genom artiklarna 5.1 a och 6.1 i den brittiska dataskyddsförordningen som är identiska med respektive bestämmelser i förordning (EU) 2016/679. ⁽⁴⁰⁾ Avsnitt 8 i 2018 års dataskyddslag kompletterar artikel 6.1 e genom att föreskriva att behandling av personuppgifter enligt artikel 6.1 e i den brittiska dataskyddsförordningen (som är nödvändig för att utföra en uppgift av allmänintresse eller som ett led i utövandet av den

⁽³³⁾ Artikel 2.2 b och 2.2 c i den brittiska dataskyddsförordningen.

⁽³⁴⁾ Samma territoriella tillämpningsområde gäller för behandling av personuppgifter enligt del 2 i 2018 års dataskyddslag som kompletterar den brittiska dataskyddsförordningen (avsnitt 207 (1A)).

⁽³⁵⁾ Detta innebär i synnerhet att 2018 års dataskyddslag, och därmed detta beslut, inte är tillämpliga på Förenade kungarikets kronbesittningar (Jersey, Guernsey och Isle of Man) och utomeuropeiska territorier, till exempel Falklandsöarna och territoriet Gibraltar.

⁽³⁶⁾ Artiklarna 4.1, 4.2, 4.5, 4.7 och 4.8 i den brittiska dataskyddsförordningen.

⁽³⁷⁾ Biometriska uppgifter innebär personuppgifter som härrör från en specifik teknisk behandling som rör en persons fysiska, fysiologiska eller beteendemässiga egenskaper och som möjliggör eller bekräftar en unik identifiering av den personen, till exempel ansiktsbilder eller fingeravtrycksuppgifter.

⁽³⁸⁾ Uppgifter om hälsa innebär personuppgifter om en persons fysiska eller psykiska hälsa, inbegripet hälso- och sjukvårdstjänster, som avslöjar information om personens hälsotillstånd.

⁽³⁹⁾ Genetiska uppgifter innebär personuppgifter som rör en individs ärvda eller förvärvade genetiska egenskaper och som ger unik information om den personens fysiologi eller hälsa och som i synnerhet är resultatet av en analys av ett biologiskt prov från den berörda personen.

⁽⁴⁰⁾ Enligt artikel 6.1 i den brittiska dataskyddsförordningen är behandling laglig endast om och i den utsträckning som a) den registrerade har lämnat sitt samtycke till att hans eller hennes personuppgifter behandlas för ett eller flera specifika ändamål, b) behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett avtal ingås, c) behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvariga, d) behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person, e) behandlingen är nödvändig för att utföra en arbetsuppgift av allmänt intresse eller som ett led i myndighetsutövning som utförs av den personuppgiftsansvariga och f) behandlingen är nödvändig för ändamål som rör den personuppgiftsansvarigas eller en tredje parts berättigade intressen, utom när sådana intressen uppvägs av den registrerades intressen respektive hans eller hennes grundläggande fri- och rättigheter som kräver skydd av personuppgifter, särskilt när den registrerade är ett barn.

personuppgiftsansvarigas officiella befogenheter) omfattar behandling av personuppgifter som är nödvändig för rättskipningen, utövande av en funktion i någondera av parlamentets kammare, utövande av en funktion som tilldelats en person genom förordning eller en rättsregel, främjar utövandet av kronans funktioner, en av kronans ministrar eller ett regeringsministerium eller en aktivitet som stöder eller gynnar demokratiskt engagemang.

- (26) När det gäller samtycke (en av grunderna för laglig behandling) behåller den brittiska dataskyddsförordningen även de villkor som anges i artikel 7 i förordning (EU) 2016/679 utan ändringar, dvs. att den personuppgiftsansvariga måste kunna visa att den registrerade har gett sitt samtycke, att en skriftlig begäran om samtycke måste lämnas in på ett klart och tydligt språk, att den registrerade måste ha rätt att när som helst dra tillbaka sitt samtycke och vid bedömningen av huruvida samtycket lämnas frivilligt bör hänsyn tas till huruvida fullgörandet av ett avtal är villkorat av att samtycke inte krävs för behandling av personuppgifter. Enligt artikel 8 i den brittiska dataskyddsförordningen är dessutom ett barns samtycke i samband med tillhandahållande av informationssamhällets tjänster lagligt endast om barnet är minst 13 år gammalt. Detta ligger inom den åldersgrupp som fastställs i artikel 8 i förordning (EU) 2016/679.

2.5.2 *Behandling av särskilda kategorier av personuppgifter*

- (27) Specifika skyddsåtgärder bör vidtas när "särskilda kategorier av uppgifter" behandlas.
- (28) Den brittiska dataskyddsförordningen och 2018 års dataskyddslag innehåller särskilda regler för behandling av särskilda kategorier av personuppgifter som definieras i artikel 9.1 i den brittiska dataskyddsförordningen på samma sätt som i förordning (EU) 2016/679 (se skäl 23 ovan). Enligt artikel 9 i den brittiska dataskyddsförordningen är behandling av särskilda kategorier av uppgifter i princip förbjuden, såvida inte ett särskilt undantag gäller.
- (29) Dessa undantag (som förtecknas i artikel 9.2 och 3 i den brittiska dataskyddsförordningen) ändrar inte innehållet i artikel 9.2 och 3 i förordning (EU) 2016/679. Såvida inte den registrerade har lämnat sitt uttryckliga samtycke till behandlingen av dessa personuppgifter är behandling av särskilda kategorier av personuppgifter endast tillåten under särskilda och begränsade omständigheter. I de flesta fall måste behandlingen av känsliga uppgifter vara nödvändig för ett specifikt ändamål som definieras i den relevanta bestämmelsen (se artikel 9.2 b, c, f, g, h, i och j).
- (30) Om ett undantag enligt artikel 9.2 i den brittiska dataskyddsförordningen kräver tillstånd enligt lag eller hänvisar till allmänintresset anges dessutom i avsnitt 10 i 2018 års dataskyddslag tillsammans med tillägg 1 till samma lag vilka villkor som måste vara uppfyllda för att undantagen ska kunna återopas. När det till exempel gäller behandling av känsliga uppgifter för att skydda "folkhälsan" (artikel 9.2 i) i den brittiska dataskyddsförordningen) krävs det i punkt 3 b i del 1 i tillägg 1 att sådan behandling, utöver nödvändighetstestet, utförs "av eller på ansvar av hälso- och sjukvårdspersonal" eller "av en annan person som är skyldig att iakttä tystnadsplikt enligt en lag eller en rättsregel", inbegripet enligt den väletablerade sedvanerättsliga tystnadsplikten.
- (31) När känsliga uppgifter behandlas av skäl som rör ett väsentligt allmänintresse (artikel 9.2 g i den brittiska dataskyddsförordningen) innehåller del 2 i bilaga 1 till 2018 års dataskyddslag en uttömmande förteckning över ändamål som kan anses vara av väsentligt allmänt intresse och för vart och ett av dessa syften fastställs särskilda ytterligare villkor. Till exempel erkänns främjande av mångfald när det gäller rastillhörighet och etniskt ursprung på högre nivåer i organisationer som ett viktigt allmänintresse. Behandling av känsliga uppgifter för detta särskilda ändamål omfattas av detaljerade krav, bland annat att behandlingen utförs som ett led i en process för att identifiera lämpliga personer som kan inneha höga befattningar och är nödvändig för att främja mångfald när det gäller raser samt etnisk mångfald och sannolikt inte kommer att orsaka den registrerade betydande skada eller betydande lidande.
- (32) I avsnitt 11.1 i 2018 års dataskyddslag fastställs villkor för behandling av personuppgifter under de omständigheter som beskrivs i artikel 9.3 i den brittiska dataskyddsförordningen avseende tystnadsplikt. Detta inbegriper omständigheter under vilka det utförs av eller under ansvar av hälso- och sjukvårdspersonal eller socialarbetare eller av en annan person som under dessa omständigheter är skyldig att iakttä tystnadsplikt enligt en lag eller en rättsregel.
- (33) Dessutom kräver många av de undantag som anges i artikel 9.2 i den brittiska dataskyddsförordningen lämpliga och specifika skyddsåtgärder för att de ska kunna användas. Beroende på behandlingens art och risknivån för de registrerades rättigheter och friheter fastställs olika skyddsåtgärder i villkoren för behandling i bilaga 1 – till 2018 års dataskyddslag. I tillägg 1 anges villkoren för varje behandlingssituation i tur och ordning.

- (34) I vissa fall reglerar och begränsar 2018 års dataskyddslag den typ av känsliga uppgifter som får behandlas för att en viss rättslig grund ska efterlevas. Exempelvis är det enligt punkt 8 i tillägg 1 tillåtet att behandla känsliga uppgifter i syfte att främja lika möjligheter eller likabehandling. Detta behandlingstillstånd får endast användas om uppgifterna avslöjar ras eller etniskt ursprung, religiös eller filosofisk övertygelse, sexuell läggning eller hälsouppgifter.
- (35) I vissa fall begränsar 2018 års dataskyddslag den typ av personuppgiftsansvarig som får använda behandlingsvillkoret. I punkt 23 i tillägg 1 föreskrivs exempelvis behandling av känsliga uppgifter i samband med de förtroendevaldas svar till allmänheten. Detta behandlingsvillkor kan endast användas om den personuppgiftsansvariga är vald företrädare eller agerar under deras överinseende.
- (36) I vissa andra fall fastställs gränser för vilka kategorier av registrerade som får användas i 2018 års dataskyddslag. I punkt 21 i tillägg 1 regleras exempelvis behandlingen av känsliga uppgifter för tjänstepensionssystem. Detta villkor kan endast användas om den registrerade är syskon, förälder, mor- eller farförälder eller gammelmor- eller gammelfarförälder till försäkringstagaren.
- (37) När den personuppgiftsansvariga dessutom åberopar de undantag i artikel 9.2 i den brittiska dataskyddsförordningen som specificeras närmare i avsnitt 10 i 2018 års dataskyddslag tillsammans med tillägg 1 till 2018 års dataskyddslag måste den personuppgiftsansvariga i de flesta fall utarbeta ett lämpligt policydokument. Det måste beskriva den personuppgiftsansvariges förfaranden för att säkerställa överensstämmelse med principerna i artikel 5 i den brittiska dataskyddsförordningen. Det ska också innehålla riktlinjer för lagring och radering med uppgift om den sannolika lagringsperioden. Personuppgiftsansvariga ska se över och uppdatera detta dokument när så är lämpligt. Den personuppgiftsansvariga ska bevara policydokumentet i sex månader efter det att behandlingen avslutats och på begäran göra det tillgängligt för *the Information Commissioner* ⁽⁴¹⁾.
- (38) Enligt punkt 41 i bilaga 1 till 2018 års dataskyddslag ska policydokumentet alltid åtföljas av en utökad registrering av behandlingen. Detta register måste följa de åtaganden som ingår i policydokumentet, dvs. huruvida uppgifterna raderas eller lagras i enlighet med riktlinjerna. Om riktlinjerna inte har följts ska skälen till detta registreras i protokollet. I dokumentationen ska det också beskrivas hur behandlingen uppfyller artikel 6 i den brittiska dataskyddsförordningen (behandlings laglighet) och det särskilda villkoret i tillägg 1 till 2018 års dataskyddslag som åberopas.
- (39) I likhet med förordning (EU) 2016/679 innehåller den brittiska dataskyddsförordningen också allmänna skyddsåtgärder för viss behandling av särskilda kategorier av uppgifter. Enligt artikel 35 i den brittiska dataskyddsförordningen krävs en konsekvensbedömning avseende dataskydd om särskilda kategorier av uppgifter behandlas i stor skala. Enligt artikel 37 i den brittiska dataskyddsförordningen måste en personuppgiftsansvarig eller ett personuppgiftsbiträde utse ett dataskyddsbud om hans eller hennes kärnverksamhet består i behandling av särskilda kategorier av uppgifter i stor skala.
- (40) När det gäller personuppgifter som rör fällande domar i brottmål och brott är artikel 10 i den brittiska dataskyddsförordningen identisk med artikel 10 i förordning (EU) 2016/679. Den tillåter behandling av personuppgifter som rör fällande domar i brottmål och överträdelser endast under kontroll av en myndighet eller när behandlingen är tillåten enligt nationell lagstiftning som föreskriver lämpliga skyddsåtgärder för de registrerades rättigheter och friheter.
- (41) Om behandlingen av uppgifter som rör fällande domar i brottmål och överträdelser inte sker under kontroll av en myndighet, föreskrivs i avsnitt 10.5 i 2018 års dataskyddslag att sådan behandling endast får ske för de särskilda ändamål/i de särskilda situationer som anges i delarna 1, 2 och 3 i bilaga 1 till 2018 års dataskyddslag och omfattas av de särskilda krav som fastställs för vart och ett av dessa ändamål/situationer. Uppgifter om fällande domar i brottmål kan till exempel behandlas av organ utan vinstsyfte om behandlingen utförs a) inom ramen för dess legitima verksamhet med lämpliga skyddsåtgärder av en stiftelse, en förening eller ett annat icke vinstdrivande organ med politiskt, filosofiskt, religiöst eller fackligt syfte och b) under förutsättning att i) behandlingen endast avser organets medlemmar eller tidigare medlemmar eller personer som har regelbunden kontakt med organet i samband med dess ändamål och ii) personuppgifterna inte lämnas ut.

⁽⁴¹⁾ Punkterna 38–40 i tillägg 1 till 2018 års dataskyddslag.

- (42) I del 3 i tillägg 1 till 2018 års dataskyddslag anges dessutom ytterligare omständigheter under vilka uppgifter om fallande domar i brottmål får användas som motsvarar de rättsliga grunderna för behandling av känsliga uppgifter i artikel 9.2 i förordning (EU) 2016/679 och den brittiska dataskyddsförordningen (t.ex. den registrerades samtycke, en persons vitala intressen om den registrerade är rättsligt eller fysiskt oförmögen att ge sitt samtycke, om uppgifterna redan på ett uppenbart sätt har offentliggjorts av den registrerade, om behandlingen är nödvändig för att fastställa, göra gällande eller försvara ett rättsligt anspråk osv.).

2.5.3 Ändamålsbegränsning, noggrannhet, dataminimering, lagringsbegränsning och datasäkerhet

- (43) Personuppgifter ska behandlas för ett specifikt ändamål och därefter användas endast i den utsträckning som detta är förenligt med behandlingens ändamål.
- (44) Denna princip föreskrivs i artikel 5.1 b i förordning (EU) 2016/679 och har behållits utan ändringar i artikel 5.1 b i den brittiska dataskyddsförordningen. Villkoren för ytterligare förenlig behandling enligt artikel 6.4 i förordning (EU) 2016/679 har också behållits utan några väsentliga ändringar i artikel 6.4 a–e i den brittiska dataskyddsförordningen.
- (45) Dessutom bör uppgifterna vara korrekta och vid behov hållas aktuella. De bör också vara adekvata, relevanta och inte överdrivet omfattande i förhållande till de ändamål för vilka de behandlas och i princip inte lagras längre än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas.
- (46) Principerna om uppgiftsminimering, noggrannhet och lagringsbegränsning fastställs i artikel 5.1 c–e i förordning (EU) 2016/679 och behålls utan ändringar i artikel 5.1 c–e i den brittiska dataskyddsförordningen.
- (47) Personuppgifter bör också behandlas på ett sätt som innebär att säkerheten garanteras, inbegripet skydd mot obehörig eller otillåten behandling och mot oavsiktlig förlust, förstörelse eller skada. I detta syfte bör de ekonomiska aktörerna vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter från eventuella hot. Dessa åtgärder bör utvärderas med hänsyn till den senaste tekniken och kostnaderna.
- (48) Datasäkerhet är förankrad i Förenade kungarikets lagstiftning genom principen om integritet och konfidentialitet i artikel 5.1 f i den brittiska dataskyddsförordningen och i artikel 32 i den brittiska dataskyddsförordningen om säkerhet vid behandling. Dessa bestämmelser är identiska med respektive bestämmelser i förordning (EU) 2016/679. Enligt samma villkor som de som anges i artiklarna 33 och 34 i förordning (EU) 2016/679 kräver den brittiska dataskyddsförordningen dessutom att en personuppgiftsincident anmäls till tillsynsmyndigheten (artikel 33 i den brittiska dataskyddsförordningen) och att en personuppgiftsincident meddelas den registrerade (artikel 34 i den brittiska dataskyddsförordningen).

2.5.4 Insyn

- (49) De registrerade bör underrättas om de viktigaste dragen i behandlingen av sina personuppgifter.
- (50) Detta säkerställs genom artiklarna 13 och 14 i den brittiska dataskyddsförordningen som utöver en allmän princip om öppenhet innehåller regler om vilken information som ska lämnas till den registrerade⁽⁴²⁾. Den brittiska dataskyddsförordningen innebär inga väsentliga ändringar av dessa regler jämfört med motsvarande artiklar i förordning (EU) 2016/679. Liksom enligt förordning (EU) 2016/679 omfattas dock transparenskraven i dessa artiklar av flera undantag som fastställs i 2018 års dataskyddslag (se skälen 55–72).

⁽⁴²⁾ I artiklarna 13.1 f och 14.1 f har hänvisningarna till kommissionens beslut om adekvat skyddsnivå ersatts med hänvisningar till motsvarande instrument i Förenade kungariket, dvs. förordningar om adekvat skyddsnivå enligt 2018 års dataskyddslag. I artiklarna 14.5 c–d har hänvisningarna till EU:s eller medlemsstaternas lagstiftning ersatts med en hänvisning till nationell lagstiftning (som exempel på sådan nationell lagstiftning som kan omfattas av artikel 14.5 c har Förenade kungariket hänvisat till avsnitt 7 i *Scrap Metal Dealers Act 2013* som innehåller regler för register över metallskrotningstillstånd eller del 35 i *Companies Act 2006* som innehåller regler för bolagsregistret. På liknande sätt skulle ett exempel på nationell lagstiftning som kan omfattas av artikel 14.5 d kunna omfatta lagstiftning som fastställer regler om tystnadsplikt eller skyldigheter som återspeglas i anställningsavtal eller den allmänna lagstiftningens tystnadsplikt (t.ex. personuppgifter som behandlas av hälso- och sjukvårdspersonal, personal, socialarbetare osv.).

2.5.5 Individuella rättigheter

- (51) De registrerade bör ha vissa rättigheter som kan göras gällande mot den personuppgiftsansvariga eller personuppgiftsbiträdet, särskilt rätten till tillgång till uppgifter, rätten att invända mot behandlingen och rätten att få uppgifter rättade och raderade. Samtidigt kan sådana rättigheter omfattas av restriktioner i den mån dessa begränsningar är nödvändiga och proportionerliga för att skydda den allmänna säkerheten eller andra viktiga mål av allmänt intresse.

2.5.5.1 Materiella rättigheter

- (52) Den brittiska dataskyddsförordningen ger enskilda samma verkställbara rättigheter som förordning (EU) 2016/679. Bestämmelserna om enskildas rättigheter har bibehållits i den brittiska dataskyddsförordningen utan några väsentliga ändringar.
- (53) Rättigheterna omfattar den registrerades rätt till tillgång (artikel 15 i den brittiska dataskyddsförordningen), rätten till rättelse (artikel 16 i den brittiska dataskyddsförordningen), rätten till radering (artikel 17 i den brittiska dataskyddsförordningen), rätten till begränsning av behandlingen (artikel 18 i den brittiska dataskyddsförordningen), en anmälningsskyldighet avseende rättelse eller radering av personuppgifter eller begränsning av behandling (artikel 19 i den brittiska dataskyddsförordningen), rätten till dataportabilitet (artikel 20 i den brittiska dataskyddsförordningen) och rätten att göra invändningar (artikel 21 i den brittiska dataskyddsförordningen) ⁽⁴³⁾. Det senare omfattar också den registrerades rätt att invända mot behandling av personuppgifter för direkt marknadsföring enligt artikel 21.2 och 3 i förordning (EU) 2016/679. Dessutom ska *the Information Commissioner* enligt avsnitt 122 i 2018 års dataskyddslag utarbeta en uppförandekod för genomförandet av direktmarknadsföring i enlighet med kraven i dataskyddslagstiftningen (och 2003 års förordning om integritet och elektronisk kommunikation) och sådana andra riktlinjer för att främja god praxis vid direktmarknadsföring som *the Information Commissioner* anser vara lämpliga. ICO (*Information Commissioner's Office*) håller för närvarande på att utarbeta en uppförandekod för direktmarknadsföring ⁽⁴⁴⁾.
- (54) Den registrerades rätt att inte bli föremål för ett beslut som enbart grundar sig på automatiserad behandling som har rättsliga följder för dem eller som på liknande sätt påverkar dem på ett betydande sätt i enlighet med artikel 22 i dataskyddsförordningen har också behållits i den brittiska dataskyddsförordningen utan några väsentliga ändringar. En ny punkt 3A har dock lagts till för att hänvisa till att avsnitt 14 i 2018 års dataskyddslag innehåller skyddsåtgärder för registrerades rättigheter, friheter och berättigade intressen när behandlingen utförs enligt artikel 22.2 b i den brittiska dataskyddsförordningen. Detta gäller endast när grunden för ett sådant beslut är ett tillstånd eller ett krav enligt brittisk lag och inte om beslutet är nödvändigt enligt ett avtal eller med den registrerades uttryckliga samtycke. Om avsnitt 14 i 2018 års dataskyddslag är tillämpligt ska den personuppgiftsansvariga så snart det rimligen är praktiskt möjligt skriftligen underrätta den registrerade om att ett beslut har fattats enbart på grundval av automatiserad behandling. Den registrerade har rätt att begära att den personuppgiftsansvariga – inom en månad efter mottagandet av underrättelsen – ompröva beslutet eller att fatta ett nytt beslut som inte enbart grundar sig på automatiserad behandling. Den ansvariga ministern har befogenhet att anta ytterligare skyddsåtgärder när det gäller automatiserat beslutsfattande. Denna befogenhet har ännu inte utövats.

2.5.5.2 Begränsningar av individuella rättigheter och andra bestämmelser

- (55) 2018 års dataskyddslag innehåller flera begränsningar av individuella rättigheter som passar inom ramen för artikel 23 i den brittiska dataskyddsförordningen. Inga begränsningar införs inom denna ram när det gäller rätten att invända mot direkt marknadsföring enligt artikel 21.2 och 3 i den brittiska dataskyddsförordningen eller rätten att inte bli föremål för automatiserat beslutsfattande i enlighet med artikel 22 i den brittiska dataskyddsförordningen.
- (56) Begränsningarna beskrivs närmare i bilagorna 2–4 till 2018 års dataskyddslag. De brittiska myndigheterna har förklarat att de vägleds av principen om specificitet (en detaljerad strategi, uppdelning av breda begränsningar i flera, mer specifika bestämmelser) och principen om villkorlighet (varje bestämmelse kompletteras med skyddsåtgärder i form av begränsningar eller villkor för att förhindra missbruk) ⁽⁴⁵⁾.

⁽⁴³⁾ I artiklarna 17.1 e och 17.3 b har hänvisningarna till EU:s eller medlemsstaternas lagstiftning ersatts med en hänvisning till nationell rätt (som exempel på sådan nationell lagstiftning enligt artikel 17.1 e har Förenade kungariket nämnt *Education (Pupil Information) (England) Regulations 2006* som föreskriver att elevers namn ska raderas ur skolregistret efter det att de har lämnat skolan eller *Medical Act 1983*, avsnitt 34F, som innehåller bestämmelser om strykning av namn från *General Practitioner Register* och *Specialist Register*).

⁽⁴⁴⁾ Utkastet till uppförandekod finns på följande länk: <https://ico.org.uk/media/about-the-ico/consultations/2616882/direct-marketing-code-draft-guidance.pdf>.

⁽⁴⁵⁾ *UK Explanatory Framework for Adequacy Discussions, Section E: Restrictions*, s. 1, finns på följande länk: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf.

- (57) De begränsningar som beskrivs i artikel 23.1 i den brittiska dataskyddsförordningen är utformade för att säkerställa att de endast tillämpas under särskilda omständigheter när detta är nödvändigt i ett demokratiskt samhälle och står i proportion till det legitima mål som de eftersträvar. I enlighet med etablerad rättspraxis om tolkning av begränsningar kan dessutom ett undantag från ordningen för dataskydd endast tillämpas i varje enskilt fall om det är nödvändigt och proportionerligt för att göra det ⁽⁴⁶⁾. Nödvändighetstestet ska vara "strikt, vilket innebär att varje ingrepp i den registrerades rättigheter ska stå i proportion till hur allvarligt hotet mot allmänintresset är. Det handlar därför om en klassisk proportionalitetsanalys ⁽⁴⁷⁾".
- (58) Syftet med dessa begränsningar motsvarar dem som förtecknas i artikel 23 i förordning (EU) 2016/679 med undantag för de begränsningar för nationell säkerhet och försvar som i stället regleras genom avsnitt 26 i 2018 års dataskyddslag men som omfattas av samma krav på nödvändighet och proportionalitet (se skälen 63–66).
- (59) Vissa av begränsningarna, till exempel de som rör förebyggande eller avslöjande av brott, gripande eller lagföring av gärningsmän och fastställande eller uppbörd av skatter eller avgifter ⁽⁴⁸⁾ tillåter begränsningar av alla individuella rättigheter och skyldigheter avseende insyn (med undantag för rättigheter enligt artikel 21.2 och artikel 22). Tillämpningsområdet för andra begränsningar är begränsat till skyldigheter avseende transparens och tillträdesrätt, till exempel begränsningar av advokatsekretessen ⁽⁴⁹⁾, rätten till frihet från ett krav på att lämna information som skulle leda till självangivelse ⁽⁵⁰⁾ och till företagsfinansiering, särskilt förhindrande av insiderhandel ⁽⁵¹⁾. Få av begränsningarna tillåter en begränsning av den personuppgiftsansvarigas skyldighet att informera den registrerade om ett personuppgiftsbrott och principerna om ändamålsbegränsning samt om laglighet, rättvisa och insyn i behandlingen ⁽⁵²⁾.
- (60) Vissa av begränsningarna gäller automatiskt "i sin helhet" för en viss typ av behandling av personuppgifter (till exempel är tillämpningen av öppenhetsskyldigheter och individuella rättigheter utesluten när personuppgifter behandlas för att bedöma en persons lämplighet för domarämbetet eller personuppgifter behandlas av en domstol eller en enskild person som handlar i egenskap av en dömande myndighet).
- (61) I de flesta fall anges dock i den relevanta punkten i tillägg 2 till 2018 års dataskyddslag att begränsningen endast gäller när (och i den mån) tillämpningen av bestämmelserna "sannolikt skulle skada" det berättigade mål som eftersträvas med begränsningen och exempelvis är de angivna bestämmelserna i den brittiska dataskyddsförordningen inte tillämpliga på personuppgifter som behandlas för att förebygga eller upptäcka brott, gripa eller lagföra gärningsmän eller för att fastställa eller uppbära en skatt eller avgift "i den mån tillämpningen av dessa bestämmelser sannolikt skulle skada" någon av dessa frågor ⁽⁵³⁾.
- (62) Normen "sannolikt skulle skada" har konsekvent tolkats av brittiska domstolar som "en mycket betydande och tungt vägande risk för skada för det identifierade allmänintresset" ⁽⁵⁴⁾. En begränsning som omfattas av prövningen av konkret och faktisk skada kan därför endast återopas om och i den mån det föreligger en mycket betydande och tungt vägande risk för att beviljandet av en viss rättighet skulle skada det berörda allmänintresset. Den personuppgiftsansvariga ansvarar för att från fall till fall bedöma om dessa villkor är uppfyllda ⁽⁵⁵⁾.
- (63) Utöver de begränsningar som anges i tillägg 2 till 2018 års dataskyddslag föreskrivs i avsnitt 26 i denna lag ett undantag som kan tillämpas på vissa bestämmelser i den brittiska dataskyddsförordningen och 2018 års dataskyddslag om detta undantag krävs för att skydda den nationella säkerheten eller för försvarsändamål. Detta undantag gäller dataskyddsprinciperna (med undantag för principen om laglighet), transparenskraven, den registrerades rättigheter, skyldigheten att anmäla ett uppgiftsbrott, regler om internationella överföringar, vissa av skyldigheter och befogenheter som *the Information Commissioner* har samt reglerna om rättsmedel, ansvar och

⁽⁴⁶⁾ Open Rights Group & Anor, R (On the Application Of)/Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin), punkterna 40 och 41.

⁽⁴⁷⁾ Guriev/Community Safety Development (United Kingdom) Ltd [2016] EWHC 643 (QB), punkt 43. Se även domen i det ovannämnda målet Lin/Commissioner of Police for the Metropolis [2015] EWHC 2484 (QB), punkt 80.

⁽⁴⁸⁾ Punkt 2 i tillägg 2 till 2018 års dataskyddslag.

⁽⁴⁹⁾ Punkt 19 i tillägg 2 till 2018 års dataskyddslag.

⁽⁵⁰⁾ Punkt 20 i tillägg 2 till 2018 års dataskyddslag.

⁽⁵¹⁾ Punkt 21 i tillägg 2 till 2018 års dataskyddslag.

⁽⁵²⁾ Begränsningar av rätten till anmälan av personuppgiftsbrott är exempelvis endast tillåtna när det gäller brott och beskattning (punkt 2 i bilaga 2 till 2018 års dataskyddslag), parlamentariska privilegier (punkt 13 i tillägg 2 till 2018 års dataskyddslag) och behandling för journalistiska, akademiska, konstnärliga och litterära ändamål (punkt 26 i tillägg 2 till 2018 års dataskyddslag).

⁽⁵³⁾ Punkt 2 i tillägg 2 till 2018 års dataskyddslag.

⁽⁵⁴⁾ R (Lord)/Secretary of State for the Home Department [2003] EWHC 2073 (Admin), punkt 100, och Guriev/Community Safety Development (United Kingdom) Ltd [2016] EWHC 643 (QB), punkt 43.

⁽⁵⁵⁾ Open Rights Group & Anor, R (On the Application Of)/Secretary of State for the Home Department & Anor, punkt 31.

påföljder, med undantag för bestämmelsen om de allmänna villkoren för åläggande av administrativa sanktionsavgifter i artikel 83 i den brittiska dataskyddsförordningen och bestämmelsen om påföljder i artikel 84 i den brittiska dataskyddsförordningen. Avsnitt 28 i 2018 års dataskyddslag ändrar dessutom tillämpningen av artikel 9.1 för att möjliggöra behandling av särskilda kategorier av uppgifter i artikel 9.1 i den brittiska dataskyddsförordningen i den mån behandlingen utförs för att skydda den nationella säkerheten eller för försvarsändamål och med lämpliga skyddsåtgärder för de registrerades rättigheter och friheter ⁽⁵⁶⁾.

- (64) Undantaget kan endast tillämpas i den mån det krävs för att skydda den nationella säkerheten eller försvaret. Precis som för de övriga undantag som föreskrivs i 2018 års dataskyddslag måste detta beaktas och åberopas av den personuppgiftsansvariga från fall till fall. Dessutom måste varje tillämpning av undantaget vara förenlig med människorättsnormer (med stöd av *Human Rights Act 1998*) enligt vilken varje ingrepp i rätten till integritet bör vara nödvändigt och proportionerligt i ett demokratiskt samhälle ⁽⁵⁷⁾.
- (65) Denna tolkning av undantaget bekräftas av ICO, som har utfärdat detaljerad vägledning om tillämpningen av undantaget avseende nationell säkerhet och försvaret, och där det klargörs att den personuppgiftsansvariga måste överväga och tillämpa undantaget från fall till fall ⁽⁵⁸⁾. I vägledningen betonas särskilt att "[d]etta inte är ett generellt undantag" och att det för att åberopa undantaget "inte är tillräckligt att uppgifterna behandlas för ändamål som rör nationell säkerhet". Tvärtom måste personuppgiftsansvariga som åberopar undantaget "visa att det finns en verklig risk för att den nationella säkerheten kan påverkas negativt", och den personuppgiftsansvariga förväntas vid behov "förse ICO med uppgifter som styrker [den personuppgiftsansvarigas] beslut att tillämpa detta undantag". Vägledningen innehåller en checklista och ett antal exempel för att ytterligare klargöra villkoren för att åberopa detta undantag.
- (66) Det faktum att uppgifterna behandlas för ändamål som rör den nationella säkerheten eller försvaret är därför inte i sig tillräckligt för att undantaget ska kunna tillämpas. En personuppgiftsansvarig måste överväga de faktiska konsekvenserna för den nationella säkerheten om han eller hon måste följa den särskilda dataskyddsbestämmelsen. Undantaget kan endast tillämpas på de särskilda bestämmelser som har fastställts utgöra en risk och måste tillämpas så restriktivt som möjligt ⁽⁵⁹⁾.
- (67) Detta synsätt har bekräftats av Information Tribunal ⁽⁶⁰⁾. I målet *Baker/Secretary of State for the Home Department ("Baker/Secretary of State")* fastställde tribunalen att det var olagligt att tillämpa undantaget för nationell säkerhet som ett generellt undantag för ansökningar om tillgång till handlingar som mottagits av underrättelsetjänsterna. I stället var det nödvändigt att tillämpa undantaget från fall till fall genom att undersöka varje begäran på grundval av sina egna meriter och med hänsyn till enskildas rätt till respekt för sitt privatliv ⁽⁶¹⁾.

⁽⁵⁶⁾ Enligt den information som lämnats av de brittiska myndigheterna kommer personuppgiftsansvariga, när behandlingen sker i ett nationellt säkerhetssammanhang, vanligtvis att tillämpa skärpta skyddsåtgärder och säkerhetsåtgärder på behandlingen, vilket återspeglar behandlingens känsliga karaktär. Vilka skyddsåtgärder som är lämpliga beror på riskerna med den behandling som utförs. Detta skulle kunna omfatta begränsningar av tillgången till uppgifterna så att de endast kan göras tillgängliga för behöriga personer med lämplig säkerhetsprövning, strikta restriktioner för utbyte av uppgifter och den höga säkerhetsstandard som tillämpas på lagrings- och hanteringsförfarandena.

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

⁽⁵⁸⁾ Se ICO:s vägledning om undantaget avseende nationell säkerhet och försvar, som finns på följande länk <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/national-security-and-defence/>

⁽⁵⁹⁾ Enligt ett exempel från de brittiska myndigheterna skulle det, om en misstänkt terrorist som är föremål för en aktiv utredning av MI5 har lämnat in en begäran om tillgång till inrikesministeriet (t.ex. på grund av att han är inblandad i en tvist med inrikesministeriet om invandringsfrågor), vara nödvändigt att undanhålla den registrerade eventuella uppgifter som MI5 kan ha delat med inrikesministeriet om pågående utredningar som kan skada känsliga källor, metoder eller tekniker och/eller leda till en ökning av hotet från den enskilda. Under sådana omständigheter är det sannolikt att tröskeln för att tillämpa undantaget i avsnitt 26 skulle ha uppnåtts och att ett undantag från skyldigheten att lämna ut information skulle krävas för att skydda den nationella säkerheten. Om inrikesministeriet emellertid även innehade personuppgifter om den enskilde som inte avsåg MI5-utredningen och denna information kunde lämnas utan risk för att den nationella säkerheten skadas skulle undantaget för nationell säkerhet inte vara tillämpligt när man överväger att lämna ut information till den enskilda. ICO håller för närvarande på att utarbeta vägledning om hur personuppgiftsansvariga bör närma sig tillämpningen av undantaget i avsnitt 26. Vägledningen förväntas offentliggöras i slutet av mars 2021.

⁽⁶⁰⁾ Information Tribunal inrättades för att handlägga överklaganden av dataskydd enligt dataskyddslagen från 1984. År 2010 blev *Information Tribunal* en del av *General Regulatory Chamber* av *First Tier Tribunal*, som en del av reformen av det brittiska domstolssystemet.

⁽⁶¹⁾ Se *Baker/Secretary of State for the Home Department* [2001] UKIT NSA2 ("Baker mot Secretary of State").

2.5.6 Begränsningar för personuppgifter som behandlas för journalistiska, konstnärliga, akademiska och litterära ändamål samt för arkivering och forskning

- (68) Enligt artikel 85.2 i den brittiska dataskyddsförordningen får personuppgifter som behandlas för journalistiska, konstnärliga, akademiska och litterära ändamål undantas från flera bestämmelser i den brittiska dataskyddsförordningen. I del 5 i tillägg 2 till 2018 års dataskyddslag anges undantagen för behandling för dessa ändamål. Det innehåller bestämmelser om undantag från dataskyddsprinciperna (med undantag för principen om integritet och konfidentialitet), de rättsliga grunderna för behandling (däribland särskilda kategorier av uppgifter och fällande domar i brottmål osv.), villkoren för samtycke, transparenskraven, de registrerades rättigheter, skyldigheten att anmäla personuppgiftsbrott, kravet på samråd med *the Information Commissioner* före behandling med hög risk och reglerna om internationella överföringar⁽⁶²⁾. I detta avseende avviker den brittiska dataskyddsförordningen inte i sak från förordning (EU) 2016/679 som i artikel 85 också föreskriver en möjlighet att undanta behandling som utförs för journalistiska ändamål eller för akademiska, konstnärliga eller litterära ändamål från ett antal krav i förordning (EU) 2016/679. Bestämmelserna i 2018 års dataskyddslag, särskilt tillägg 2 del 5, är förenliga med den brittiska dataskyddsförordningen.
- (69) Den centrala avvägning som ska göras enligt artikel 85 i den brittiska dataskyddsförordningen gäller huruvida ett undantag från de dataskyddsregler som nämns i skäl 68 är "nödvändigt för att förena rätten till skydd av personuppgifter med yttrande- och informationsfriheten" (63). Enligt bilaga 2, punkterna 26.2 och 3 i 2018 års dataskyddslag, tillämpar Förenade kungariket ett skälighetstest för att uppnå denna balans. För att ett undantag ska vara motiverat måste den personuppgiftsansvariga rimligen tro i) att offentliggörandet ligger i allmänhetens intresse, och ii) att tillämpningen av den relevanta bestämmelsen i dataskyddsförordningen skulle vara oförenlig med journalistiska, akademiska, konstnärliga eller litterära ändamål. Enligt rättspraxis⁽⁶⁴⁾ har kriteriet om rimlig tro både en subjektiv och en objektiv komponent för det räcker inte för den personuppgiftsansvariga att visa att han eller hon själv trodde att kraven inte var uppfyllda. Hans eller hennes övertygelse måste vara rimlig, dvs. den kan antas av en förnuftig person som känner till relevanta fakta. Den personuppgiftsansvariga måste därför visa tillbörlig aktsamhet när han eller hon bildar sin tro för att kunna visa rimlighet. Enligt de förklaringar som lämnats av de brittiska myndigheterna måste skälighetstestet genomföras på grundval av undantag för varje enskilt fall⁽⁶⁵⁾. Om villkoren är uppfyllda anses undantaget vara nödvändigt och proportionerligt enligt Förenade kungarikets lagstiftning.
- (70) Enligt avsnitt 124 i 2018 års dataskyddslag ska ICO utarbeta en uppförandekod om dataskydd och journalistik. Arbetet med denna kod pågår. Vägledning i frågan har utfärdats enligt dataskyddslagen från 1998 där det särskilt betonas att det för att åberopa detta undantag inte räcker att endast ange att efterlevnad skulle vara en olägenhet för journalisternas verksamhet utan det måste finnas ett tydligt argument för att bestämmelsen i

⁽⁶²⁾ Se artikel 85 i den brittiska dataskyddsförordningen och tillägg 2, del 5, punkt 26.9 i 2018 års dataskyddslag.

⁽⁶³⁾ I enlighet med tillägg 2 del 5 punkt 26.2 till 2018 års dataskyddslag är undantaget tillämpligt på behandling av personuppgifter som utförs för särskilda ändamål (journalistiska, akademiska, konstnärliga och litterära ändamål) om behandlingen utförs i syfte att en person ska publicera journalistiskt, akademiskt, konstnärligt eller litterärt material och den personuppgiftsansvariga rimligen tror att offentliggörandet av detta material skulle ligga i allmänhetens intresse. Vid bedömningen av huruvida ett offentliggörande skulle vara i allmänhetens intresse måste den personuppgiftsansvariga ta hänsyn till det allmänna intressets särskilda betydelse för yttrande- och informationsfriheten. Dessutom måste den personuppgiftsansvariga beakta uppförandekoder eller riktlinjer som är relevanta för offentliggörandet i fråga (*BBC Editorial Guidelines*, *Ofcom Broadcasting Code* och *Editors' Code of Practice*). För att ett undantag ska vara tillämpligt måste den personuppgiftsansvariga dessutom rimligen tro att överensstämmelse med den relevanta bestämmelsen skulle vara oförenlig med de särskilda ändamålen (punkt 26.3 i bilaga 2 till 2018 års dataskyddslag).

⁽⁶⁴⁾ I domen NT1/Google [2018] EWHC 799 (QB), punkt 102, behandlades en diskussion om huruvida den personuppgiftsansvariga hade rimliga skäl att anse att offentliggörandet låg i allmänhetens intresse och att efterlevnaden av de relevanta bestämmelserna var oförenlig med de särskilda ändamålen. Domstolen konstaterade att avsnitt 32.1 b och c i dataskyddslagen från 1998 hade följande subjektiva och objektiva inslag: Den personuppgiftsansvariga måste visa att han eller hon trodde att ett offentliggörande skulle ligga i allmänhetens intresse och att denna uppfattning var objektivt rimlig. Det är nödvändigt att fastställa en subjektiv övertygelse om att det skulle vara oförenligt med det särskilda ändamålet i fråga att iakttäva den bestämmelse från vilken den har ansökt om undantag.

⁽⁶⁵⁾ Ett exempel på hur testet med "skälig misstanke" tillämpas ingår ICO om att bötfälla True Visions Productions som fattades enligt dataskyddslagen från 1998. ICO godtog att den personuppgiftsansvariga hade en subjektiv övertygelse om att efterlevnaden av den första principen om dataskydd (rättvisa och lagenlighet) var oförenlig med journalistiska ändamål. ICO godtog dock inte denna uppfattning objektivt sett. ICO:s beslut finns på följande länk: <https://ico.org.uk/media/action-weve-taken/mpns/2614746/true-visions-productions-20190408.pdf>.

fråga utgör ett hinder för ansvarsfull journalistik⁽⁶⁶⁾. Vägledning om tillämpningen av prövningen av allmänintresset och avvägningen mellan allmänintresset och en enskilds intresse av personlig integritet har också offentliggjorts av Förenade kungarikets tillsynsmyndighet för telekommunikation OFCOM och BBC i dess redaktionella riktlinjer⁽⁶⁷⁾. I riktlinjerna ges särskilt exempel på information som kan anses ligga i allmänhetens intresse och behovet av att kunna visa att allmänintresset väger tyngre än rätten till integritet under de särskilda omständigheterna i fallet förklaras.

- (71) I likhet med vad som föreskrivs i artikel 89 i dataskyddsförordningen kan personuppgifter som behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål också undantas från ett antal förtecknade bestämmelser i den brittiska dataskyddsförordningen⁽⁶⁸⁾. Beträffande forskning och statistik är det möjligt att göra undantag från bestämmelserna i den brittiska dataskyddsförordningen vad gäller bekräftelse av behandling och tillgång till uppgifter och skyddsåtgärder för överföringar från tredjeland, rätt till rättelse, begränsning av behandling och invändningar mot behandling. När det gäller arkivering i allmänhetens intresse är det också möjligt att göra undantag från anmälningsskyldigheten när det gäller rättelse eller radering av personuppgifter eller begränsning av behandling och rätten till dataportabilitet.
- (72) Enligt punkterna 27.1 och 28.1 i tillägg 2 till 2018 års dataskyddslag är undantag från de förtecknade bestämmelserna i den brittiska dataskyddsförordningen möjliga om tillämpningen av bestämmelserna skulle "hindra eller allvarligt försämra uppnåendet" av ändamålen i fråga⁽⁶⁹⁾.
- (73) Med tanke på deras relevans för ett effektivt utövande av individuella rättigheter kommer all relevant utveckling när det gäller tolkning och tillämpning av de ovannämnda undantagen i praktiken (utöver undantaget om upprätthållande av en ändamålsenlig invandringskontroll såsom förklaras i skäl 6), inklusive ytterligare utveckling av rättspraxis samt vägledning och verkställande åtgärder från ICO, vederbörligen beaktas i samband med den fortlöpande övervakningen av detta beslut⁽⁷⁰⁾.

2.5.7 Begränsningar av vidare överföringar

- (74) Den skyddsnivå som ges för personuppgifter som överförs från Europeiska unionen till personuppgiftsansvariga eller personuppgiftsbiträden i Förenade kungariket får inte undergrävas av vidare överföring av sådana uppgifter till mottagare i ett tredjeland. Sådana "vidare överföringar" som ur den personuppgiftsansvarigas eller personuppgiftsbiträdets synvinkel utgör internationella överföringar från Förenade kungariket bör endast tillåtas om den ytterligare mottagaren utanför Förenade kungariket själv omfattas av regler som säkerställer en skyddsnivå som liknar den som garanteras i Förenade kungarikets rättsordning. Därför är tillämpningen av bestämmelserna i den brittiska dataskyddsförordningen och 2018 års dataskyddslag på internationella överföringar av personuppgifter en viktig faktor för att säkerställa kontinuiteten i skyddet när det gäller personuppgifter som överförs från Europeiska unionen till Förenade kungariket enligt detta beslut.

⁽⁶⁶⁾ Enligt vägledningen måste organisationerna kunna förklara varför det är oförenligt med journalistikens syften att följa den relevanta bestämmelsen i dataskyddslagen från 1998. Personuppgiftsansvariga måste särskilt väga den negativa effekt som efterlevnaden skulle ha på journalistiken mot den negativa inverkan bristande efterlevnad skulle ha på den registrerades rättigheter. Om en journalist rimligen kan uppnå sina redaktionella syften på ett sätt som överensstämmer med standardbestämmelserna i dataskyddslagen, måste han eller hon göra detta. Organisationerna måste kunna motivera sin användning av begränsningen med avseende på varje bestämmelse som de inte har följt. *Data protection and journalism: a guide for the media*, finns på följande länk: <https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf>.

⁽⁶⁷⁾ Exempel på allmänintresse är att avslöja eller upptäcka brott, skydda folkhälsan eller den allmänna säkerheten, avslöja vilseledande påståenden från enskilda eller organisationer eller avslöja inkompetens som påverkar allmänheten. Se OFCOM:s vägledning på följande länk: https://www.ofcom.org.uk/_data/assets/pdf_file/0017/132083/Broadcast-Code-Section-8.pdf och BBC:s redaktionella riktlinjer, finns på följande länk: <https://www.bbc.com/editorialguidelines/guidelines/privacy>.

⁽⁶⁸⁾ Se artikel 89 i den brittiska dataskyddsförordningen och punkterna 27.2 och 28.2 i del 6 i tillägg 2 till 2018 års dataskyddslag.

⁽⁶⁹⁾ Detta omfattas av kravet att personuppgifter ska behandlas i enlighet med artikel 89.1 i den brittiska dataskyddsförordningen, kompletterad genom avsnitt 19 i 2018 års dataskyddslag.

⁽⁷⁰⁾ Se skälen 281–287.

- (75) Ordningen för internationella överföringar av personuppgifter från Förenade kungariket fastställs i artiklarna 44–49 i den brittiska dataskyddsförordningen, kompletterad av 2018 års dataskyddslag, och är i sak identisk med de bestämmelser som fastställs i kapitel V i förordning (EU) 2016/679 ⁽⁷¹⁾. Överföring av personuppgifter till ett tredjeland eller en internationell organisation kan endast ske på grundval av förordningar om adekvat skyddsnivå (Förenade kungariket motsvarar ett beslut om adekvat skyddsnivå enligt förordning (EU) 2016/679), eller i avsaknad av förordningar om adekvat skyddsnivå, om den personuppgiftsansvariga eller personuppgiftsbiträdet har vidtagit lämpliga skyddsåtgärder i enlighet med artikel 46 i den brittiska dataskyddsförordningen. I avsaknad av förordningar om adekvat skyddsnivå eller lämpliga skyddsåtgärder kan en överföring endast ske på grundval av de undantag som anges i artikel 49 i den brittiska dataskyddsförordningen.
- (76) I de bestämmelser om adekvat skyddsnivå som utfärdas av den ansvariga ministern kan det föreskrivas att ett tredjeland (eller ett territorium eller en sektor inom ett tredjeland), en internationell organisation eller en beskrivning ⁽⁷²⁾ av ett sådant land, territorium, sektor eller organisation säkerställer en adekvat skyddsnivå för personuppgifter. Vid bedömningen av om skyddsnivån är adekvat måste den ansvarige ministern beakta samma faktorer som kommissionen är skyldig att bedöma enligt artikel 45.2 a-c i förordning (EU) 2016/679, tolkad tillsammans med skäl 104 i förordning (EU) 2016/679 och bibehållen EU-rättspraxis. Detta innebär att vid bedömningen av en adekvat skyddsnivå i ett tredjeland kommer den relevanta normen att vara huruvida det berörda tredjelandet säkerställer en skyddsnivå som "i allt väsentligt är likvärdig" med den som garanteras i Förenade kungariket.
- (77) När det gäller förfarandet omfattas förordningar om adekvat skyddsnivå av de "allmänna" formföreskrifter som anges i avsnitt 182 i 2018 års dataskyddslag. Enligt detta förfarande måste den ansvarige ministern samråda med *the Information Commissioner* vid förslag om antagande av brittiska förordningar om adekvat skyddsnivå ska antas ⁽⁷³⁾. När dessa förordningar har antagits av den ansvarige ministern läggs de fram inför parlamentet och omfattas av förfarandet för "negativ resolution" enligt vilket båda kamrarna kan granska förordningarna och kunna anta ett förslag om ogiltigförklaring av förordningarna inom en 40-dagarsperiod ⁽⁷⁴⁾.
- (78) Enligt avsnitt 17B.1 i 2018 års dataskyddslag ska bestämmelserna om adekvat skyddsnivå ses över med högst fyra års mellanrum och ministern ska fortlöpande övervaka utvecklingen i tredjeländer och internationella organisationer som skulle kunna påverka beslut om att utfärda föreskrifter om adekvat skyddsnivå eller att ändra eller upphäva sådana föreskrifter. Om ministern får kännedom om att ett visst land eller en angiven organisation inte längre säkerställer en adekvat skyddsnivå för personuppgifter ska han eller hon, i den utsträckning det är nödvändigt, ändra eller upphäva föreskrifterna och inleda samråd med det berörda tredjelandet eller den berörda internationella organisationen för att avhjälpa bristen på en adekvat skyddsnivå. Dessa förfarandefrågor återspeglar också motsvarande krav i förordning (EU) 2016/679.

⁽⁷¹⁾ Med undantag för artikel 48 i förordning (EU) 2016/679 som Förenade kungariket har valt att inte ta med i den brittiska dataskyddsförordningen. I detta sammanhang bör det först och främst erinras om att den standard som ska anses tillhandahålla en adekvat skyddsnivå är standarden för "väsentlig likvärdighet", inte identitet, vilket har klargjorts av EU-domstolen (Schrems I, punkterna 73–74) och bekräftats av Europeiska dataskyddsstyrelsen (*Adequacy Referential*, s. 3). Såsom Europeiska dataskyddsstyrelsen förklarar i sin referensram för adekvat skyddsnivå är "målet inte att standarden för adekvat skyddsnivå punkt för punkt ska efterlikna EU-lagstiftningen, utan att fastställa de grundläggande och avgörande kraven i denna lagstiftning". I detta avseende är det viktigt att notera att även om Förenade kungarikets rättsordning inte formellt innehåller en bestämmelse som är identisk med artikel 48, garanteras samma effekt av andra rättsliga bestämmelser och principer, dvs. att vid en begäran om tillgång till personuppgifter från en domstol eller en administrativ myndighet i ett tredjeland kan personuppgifter endast överföras till det tredjelandet om det finns ett internationellt avtal – på grundval av vilket tredjelandets domstolsbeslut eller administrativa beslut i fråga erkänns eller verkställs i Förenade kungariket – eller om det grundar sig på en av de överföringsmekanismer som anges i kapitel V i den brittiska dataskyddsförordningen. Närmare bestämt måste domstolarna i Förenade kungariket kunna hänvisa till common law eller en lag som medger att den kan verkställas för att verkställa en utländsk dom. Varken i common law (se *Adams and Others/Cape Industries Plc.*, [1990] 2 W.L.R. 657) eller i lagen finns det några bestämmelser om verkställighet av utländska domar som kräver överföring av uppgifter utan ett internationellt avtal. Detta innebär att begäranden om tillgång till personuppgifter inte är giltiga enligt brittisk lag om det inte finns ett sådant internationellt avtal. All överföring av personuppgifter till tredjeländer – även på begäran från en utländsk domstol eller administrativ myndighet – omfattas dessutom även fortsättningsvis av de begränsningar som anges i kapitel V i den brittiska dataskyddsförordningen, vilka är identiska med de motsvarande bestämmelserna i förordning (EU) 2016/679, vilket i sin tur innebär att begäran måste baseras på en av de grunder för överföring som anges i kapitel V i enlighet med de särskilda villkor som överföringen omfattas av enligt det kapitlet.

⁽⁷²⁾ De brittiska myndigheterna har förklarat att beskrivningen av ett land eller en internationell organisation avser en situation där det skulle vara nödvändigt att göra ett specifikt och partiellt fastställande av adekvat skyddsnivå med fokuserade begränsningar (t.ex. förordningar om adekvat skyddsnivå när det gäller endast vissa typer av uppgiftsöverföringar).

⁽⁷³⁾ Se samförståndsavtalet mellan ministern för digitala frågor, kultur, media och idrott och ICO om ICO:s roll inom ramen för Förenade kungarikets nya tillräcklighetsbedömning, som 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>.

⁽⁷⁴⁾ Om en sådan omröstning antas kommer förordningarna i slutändan att upphöra att ha någon ytterligare rättslig verkan.

- (79) I avsaknad av förordningar om adekvat skyddsnivå kan internationella överföringar äga rum där den personuppgiftsansvariga eller personuppgiftsbiträdet har vidtagit lämpliga skyddsåtgärder i enlighet med artikel 46 i den brittiska dataskyddsförordningen. Dessa skyddsåtgärder liknar dem i artikel 46 i förordning (EU) 2016/679. De omfattar rättsligt bindande och verkställbara instrument mellan myndigheter eller organ, bindande företagsregler⁽⁷⁵⁾, standardiserade dataskyddsbestämmelser, godkända uppförandekoder, godkända certifieringsmekanismer och med tillstånd från *the Information Commissioner*, avtalsklausuler mellan personuppgiftsansvariga (eller personuppgiftsbiträden) eller administrativa överenskommelser mellan myndigheter. Bestämmelserna har dock ändrats ur förfarandemässig synvinkel för att fungera inom ramen för Förenade kungariket och i synnerhet kan standardklausulerna om dataskydd antas av ministern (avsnitt 17C) eller *the Information Commissioner* (avsnitt 119A) i enlighet med 2018 års dataskyddslag.
- (80) I avsaknad av ett beslut om adekvat skyddsnivå eller lämpliga skyddsåtgärder kan en överföring endast ske på grundval av de undantag som anges i artikel 49 i den brittiska dataskyddsförordningen⁽⁷⁶⁾. Den brittiska dataskyddsförordningen innebär inga väsentliga ändringar av undantagen jämfört med motsvarande regler i förordning (EU) 2016/679. Enligt den brittiska dataskyddsförordningen, liksom enligt förordning (EU) 2016/679, kan vissa undantag endast återopas om överföringen sker tillfälligt⁽⁷⁷⁾. Dessutom klargör ICO följande i sin vägledning om internationella överföringar: "Ni bör endast använda dessa som verkliga 'undantag' från den allmänna regeln att ni inte bör göra en begränsad överföring om den inte omfattas av ett beslut om adekvat skyddsnivå eller om det finns lämpliga skyddsåtgärder"⁽⁷⁸⁾. När det gäller överföringar som är nödvändiga av viktiga skäl av allmänt intresse (artikel 49.1 d) kan ministern utfärda förordningar för att specificera under vilka omständigheter en överföring av personuppgifter till ett tredjeland eller en internationell organisation är nödvändig eller inte är nödvändig av viktiga skäl av allmänt intresse. Dessutom kan ministern genom förordningar begränsa överföringen av en kategori personuppgifter till ett tredjeland eller en internationell organisation om överföringen inte kan ske på grundval av bestämmelser om adekvat skyddsnivå och den ansvariga ministern anser att begränsningen är nödvändig av viktiga skäl av allmänt intresse. Hittills har inga sådana förordningar antagits.
- (81) Denna ram för internationella överföringar har blivit tillämplig i slutet av övergångsperioden⁽⁷⁹⁾. I punkt 4 i tillägg 21 till 2018 års dataskyddslag (införd genom DPPEC Regulations) föreskrivs emellertid att vissa överföringar av personuppgifter från och med övergångsperiodens utgång behandlas som om de grundar sig på förordningar om adekvat skyddsnivå. Dessa överföringar omfattar överföringar till en EES-stat, territoriet Gibraltar, en unionsinstitution, ett unionsorgan eller en unionsbyrå som inrättats av eller på grundval av EU-fördraget och tredjeländer som var föremål för ett EU-beslut om adekvat skyddsnivå vid övergångsperiodens utgång. Följaktligen kan överföringarna till dessa länder fortsätta som före Förenade kungarikets

⁽⁷⁵⁾ I den brittiska dataskyddsförordningen behålls reglerna i artikel 47 i förordning (EU) 2016/679 med förbehåll endast för ändringar för att anpassa reglerna till inhemska sammanhang, till exempel genom att hänvisningarna till den behöriga tillsynsmyndigheten ersätts med *the Information Commissioner*, strykning av hänvisningen till mekanismen för enhetlighet i punkt 1 och strykning av hela punkt 3.

⁽⁷⁶⁾ Enligt artikel 49 i den brittiska dataskyddsförordningen är överföringar möjliga om ett av följande villkor är uppfyllt: a) Den registrerade har uttryckligen samtyckt till den föreslagna överföringen efter att ha informerats om de möjliga riskerna med sådana överföringar för den registrerade på grund av att det saknas ett beslut om adekvat skyddsnivå och lämpliga skyddsåtgärder. b) Överföringen är nödvändig för att fullgöra ett avtal mellan den registrerade och den personuppgiftsansvariga eller för att genomföra åtgärder som vidtas innan avtal ingås på den registrerades begäran. c) Överföringen är nödvändig för att ingå eller fullgöra ett avtal som ingåtts i den registrerades intresse mellan den personuppgiftsansvariga och en annan fysisk eller juridisk person. d) Överföringen är nödvändig av viktiga skäl av allmänt intresse. e) Överlåtelsen är nödvändig för att fastställa, göra gällande eller försvara rättsliga anspråk. f) Överföringen är nödvändig för att skydda den registrerades eller andra personers vitala intressen om den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke. g) Överföringen sker från ett register som enligt nationell rätt är avsett att ge allmänheten information och som är tillgängligt antingen för allmänheten eller för var och en som styrka ett berättigat intresse men endast i den mån som de villkor för tillgång som föreskrivs i nationell rätt är uppfyllda i det enskilda fallet. Om inget av ovanstående villkor är tillämpligt får en överföring dessutom endast ske om den inte upprepas, berör endast ett begränsat antal registrerade, är nödvändig för att uppnå tvingande berättigade intressen hos den personuppgiftsansvariga som inte uppvägs av den registrerades intressen eller rättigheter och friheter och den personuppgiftsansvariga har bedömt alla omständigheter kring uppgiftsöverföringen och på grundval av denna bedömning har vidtagit lämpliga skyddsåtgärder med avseende på skyddet av personuppgifter.

⁽⁷⁷⁾ I skäl 111 i den brittiska dataskyddsförordningen anges att överföringar i samband med ett avtal eller ett rättsligt anspråk endast får ske om de är tillfälliga.

⁽⁷⁸⁾ Vägledning från ICO om internationella överföringar, finns på följande länk: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/#ib7>.

⁽⁷⁹⁾ Under en period på högst sex månader som slutar senast den 30 juni 2021 måste tillämpningen av denna nya ram läsas mot bakgrund av artikel 782 i handels- och samarbetsavtalet mellan Europeiska unionen och Europeiska atomenergigemenskapen, å ena sidan, och Förenade konungariket Storbritannien och Nordirland, å andra sidan (EUT L 444, 31.12.2020, s. 14) (*avtalet om handel och samarbete mellan EU och Förenade kungariket*), som finns på följande länk: [https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:22020A1231\(01\)&from=EN](https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:22020A1231(01)&from=EN).

utträde ur EU. Efter övergångsperiodens utgång måste ministern under en fyraårsperiod, dvs. före utgången av december 2024, göra en översyn av dessa konstateranden om adekvat skyddsnivå. Enligt den förklaring som lämnats av de brittiska myndigheterna innehåller övergångsbestämmelserna inte någon bestämmelse om tidsbegränsning, även om den ansvariga ministern måste göra en sådan översyn senast i slutet av december 2024, och de relevanta övergångsbestämmelserna kommer inte automatiskt att upphöra att gälla om en översyn inte är slutförd i slutet av december 2024.

- (82) Vad gäller den framtida utvecklingen av det brittiska systemet för internationella överföringar – genom antagandet av de nya bestämmelserna om adekvat skyddsnivå, ingåendet av internationella avtal eller utveckling av andra överföringsmekanismer – kommer kommissionen noga övervaka situationen, bedöma om de olika överföringsmekanismerna används på ett sätt som säkerställer fortsatt skydd och, vid behov, vidta lämpliga åtgärder för att hantera eventuella negativa verkningar för ett sådant fortsatt skydd (se skälen 278–287). Eftersom EU och Förenade kungariket har liknande regler för internationella överföringar förväntas problematiska avvikelser även kunna undvikas genom samarbete, informationsutbyte och erfarenhetsutbyte, bland annat mellan ICO och Europeiska dataskyddsstyrelsen.

2.5.8 Ansvarsskyldighet

- (83) Enligt principen om ansvarsskyldighet är enheter som behandlar uppgifter skyldiga att införa lämpliga tekniska och organisatoriska åtgärder för att effektivt fullgöra sina skyldigheter att skydda uppgifter och kunna uppvisa sådan överensstämmelse, särskilt för den behöriga tillsynsmyndigheten.
- (84) Principen om ansvarsskyldighet i förordning (EU) 2016/679 har behållits i artikel 5.2 i den brittiska dataskyddsförordningen utan någon väsentlig ändring och detsamma gäller artikel 24 om den personuppgiftsansvarigas ansvar, artikel 25 om inbyggt dataskydd, dataskydd som standard och artikel 30 om register över behandlingsverksamhet. Artiklarna 35 och 36 om konsekvensbedömning avseende dataskydd och föregående samråd med tillsynsmyndigheten har också behållits. Artiklarna 37–39 i förordning (EU) 2016/679 om att utse dataskyddsbud och dataskyddsbudens uppgifter har behållits i den brittiska dataskyddsförordningen utan några väsentliga ändringar. Dessutom har bestämmelserna i artiklarna 40 och 42 i förordning (EU) 2016/679 om uppförandekoder och certifiering behållits i den brittiska dataskyddsförordningen ⁽⁸⁰⁾.

2.6 Tillsyn och efterlevnad

2.6.1 Oberoende tillsyn

- (85) För att säkerställa att en adekvat dataskyddsnivå garanteras i praktiken bör det finnas en oberoende tillsynsmyndighet med befogenhet att övervaka och verkställa efterlevnaden av dataskyddsbestämmelserna. Denna myndighet bör agera helt oavhängigt och opartiskt vid fullgörandet av sina skyldigheter och utövandet av sina befogenheter.
- (86) I Förenade kungariket övervakas och verkställs efterlevnaden av den brittiska dataskyddsförordningen och 2018 års dataskyddslag av *the Information Commissioner*. *The Information Commissioner* är en "Corporation Sole", en separat juridisk person som består av en enda person. *The Information Commissioner* bistås i sitt arbete av ett kontor. Den 31 mars 2020 hade ICO 768 fast anställda ⁽⁸¹⁾. Uppdragsgivande ministerium för *the Information Commissioner* är ministeriet för digitala frågor, kultur, media och idrott ⁽⁸²⁾.
- (87) Att *the Commissioner* är oberoende fastställs uttryckligen i artikel 52 i den brittiska dataskyddsförordningen som inte innebär några väsentliga ändringar av artikel 52.1–3 i dataskyddsförordningen. *The Commissioner* måste agera fullständigt oberoende vid utförandet av sina uppgifter och utöva sina befogenheter i enlighet med den brittiska dataskyddsförordningen, vara fri från yttre påverkan, direkt eller indirekt, i förhållande till dessa uppgifter och

⁽⁸⁰⁾ Vid behov ersätts dessa hänvisningar med hänvisningar till de brittiska myndigheterna. Enligt avsnitt 17 i 2018 års dataskyddslag kan t.ex. *the Information Commissioner* eller det nationella ackrediteringsorganet i Förenade kungariket ackreditera en person som uppfyller kraven i artikel 43 i den brittiska dataskyddsförordningen för att övervaka efterlevnaden av en certifiering.

⁽⁸¹⁾ Information Commissioner: *Annual Report and Financial Statements 2019–2020*, som finns på följande länk: <https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf>

⁽⁸²⁾ Ett förvaltningsavtal reglerar förhållandet mellan dem. De viktigaste uppgifterna för ministeriet för digitala frågor, kultur, media och idrott, i egenskap av uppdragsgivande avdelning, omfattar följande: Se till att *the Information Commissioner* får tillräcklig finansiering och tillräckliga resurser. Företräda de intressen som *the Information Commissioner* har inför parlamentet och andra regeringsministerier. Se till att det finns en stabil nationell ram för dataskydd. Ge vägledning och stöd till ICO om företagsfrågor som fastighetsfrågor, hyresavtal och upphandling (förvaltningsavtalet 2018–2021, som finns på följande länk: <https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf>).

befogenheter och varken begära eller ta emot instruktioner från någon. *The Commissioners* ska också avhålla sig från varje handling som är oförenlig med hans eller hennes uppdrag och får inte utöva någon avlönad eller oavlönad yrkesverksamhet under tiden som han eller hon innehar sitt ämbete.

- (88) Villkoren för utnämning och avsättning av *the Information Commissioners* anges i bilaga 12 till 2018 års dataskyddslag. *The Information Commissioners* utses av drottningen på rekommendation av regeringen i enlighet med ett rättvist och öppet uttagningsförfarande. Den sökande måste ha lämpliga kvalifikationer, färdigheter och kompetenser. I enlighet med förvaltningskodexen om offentliga utnämningar ⁽⁸³⁾ upprättas en förteckning över kandidater som kan utnämnas av en rådgivande utvärderingspanel. Innan ministern vid ministeriet för digitala frågor, kultur, media och idrott slutför sitt beslut måste det berörda särskilda utskottet i parlamentet genomföra en kontroll före utnämningen. Kommitténs ståndpunkt offentliggörs ⁽⁸⁴⁾.
- (89) *The Information Commissioners* har en mandatperiod på upp till sju år. En person kan inte utses till *Information Commissioner* mer än en gång. *The Information Commissioner* kan avsättas av drottningen efter en *address* från båda kamrarna i parlamentet ⁽⁸⁵⁾. Ingen begäran om entledigande av *the Information Commissioners* kan lämnas in till någon av parlamentets kammare om inte en minister har lagt fram en rapport som visar att han eller hon är övertygad om att *the Information Commissioners* gjort sig skyldig till allvarlig försummelse och/eller inte längre uppfyller de villkor som krävs för att kunna fullgöra sina uppgifter ⁽⁸⁶⁾.
- (90) Finansieringen av *the Information Commissioners* kommer från följande tre källor: i) Avgifter för dataskydd som betalas av personuppgiftsansvariga, som fastställs i den ansvarige ministrarnas föreskrifter ⁽⁸⁷⁾ (Data Protection (Charges and Information) Regulations 2018) och uppgår till 85 % – 90 % av myndighetens årliga budget ⁽⁸⁸⁾. ii) Bidrag i form av statligt stöd till *the Informations Commissioners*. Bidrag i form av stöd används främst för att finansiera de driftskostnader *the Information Commissioners* har vad gäller uppgifter som inte rör dataskydd ⁽⁸⁹⁾. iii) Avgifter som tas ut för tjänster ⁽⁹⁰⁾. För närvarande tas inga sådana avgifter ut.
- (91) De allmänna arbetsuppgifter som *the Information Commissioner* har vad gäller behandling av personuppgifter som omfattas av den brittiska dataskyddsförordningen fastställs i artikel 57 i den brittiska dataskyddsförordningen som nära återspeglar motsvarande regler i förordning (EU) 2016/679. Dess uppgifter omfattar övervakning och verkställande av den brittiska dataskyddsförordningen, främjande av allmänhetens medvetenhet, hantering av klagomål från registrerade, genomförande av utredningar osv. I avsnitt 115 i 2018 års dataskyddslag fastställs dessutom andra allmänna uppgifter för *the Commissioners*, däribland en skyldighet att ge råd till parlamentet, regeringen och andra institutioner och organ om lagstiftningsåtgärder och administrativa åtgärder som rör skyddet

⁽⁸³⁾ Styrningskoden för offentliga utnämningar, finns på följande länk: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/578498/governance_code_on_public_appointments_16_12_2016.pdf.

⁽⁸⁴⁾ Andra rapporten från sammanträdesperioden 2015–2016 från utskottet för kultur, medier och idrott i underhuset finns på följande länk: <https://publications.parliament.uk/pa/cm201516/cmselect/cmcomeds/990/990.pdf>.

⁽⁸⁵⁾ Framställningen utgörs av en *address* som en motion som lagts fram för parlamentet och som syftar till att göra monarken medveten om parlamentets yttranden i en viss fråga.

⁽⁸⁶⁾ Punkt 3.3 i tillägg 12 till 2018 års dataskyddslag.

⁽⁸⁷⁾ Avsnitt 137 i 2018 års dataskyddslag, se skäl 17.

⁽⁸⁸⁾ Avsnitten 137 och 138 i 2018 års dataskyddslagen innehåller ett antal skyddsåtgärder för att säkerställa att avgifterna fastställs på en lämplig nivå. Särskilt avsnitt 137.4 innehåller en förteckning över de omständigheter som ministern måste beakta när han eller hon fastställer det belopp som olika organisationer ska betala. För det andra innehåller avsnitt 138.1 och avsnitt 182 i 2018 års dataskyddslag även en rättslig skyldighet för ministern att samråda med *the Information Commissioners* och andra företrädare för personer som kan komma att beröras av förordningarna innan de framförs för att deras synpunkter ska kunna beaktas. Enligt avsnitt 138.2 i 2018 års dataskyddslag är *the Information Commissioners* dessutom skyldig att se över avgiftsförordningarnas funktion och kan lämna förslag till ministern om ändringar av förordningarna. Slutligen, utom i de fall då bestämmelser endast utarbetas för att ta hänsyn till en ökning av konsumentprisindex (då de kommer att omfattas av ett negativt resolutionsförfarande), omfattas föreskrifterna av ett positivt resolutionsförfarande och får inte utfärdas förrän de har godkänts genom ett beslut av varje kammare.

⁽⁸⁹⁾ I förvaltningsavtalet klargjordes att den ansvarige ministern får göra utbetalningar till *Information Commissioners* med medel som tillhandahålls av parlamentet enligt punkt 9 i bilaga 12 till 2018 års dataskyddslag. Efter samråd med *the Information Commissioners* ska DCMS betala lämpliga belopp (bidraget i form av stöd) för ICO:s administrativa kostnader och utövandet av de arbetsuppgifter som *the Information Commissioners* har i samband med ett antal specifika funktioner, däribland informationsfrihet” (förvaltningsavtal 2018–2021, punkt 1.12, se fotnot 82).

⁽⁹⁰⁾ Se avsnitt 134 i 2018 års dataskyddslag.

av enskildas fri- och rättigheter i samband med behandling av personuppgifter och en befogenhet att på eget initiativ eller på begäran avge yttranden till parlamentet, regeringen eller andra institutioner och organ samt till allmänheten i alla frågor som rör skyddet av personuppgifter. För att upprätthålla rättsväsendets oberoende är *the Information Commissioner* inte behörig att utföra sina uppgifter i samband med behandling av personuppgifter som utförs av en enskild person som handlar i egenskap av en dömande myndighet eller av en domstol eller tribunal som agerar inom ramen för sin dömande verksamhet. Tillsynen över rättsväsendet säkerställs dock av specialiserade organ (se skälen 99–103).

2.6.2 Verkställighet, inklusive påföljder

- (92) De befogenheter som *the Information Commissioner* har finns fastställda i artikel 58 i den brittiska dataskyddsförordningen som inte innebär några väsentliga ändringar av motsvarande artikel i förordning (EU) 2016/679. 2018 års dataskyddslag innehåller kompletterande bestämmelser om hur dessa befogenheter kan utövas. *The Commissioner* har särskilt befogenhet att a) förelägga den personuppgiftsansvariga och personuppgiftsbiträdet (och under vissa omständigheter valfri annan person) att lämna nödvändig information genom att utfärda ett informationsföreläggande ("information notice")⁽⁹¹⁾, b) utföra utredningar och revisioner genom att utfärda ett bedömningsföreläggande ("assessment notice") som kan ålägga den personuppgiftsansvariga eller personuppgiftsbiträdet att ge *the Commissioner* tillträde till särskilda lokaler, inspekterar eller undersöker handlingar eller utrustning, frågar ut personer som behandlar personuppgifter för den personuppgiftsansvarigas räkning osv.⁽⁹²⁾, c) på annat sätt få tillgång till handlingar m.m. för personuppgiftsansvariga och personuppgiftsbiträden och tillträde till deras lokaler i enlighet med avsnitt 154 i 2018 års dataskyddslag ("befogenheter för tillträde och inspektion"), d) utöva korrigerande befogenheter, bland annat genom varningar och reprimander eller utfärda förelägganden genom att utfärda ett verkställighetsföreläggande ("enforcement notice"), genom vilka personuppgiftsansvariga/personuppgiftsbiträden åläggs att vidta eller avstå från att vidta specificerade åtgärder, däribland att förelägga den personuppgiftsansvariga eller personuppgiftsbiträdet att utföra något som anges i artikel 58.2 c-g och j i den brittiska dataskyddsförordningen⁽⁹³⁾ e) och utdöma administrativa sanktionsavgifter i form av ett påföljdsföreläggande ("penalty notice")⁽⁹⁴⁾. Påföljdsföreläggande kan även utfärdas om en myndighet inte har följt bestämmelserna i den brittiska dataskyddsförordningen⁽⁹⁵⁾.
- (93) ICO:s policy för lagstiftningsåtgärder anges under vilka omständigheter det kommer att utfärda ett föreläggande om information, bedömning, verkställighet eller påföljder⁽⁹⁶⁾. Ett verkställighetsföreläggande som lämnas till följd av personuppgiftsansvarigs eller ett personuppgiftsbiträdes underlåtenhet får endast ställa krav som *the Commissioner* anser vara lämpliga för att avhjälpa underlåtenheten. Verkställighetsförelägganden och påföljdsförelägganden får utfärdas till en personuppgiftsansvariga eller ett personuppgiftsbiträde i samband med överträdelser av kapitel II i den brittiska dataskyddsförordningen (principerna för behandling), artiklarna 12–22 (den registrerades rättigheter), artiklarna 25–39 (skyldigheter för personuppgiftsansvariga och personuppgiftsbiträden) och artiklarna 44–49 (internationella överföringar) i den brittiska dataskyddsförordningen. Ett verkställighetsföreläggande får även lämnas om en personuppgiftsansvarig har underlåtit att uppfylla skyldigheten att betala en avgift enligt föreskrifter i avsnitt 137 i 2018 års dataskyddslag. Dessutom kan ett övervakningsorgan enligt artikel 41 eller en tillhandahållare av certifiering få ett verkställighetsföreläggande om de underlåter att uppfylla sina skyldigheter enligt den brittiska dataskyddsförordningen. Ett påföljdsföreläggande kan även lämnas till en person som inte har följt ett informationsföreläggande, ett bedömningsföreläggande eller ett verkställighetsföreläggande.
- (94) Enligt påföljdsföreläggandet ska personen betala ett belopp som anges i föreläggandet till *the Information Commissioner*. Vid fastställandet av huruvida en person ska få ett påföljdsföreläggande och bestämning av storleken på sanktionsavgiften måste *the Information Commissioner* beakta de omständigheter som anges i artikel 83.1 och 2 i den brittiska dataskyddsförordningen som är identiska med motsvarande bestämmelser i förordning (EU) 2016/679⁽⁹⁷⁾. Enligt artikel 83.4 och 5 är det högsta beloppet för administrativa sanktionsavgifter vid

⁽⁹¹⁾ Avsnitt 142 i 2018 års dataskyddslag (med förbehåll för begränsningarna i avsnitt 143 i 2018 års dataskyddslag).

⁽⁹²⁾ Avsnitt 146 i 2018 års dataskyddslag (med förbehåll för begränsningarna i avsnitt 147 i 2018 års dataskyddslag).

⁽⁹³⁾ Avsnitt 149–151 i 2018 års dataskyddslag (med förbehåll för begränsningarna i avsnitt 152 i 2018 års dataskyddslag).

⁽⁹⁴⁾ Avsnitt 155 i 2018 års dataskyddslag och artikel 83 i den brittiska dataskyddsförordningen.

⁽⁹⁵⁾ Detta följer av avsnitt 155.1 jämfört med avsnitt 149.2 och 149.5 samt avsnitt 156.4 i 2018 års dataskyddslag, som begränsar utfärdandet av påföljdsföreläggande med avseende på *the Crown Estate Commissioners* och personuppgiftsansvariga från de kungliga hovstaterna (*Royal Household*) enligt avsnitt 209.4 i 2018 års dataskyddslag.

⁽⁹⁶⁾ Policyn för lagstiftningsåtgärder (*Regulatory Action Policy*), finns på följande länk: <https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf>.

⁽⁹⁷⁾ Inbegripet överträdelsens art och allvar (med beaktande av den berörda behandlingens art eller syfte samt antalet registrerade som påverkas och omfattningen av den skada som de lidit), överträdelsens avsiktliga eller försumliga karaktär, alla åtgärder som vidtas av den personuppgiftsansvariga för att lindra den skada som de registrerade lidit, den personuppgiftsansvarigas eller personuppgiftsbiträdets grad av ansvar (med beaktande av den personuppgiftsansvarigas eller personuppgiftsbiträdets tekniska och organisatoriska åtgärder), alla relevanta tidigare överträdelser som den personuppgiftsansvariga eller personuppgiftsbiträdet gjort sig skyldig till, graden av samarbete med *the Commissioner*, de kategorier av personuppgifter som påverkas av misslyckandet, andra försvårande eller förmildrande faktorer som är tillämpliga på omständigheterna i fallet, till exempel ekonomiska fördelar eller förluster som direkt eller indirekt undvikits genom överträdelsen.

underlåtenhet att uppfylla de skyldigheter som avses i dessa bestämmelser 8 700 000 pund respektive 17 500 000 pund. När det gäller ett företag kan *the Information Commissioner* också ålägga sanktionsavgifter som en procentandel av den globala årsomsättningen om detta ger ett högre belopp. Liksom i motsvarande bestämmelser i förordning (EU) 2016/679 fastställs dessa belopp till 2 % respektive 4 % i artiklarna 83.4 och 5. Vid underlåtenhet att följa ett informationsföreläggande, ett bedömningsföreläggande eller ett verkställighetsföreläggande är den högsta påföljdsbelopp som kan utdömas genom ett påföljdsföreläggande det högre av 17 500 000 GBP eller, om det rör sig om ett företag, 4 % av den globala årsomsättningen.

- (95) Den brittiska dataskyddsförordningen har tillsammans med 2018 års dataskyddslag också stärkt andra befogenheter för *the Information Commissioner*. Till exempel kan *the Commissioner* nu utföra obligatoriska revisioner av alla personuppgiftsansvariga eller personuppgiftsbiträden med hjälp av bedömningsförelägganden medan *the Commissioner* enligt den tidigare lagstiftningen, dataskyddslagen från 1998, endast hade denna befogenhet när det gäller statliga myndighetsorgan samt hälso- och sjukvårdsorganisationer medan andra måste samtycka till en revision.
- (96) Sedan förordning (EU) 2016/679 infördes hanterar ICO omkring 40 000 klagomål från registrerade per år ⁽⁹⁸⁾ och genomför dessutom cirka 2 000 undersökningar på eget initiativ ⁽⁹⁹⁾. En majoritet av klagomålen rör rätten att få tillgång till och utlämnande av uppgifter. Efter sina utredningar vidtar *the Commissioner* verkställighetsåtgärder inom en rad olika sektorer. Enligt de senaste årsrapporten från *the Information Commissioner* (2019–2020) ⁽¹⁰⁰⁾ utfärdade denne närmare bestämt 54 informationsförelägganden, 8 påföljdsförelägganden, 7 verkställighetsförelägganden, 4 varningar, 8 åtal och 15 sanktionsavgifter under rapporteringsperioden ⁽¹⁰¹⁾.
- (97) Detta inbegriper flera betydande sanktionsavgifter som utdömts enligt förordning (EU) 2016/679 och 2018 års dataskyddslag. I oktober 2020 bötfällde *the Information Commissioner* ett brittiskt flygbolag med 20 miljoner pund för ett uppgiftsbrott som berörde mer än 400 000 kunder. I slutet av oktober 2020 bötfölls en internationell hotellkedja med 18,4 miljoner pund för att ha underlåtit att skydda miljontals kunders personuppgifter och i november 2020 bötfölls en brittisk tjänsteleverantör som sålde evenemangsbiljetter online med 1,25 miljoner pund för att ha underlåtit att skydda kundernas betalningsuppgifter ⁽¹⁰²⁾.
- (98) Utöver de tillsynsbefogenheter som *the Information Commissioner* har, som beskrivs i skäl 92, utgör vissa överträdelser av dataskyddslagstiftningen lagbrott och kan därför bli föremål för straffrättsliga påföljder (avsnitt 196 i 2018 års dataskyddslag). Detta gäller till exempel medvetet eller vårdslöst erhållande eller utlämnande av personuppgifter utan den personuppgiftsansvarigas samtycke, säkerställande av utlämnande av personuppgifter till en annan person utan den personuppgiftsansvarigas ⁽¹⁰³⁾ samtycke, återidentifiering av information som är avidentifierade personuppgifter ⁽¹⁰⁴⁾ utan samtycke från den personuppgiftsansvariga som ansvarar för avidentifieringen, avsiktlig inskränkning av den rätt *the Commissioner* har att utöva sina befogenheter vad gäller kontroll av personuppgifter i enlighet med internationella skyldigheter ⁽¹⁰⁵⁾, lämnande av oriktiga uppgifter som svar på ett informationsföreläggande eller förstörande av information i samband med informations- och bedömningsförelägganden ⁽¹⁰⁶⁾.

⁽⁹⁸⁾ Enligt den information som lämnats av de brittiska myndigheterna konstaterades under den period som omfattas av *the Information Commissioner's Annual Report 2019–2020* ingen överträdelse i omkring 25 % av fallen, i omkring 29 % av fallen ombads den registrerade antingen att ta upp frågan med den personuppgiftsansvariga första gången, att invänta den personuppgiftsansvarigas svar eller att fortsätta en pågående dialog med den personuppgiftsansvariga, i omkring 17 % av fallen konstaterades ingen överträdelse men råd gavs till den personuppgiftsansvariga, i ungefär 25 % av fallen upptäckte *Information Commissioner* en överträdelse och gav antingen råd till den personuppgiftsansvariga eller också var den personuppgiftsansvariga tvungen att vidta vissa åtgärder, i ungefär 3 % av fallen bestämdes det att klagomålet inte omfattas av förordning (EU) 2016/679 och ungefär 1 % av fallen hänvisades till en annan dataskyddsmyndighet inom ramen för Europeiska dataskyddsstyrelsen.

⁽⁹⁹⁾ ICO kan inleda dessa utredningar på grundval av information från en rad olika källor, bland annat anmälningar om personuppgiftsbrott, anmälningar från andra brittiska myndigheter eller utländska dataskyddsmyndigheter och klagomål från enskilda personer eller organisationer i det civila samhället.

⁽¹⁰⁰⁾ *Information Commissioner's Annual Report and Financial Statements 2019–2020* (se fotnot 81).

⁽¹⁰¹⁾ Enligt den föregående årsberättelse för perioden 2018–2019 utfärdade *the Information Commissioner* 22 påföljdsförelägganden enligt dataskyddslagen från 1998 under rapporteringsperioden med sanktionsavgifter på totalt 3 010 610 pund, varav två sanktionsavgifter på 500 000 pund (det högsta tillåtna beloppet enligt dataskyddslagen från 1998). Under 2018 genomförde *the Information Commissioner* en undersökning av användningen av dataanalys för politiska ändamål efter avslöjandena om Cambridge Analytica. Utredningen resulterade i en policyrapport, en uppsättning rekommendationer, sanktionsavgifter på 500 000 pund mot Facebook och ett verkställighetsföreläggande till Aggregate IQ, en kanadensisk datamäklare, som ålägger företaget att radera personuppgifter om brittiska medborgare och invånare (se *the Information Commissioner's Annual Report and Financial Statement 2018–2019*, som finns på följande länk: <https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf>).

⁽¹⁰²⁾ För en sammanfattning av de verkställighetsåtgärder som vidtagits, se webbplatsen för ICO, som finns på följande länk: <https://ico.org.uk/action-weve-taken/enforcement/>.

⁽¹⁰³⁾ Avsnitt 170 i 2018 års dataskyddslag.

⁽¹⁰⁴⁾ Avsnitt 171 i 2018 års dataskyddslag.

⁽¹⁰⁵⁾ Avsnitt 119 i 2018 års dataskyddslag.

⁽¹⁰⁶⁾ Avsnitten 144 och 148 i 2018 års dataskyddslag.

2.6.3 Tillsyn över rättsväsendet

- (99) Tillsynen över domstolarnas och rättsväsendets behandling av personuppgifter är dubbel. Om en innehavare av ett domarämbete eller en domstol inte agerar inom ramen för sin dömande verksamhet står ICO för tillsyn. Om den personuppgiftsansvariga agerar inom ramen för sin dömande verksamhet kan ICO inte utöva sina tillsynsfunktioner ⁽¹⁰⁷⁾ utan tillsynen utförs av särskilda organ. Detta återspeglar det tillvägagångssätt som antagits i förordning (EU) 2016/679 (artikel 55.3).
- (100) I synnerhet i det andra scenariot, för domstolarna i England och Wales samt *First-tier Tribunals* och *Upper Tribunals* i England och Wales, tillhandahålls sådan tillsyn av *Judicial Data Protection Panel* ⁽¹⁰⁸⁾. *Lord Chief Justice* och *Chief President of Tribunals* har dessutom utfärdat ett meddelande om skydd av personuppgifter ⁽¹⁰⁹⁾ som beskriver hur domstolarna i England och Wales behandlar personuppgifter för en rättslig funktion. Ett liknande meddelande har utfärdats av de nordirländska ⁽¹¹⁰⁾ och skotska domstolarna ⁽¹¹¹⁾.
- (101) I Nordirland har dessutom *Lord Chief Justice of Northern Ireland* utsett en domare vid High Court som datatillsynsdomare (*Data Supervisory Judge, DSJ*) ⁽¹¹²⁾. De har också gett vägledning till det nordirländska domstolsväsendet om vad som ska göras i händelse av förlust eller potentiell förlust av uppgifter och förfarandet för att hantera eventuella problem som uppstår till följd av detta ⁽¹¹³⁾.
- (102) I Skottland har Lord President utsett en datatillsynsdomare som ska utreda eventuella klagomål med hänvisning till dataskydd. Detta anges i de regler för klagomål till domstol som motsvarar dem som gäller för England och Wales ⁽¹¹⁴⁾.
- (103) I högsta domstolen utses slutligen en av högsta domstolens domare för att övervaka dataskyddet.

2.6.4 Prövningsmöjligheter

- (104) För att säkerställa adekvat skydd, och i synnerhet tillämpningen av individuella rättigheter, bör den registrerade tillförsäkras effektiv administrativ och rättslig prövning, inbegripet ersättning för skador.

⁽¹⁰⁷⁾ Avsnitt 117 i 2018 års dataskyddslag.

⁽¹⁰⁸⁾ Panelen ansvarar för att ge domstolsväsendet vägledning och utbildning. Den behandlar också klagomål från registrerade med avseende på behandling av personuppgifter som utförs av domstolar och enskilda personer som handlar i egenskap av en dömande myndighet. Panelen har för avsikt att tillhandahålla de medel som kan användas för att lösa eventuella klagomål. Om en klagande var missnöjd med panelens beslut och lade fram ytterligare bevisning skulle panelen kunna ompröva sitt beslut. Även om panelen själv inte utdömer ekonomiska sanktioner kan den, om den anser att det föreligger en tillräckligt klar överträdelse av 2018 års dataskyddslag, hänskjuta den till JCIO (*Judicial Conduct Investigation Office*), som kommer att utreda klagomålet. Om klagomålet godtas ankommer det på Lord Chancellor och Lord Chief Justice (eller en högre domare som delegerats att agera på hans eller hennes vägnar) att besluta om vilka åtgärder som ska vidtas mot befattningshavaren. Detta kan, beroende på svårighetsgrad, omfatta formell rådgivning, formell varning och reprimand och, i slutändan, entledigande. Om en person är missnöjd med det sätt på vilket klagomålet har utretts av JCIO kan han eller hon lämna in ett klagomål till *Judicial Appointments and Conduct Ombudsman* (se <https://www.gov.uk/government/organisations/judicial-appointments-and-conduct-ombudsman>). Ombudsmannen har befogenhet att be JCIO att utreda ett klagomål på nytt och kan föreslå att klaganden ska få ersättning om han eller hon anser sig ha lidit skada till följd av administrativa missförhållanden.

⁽¹⁰⁹⁾ Meddelandet om skydd av personuppgifter från *Lord Chief Justice* and *Senior President of Tribunals*, finns på följande länk: <https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice>

⁽¹¹⁰⁾ Meddelandet om skydd av personuppgifter från *Lord Chief Justice of Northern Ireland*, finns på följande länk: <https://judiciaryni.uk/data-privacy>

⁽¹¹¹⁾ Meddelandet om skydd av personuppgifter för skotska domstolar och tribunaler finns på följande länk: <https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice>

⁽¹¹²⁾ Datatillsynsdomaren ger vägledning till rättsväsendet och utreder överträdelser och/eller klagomål som rör behandling av personuppgifter som utförs av domstolar eller enskilda personer som handlar i egenskap av en dömande myndighet.

⁽¹¹³⁾ Om klagomålet eller brottet bedöms vara allvarligt hänskjuts det till *Judicial Complaints Officer* för vidare utredning i enlighet med *Lord Chief Justice in Northern Ireland's Code of Practice on Complaints*. Ett sådant klagomål skulle kunna omfatta inga ytterligare åtgärder, råd, utbildning eller mentorskap, informell varning, formell varning, slutlig varning, begränsning av praxis eller hänskjutande till en lagstadgad domstol. *Code of Practice on Complaints* som utfärdats av *Lord Chief Justice* i Nordirland finns på följande länk: https://judiciaryni.uk/sites/judiciary/files/media-files/14G.%20CODE%20OF%20PRACTICE%20Judicial%20~%2028%20Feb%2013%20%28Final%29%20updated%20with%20new%20comp.._1.pdf.

⁽¹¹⁴⁾ Varje klagomål utreds av en datatillsynsdomare och hänskjuts till Lord President som har befogenhet att utfärda råd, en formell varning eller en reprimand om han anser det nödvändigt (likvärdiga regler finns för domstolsledamöter och de finns på följande länk: https://www.judiciary.scot/docs/librariesprovider3/judiciarydocuments/complaints/complaintsaboutthejudiciaryscotlandrules2017_1d392ab6e14f6425aa0c7f48d062f5cc5.pdf?sfvrsn=5d3eb9a1_2)

- (105) För det första har en registrerad rätt att lämna in ett klagomål till *the Information Commissioner* om den registrerade anser att det föreligger en överträdelse av den brittiska dataskyddsförordningen i samband med personuppgifter som rör honom eller henne ⁽¹¹⁵⁾. Den brittiska dataskyddsförordningen bibehåller bestämmelserna om denna rätt i artikel 77 i förordning (EU) 2016/679 utan några väsentliga ändringar. Detsamma gäller för artikel 57.1 f och 57.2 som fastställer *the Commissioner* uppgifter i samband med handläggningen av klagomål. Enligt beskrivningen i skälen 92–98 ovan har *the Information Commissioner* befogenhet att bedöma den personuppgiftsansvarigas och personuppgiftsbiträdets efterlevnad av den brittiska dataskyddsförordningen och 2018 års dataskyddslag och kräva att de vidtar eller avstår från att vidta nödvändiga åtgärder vid bristande efterlevnad och att utdöma sanktionsavgifter.
- (106) För det andra ger den brittiska dataskyddsförordningen och 2018 års dataskyddslag rätt till rättsmedel mot *the Information Commissioner*. Enligt artikel 78.1 i den brittiska dataskyddsförordningen har enskilda rätt till ett effektivt rättsmedel mot ett rättsligt bindande beslut rörande dem som meddelats av *the Commissioner*. Inom ramen för domstolsprövningen prövar domaren det beslut som ifrågasätts i ansökan och prövar huruvida *the Information Commissioner* har handlat lagenligt. Enligt artikel 78.2 i den brittiska dataskyddsförordningen har den klagande dessutom tillgång till rättsmedel om *the Commissioner* underlåter att behandla ett klagomål från den registrerade ⁽¹¹⁶⁾. Han eller hon kan vända sig till en *First Tier Tribunal* för att förelägga *the Information Commissioner* att vidta lämpliga åtgärder för att besvara klagomålet eller informera den klagande om hur ärendet fortskrider ⁽¹¹⁷⁾. Dessutom kan varje person som delgetts ett av de ovannämnda föreläggandena (information, bedömning, verkställighet eller påföljd) av *the Information Commissioner* överklaga till en *First Tier Tribunal* ⁽¹¹⁸⁾. Om tribunalen anser att det beslut som *the Commissioner* har fattat inte är förenligt med lagen eller att *the Information Commissioner* borde ha utövat sitt utrymme för skönmässig bedömning på ett annat sätt ska tribunalen bifalla överklagandet eller ersätta ett annat föreläggande eller beslut som *the Information Commissioner* skulle ha kunnat lämna eller fatta.
- (107) För det tredje kan enskilda personer få rättslig prövning av personuppgiftsansvariga och personuppgiftsbiträden direkt vid domstol i enlighet med artikel 79 i den brittiska dataskyddsförordningen och avsnitt 167 i 2018 års dataskyddslag. Om en domstol på begäran av en registrerad är övertygad om att det har skett en överträdelse av den registrerades rättigheter enligt dataskyddslagstiftningen får domstolen förelägga den personuppgiftsansvariga att vidta de åtgärder som anges i beslutet eller att avstå från att vidta de åtgärder som anges i beslutet.
- (108) Enligt artikel 82 i den brittiska dataskyddsförordningen och avsnitt 168 i 2018 års dataskyddslag har dessutom varje person som har lidit materiell eller immateriell skada till följd av en överträdelse av den brittiska dataskyddsförordningen rätt att få ersättning från den personuppgiftsansvariga eller personuppgiftsbiträdet för den skada som lidits. Reglerna om ersättning och ansvar i artikel 82.1–5 i den brittiska dataskyddsförordningen är identiska med motsvarande regler i förordning (EU) 2016/679. Enligt avsnitt 168 i 2018 års dataskyddslag omfattar ideell skada även lidande. Enligt artikel 80 i den brittiska dataskyddsförordningen har den registrerade också rätt att ge ett representativt organ eller en representativ organisation i uppdrag att lämna in klagomål till *the Commissioner* för hans eller hennes räkning (enligt artikel 77 i den brittiska dataskyddsförordningen) och att utöva de rättigheter som avses i artiklarna 78 (rätt till effektivt rättsmedel mot *the Commissioner*), 79 (rätt till ett effektivt rättsmedel mot en personuppgiftsansvarig eller ett personuppgiftsbiträde) och 82 (rätt till ersättning och ansvar) i den brittiska dataskyddsförordningen för hans eller hennes räkning.
- (109) För det fjärde, och utöver de möjligheter till rättslig prövning som beskrivs ovan, kan varje person som anser att hans eller hennes rättigheter, däribland rätten till integritet och dataskydd, har kränkts av myndigheter, få sin sak prövad i domstol i Förenade kungariket enligt *Human Rights Act 1998* ⁽¹¹⁹⁾. En enskild person som hävdar att en myndighet har agerat (eller avser att agera) på ett sätt som är oförenligt med en rättighet enligt konventionen och följaktligen är olaglig enligt avsnitt 6.1 i *Human Rights Act 1998* kan väcka talan mot myndigheten vid behörig domstol eller åberopa de berörda rättigheterna i ett rättsligt förfarande när han eller hon är (eller skulle vara) offer för den olagliga handlingen.
- (110) Om domstolen finner att en åtgärd som vidtas av en myndighet är rättsstridig kan den bevilja en sådan befrielse eller ett sådant rättsmedel eller fatta ett sådant beslut inom ramen för sina befogenheter som den anser vara skäligt och lämpligt ⁽¹²⁰⁾. Domstolen kan också förklara att en bestämmelse i primärrätten är oförenlig med en rättighet enligt konventionen.

⁽¹¹⁵⁾ Artikel 77 i den brittiska dataskyddsförordningen.

⁽¹¹⁶⁾ I avsnitt 166 i 2018 års dataskyddslag hänvisas särskilt till följande situationer: a) *The Commissioner* underlåter att vidta lämpliga åtgärder för att besvara klagomålet, b) han eller hon underlåter att informera den klagande om hur ärendet fortskrider eller om resultatet av klagomålet före utgången av den period på 3 månader som började vid mottagandet av klagomålet eller c) om hans eller hennes behandling av klagomålet inte avslutas under den perioden inte ger klaganden sådan information under en senare period på 3 månader.

⁽¹¹⁷⁾ Artikel 78.2 i den brittiska dataskyddsförordningen och avsnitt 166 i 2018 års dataskyddslag.

⁽¹¹⁸⁾ Artikel 78.1 i den brittiska dataskyddsförordningen och avsnitt 162 i 2018 års dataskyddslag.

⁽¹¹⁹⁾ Avsnitt 7.1 i *Human Rights Act 1998*. Enligt avsnitt 7.7 är en person endast offer för en rättsstridig handling om han eller hon är ett offer i den mening som avses i artikel 34 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna om talan väcktes vid Europeiska domstolen för de mänskliga rättigheterna avseende denna handling.

⁽¹²⁰⁾ Avsnitt 8.1 i *Human Rights Act 1998*.

- (111) Slutligen kan en enskild person, efter att ha uttömt nationella rättsmedel, vända sig till Europeiska domstolen för de mänskliga rättigheterna för kränkningar av de rättigheter som garanteras enligt Europakonventionen om de mänskliga rättigheterna.

3. TILLGÅNG TILL OCH ANVÄNDNING AV PERSONUPPGIFTER SOM ÖVERFÖRS FRÅN EUROPEISKA UNIONEN AV MYNDIGHETER I FÖRENADE KUNGARIKET

- (112) Kommissionen bedömde också Förenade kungarikets rättsliga ram för insamling och senare användning av personuppgifter som brittiska myndigheter överfört till näringsidkare i Förenade kungariket i allmänhetens intresse, särskilt för ändamål som rör brottsbekämpning och nationell säkerhet ("myndigheternas tillgång"). Vid bedömningen av om villkoren för myndigheternas tillgång till uppgifter som överförs till Förenade kungariket enligt detta beslut skulle uppfylla kriteriet om "väsentlig likvärdighet" i enlighet med artikel 45.1 i förordning (EU) 2016/679 som den tolkats av Europeiska unionens domstol mot bakgrund av stadgan om de grundläggande rättigheterna, tog kommissionen särskilt hänsyn till följande kriterier.
- (113) För det första ska varje begränsning av rätten till skydd av personuppgifter föreskrivas i lag och den rättsliga grund som möjliggör ett ingrepp i en sådan rättighet måste själv definiera omfattningen av begränsningen av utövandet av den berörda rättigheten ⁽¹²¹⁾.
- (114) För att uppfylla proportionalitetskravet, enligt vilket undantag från och begränsningar av skyddet av personuppgifter endast får tillämpas i den mån det är absolut nödvändigt i ett demokratiskt samhälle för att uppfylla särskilda mål av allmänintresse som motsvarar dem som erkänns av EU, ska det i lagstiftningen i det berörda tredjelandet, enligt vilken ingreppet är tillåtet, fastställas klara och precisa regler för omfattningen och tillämpningen av åtgärderna i fråga och införas minimigarantier så att de personer vars uppgifter har överförts har tillräckliga garantier för att effektivt skydda sina personuppgifter mot risken för missbruk ⁽¹²²⁾. Lagstiftningen måste särskilt ange under vilka omständigheter och på vilka villkor en åtgärd som föreskriver behandling av sådana uppgifter får antas ⁽¹²³⁾ samt ställa krav på oberoende tillsyn för uppfyllandet av dessa krav ⁽¹²⁴⁾.
- (115) För det tredje måste denna lagstiftning vara rättsligt bindande enligt nationell rätt och dessa rättsliga krav måste inte bara vara bindande för myndigheterna utan även kunna göras gällande inför domstol mot myndigheterna i det berörda tredjelandet ⁽¹²⁵⁾. I synnerhet måste de registrerade ha möjlighet att väcka talan vid en oberoende och opartisk domstol för att få tillgång till sina personuppgifter eller för att få dessa uppgifter rättade eller raderade ⁽¹²⁶⁾.

3.1 Lagstiftning

- (116) I egenskap av myndighetsutövning måste myndigheternas tillgång i Förenade kungariket ske med full respekt för lagen. Förenade kungariket har ratificerat den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (se skäl 9) och alla brittiska myndigheter är skyldiga att agera i enlighet med konventionen ⁽¹²⁷⁾. I artikel 8 i konventionen föreskrivs att varje ingrepp i privatlivet ska vara förenligt med lagen, med hänsyn till något av de syften som anges i artikel 8.2, och stå i proportion till detta syfte. I artikel 8 föreskrivs också att ingreppet ska vara "förutsebart", dvs. ha en tydlig och tillgänglig rättslig grund och att lagen ska innehålla lämpliga skyddsåtgärder för att förhindra missbruk.
- (117) Dessutom har Europeiska domstolen för de mänskliga rättigheterna i sin rättspraxis angett att varje ingrepp i rätten till integritet och dataskydd bör omfattas av ett effektivt, oberoende och opartiskt tillsynssystem som ska tillhandahållas antingen av en domare eller av ett annat oberoende organ ⁽¹²⁸⁾ (t.ex. en administrativ myndighet eller ett parlamentariskt organ).

⁽¹²¹⁾ Se Schrems II, punkterna 174–175 och där angiven rättspraxis. Se även, när det gäller tillgång för myndigheter i medlemsstaterna, mål C-623/17, Privacy International, ECLI:EU:C:2020:790, punkt 65 och mål C-511/18, C-512/18 och C-520/18, La Quadrature du Net m.fl., ECLI:EU:C:2020:791, punkt 175.

⁽¹²²⁾ Se Schrems II, punkterna 176 och 181, samt där angiven rättspraxis. Se även, när det gäller tillgång för medlemsstaternas myndigheter, Privacy International, punkt 68 och La Quadrature du Net m.fl., punkt 132.

⁽¹²³⁾ Se domen i det ovannämnda målet Schrems II, punkt 176. Se även, när det gäller tillgång för medlemsstaternas myndigheter, Privacy International, punkt 68 och La Quadrature du Net m.fl., punkt 132.

⁽¹²⁴⁾ Se domen i det ovannämnda målet Schrems II, punkt 179.

⁽¹²⁵⁾ Se Schrems II, punkterna 181–182.

⁽¹²⁶⁾ Se Schrems I, punkt 95, och Schrems II, punkt 194. I detta avseende har EU-domstolen särskilt betonat att efterlevnaden av artikel 47 i stadgan om de grundläggande rättigheterna, som garanterar rätten till ett effektivt rättsmedel inför en oavhängig och opartisk domstol, "bidrar till den skyddsnivå som krävs i Europeiska unionen [och] måste fastställas av kommissionen innan den fattar ett beslut om adekvat skyddsnivå i enlighet med artikel 45.1 i förordning (EU) 2016/679" (Schrems II, punkt 186).

⁽¹²⁷⁾ Avsnitt 6 i Human Rights Act 1998.

⁽¹²⁸⁾ Europeiska domstolen för de mänskliga rättigheterna, Klass m.fl./Tyskland, ansökan nr 5029/71, punkterna 17–51.

- (118) Dessutom måste enskilda ges tillgång till ett effektivt rättsmedel och Europeiska domstolen för de mänskliga rättigheterna har klargjort att rättsmedlet måste erbjudas av ett oberoende och opartiskt organ som har antagit sin egen arbetsordning bestående av medlemmar som måste inneha eller ha innehaft höga domarämbeten eller ha erfarenhet av jurister och att det inte får finnas någon bevisbörda som behöver övervinnas för att lämna in en ansökan till domstolen. När det oberoende och opartiska organet granskar klagomål från enskilda bör det ha tillgång till all relevant information, inklusive hemligt material. Slutligen bör det ha befogenhet att åtgärda bristande efterlevnad ⁽¹²⁹⁾.
- (119) Förenade kungariket ratificerade även Europarådets konvention om skydd för enskilda personer vid automatisk databehandling av personuppgifter (konvention 108) och undertecknade 2018 protokollet om ändring av konventionen om skydd för enskilda personer vid automatisk databehandling av personuppgifter (kallad konvention 108+) ⁽¹³⁰⁾. I artikel 9 i konvention 108 föreskrivs att undantag från de allmänna dataskyddsprinciperna (artikel 5 om uppgifternas kvalitet), bestämmelserna om särskilda kategorier av uppgifter (artikel 6 Särskilda kategorier av uppgifter) och den registrerades rättigheter (artikel 8 Ytterligare skyddsåtgärder för den registrerade) endast är tillåtna när ett sådant undantag föreskrivs i partens lagstiftning och utgör en nödvändig åtgärd i ett demokratiskt samhälle för att skydda statens säkerhet, den allmänna säkerheten, statens ekonomiska intressen eller bekämpande av brott eller för att skydda den registrerade eller andra personers fri- och rättigheter ⁽¹³¹⁾.
- (120) Genom medlemskap i Europarådet, anslutning till den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna och hänvändelse till Europeiska domstolen för de mänskliga rättigheterna omfattas Förenade kungariket därför av ett antal skyldigheter som är inskrivna i internationell rätt, som utgör ramen för landets system för statlig tillgång på grundval av principer, skyddsåtgärder och individuella rättigheter som liknar dem som garanteras enligt unionsrätten och som är tillämpliga på medlemsstaterna. Enligt skäl 19 är fortsatt anslutning till sådana instrument därför ett särskilt viktigt inslag i den bedömning som ligger till grund för detta beslut.
- (121) Dessutom garanteras särskilda dataskyddsgarantier och rättigheter av 2018 års dataskyddslag när uppgifter behandlas av myndigheter, inbegripet brottsbekämpande organ och nationella säkerhetsorgan.
- (122) I synnerhet fastställs ordningen för behandling av personuppgifter i samband med brottsbekämpning i del 3 i 2018 års dataskyddslag, som antogs för att införliva direktiv (EU) 2016/680. Del 3 i 2018 års dataskyddslag är tillämplig på behöriga myndigheters behandling av personuppgifter i syfte att förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inbegripet att skydda mot samt förebygga hot mot den allmänna säkerheten ⁽¹³²⁾.
- (123) Begreppet "behörig myndighet" definieras i avsnitt 30 i dataskyddslagen som en person som förtecknas i tillägg 7 till 2018 års dataskyddslag samt varje annan person i den mån personen har lagstadgade uppgifter för något av de brottsbekämpande ändamålen ⁽¹³³⁾. Såsom förklaras ovan (se skäl 139), kan vissa behöriga myndigheter (t.ex. den nationella brottsmyndigheten (*National Crime Agency*) på vissa villkor använda de befogenheter som anges i *Investigatory Power Act 2016* (2016 års lag om utredningsbefogenheter). I detta fall gäller skyddsåtgärderna enligt 2016 års lag om utredningsbefogenheter utöver de skyddsåtgärder som anges i del 3 i 2018 års dataskyddslag. Underrättelsetjänsterna (*Secret Intelligence Service, Security Service och Government Communications Headquarters*) är inte behöriga myndigheter ⁽¹³⁴⁾ enligt del 3 i 2018 års dataskyddslag, och bestämmelserna däri är därför inte tillämpliga på någon av deras verksamheter. En del av 2018 års dataskyddslag (del 4) ägnas särskilt åt underrättelsetjänsters behandling av personuppgifter (närmare information ges i skäl 125)
-
- ⁽¹²⁹⁾ Europeiska domstolen för de mänskliga rättigheterna, Kennedy/United Kingdom, ansökan nr 26839/05 (Kennedy), punkterna 167 och 190.
- ⁽¹³⁰⁾ För mer information om den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna och dess införlivande i Förenade kungarikets lagstiftning genom *Human Rights Act 1998* samt konvention 108, se skäl 9 ovan.
- ⁽¹³¹⁾ På samma sätt är, enligt artikel 11 i konvention 108+, begränsningar av vissa specifika rättigheter och skyldigheter i konventionen av hänsyn till nationell säkerhet eller förebyggande, utredning och lagföring av brott samt verkställighet av straffrättsliga påföljder endast tillåtna om en sådan begränsning föreskrivs i lag, respekterar det väsentliga innehållet i de grundläggande rättigheterna och friheterna och utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle. Behandling av uppgifter för ändamål som rör nationell säkerhet och försvar måste också vara föremål för oberoende och effektiv översyn och övervakning enligt respektive konventionsparts nationella lagstiftning.
- ⁽¹³²⁾ Avsnitt 31 i 2018 års dataskyddslag.
- ⁽¹³³⁾ De behöriga myndigheter som förtecknas i bilaga 7 omfattar inte bara polisen utan även alla brittiska ministerier och andra myndigheter med utredningsfunktioner (t.ex. *Commissioner for Her Majesty's Revenue and Customs, National Crime Agency, Welsh Revenue Authority, Competition and Markets Authority* eller *Her Majesty's Land Register*), åklagarmyndigheter, andra straffrättsliga myndigheter och andra innehavare eller organisationer som bedriver brottsbekämpande verksamhet (i tillägg 7 till 2018 års dataskyddslag förtecknas bland andra *Directors of Public Prosecutors, Director of Public Prosecutors for Northern Ireland* och *Information Commission*).
- ⁽¹³⁴⁾ Avsnitt 30.2 i 2018 års dataskyddslag.

- (124) I likhet med direktiv (EU) 2016/680 fastställs i del 3 i 2018 års dataskyddslag principerna om laglighet och rättvisa ⁽¹³⁵⁾, ändamålsbegränsning ⁽¹³⁶⁾, uppgiftsminimering ⁽¹³⁷⁾, noggrannhet ⁽¹³⁸⁾, lagringsbegränsning ⁽¹³⁹⁾ och säkerhet ⁽¹⁴⁰⁾. Lagstiftningen föreskriver särskilda transparenskrav ⁽¹⁴¹⁾ och ger enskilda personer rätt till tillgång ⁽¹⁴²⁾, rättelse och radering ⁽¹⁴³⁾ samt rätt att inte bli föremål för automatiserat beslutsfattande ⁽¹⁴⁴⁾. De behöriga myndigheterna är också skyldiga att införa inbyggt dataskydd som standard, att föra register över behandling och, för vissa typer av behandling, att genomföra konsekvensbedömningar avseende dataskydd och att i förväg samråda med *the Information Commissioner* ⁽¹⁴⁵⁾. Enligt avsnitt 56 i 2018 års dataskyddslag är de skyldiga att visa att de uppfyller kraven. De är dessutom skyldiga att vidta lämpliga åtgärder för att säkerställa behandlingens säkerhet ⁽¹⁴⁶⁾ och omfattas av särskilda skyldigheter vid ett personuppgiftsbrott, inbegripet anmälan av sådana överträdelse till *the Information Commissioner* och de registrerade ⁽¹⁴⁷⁾. Liksom i direktiv (EU) 2016/680 finns det också ett krav på att en personuppgiftsansvarig (såvida det inte är en domstol eller annan rättslig myndighet som agerar inom ramen för sin rättsliga verksamhet) utser ett dataskyddsombud ⁽¹⁴⁸⁾ som hjälper den personuppgiftsansvariga att fullgöra sina skyldigheter och övervaka efterlevnaden ⁽¹⁴⁹⁾. Dessutom innehåller lagstiftningen särskilda krav för internationella överföringar av personuppgifter för brottsbekämpande ändamål till tredjeländer eller internationella organisationer för att säkerställa kontinuitet i skyddet ⁽¹⁵⁰⁾. Samma dag som detta beslut [antog] kommissionen ett beslut om adekvat skyddsnivå 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 säkerställer en skyddsnivå som i allt väsentligt är likvärdig med den som garanteras enligt direktiv (EU) 2016/680.
- (125) Del 4 i 2018 års dataskyddslag gäller all behandling som utförs av underrättelsetjänsterna eller för deras räkning. Framför allt fastställs de viktigaste dataskyddsprinciperna (laglighet, rättvisa och öppenhet ⁽¹⁵¹⁾), ändamålsbegränsning ⁽¹⁵²⁾, uppgiftsminimering ⁽¹⁵³⁾, precision ⁽¹⁵⁴⁾, lagringsbegränsningar ⁽¹⁵⁵⁾ och säkerhet ⁽¹⁵⁶⁾, villkor för behandling av särskilda kategorier av uppgifter ⁽¹⁵⁷⁾, bestämmelser om registrerades rättigheters ⁽¹⁵⁸⁾, krav på

⁽¹³⁵⁾ Avsnitt 35 i 2018 års dataskyddslag.

⁽¹³⁶⁾ Avsnitt 36 i 2018 års dataskyddslag.

⁽¹³⁷⁾ Avsnitt 37 i 2018 års dataskyddslag.

⁽¹³⁸⁾ Avsnitt 38 i 2018 års dataskyddslag.

⁽¹³⁹⁾ Avsnitt 39 i 2018 års dataskyddslag.

⁽¹⁴⁰⁾ Avsnitt 40 i 2018 års dataskyddslag.

⁽¹⁴¹⁾ Avsnitt 44 i 2018 års dataskyddslag.

⁽¹⁴²⁾ Avsnitt 45 i 2018 års dataskyddslag.

⁽¹⁴³⁾ Avsnitten 46 och 47 i 2018 års dataskyddslag.

⁽¹⁴⁴⁾ Avsnitten 49 och 50 i 2018 års dataskyddslag.

⁽¹⁴⁵⁾ Avsnitten 56–65 i 2018 års dataskyddslag.

⁽¹⁴⁶⁾ Avsnitt 66 i 2018 års dataskyddslag.

⁽¹⁴⁷⁾ Avsnitten 67–68 i 2018 års dataskyddslag.

⁽¹⁴⁸⁾ Avsnitten 69–71 i 2018 års dataskyddslag.

⁽¹⁴⁹⁾ Avsnitten 67–68 i 2018 års dataskyddslag.

⁽¹⁵⁰⁾ Del 3 kapitel 5 i 2018 års dataskyddslag.

⁽¹⁵¹⁾ Enligt avsnitt 86.6 i 2018 års dataskyddslag ska den metod med vilken den erhålls beaktas för att avgöra om behandlingen sker på ett rättvist och öppet sätt. I detta avseende uppfylls kravet på rättvisa och öppenhet om uppgifterna erhålls från en person som lagligen har tillstånd eller är skyldig att tillhandahålla dem.

⁽¹⁵²⁾ Enligt avsnitt 87 i 2018 års dataskyddslag ska ändamålen med behandlingen vara specifika, uttryckligt angivna och legitima. Uppgifterna får inte behandlas på ett sätt som är oförenligt med de ändamål för vilka de samlades in. Enligt avsnitt 87.3 i 2018 års dataskyddslag kan ytterligare kompatibel behandling av personuppgifter endast tillåtas om den personuppgiftsansvariga enligt lag har rätt att behandla uppgifterna för det ändamålet och behandlingen är nödvändig och står i proportion till det andra ändamålet. Behandlingen bör anses vara förenlig om behandlingen består av behandling för arkivändamål av allmänt intresse, för vetenskapliga eller historiska forskningsändamål eller för statistiska ändamål och är föremål för lämpliga skyddsåtgärder (avsnitt 87.4 i 2018 års dataskyddslag).

⁽¹⁵³⁾ Personuppgifter måste vara adekvata, relevanta och inte överdrivet omfattande (avsnitt 88 i 2018 års dataskyddslag).

⁽¹⁵⁴⁾ Personuppgifter måste vara korrekta och aktuella (avsnitt 89 i 2018 års dataskyddslag).

⁽¹⁵⁵⁾ Personuppgifter får inte lagras längre än nödvändigt (avsnitt 90 i 2018 års dataskyddslag).

⁽¹⁵⁶⁾ Den sjätte principen om dataskydd är att personuppgifter ska behandlas på ett sätt som inbegriper vidtagande av lämpliga säkerhetsåtgärder när det gäller risker i samband med behandling av personuppgifter. Riskerna omfattar (men är inte begränsade till) oavsiktlig eller obehörig åtkomst till eller förstörelse, förlust, användning, ändring eller utlämnande av personuppgifter (avsnitt 91 i 2018 års dataskyddslag). I avsnitt 107 föreskrivs också att 1) varje personuppgiftsansvarig ska vidta lämpliga säkerhetsåtgärder som är lämpliga med hänsyn till de risker som uppstår i samband med behandlingen av personuppgifter och 2) vid automatiserad behandling ska varje personuppgiftsansvarig och personuppgiftsbiträde vidta förebyggande eller begränsande åtgärder på grundval av en riskbedömning.

⁽¹⁵⁷⁾ Avsnitt 86.2 b i och tillägg 10 till 2018 års dataskyddslag.

⁽¹⁵⁸⁾ Del 4 kapitel 3 i 2018 års dataskyddslag, särskilt när det gäller rättigheterna om tillgång, rättelse och radering, invända mot behandlingen och inte vara föremål för automatiserat beslutsfattande, att ingripa i automatiserat beslutsfattande och informeras om beslutsfattandet. Dessutom måste den personuppgiftsansvariga informera den registrerade om behandlingen av hans eller hennes personuppgifter. Såsom förklaras i ICO:s vägledning om underrättelsetjänsters behandling av personuppgifter kan enskilda personer utöva alla sina rättigheter (även begära rättelse) genom att inge ett klagomål till ICO eller väcka talan (se ICO:s vägledning till underrättelsetjänster som behandlar personuppgifter, som finns på följande länk: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-intelligence-services-processing/>).

inbyggt dataskydd⁽¹⁵⁹⁾ och internationella överföringar av personuppgifter⁽¹⁶⁰⁾. ICO har nyligen utfärdat detaljerad vägledning om underrättelsetjänsters behandling av personuppgifter enligt del 4 i 2018 års dataskyddslag⁽¹⁶¹⁾.

- (126) Samtidigt föreskrivs i avsnitt 110 i 2018 års dataskyddslag ett undantag från de specificerade bestämmelserna i del 4 i denna lag⁽¹⁶²⁾ när ett sådant undantag krävs för att skydda den nationella säkerheten. Detta undantag kan grundas på en analys från fall till fall⁽¹⁶³⁾. Enligt de brittiska myndigheternas förklaring och enligt bekräftelse i rättspraxis måste personuppgiftsansvariga beakta de faktiska konsekvenserna för den nationella säkerheten eller försvaret om de var tvungna att följa den särskilda dataskyddsbestämmelsen och om de rimligen kunde följa den vanliga regeln utan att det påverkar den nationella säkerheten eller det nationella försvaret⁽¹⁶⁴⁾. Huruvida undantaget har använts på lämpligt sätt omfattas av ICO:s tillsyn⁽¹⁶⁵⁾.
- (127) När det gäller möjligheten att för skyddet av "nationell säkerhet" begränsa tillämpningen av de ovannämnda bestämmelserna i avsnitt 111 i 2018 års dataskyddslag kan dessutom en personuppgiftsansvarig ansöka om ett intyg som undertecknats av en minister eller *Attorney General* som intygar att en begränsning av sådana rättigheter är en nödvändig och proportionerlig åtgärd för att skydda den nationella säkerheten⁽¹⁶⁶⁾.
- (128) Den brittiska regeringen har utfärdat riktlinjer för att bistå personuppgiftsansvariga när de överväger huruvida de ska ansöka om ett nationellt säkerhetsintyg enligt 2018 års dataskyddslag där det särskilt betonas att varje begränsning av registrerades rättigheter för att skydda den nationella säkerheten måste vara proportionerlig och nödvändig⁽¹⁶⁷⁾. Alla nationella säkerhetsintyg måste publiceras på ICO:s webbplats⁽¹⁶⁸⁾.

⁽¹⁵⁹⁾ Avsnitt 103 i 2018 års dataskyddslag.

⁽¹⁶⁰⁾ Avsnitt 109 i 2018 års dataskyddslag. Överföring av personuppgifter till internationella organisationer eller länder utanför Förenade kungariket är möjlig om överföringen är en nödvändig och proportionell åtgärd som utförs inom ramen för den personuppgiftsansvarigas lagstadgade uppgifter eller för andra ändamål som anges i särskilda avsnitt i *Security Service Act 1989* och *Intelligence Services Act 1994*.

⁽¹⁶¹⁾ ICO:s vägledning, se fotnot 158.

Avsnitt 30 i 2018 års dataskyddslag och tillägg 7 till denna lag.

⁽¹⁶²⁾ I avsnitt 110.2 i 2018 års dataskyddslag förtecknas de bestämmelser från vilka undantag är tillåtna. Detta omfattar dataskyddsprinciperna (med undantag för legalitetsprincipen), den registrerades rättigheter, skyldigheten att informera *the Information Commissioner* om ett personuppgiftsbrott, dennes inspektionsbefogenheter i enlighet med internationella skyldigheter, vissa av dennes verkställighetsbefogenheter, bestämmelser som gör vissa dataskydsbrott till lagbrott och bestämmelser om särskilda ändamål för behandling, till exempel journalistiska, akademiska eller konstnärliga ändamål.

⁽¹⁶³⁾ Se Baker/Secretary of State, se fotnot 61.

⁽¹⁶⁴⁾ *UK Explanatory Framework for Adequacy Discussions*, avsnitt H: *National Security Data Protection and Investigatory Powers Framework*, s. 15–16 (se fotnot 31). Se även Baker/Secretary of State (se fotnot 61) där domstolen upphävde ett nationellt säkerhetsintyg som utfärdats av inrikesministern och bekräftade tillämpningen av undantaget för nationell säkerhet eftersom den ansåg att det inte fanns någon anledning att föreskriva ett generellt undantag från skyldigheten att besvara begäranden om tillgång och att ett sådant undantag under alla omständigheter utan en bedömning i varje enskilt fall överskred vad som var nödvändigt och proportionerligt för skyddet av den nationella säkerheten.

⁽¹⁶⁵⁾ Se samförståndsavtalet mellan ICO och UKIC enligt vilket "ICO kommer att vilja försäkra sig om att frågan har hanterats korrekt och, i förekommande fall, att tillämpningen av eventuella undantag har använts på lämpligt sätt". *Memorandum of Understanding between Information Commissioner's Office and the UK Intelligence Community*, punkt 16, finns på följande länk: <https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf>

⁽¹⁶⁶⁾ Möjligheten att utfärda intyg enligt avsnitt 28.2 i 1998 års dataskyddslag har upphävts genom 2018 års dataskyddslag. Det är dock fortfarande möjligt att utfärda "gamla intyg" i den mån det föreligger tidigare domstolsprövningar enligt lagen från 1998 (se punkt 17 del 5 tillägg 20 till 2018 års dataskyddslag). Denna möjlighet verkar dock utnyttjas mycket sällan och kommer endast att gälla i begränsade fall, till exempel om en registrerad väcker talan mot tillämpningen av ett undantag avseende nationell säkerhet i samband med en myndighets behandling av personuppgifter som skedde enligt lagen från 1998. Det ska noteras att i dessa fall kommer avsnitt 28 i dataskyddslagen från 1998 att gälla i sin helhet, vilket innebär att registrerade har möjlighet att väcka talan angående vid domstol angående sådana intyg.

⁽¹⁶⁷⁾ Den brittiska regeringens vägledning om nationella säkerhetscertifikat (*UK Government Guidance on National Security Certificates*) enligt 2018 års dataskyddslag, finns på följande länk: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf. Enligt de brittiska myndigheternas förklaring är ett intyg ett avgörande bevis för att undantaget är tillämpligt när det gäller uppgifter eller behandling som beskrivs i certifikatet men det tar inte bort kravet på att den personuppgiftsansvariga ska överväga om det finns ett behov av att förlita sig på undantaget från fall till fall.

⁽¹⁶⁸⁾ Enligt avsnitt 130 i 2018 års dataskyddslag kan *the Information Commissioner* besluta att inte offentliggöra texten eller delar av texten i ett intyg om detta skulle strida mot nationella säkerhetsintressen eller mot allmänintresset eller skulle kunna äventyra någon persons säkerhet. I sådana fall kommer ICO emellertid att offentliggöra omständigheten att intyget har utfärdats.

- (129) Intyget bör gälla för en bestämd period på högst fem år så att det regelbundet ses över av den verkställande makten ⁽¹⁶⁹⁾. I ett certifikat ska det anges vilka personuppgifter eller kategorier av personuppgifter som omfattas av undantaget samt vilka bestämmelser i 2018 års dataskyddslag som undantaget gäller ⁽¹⁷⁰⁾.
- (130) Det är viktigt att notera att nationella säkerhetsintyg inte utgör en ytterligare grund för att begränsa dataskydds rättigheter av skäl som rör den nationella säkerheten. Den personuppgiftsansvariga eller personuppgiftsbiträdet kan med andra ord endast förlita sig på ett intyget när han eller hon har konstaterat att det är nödvändigt att förlita sig på undantaget för nationell säkerhet vilket, enligt förklaringen ovan, måste tillämpas från fall till fall ⁽¹⁷¹⁾. Även om ett nationellt säkerhetsintyg är tillämpligt på ärendet i fråga kan ICO undersöka om det var motiverat att åberopa undantaget för nationell säkerhet i ett visst fall ⁽¹⁷²⁾.
- (131) Varje person som direkt berörs av utfärdandet av certifikatet kan överklaga detta till *Upper Tribunal* ⁽¹⁷³⁾ eller ⁽¹⁷⁴⁾ bestrida tillämpningen av certifikatet när det gäller specifika uppgifter om certifikatet identifierar uppgifter med hjälp av en allmän beskrivning, ⁽¹⁷⁵⁾. Skiljedomstolen kommer att ompröva beslutet att utfärda ett certifikat och besluta om det fanns rimliga skäl att utfärda intyget ⁽¹⁷⁶⁾. Den kan behandla ett stort antal frågor, bland annat nödvändighet, proportionalitet och laglighet, med beaktande av konsekvenserna för de registrerades rättigheter och avvägningen av behovet av att skydda den nationella säkerheten. Till följd av detta kan domstolen fastställa att intyget inte är tillämpligt på specifika personuppgifter som är föremål för överklagandet ⁽¹⁷⁷⁾.
- (132) En annan uppsättning möjliga begränsningar gäller dem som enligt tillägg 11 till 2018 års dataskyddslag är tillämpliga på vissa bestämmelser i del 4 i denna lag ⁽¹⁷⁸⁾ för att skydda andra viktiga mål av allmänt intresse eller skyddade intressen, till exempel parlamentariska privilegier, rätten till förtrolig kommunikation mellan advokat och klient, genomförandet av rättsliga förfaranden eller de väpnade styrkornas stridsförmåga ⁽¹⁷⁹⁾. Tillämpningen av dessa bestämmelser är antingen undantagen för vissa kategorier av information ("typbaserad") eller undantagen i den mån tillämpningen av dessa bestämmelser sannolikt skulle skada det skyddade intresset ("skadebaserad") ⁽¹⁸⁰⁾. Skadebaserade undantag kan endast åberopas i den mån tillämpningen av den angivna dataskyddsbestämmelsen

⁽¹⁶⁹⁾ Den brittiska regeringens vägledning om nationella säkerhetscertifikat, punkt 15, se fotnot 167.

⁽¹⁷⁰⁾ Den brittiska regeringens vägledning om nationella säkerhetscertifikat, punkt 5, se fotnot 167.

⁽¹⁷¹⁾ Se fotnot 164.

⁽¹⁷²⁾ Enligt avsnitt 102 i 2018 års dataskyddslag ska den personuppgiftsansvariga kunna visa att han eller hon har följt denna lag. Detta innebär att en underrättelsetjänst skulle behöva visa för ICO att den har beaktat de särskilda omständigheterna i fallet när den förlitar sig på undantaget. ICO publicerar också en förteckning över de nationella säkerhetscertifikaten, som finns på följande länk: <https://ico.org.uk/about-the-ico/our-information/national-security-certificates/>.

⁽¹⁷³⁾ *Upper Tribunal* är den domstol som är behörig att pröva överklaganden av beslut som fattats av lägre förvaltningsdomstolar och har särskild behörighet att överklaga beslut från vissa statliga organ.

⁽¹⁷⁴⁾ Avsnitt 111.3 i 2018 års dataskyddslag.

⁽¹⁷⁵⁾ Avsnitt 111.5 i 2018 års dataskyddslag.

⁽¹⁷⁶⁾ I målet *Baker/Secretary of State* (se fotnot 61) upphävde *Information Tribunal* ett nationellt säkerhetscertifikat som utfärdats av inrikesministern eftersom den ansåg att det inte fanns någon anledning att föreskriva ett generellt undantag från skyldigheten att besvara begäranden om tillgång och att ett sådant undantag under alla omständigheter utan en analys från fall till fall överskred vad som var nödvändigt och proportionerligt för att skydda den nationella säkerheten.

⁽¹⁷⁷⁾ Den brittiska regeringens vägledning om nationella säkerhetscertifikat, punkt 25, se fotnot 167.

⁽¹⁷⁸⁾ Detta innefattar i) del 4 av dataskyddsprinciperna, med undantag för kravet på att behandlingen ska vara laglig enligt den första principen och det faktum att behandlingen måste uppfylla ett av de relevanta villkor som anges i tilläggen 9 och 10, ii) de registrerades rättigheter, och iii) skyldigheterna att rapportera överträdelser till ICO.

⁽¹⁷⁹⁾ I del 4 i 2018 års dataskyddslag fastställs den rättsliga ram som gäller för alla typer av behandling av personuppgifter som utförs av underrättelsetjänster (inte bara i samband med deras fullgörande av uppgifter som rör den nationella säkerheten). Del 4 gäller därför när underrättelsetjänster exempelvis behandlar personuppgifter i samband med personaladministration, tvister eller offentlig upphandling. De begränsningar som anges i tillägg 11 är främst avsedda att tillämpas i dessa andra sammanhang. I händelse av tvister med anställda kan till exempel begränsningen avseende "rättsliga förfaranden" åberopas, medan det i samband med offentlig upphandling är möjligt att åberopa begränsningen avseende "förhandlingsskal" osv. Detta avspeglas i ICO:s vägledning om underrättelsetjänsters behandling av personuppgifter, där förhandlingar om uppgörelse mellan en underrättelsetjänst och en tidigare anställd om lönefordringar nämns som ett exempel på tillämpningen av begränsningar enligt tillägg 11 (se fotnot 161). Det bör också noteras att samma begränsningar finns tillgängliga för andra myndigheter enligt tillägg 2 till del 2 i 2018 års dataskyddslag.

⁽¹⁸⁰⁾ Enligt Förenade kungarikets förklarande ram är de undantag som är "typbaserade" följande: i) Information om tilldelning av statliga hedersbetygelser och värdigheter. ii) Yrkesmässiga privilegier. iii) Konfidentiella uppgifter om anställning, yrkesutbildning eller utbildning. iv) Skriftliga prov och betyg. De "skadebaserade" undantagen rör frågorna i) förebyggande eller avslöjande av brott, gripande och lagföring av gärningsmän, ii) parlamentariskt privilegium, iii) rättsliga förfaranden, iv) kronans väpnade styrkors stridsförmåga, v) Förenade kungarikets ekonomiska välbefinnande, vi) förhandlingar med den registrerade, vii) vetenskaplig eller historisk forskning eller statistiska ändamål och viii) arkivering i allmänhetens intresse. *UK Explanatory Framework for Adequacy Discussions*, avsnitt H: *National Security*, s. 13, se fotnot 31.

sannolikt skulle skada det specifika intresset i fråga. Användning av ett undantag måste därför alltid motiveras med hänvisning till den relevanta skada som sannolikt skulle uppstå i det enskilda fallet. Typbaserade undantag kan endast återopas med avseende på den specifika, snävt definierade informationskategori för vilken undantaget beviljas. Dessa liknar varandra i syfte och verkan med flera av undantagen i den brittiska dataskyddsförordningen (enligt förteckning 2 (Schedule 2) i 2018 års dataskyddslag) som i sin tur återspeglar undantagen i artikel 23 i dataskyddsförordningen.

- (133) Av ovanstående följer att begränsningar och villkor finns i tillämplig brittisk lagstiftning, som den också tolkas av domstolarna och *the Information Commission*, för att säkerställa att dessa undantag och begränsningar håller sig inom gränserna för vad som är nödvändigt och proportionerligt för att skydda den nationella säkerheten.

3.2 Tillgång till och användning av brittiska myndigheter i brottsbekämpningssyfte

- (134) Förenade kungarikets lagstiftning föreskriver ett antal begränsningar av tillgången till och användningen av personuppgifter i brottsbekämpningssyfte och tillhandahåller tillsyns- och prövningsmekanismer på detta område som är i linje med de krav som avses i skälen 113–115 i detta beslut. Villkoren för sådan tillgång och de garantier som gäller för utövandet av dessa befogenheter bedöms i detalj i följande avsnitt.

3.2.1 Rättslig grund och tillämpliga begränsningar och skyddsåtgärder

- (135) Enligt den legalitetsprincip som garanteras i avsnitt 35 i 2018 års dataskyddslag är behandling av personuppgifter för något av de brottsbekämpande ändamålen laglig endast om den registrerade har lämnat sitt samtycke till behandlingen för detta ändamål ⁽¹⁸¹⁾ eller om behandlingen är nödvändig för att utföra en arbetsuppgift som utförs för detta ändamål av en behörig myndighet.

3.2.1.1 Beslut om husrannsakan och utlämnandeorder

- (136) I Förenade kungarikets rättsliga ram är insamling av personuppgifter från näringsidkare, däribland sådana som skulle behandla uppgifter som överförts från EU enligt detta beslut om adekvat skyddsnivå, tillåten i brottsbekämpningssyfte på grundval av beslut om husrannsakan ⁽¹⁸²⁾ och utlämnandeorder ⁽¹⁸³⁾.
- (137) Beslut om husrannsakan utfärdas av en domstol, vanligtvis på begäran av utredaren. De gör det möjligt för tjänstemän att få tillträde till lokaler för att söka efter material eller personer som är relevanta för deras utredning och behålla allt för vilket en husrannsakan har bemyndigats, däribland alla relevanta handlingar eller material som innehåller personuppgifter ⁽¹⁸⁴⁾. En utlämnandeorder, som också måste utfärdas av en domstol, kräver att den person som anges i beslutet framställer eller ger tillgång till material som de innehar eller kontrollerar. Sökanden måste motivera för domstolen varför beslutet eller ordern är nödvändigt samt varför det ligger i allmänhetens intresse. Det finns flera lagstadgade befogenheter som gör det möjligt att

⁽¹⁸¹⁾ Användningen av samtycke förefaller inte relevant i ett tillräcklighetsscenario eftersom uppgifterna i en överföringssituation inte kommer att ha samlats in direkt från en registrerad i EU av en brittisk brottsbekämpande myndighet på grundval av samtycke.

⁽¹⁸²⁾ För relevant rättslig grund, se avsnitt 8 och följande artiklar i *PACE 1984* (för England och Wales), avsnitt 10 och följande artiklar i *Police and Criminal Evidence Order (Northern Ireland) 1989* och för Skottland enligt common law (se avsnitt 46 i *Criminal Justice (Scotland) Act 2016*) och avsnitt 23B i *Criminal Law (Consolidation) (Scotland)*. För ett beslut om husrannsakan som utfärdats efter gripandet är den rättsliga grunden avsnitt 18 i *PACE 1984* (för England och Wales), avsnitt 20 ff. i *Police and Criminal Evidence Order (Northern Ireland) 1989* och för Skottland erhålls den enligt common law (se avsnitt 46 i *Criminal Justice (Scotland) Act 2016*). De brittiska myndigheterna klargjorde att beslut om husrannsakan utfärdas av en domstol på begäran av utredaren. Den gör det möjligt för en tjänsteman att få tillträde till lokaler för att söka efter material eller personer som är relevanta för deras utredning. Verkställandet av beslut om husrannsakan kommer ofta att kräva hjälp av en polisstyrka.

⁽¹⁸³⁾ När utredningen gäller penningtvätt (inklusive konfiskering och civilrättsligt återvinningsförfarande) är den relevanta rättsliga grunden för att ansöka om en utlämnandeorder avsnitt 345 ff. för England, Wales och Nordirland och avsnitt 380 ff. i *Proceeds of Crime Act 2002* för Skottland. När utredningen gäller andra frågor än penningtvätt kan en ansökan om utlämnandeorder lämnas in enligt avsnitt 9 och bilaga 1 till *PACE 1984* för England och Wales och avsnitt 10 ff. i *Police and Criminal Evidence Order (Northern Ireland) 1989* för Nordirland. För Skottland erhålls den enligt common law (se avsnitt 46 i *Criminal Justice (Scotland) Act 2016*) och avsnitt 23B i *Criminal Law* (förening av mål) (Skottland). De brittiska myndigheterna klargjorde att en utlämnandeorder kräver att den person som anges i den framställer eller ger tillgång till det material som de innehar eller kontrollerar (se punkt 4 i tillägg 1 till *PACE 1984*).

⁽¹⁸⁴⁾ *PACE 1984* innehåller till exempel befogenheter i avsnitten 8 och 18 att beslagta och behålla allt som har godkänts för husrannsakan.

utfärda ett beslut om husrannsakan och en utlämnandeorder. Varje bestämmelse har en egen uppsättning lagstadgade villkor som måste vara uppfyllda för att ett beslut om husrannsakan⁽¹⁸⁵⁾ eller en utlämnandeorder⁽¹⁸⁶⁾ ska kunna utfärdas.

- (138) Utlämnandeorder och beslut om husrannsakan kan överklagas genom rättslig prövning⁽¹⁸⁷⁾. När det gäller skyddsåtgärder bör alla brottsbekämpande myndigheter som omfattas av del 3 i 2018 års dataskyddslag endast få tillgång till personuppgifter – vilket är en form av behandling – i enlighet med de principer och krav som fastställs i den lagen (se skälen 122 och 124 ovan). Därför bör en

⁽¹⁸⁵⁾ Till exempel reglerar avsnitt 8 och avsnitt 18 i PACE befogenheten för fredsdomare att ge tillstånd till en husrannsakan respektive en polistjänsteman att göra husrannsakan. I det första fallet (avsnitt 8) ska fredsdomaren innan ett beslut utfärdas först försäkra sig om att det finns rimliga skäl att anta att i) ett åtalbart brott har begåtts, ii) det finns material i lokalerna som kan vara av betydande värde (antingen i sig självt eller tillsammans med annat material) för utredningen av brottet, iii) materialet sannolikt kommer att utgöra relevant bevisning, iv) det inte består av eller innehåller föremål som omfattas av rättsliga privilegier, uteslutna material eller material för särskilda förfaranden och v) det inte skulle vara möjligt att få tillträde utan ett beslut. I det andra fallet får en polistjänsteman enligt avsnitt 18 göra husrannsakan hos en person som gripits för ett åtalbart brott för annat material än sådant som omfattas av rättsliga privilegier, om han eller hon har skälig anledning att misstänka att det finns bevis i lokalerna som hänför sig till brottet eller något annat liknande eller därmed sammanhängande brott. En sådan husrannsakan måste begränsas till att avslöja detta material och måste skriftligen godkännas av en polistjänsteman med lägst kommissaries rang, såvida det inte är nödvändigt för att utreda brottet. I så fall ska en tjänsteman med lägst kommissaries rang informeras så snart som möjligt efter det att den har utförts. Skälen för husrannsakan och arten av den bevisning som begärs ska registreras. I avsnitt 15 och 16 i PACE 1984 föreskrivs dessutom lagstadgade garantier som måste följas vid ansökan om beslut om husrannsakan. I avsnitt 15 anges vilka krav som gäller för att erhålla ett beslut om husrannsakan (bl.a. innehållet i den ansökan som lämnats in av den berörda personen och det faktum att beslutet bland annat ska ange enligt vilken lag beslutet utfärdas och, så långt det är möjligt, identifiera de föremål och personer som ska eftersökas och de lokaler som ska genomsökas). I avsnitt 16 regleras hur husrannsakan ska utföras efter beslut har utfärdats (i avsnitt 16.5 föreskrivs exempelvis att den tjänsteman som verkställer husrannsakan förser innehavaren med en kopia av beslutet, enligt avsnitt 16.11 ska beslutet om husrannsakan, när det har verkställts, bevaras i 12 månader, enligt avsnitt 16.12 har besittningsinnehavaren rätt att ta del av beslutet om husrannsakan under denna period om han eller hon så önskar). Dessa avsnitt bidrar till att säkerställa efterlevnaden av artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (se t.ex. *Kent Pharmaceuticals/ Director of the Serious Fraud Office* [2002] EWHC 3023 (QB) i [30] av Lord Woolf CJ). Om dessa skyddsåtgärder inte följs kan husrannsakan förklaras olaglig (exempel är *R (Brook)/Preston Crown Court* [2018] EWHC 2024 (Admin), [2018] ACD 95, *R (Superior Import/Export Ltd)/Revenue and Customs Commissioners* [2017] EWHC 3172 (Admin), [2018] Lloyd's Rep FC 115 och *R (F)/Blackfriars Crown Court* [2014] EWHC 1541 (Admin)). Avsnitten 15 och 16 i PACE 1984 kompletteras av kod B i Europarådets parlamentariska församling, en uppförandekod som reglerar utövandet av polisens befogenheter att genomföra husrannsakan.

⁽¹⁸⁶⁾ Vid utfärdande av en utlämnandeorder enligt *Proceeds of Crime Act 2002*, utöver kravet på att ha rimliga skäl att uppfylla de villkor som anges i 346.2 i *Proceeds of Crime Act 2002*, bör det finnas rimliga skäl att personen innehar eller kontrollerar det material som anges på detta sätt och att materialet sannolikt kommer att vara av betydande värde. Ett annat krav för att en utlämnandeorder ska utfärdas är att det måste finnas rimliga skäl att anta att det ligger i allmänhetens intresse att materialet presenteras eller att allmänheten ges tillgång till det med hänsyn till a) den nytta som undersökningen sannolikt kommer att få om materialet anskaffats och b) de omständigheter under vilka den person som ansökan avser anser sig inneha eller ha kontroll över det material som innehåller deras uppgifter. På samma sätt måste en domstol som prövar en ansökan om utlämnandeorder enligt tillägg 1 till PACE 1984 vara övertygad om att vissa villkor är uppfyllda. I synnerhet i tillägg 1 i PACE anges två olika alternativa uppsättningar villkor, varav ett måste vara uppfyllt för att en domare ska kunna utfärda en utlämnandeorder. Den första uppsättningen kräver att domaren har rimliga skäl att anta i) att ett åtalbart brott har begåtts, ii) att det material som efterfrågas i lokalerna består av eller omfattar särskilt förfarande men inte undantaget material och iii) att det sannolikt kommer att ha ett betydande värde för undersökningen antingen som sådant eller tillsammans med annat material iv) och att det sannolikt kommer att vara relevant bevisning, v) andra metoder för att anskaffa materialet antingen har varit föremål för försök eller inte har varit föremål för försök på grund av att de inte skulle kunna undgå att misslyckas och vi) efter att ha övervägt nyttan med undersökningen och de omständigheter under vilka den enskilda personen innehar materialet ligger det i allmänhetens intresse att materialet visas upp eller att tillgång ges till det. För den andra uppsättningen villkor krävs att i) det finns material i lokalerna som består av ett särskilt förfarande eller uteslutet material, ii) om det inte hade varit fråga om ett förbud mot husrannsakan på grundval av lagstiftning som antagits före PACE om ett särskilt förfarande, undantaget material eller rättsligt privilegium, skulle ett beslut om husrannsakan för materialet ha kunnat utfärdas och iii) det hade varit lämpligt att göra detta.

⁽¹⁸⁷⁾ Rättslig prövning är det rättsliga förfarande genom vilket ett offentligt organs beslut kan överklagas till överdomstolen (High Court). Domstolarna "kontrollerar" det beslut som överklagas och avgör om det kan hävdas att beslutet är rättsligt felaktigt med beaktande av offentligrättsliga begrepp/principer. De viktigaste grunderna för domstolsprövningen är rättsstridighet, irrationalitet, förfarandefel, berättigade förväntningar och mänskliga rättigheter. Efter en framgångsrik rättslig prövning kan en domstol besluta om ett antal olika rättsmedel varav det vanligaste är en ogiltigförklaring (som skulle ogiltigförklara eller upphäva det ursprungliga beslutet – dvs. beslutet om att utfärda en husrannsakan) och i vissa fall kan detta även omfatta beviljande av ekonomisk ersättning. Ytterligare information om rättslig prövning i Förenade kungariket finns i publikationen från regeringens juridiska avdelning *Judge Over Your Shoulder – a guide to good decisions*, som finns på följande länk: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746170/JOYS-OCT-2018.pdf

begäran från en brottsbekämpande myndighet vara förenlig med principen att ändamålen med behandlingen måste specificeras, vara uttryckliga och berättigade ⁽¹⁸⁸⁾ och att de personuppgifter som behandlas av en behörig myndighet måste vara relevanta för detta ändamål och inte överdrivna ⁽¹⁸⁹⁾.

3.2.1.2 Utredningsbefogenheter för brottsbekämpande ändamål

- (139) För att förebygga eller endast för att upptäcka grova brott ⁽¹⁹⁰⁾ kan vissa brottsbekämpande myndigheter, till exempel *National Crime Agency* eller *Chief of Police* ⁽¹⁹¹⁾, använda riktade utredningsbefogenheter enligt 2016 års lag om utredningsbefogenheter. I detta fall gäller skyddsåtgärderna enligt 2016 års lag om utredningsbefogenheter utöver de skyddsåtgärder som anges i del 3 i 2018 års dataskyddslag. 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), lagring av kommunikationsuppgifter (del 4 i 2016 års lag om utredningsbefogenheter) och riktat ingrepp i utrustning (del 5 i 2016 års lag om utredningsbefogenheter). Avlyssning omfattar inhämtande av innehåll i en kommunikation ⁽¹⁹²⁾ medan inhämtande och lagring av kommunikationsuppgifter inte syftar till att erhålla innehållet i kommunikationen utan till "vem", "när", "var" och "hur" när det gäller kommunikationen. Detta omfattar t.ex. tid och varaktighet för kommunikationen, telefonnumret eller e-postadressen till avsändaren och mottagaren av kommunikationen och ibland platsen för den utrustning från vilken kommunikationen gjordes, abonnenten på en telefonitjänst eller en specificerad räkning ⁽¹⁹³⁾. Utrustning är en uppsättning teknikutrustningar som används för att erhålla olika data från utrustning, däribland datorer, surfplattor och smarttelefoner samt kablar, ledningar och lagringsenheter ⁽¹⁹⁴⁾.
- (140) Riktade avlyssningsbefogenheter kan också användas när det är nödvändigt för att ge verkan åt bestämmelserna i ett EU-instrument för ömsesidigt bistånd eller ett internationellt avtal om ömsesidigt bistånd (så kallad beslut om ömsesidigt bistånd ⁽¹⁹⁵⁾). Beslut om ömsesidigt bistånd ges endast i samband med avlyssning, inte inhämtande av kommunikationsuppgifter eller ingrepp i utrustning. Dessa riktade befogenheter regleras i 2016 års lag om utredningsbefogenheter (IPA 2016) ⁽¹⁹⁶⁾ som tillsammans med 2000 års lag om utredningsbefogenheter (RIPA) för England, Wales and Nordirland och 2000 års lag om utredningsbefogenheter (Skottland) (*Regulation of Investigatory Powers (Scotland) Act 2000*, RIPSa) för Skottland utgör den rättsliga grunden och fastställer tillämpliga begränsningar och skyddsåtgärder för användningen av sådana befogenheter. 2016 års lag om masutredningsbefogenheter innehåller också ett system för utnyttjande av massutredningsbefogenheter även om dessa inte är tillgängliga för brottsbekämpande myndigheter (endast underrättelsetjänster kan utnyttja dem) ⁽¹⁹⁷⁾.

⁽¹⁸⁸⁾ Avsnitt 36.1 i 2018 års dataskyddslag.

⁽¹⁸⁹⁾ Avsnitt 37 i 2018 års dataskyddslag.

⁽¹⁹⁰⁾ I avsnitt 263.1 i 2016 års lag om utredningsbefogenheter föreskrivs att med "grovt brott" avses ett brott för vilket en vuxen, som inte tidigare har dömts, rimligen kan förväntas dömas till fängelse i 3 år eller mer eller att handlingen inbegriper våld, leder till betydande ekonomisk vinning eller begås av ett stort antal personer. När det gäller inhämtande av kommunikationsuppgifter enligt del 4 i 2016 års lag om utredningsbefogenheter föreskrivs dessutom i avsnitt 87.10B att med grovt brott avses ett brott för vilket ett fängelsestraff på 12 månader eller mer kan utdömas eller ett brott som begås av en person som inte är en enskild eller som en integrerad del av brottet innebär att en kommunikation skickas eller att en persons privatliv kränks.

⁽¹⁹¹⁾ Följande brottsbekämpande myndigheter kan ansöka om ett riktat beslut om avlyssning: *Director General of the National Crime Agency*, *Commissioner of Police of the Metropolis*, *Chief Constable of the Police Service of Northern Ireland*, *Chief Constable of the Police Service of Scotland*, *Commissioner for Her Majesty's Revenue and Customs*, *Chief of Defence Intelligence* och en person som är behörig myndighet i ett land eller territorium utanför Förenade kungariket med avseende på ett EU-instrument för ömsesidigt bistånd eller ett internationellt avtal om ömsesidigt bistånd (avsnitt 18.1 i 2016 års lag om utredningsbefogenheter).

⁽¹⁹²⁾ Se avsnitt 4 i 2016 års lag om utredningsbefogenheter.

⁽¹⁹³⁾ Se avsnitt 261.5 i 2016 års lag om massutredningsbefogenheter och *Code of Practice on Bulk Acquisition of Communications Data*, som finns på följande länk: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf, punkt 2.9.

⁽¹⁹⁴⁾ *Code of Practice on Equipment Interference* finns på följande länk: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf, punkt 2.2.

⁽¹⁹⁵⁾ Ett beslut om ömsesidigt bistånd ger en brittisk myndighet rätt att bistå en myndighet utanför Förenade kungarikets territorium för avlyssning och utlämnande av det avlyssnade materialet till en sådan myndighet i enlighet med ett internationellt instrument för ömsesidigt bistånd (avsnitt 15.4 i 2016 års lag om utredningsbefogenheter).

⁽¹⁹⁶⁾ 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 (RIPA) som innehöll den tidigare allmänna rättsliga ramen för brottsbekämpande och nationella säkerhetsmyndigheters användning av utredningsbefogenheter.

⁽¹⁹⁷⁾ avsnitten 138.1, 158.1, 178.1, 199.1 i 2016 års lag om utredningsbefogenheter.

- (141) För att kunna utöva dessa befogenheter måste myndigheterna erhålla ett beslut ⁽¹⁹⁸⁾ som utfärdats av behörig myndighet ⁽¹⁹⁹⁾ och som godkänts av en oberoende *Judicial Commissioner* ⁽²⁰⁰⁾ (det så kallade "double lock-förfarandet"). Erhållandet av ett sådant beslut är föremål för en nödvändighets- och proportionalitetsprövning ⁽²⁰¹⁾. Eftersom dessa riktade utredningsbefogenheter enligt 2016 års lag om utredningsbefogenheter är desamma som de som nationella säkerhetsmyndigheter har tillgång till behandlas de villkor, begränsningar och skyddsåtgärder som gäller för sådana befogenheter i detalj i avsnittet om brittiska myndigheters tillgång till och användning av personuppgifter för ändamål som rör nationell säkerhet (se skäl 177 och följande).

3.2.2 Vidare användning av de insamlade uppgifterna

- (142) 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 av vissa villkor.
- (143) I likhet med vad som föreskrivs i artikel 4.2 i direktiv (EU) 2016/680 tillåter avsnitt 36.3 i 2018 års dataskyddslag att personuppgifter som samlats in av en behörig myndighet för brottsbekämpande ändamål får behandlas ytterligare (antingen av den ursprungliga personuppgiftsansvariga eller av en annan personuppgiftsansvarig) för andra brottsbekämpande ändamål, förutsatt att den personuppgiftsansvariga enligt lag är bemyndigad att behandla uppgifter för det andra ändamålet och att behandlingen är nödvändig och står i proportion till detta ändamål ⁽²⁰²⁾. I detta fall gäller alla skyddsåtgärder som föreskrivs i del 3 i 2018 års dataskyddslag och som avses i skälen 122 och 124 är tillämpliga på den behandling som utförs av den mottagande myndigheten.
- (144) I Förenade kungarikets rättsordning tillåter olika lagar uttryckligen sådan vidare delning. I synnerhet i) 2017 års lag om den digitala ekonomin tillåter delning mellan myndigheter för flera ändamål, till exempel vid bedrägeri mot den offentliga sektorn som skulle innebära förlust eller risk för förlust för en myndighet ⁽²⁰³⁾ eller vid en skuld till en myndighet eller till staten ⁽²⁰⁴⁾, ii) *Crime and Courts Act 2013* som tillåter informationsutbyte med den nationella brottsmyndigheten för bekämpning ⁽²⁰⁵⁾, utredning och lagföring av grov och organiserad brottslighet, iii) *Serious Crime Act 2007* som gör det möjligt för myndigheter att lämna ut information till bedrägeribekämpningsorganisationer i syfte att förebygga bedrägeri ⁽²⁰⁶⁾.
- (145) I dessa lagar föreskrivs uttryckligen att informationsutbytet bör ske i enlighet med de principer som fastställs i 2018 års dataskyddslag. Dessutom har polisakademin utfärdat en auktoriserad yrkespraxis för informationsutbyte ⁽²⁰⁷⁾ för att hjälpa polisen att uppfylla sina dataskyddsskyldigheter enligt den brittiska dataskyddsförordningen, dataskyddslagen och *Human Rights Act 1998*.

⁽¹⁹⁸⁾ I del 2 kapitel 2 i 2016 års lag om utredningsbefogenheter föreskrivs ett begränsat antal fall där ingripanden kan verkställas utan beslut. Detta innefattar 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.

⁽¹⁹⁹⁾ 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.

⁽²⁰⁰⁾ *Judicial Commissioners* bistår *the Investigatory Powers Commissioner*, ett oberoende organ som utövar tillsyn över underrättelse-tjänsternas användning av utredningsbefogenheter (se skäl 162 ff. för mer information).

⁽²⁰¹⁾ Se särskilt avsnitten 19 och 23 i 2016 års lag om utredningsbefogenheter.

⁽²⁰²⁾ Avsnitt 36.3 i 2018 års dataskyddslag.

⁽²⁰³⁾ Avsnitt 56 i *Digital Economy Act 2017*, finns på följande länk: <https://www.legislation.gov.uk/ukpga/2017/30/section/56>

⁽²⁰⁴⁾ Avsnitt 48 i *Digital Economy Act 2017*.

⁽²⁰⁵⁾ Avsnitt 7 i *Crime and Courts Act 2013*, finns på följande länk: <https://www.legislation.gov.uk/ukpga/2013/22/section/7>

⁽²⁰⁶⁾ Avsnitt 68 i *Serious Crime Act 2007*, finns på följande länk: <https://www.legislation.gov.uk/ukpga/2007/27/contents>

⁽²⁰⁷⁾ *Authorised Professional Practice on Information Sharing*, finns på följande länk: <https://www.app.college.police.uk/app-content/information-management/sharing-police-information>

Naturligtvis äger en rättslig prövning rum för att undersöka om utbytet överensstämmer med den tillämpliga rättsliga ramen för dataskydd ⁽²⁰⁸⁾.

- (146) I likhet med vad som anges i artikel 9 i direktiv (EU) 2016/680 föreskriver 2018 års dataskyddslag dessutom att personuppgifter som samlas in för brottsbekämpningsändamål får behandlas för ett ändamål som inte är brottsbekämpningssyfte när behandlingen är tillåten enligt lag ⁽²⁰⁹⁾.
- (147) Denna typ av delning omfattar de två scenarierna 1) när en brottsbekämpande myndighet delar uppgifter med en annan icke-straffrättslig brottsbekämpande myndighet än en underrättelsetjänst (t.ex. en finans- eller skattemyndighet, en konkurrensmyndighet, en barn- och ungdomsmyndighet osv.) och 2) när en brottsbekämpande myndighet delar uppgifter med en underrättelsetjänst. I det första scenariot kommer behandlingen av personuppgifter att omfattas av den brittiska dataskyddsförordningen och av del 2 i 2018 års dataskyddslag. Kommissionen har bedömt de skyddsåtgärder som föreskrivs i den brittiska dataskyddsförordningen och del 2 i 2018 års dataskyddslag i skälen 12–111 och har dragit slutsatsen att Förenade kungariket säkerställer en adekvat skyddsnivå för personuppgifter som överförs inom tillämpningsområdet för förordning (EU) 2016/679 från Europeiska unionen till Förenade kungariket.
- (148) I det andra scenariot, när det gäller utbyte av uppgifter som samlats in av en brottsbekämpande myndighet med en underrättelsetjänst för ändamål som rör nationell säkerhet är den rättsliga grunden för sådant utbyte avsnitt 19 i *Counter Terrorism Act 2008* (CTA 2008) ⁽²¹⁰⁾. Enligt denna lag får var och en lämna uppgifter till någon av underrättelsetjänsterna i syfte att fullgöra någon av dess funktioner, inbegripet "nationell säkerhet".
- (149) När det gäller villkoren för utbyte av uppgifter för nationella säkerhetsändamål begränsar *Intelligence Services Act* ⁽²¹¹⁾ och *Security Services Act* ⁽²¹²⁾ underrättelsetjänsternas möjligheter att inhämta uppgifter till vad som är nödvändigt för att de ska kunna fullgöra sina lagstadgade uppgifter. Brottsbekämpande organ som vill utbyta uppgifter med underrättelsetjänsterna kommer att behöva ta hänsyn till ett antal faktorer/begränsningar, utöver myndigheternas lagstadgade uppgifter som fastställs i lagen om underrättelsetjänster och lagen om säkerhetstjänster ⁽²¹³⁾. I avsnitt 20 i *Counter Terrorism Act 2008* klargörs att all datadelning enligt avsnitt 19 fortfarande måste vara förenlig med dataskyddslagstiftningen, vilket innebär att alla begränsningar och krav i del 3 i 2018 års dataskyddslag gäller. Eftersom behöriga myndigheter är myndigheter i den mening som avses i *Human Rights Act 1998* måste de dessutom se till att de agerar i enlighet med rättigheterna i konventionen, däribland artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna. Dessa begränsningar säkerställer att allt uppgiftsutbyte mellan brottsbekämpande organ och underrättelsetjänster är förenligt med dataskyddslagstiftningen och den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna.

⁽²⁰⁸⁾ Se t.ex. målet *M, R/Chief Constable of Sussex Police* [2019] EWHC 975 (Admin), där överdomstolen (High Court) ombads att överväga utbyte av uppgifter mellan polisen och *Business Crime Reduction Partnership* (BCRP), en organisation som har befogenhet att förvalta system för undantag och som förbjuder personer att komma in i medlemmarnas affärslokaler. Domstolen granskade utbytet av uppgifter, som ägde rum på grundval av ett avtal som syftade till att skydda allmänheten och förebygga brott och kom slutligen fram till att de flesta aspekterna av datadelning var lagliga utom när det gäller viss känslig information som delas mellan polisen och de grundläggande rättigheterna. Ett annat exempel är målet *Cooper/NCA* [2019] EWCA Civ 16, där appellationsdomstolen bekräftade datadelningen mellan polisen och Serious Organised Crime Agency (SOCA), en brottsbekämpande myndighet som för närvarande ingår i NCA (nationella konkurrensmyndigheten).

⁽²⁰⁹⁾ Avsnitt 36.4 i 2018 års dataskyddslag.

⁽²¹⁰⁾ *Counter Terrorism Act 2008* finns på följande länk: <https://www.legislation.gov.uk/ukpga/2008/28/section/19>

⁽²¹¹⁾ *Intelligence Services Act 1994* finns på följande länk: <https://www.legislation.gov.uk/ukpga/1994/13/contents>

⁽²¹²⁾ *Security Services Act 1989* finns på följande länk: <https://www.legislation.gov.uk/ukpga/1989/5/contents>

⁽²¹³⁾ I avsnitt 2.2 i *Intelligence Service Act 1994* föreskrivs att "chefen för underrättelsetjänsten ska ansvara för dess effektivitet och det ska vara hans eller hennes skyldighet att säkerställa a) att det finns arrangemang för att säkerställa att ingen information erhålls av underrättelsetjänsten utom i den mån det är nödvändigt för att den ska kunna utföra sina uppgifter på ett korrekt sätt och att ingen information lämnas ut av den utom i den mån det är nödvändigt i) för detta ändamål, ii) av hänsyn till den nationella säkerheten, iii) i syfte att förebygga eller upptäcka allvarliga brott, eller iv) i samband med straffrättsliga förfaranden och b) att underrättelsetjänsten inte vidtar några åtgärder för att främja ett politiskt partis intressen i Förenade kungariket" medan det i avsnitt 2.2 i *Security Service Act 1989* föreskrivs att "generaldirektören ska ansvara för tjänstens effektivitet och vara skyldig att se till a) att det finns arrangemang för att säkerställa att inga uppgifter erhålls av myndigheten utom i den mån det är nödvändigt för att den ska kunna utföra sina uppgifter på ett korrekt sätt eller om det är nödvändigt för detta ändamål eller för att förebygga eller avslöja allvarliga brott eller brottslig verksamhet, b) att tjänsten inte vidtar några åtgärder för att främja något politiskt partis intressen, och c) att det finns arrangemang som överenskommit med Director General för National Crime Agency för att samordna myndighetens verksamhet i enlighet med avsnitt 1.4 i denna lag med polisens, National Crime Agency's och andra brottsbekämpande organs verksamhet".

- (150) När en behörig myndighet avser att dela personuppgifter som behandlas enligt del 3 i 2018 års dataskyddslag med brottsbekämpande myndigheter i ett tredjeland gäller särskilda krav ⁽²¹⁴⁾. Sådana överföringar kan i synnerhet äga rum när de grundar sig på bestämmelser om adekvat skyddsnivå som utfärdats av ministern eller, i avsaknad av sådana bestämmelser, måste säkerställas. I avsnitt 75 i 2018 års dataskyddslag föreskrivs att lämpliga skyddsåtgärder ska vidtas om det fastställs i ett rättsligt instrument som binder den avsedda mottagaren, eller om den personuppgiftsansvariga, efter att ha bedömt alla omständigheter kring överföringar av denna typ av personuppgifter till tredjelandet eller den internationella organisationen, drar slutsatsen att det finns lämpliga skyddsåtgärder för att skydda uppgifterna.
- (151) Om en överföring inte grundar sig på en förordning om adekvat skyddsnivå eller lämpliga skyddsåtgärder kan den endast ske under vissa, specificerade omständigheter, så kallade särskilda omständigheter ⁽²¹⁵⁾. Detta är fallet när överföringen är nödvändig a) för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan person, b) för att skydda den registrerades berättigade intressen, c) för att avvärja ett omedelbart och allvarligt hot mot den allmänna säkerheten i en medlemsstat eller ett tredjeland, d) för att i enskilda fall för något av de brottsbekämpande ändamålen eller e) för att i enskilda fall för ett rättsligt ändamål (t.ex. i samband med rättsliga förfaranden eller för att erhålla juridisk rådgivning). Det kan noteras att d) och e) inte är tillämpliga om den registrerades rättigheter och friheter väger tyngre än det allmänna intresset av överföringen. Dessa omständigheter motsvarar de särskilda situationer och villkor som räknas som "undantag" enligt artikel 38 i direktiv (EU) 2016/680.
- (152) När det material som de brottsbekämpande myndigheterna inhämtat inom ramen för ett beslut som tillåter användning av avlyssning eller ingrepp i utrustning överlämnas till tredjeland införs ytterligare skyddsåtgärder genom 2016 års lag om utredningsbefogenheter. Ett sådant utlämnande, definierad som "utlämnande till utlandet" är endast tillåten om den utfärdande myndigheten anser att det finns särskilda lämpliga arrangemang som begränsar antalet personer till vilka uppgifterna lämnas ut, i vilken utsträckning allt material lämnas ut eller görs tillgängligt samt i vilken utsträckning något av materialet kopieras och antalet kopior. Den utfärdande myndigheten får dessutom ta hänsyn till att lämpliga arrangemang är nödvändiga för att säkerställa att varje kopia av någon del av materialet förstörs så snart det inte längre finns några relevanta skäl att behålla det (om det inte har förstörts tidigare) ⁽²¹⁶⁾.
- (153) Slutligen skulle särskilda former av vidare överföring från Förenade kungariket till Förenta staterna i framtiden kunna ske på grundval av avtalet mellan Förenade konungariket Storbritannien och Nordirlands regering och Amerikas förenta staters regering om tillgång till elektroniska uppgifter för bekämpning av grov brottslighet (avtalet mellan Förenade kungariket och Förenta staterna eller avtalet) ⁽²¹⁷⁾ som ingicks i oktober 2019 ⁽²¹⁸⁾. Avtalet mellan Förenade kungariket och Förenta staterna har ännu inte trätt i kraft vid tidpunkten för antagandet av detta beslut men dess förväntade ikraftträdande kan påverka vidare överföringar till Förenta staterna av uppgifter som först överfördes till Förenade kungariket på grundval av beslutet. Närmare bestämt 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 enligt detta avtal så snart det trätt i kraft. Av dessa skäl är bedömningen av de villkor och skyddsåtgärder enligt vilka sådana förelägganden kan utfärdas och verkställas relevant för detta beslut.

⁽²¹⁴⁾ Se kapitel 5 i del 3 i 2018 års dataskyddslag.

⁽²¹⁵⁾ Avsnitt 76 i 2018 års dataskyddslag.

⁽²¹⁶⁾ Avsnitten 54 och 130 i 2016 års lag om utredningsbefogenheter. De utfärdande myndigheterna måste överväga behovet av att införa särskilda skyddsåtgärder för det material som överlämnas till utländska myndigheter, för att säkerställa att uppgifterna omfattas av skyddsåtgärder när det gäller lagring, förstöring och utlämnande av uppgifter liknande dem som föreskrivs i avsnitt 53 och avsnitt 129 i 2016 års lag om utredningsbefogenheter.

⁽²¹⁷⁾ 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

⁽²¹⁸⁾ Detta är den första överenskommelse som nåts inom ramen för *US Clarifying Lawful Overseas Use of Data Act* (CLOUD Act). *The United States CLOUD Act* är en amerikansk federal lag som antogs den 23 mars 2018 och som genom en ändring av *Stored Communications Act* från 1986 klargör att amerikanska tjänsteleverantörer är skyldiga att följa Förenta staternas förelägganden om att lämna ut innehållsdata och icke-innehållsdata, oavsett var sådana data lagras. CLOUD Act gör det också möjligt att ingå verkställande avtal med utländska regeringar på grundval av vilka amerikanska tjänsteleverantörer skulle kunna leverera innehållsdata direkt till dessa utländska regeringar (texten till CLOUD Act, finns på följande länk: <https://www.congress.gov/115/bills/s2383/BILLS-115s2383is.pdf>)

- (154) I detta avseende bör det för det första noteras att avtalet, när det gäller dess materiella tillämpningsområde, endast är tillämpligt på brott som är belagda med ett maximistraff på minst tre års fängelse (definierat som "allvarlig brottslighet")⁽²¹⁹⁾, inbegripet "terroristverksamhet". För det andra får uppgifter som behandlas i den andra jurisdiktionen inhämtas enligt detta avtal endast efter ett "föreläggandet [...]" som är föremål för prövning eller tillsyn enligt den utfärdande partens nationella lagstiftning av en domstol, en domare, en fredsdomare eller en annan oberoende myndighet före eller i samband med ett förfarande för verkställighet av föreläggandet"⁽²²⁰⁾. För det tredje måste varje föreläggande "grundas på krav på rimlig motivering baserad på tydliga och trovärdiga fakta, utmärkande drag, laglighet och allvarlighetsgrad när det gäller det beteende som utreds"⁽²²¹⁾ och "vara inriktad på specifika konton samt identifiera en viss person, ett visst konto, en särskild adress eller en personlig anordning eller någon annan specifik identifierare"⁽²²²⁾. För det fjärde omfattas uppgifter som erhålls inom ramen för detta avtal av samma skydd som de särskilda skyddsåtgärder som föreskrivs i det så kallade paraplyavtalet mellan EU och USA⁽²²³⁾ – ett omfattande avtal om dataskydd som EU och Förenta staterna ingick i december 2016 och som fastställer skyddsåtgärder och rättigheter som är tillämpliga på dataöverföringar på området för brottsbekämpande samarbete – som alla införlivas i detta avtal genom hänvisning på motsvarande sätt för att särskilt ta hänsyn till den särskilda karaktären hos överföringarna (dvs. överföringar från privata aktörer till brottsbekämpande myndigheter, snarare än överföringar mellan brottsbekämpande myndigheter)⁽²²⁴⁾. I avtalet mellan Förenade kungariket och Förenta staterna föreskrivs särskilt att skydd som är likvärdigt med det som ges i paraplyavtalet mellan EU och Förenta staterna ska tillämpas "på all personlig information som framställs i samband med verkställandet av de beslut som omfattas av avtalet i syfte att ge likvärdigt skydd"⁽²²⁵⁾.
- (155) Uppgifter som överförs till de amerikanska myndigheterna enligt avtalet mellan Förenade kungariket och Förenta staterna bör därför omfattas av det skydd som föreskrivs i ett EU-rättsligt instrument med nödvändiga anpassningar för att återspegla typen av överföringar i fråga. De brittiska myndigheterna har vidare bekräftat att skyddet i paraplyavtalet kommer att gälla för all personlig information som framställs eller bevaras enligt avtalet, oavsett typ eller typ av organ som begär det (t.ex. både federala och statliga brottsbekämpande myndigheter i Förenta staterna), så att likvärdigt skydd alltid måste ges. De brittiska myndigheterna har dock också förklarat att detaljerna i det konkreta genomförandet av dataskyddsgarantierna fortfarande är föremål för diskussioner mellan Förenade kungariket och USA. I samband med samtalen med Europeiska kommissionens avdelningar om detta beslut bekräftade de brittiska myndigheterna att de inte kommer att låta avtalet träda i kraft förrän de har försäkrat sig om att genomförandet är förenligt med de rättsliga skyldigheterna i avtalet, inbegripet klarhet när det gäller efterlevnaden av dataskyddsstandarderna för alla uppgifter som begärs enligt detta avtal. Eftersom ett eventuellt ikraftträdande av avtalet kan påverka den skyddsnivå som bedöms i detta beslut bör Förenade kungariket, så snart det blir tillgängligt och i alla händelser före avtalets ikraftträdande, meddela Europeiska kommissionen all information och eventuella framtida klargöranden om hur Förenta staterna kommer att fullgöra sina skyldigheter enligt avtalet, för att säkerställa en korrekt övervakning av detta beslut i enlighet med artikel 45.4 i förordning (EU) 2016/679. Särskild uppmärksamhet kommer att ägnas åt tillämpningen och anpassningen av paraplyavtalets skydd till den särskilda typ av överföringar som omfattas av avtalet mellan Förenade kungariket och Förenta staterna.
- (156) Mer allmänt kommer all relevant utveckling när det gäller avtalets ikraftträdande och tillämpning att vederbörligen beaktas i samband med den fortlöpande övervakningen av detta beslut även när det gäller de nödvändiga konsekvenser som ska dras om det finns tecken på att en väsentligen likvärdig skyddsnivå inte längre säkerställs.

3.2.3 Tillsyn

- (157) Beroende på de befogenheter som de behöriga myndigheterna använder när de behandlar personuppgifter för brottsbekämpande ändamål (antingen enligt 2018 års dataskyddslag eller 2016 års lag om utredningsbefogenheter) säkerställer olika organ tillsynen över användningen av dessa befogenheter. I synnerhet övervakar *the Information*

⁽²¹⁹⁾ Artikel 1.14 i avtalet.

⁽²²⁰⁾ Artikel 5.2 i avtalet.

⁽²²¹⁾ Artikel 5.1 i avtalet.

⁽²²²⁾ Artikel 4.5 i avtalet. En ytterligare och strängare standard gäller för avlyssning i realtid enligt följande: Besluten måste ha begränsad varaktighet som inte får vara längre än vad som rimligen är nödvändigt för att uppnå syftet med ordern och ska endast utfärdas om samma information inte rimligen kunde erhållas genom en mindre ingripande metod (artikel 5.3 i avtalet).

⁽²²³⁾ 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, finns på följande länk: [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:2016A1210\(01\)&from=EN](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:2016A1210(01)&from=EN)

⁽²²⁴⁾ Artikel 9.1 i avtalet.

⁽²²⁵⁾ Artikel 9.1 i avtalet.

Commissioner behandlingen av personuppgifter när den omfattas av del 3 i 2018 års dataskyddslag ⁽²²⁶⁾. Oberoende och rättslig tillsyn över användningen av utredningsbefogenheter inom ramen för 2016 års lag om utredningsbefogenheter säkerställs av IPCO (*Investigatory Powers Commissioner's Office*) ⁽²²⁷⁾ (denna del behandlas i skälen 250–255). Dessutom garanteras ytterligare tillsyn av parlamentet och andra organ.

3.2.3.1 Tillsyn över del 3 i 2018 års dataskyddslag

- (158) De allmänna arbetsuppgifter som *the Information Commissioner* har – vars oberoende och organisation förklaras i skäl 87 – när det gäller behandling av personuppgifter som omfattas av del 3 i 2018 års dataskyddslag fastställs i bilaga 13 till denna lag. ICO har som huvuduppgift att övervaka och verkställa del 3 i 2018 års dataskyddslag samt att främja allmänhetens medvetenhet, ge råd till parlamentet, regeringen och andra institutioner och organ. För att upprätthålla rättsväsendets oberoende är *the Information Commissioner* inte bemyndigad att utföra sina uppgifter i samband med behandling av personuppgifter som utförs av en enskild person som handlar i egenskap av en domande myndighet eller av en domstol som agerar inom ramen för sin domande verksamhet. Under dessa omständigheter skulle andra organ utöva tillsynsfunktionerna enligt skälen 99–103.
- (159) *The Commissioner* har allmänna undersökande, korrigerande, tillståndrelaterade och rådgivande befogenheter när det gäller behandling av personuppgifter som omfattas av del 3. I synnerhet har *the Commissioner* befogenhet att underrätta den personuppgiftsansvariga eller personuppgiftsbiträdet om en påstådd överträdelse av del 3 i 2018 års dataskyddslag, att utfärda varningar eller en reprimand till en personuppgiftsansvarig eller ett personuppgiftsbiträde som har överträtt bestämmelserna i del 3 i lagen, samt att på eget initiativ eller på begäran avge yttranden till parlamentet, regeringen eller andra institutioner och organ samt till allmänheten i alla frågor som rör skydd av personuppgifter ⁽²²⁸⁾.
- (160) Dessutom har *the Commissioner* befogenhet att utfärda informationsförelägganden ⁽²²⁹⁾, bedömningsförelägganden ⁽²³⁰⁾ och verkställighetsförelägganden ⁽²³¹⁾ samt befogenhet att få tillgång till personuppgiftsansvarigas och personuppgiftsbiträdens handlingar, att få tillträde till deras lokaler ⁽²³²⁾ och att utfärda administrativa sanktionsavgifter i form av påföljdsförelägganden ⁽²³³⁾. I ICO:s policy för regleringsåtgärder (*Information Commissioner's Office Regulatory Action Policy*) anges under vilka omständigheter den utfärdar förelägganden om information, bedömning, verkställighet och påföljder ⁽²³⁴⁾ (se även skäl 93 i direktiv (EU) 2016/680 om adekvat skyddsnivå, skälen 101–102).
- (161) Enligt sina senaste årsrapporter (2018–2019 ⁽²³⁵⁾, 2019–2020 ⁽²³⁶⁾) har *the Information Commissioner* genomfört ett antal utredningar och vidtagit verkställighetsåtgärder med avseende på brottsbekämpande myndigheters behandling av uppgifter. Till exempel genomförde *the Commissioner* en utredning och offentliggjorde ett yttrande i oktober 2019 om brottsbekämpande myndigheters användning av ansiktsgenkänningsteknik på offentliga platser. Utredningen inriktades särskilt på hur South Wales Police och Metropolitan Police Service (MPS) använder sig av kapacitet för ansiktsgenkänning på plats. *The Information Commissioner* undersökte också Metropolitan Police Service "Gangs matrix" ⁽²³⁷⁾ och fann en rad allvariga överträdelser av dataskyddslagstiftningen som sannolikt skulle undergräva allmänhetens förtroende för matrisen och hur uppgifterna användes. I november 2018 utfärdade *the Information Commissioner* ett verkställighetsföreläggande och därefter vidtog Metropolitan Police Service de åtgärder som krävdes för att öka säkerheten och ansvarsskyldigheten och se till att uppgifterna användes på ett proportionerligt sätt. Ett annat exempel på verkställighetsåtgärder på

⁽²²⁶⁾ Avsnitt 116 i 2018 års dataskyddslag.

⁽²²⁷⁾ Se 2016 års lag om utredningsbefogenheter och särskilt kapitel 1 del 8.

⁽²²⁸⁾ Punkt 2 i tillägg 13 till 2018 års dataskyddslag.

⁽²²⁹⁾ Förelägga den personuppgiftsansvariga och personuppgiftsbiträdet (och under vissa omständigheter varje annan person) att lämna nödvändig information (avsnitt 142 i 2018 års dataskyddslag).

⁽²³⁰⁾ Tillåta utredningar och revisioner, vilket kan kräva att den personuppgiftsansvariga eller personuppgiftsbiträdet ger *the Commissioner* tillträde till särskilda lokaler, inspekterar eller undersöker handlingar eller utrustning, frågar ut personer som behandlar personuppgifter för den personuppgiftsansvarigas räkning (avsnitt 146 i 2018 års dataskyddslag).

⁽²³¹⁾ Tillåta utövandet av korrigerande befogenheter, vilket kräver att personuppgiftsansvariga/personuppgiftsbiträden vidtar eller avstår från att vidta specificerade åtgärder (avsnitt 149 i 2018 års dataskyddslag).

⁽²³²⁾ Avsnitt 154 i 2018 års dataskyddslag.

⁽²³³⁾ Avsnitt 155 i 2018 års dataskyddslag.

⁽²³⁴⁾ *Regulatory Action Policy*, se fotnot 96.

⁽²³⁵⁾ *Information Commissioner's Annual Report and Financial Statements 2018-19*, se fotnot 101.

⁽²³⁶⁾ *Information Commissioner's Annual Report and Financial Statements 2019-20*, se fotnot 82.

⁽²³⁷⁾ En databas med uppgifter om påstådda gruppmedlemmar och offer för gängrelaterade brott.

detta område är de sanktionsavgifter på 325 000 pund som *the Commissioner* utfärdade mot åklagarmyndigheten i maj 2018 för att ha förlorat okrypterade dvd-skivor som innehöll inspelningar av polisförhör. *The Information Commissioner* genomförde också utredningar av bredare frågor, till exempel under första halvåret 2020 om användningen av avlyssning av mobiltelefoner för polisändamål och polisens behandling av brottsoffrens uppgifter. Dessutom utreder *the Commissioner* för närvarande ett ärende som inbegriper brottsbekämpande myndigheters tillgång till uppgifter som innehas av en enhet i den privata sektorn, Clearview AI Inc. ⁽²³⁸⁾

- (162) Förutom de verkställande befogenheter som *the Information Commissioner* har som nämns i skälen 160 och 161 utgör vissa överträdelser av dataskyddslagstiftningen brott och kan därför bli föremål för straffrättsliga påföljder (avsnitt 196 i 2018 års dataskyddslag). Detta gäller till exempel för att erhålla, röja eller lagra personuppgifter utan den personuppgiftsansvarigas samtycke och för att säkerställa att personuppgifter lämnas ut till en annan person utan den personuppgiftsansvarigas samtycke ⁽²³⁹⁾, återidentifierande information som utgörs av avidentifierade personuppgifter utan samtycke från den personuppgiftsansvariga som ansvarar för avidentifieringen av personuppgifterna ⁽²⁴⁰⁾, avsiktligt hindra *the Commissioner* från att utöva sina befogenheter när det gäller kontroll av personuppgifter i enlighet med internationella skyldigheter ⁽²⁴¹⁾, lämna oriktiga uppgifter om svar på ett informationsföreläggande eller förstöra information i samband med informations- och bedömningsförelägganden ⁽²⁴²⁾.

3.2.3.2 Andra tillsynsorgan på området brottsbekämpning

- (163) Utöver *the Information Commissioner* finns det flera tillsynsorgan på det straffrättsliga området med särskilda mandat som är relevanta för dataskyddsfrågor. Detta inbegriper till exempel *the Biometrics Commissioner* ⁽²⁴³⁾ och *the Surveillance Camera Commissioner* ⁽²⁴⁴⁾.

3.2.3.3 Parlamentarisk tillsyn på området brottsbekämpning

- (164) Home Affairs Select Committee (HASC) utövar parlamentarisk tillsyn på området brottsbekämpning. Detta utskott består av 11 parlamentsledamöter från de tre största politiska partierna. Utskottet har till uppgift att granska inrikesministeriets och därmed sammanhängande offentliga organs utgifter, administration och politik, dvs. polisen och NCA – vars arbete utskottet kan granska särskilt ⁽²⁴⁵⁾.

⁽²³⁸⁾ Se ICO:s uttalande som finns på följande länk: <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/oaic-and-ico-open-joint-investigation-into-clearview-ai-inc/>

⁽²³⁹⁾ Avsnitt 170 i 2018 års dataskyddslag.

⁽²⁴⁰⁾ Avsnitt 171 i 2018 års dataskyddslag.

⁽²⁴¹⁾ Avsnitt 119.6 i 2018 års dataskyddslag.

⁽²⁴²⁾ Under det räkenskapsår som omfattade perioden 1 april 2019–31 mars 2020 har de utredningar som genomförts av ICO lett till fyra varningar och åtta åtal. Dessa ärenden lagfördes enligt avsnitt 55 i dataskyddslagen från 1998, avsnitt 77 i *Freedom of Information Act 2000* och avsnitt 170 i 2018 års dataskyddslag. I 75 % av fallen har de tilltalade gjort gällande att det inte är nödvändigt med utdragna rättegångar med tillhörande kostnader (*Information Commissioner's Annual Report and Financial Statements 2019/2020*, se fotnot 87, s. 40).

⁽²⁴³⁾ *Biometrics Commissioner* inrättades genom *Protection of Freedoms Act 2012* (se <https://www.legislation.gov.uk/ukpga/2012/9/contents>). *Biometrics Commissioner* avgör bland annat om polisen får behålla DNA-profiler och fingeravtryck från personer som gripits men inte åtalats för ett kvalificerat brott (avsnitt 63G i PACE 1984). Dessutom har *the Biometric Commissioner* ett allmänt ansvar för att se över lagringen och användningen av DNA och fingeravtryck och lagringen av nationella säkerhetsskäl (avsnitt 20.2 i POFA 2012). *The Biometric Commissioner* utses enligt *Code for Public Appointments* (koden finns på följande länk: <https://www.gov.uk/government/publications/governance-code-for-public-appointments>) och villkoren för utnämningen klargör att han eller hon endast kan avsättas av inrikesministern enligt en snävt definierad uppsättning av omständigheter, bland annat underlåtenhet att fullgöra sina skyldigheter i tjänsten under en period av tre månader, fällande dom för ett brott eller underlåtenhet att uppfylla villkoren för utnämning.

⁽²⁴⁴⁾ *The Surveillance Camera Commissioner* inrättades genom *Protection of Freedoms Act 2012* och har till uppgift att främja efterlevnaden av *the Surveillance Camera Code of Practice*, se över hur denna praxis fungerar och ge råd till ministrarna om huruvida denna praxis behöver ändras. *The Commissioner* utnämns enligt samma regler som *the Biometrics Commissioners* och har liknande befogenheter, resurser och skydd mot avsättning.

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

- (165) Utskottet kan, inom ramen för sitt ansvarsområde, välja sitt eget undersökningsobjekt, inklusive särskilda fall, så länge frågan inte är under rättslig prövning. Utskottet får också begära skriftliga och muntliga bevis från ett brett spektrum av relevanta grupper och individer. Det utarbetar rapporter om sina iakttagelser och utfärdar rekommendationer till regeringen ⁽²⁴⁶⁾. Regeringen förväntas svara på var och en av rapportens rekommendationer och måste svara inom 60 dagar ⁽²⁴⁷⁾.
- (166) På övervakningsområdet utarbetade utskottet även en rapport om 2000 års lag om utredningsbefogenheter (RIPA 2000) ⁽²⁴⁸⁾ där det konstaterades att 2000 års lag om utredningsbefogenheter inte var ändamålsenlig. Deras rapport beaktades när betydande delar av 2000 års lag om utredningsbefogenheter ersattes med 2016 års lag om utredningsbefogenheter. En fullständig förteckning över undersökningar finns på utskottets webbplats ⁽²⁴⁹⁾.
- (167) HASC:s uppgifter utförs i Skottland av *the Justice Subcommittee on Policing* och i Nordirland av *the Committee for Justice* ⁽²⁵⁰⁾.

3.2.4. Prövningsmöjligheter

- (168) När det gäller brottsbekämpande myndigheters behandling av uppgifter finns prövningsmekanismer tillgängliga i del 3 i 2018 års dataskyddslag och inom ramen för 2016 års lag om utredningsbefogenheter samt enligt *Human Rights Act 1998*.
- (169) Denna serie av mekanismer ger de registrerade effektiva administrativa och rättsliga prövningsmöjligheter som gör det möjligt för dem att särskilt säkerställa sina rättigheter, inbegripet rätten att få tillgång till sina personuppgifter eller att få dessa uppgifter rättade eller raderade.
- (170) För det första har den registrerade enligt avsnitt 165 i 2018 års dataskyddslag rätt att lämna in ett klagomål till *the Information Commissioner* om den registrerade anser att det föreligger en överträdelse av del 3 i 2018 års dataskyddslag i samband med personuppgifter som rör honom eller henne ⁽²⁵¹⁾. *The Information Commissioner* har befogenhet att bedöma den personuppgiftsansvarigas och personuppgiftsbiträdets efterlevnad av 2018 års dataskyddslag, kräva att han eller hon vidtar nödvändiga åtgärder vid bristande efterlevnad och utdöma sanktionsavgifter.

⁽²⁴⁶⁾ De utvalda utskotten, inklusive *Home Affairs Select Committee*, omfattas av underhusets arbetsordning. Arbetsordningen är de regler som underhuset har enats om för parlamentets verksamhet. De utvalda utskotten har ett brett ansvarsområde. I artikel 152.1 i arbetsordningen föreskrivs att "de särskilda utskotten ska utses för att granska utgifter, administration och politik i de viktigaste regeringsministerierna i enlighet med vad som anges i punkt 2 i denna förordning och associerade offentliga organ". Detta gör det möjligt för *Home Affairs Select Committee* att granska all politik som förvaltas av inrikesministeriet och som omfattar politik (och tillhörande lagstiftning) om utredningsbefogenheter. I artikel 152.4 i arbetsordningen klargörs dessutom att utskotten har olika befogenheter, bland annat förmågan att begära att personer avlägger vittnesmål eller handlingar i en viss fråga och att utarbeta rapporter. Kommitténs aktuella och tidigare frågor finns på följande länk: <https://committees.parliament.uk/committee/83/home-affairs-committee/>.

⁽²⁴⁷⁾ Befogenheterna för *Home Affairs Select Committee* i England och Wales anges i underhusets arbetsordning som finns på följande länk: <https://www.parliament.uk/business/publications/commons/standing-orders-public11/>.

⁽²⁴⁸⁾ Finns på följande länk: <https://publications.parliament.uk/pa/cm201415/cmselect/cmhaff/711/71103.htm>.

⁽²⁴⁹⁾ Finns på följande länk: <https://committees.parliament.uk/committee/83/home-affairs-committee>.

⁽²⁵⁰⁾ Arbetsordningen för *the Justice Subcommittee on Policing* i Skottland finns på följande länk <https://www.parliament.scot/parliamentary-business/CurrentCommittees/justice-committee.aspx> och reglerna för *the Committee of Justice* i Nordirland finns på följande länk: <http://www.niassembly.gov.uk/assembly-business/standing-orders/>.

⁽²⁵¹⁾ ICO:s senaste årsrapport innehåller en uppdelning av de mottagna och avslutade klagomålen art. Framför allt uppgår antalet mottagna klagomål för "polis- och kriminalregister" till 6 % av det totala antalet mottagna klagomål (en ökning med 1 % jämfört med föregående budgetår). Årsrapporten visar också att klagomål som rör ansökningar om tillgång till ämnen står för det högsta antalet (46 % av det totala antalet klagomål med en ökning med 8 % jämfört med föregående budgetår) (Årsrapport för ICO 2019–2020, s. 55, se fotnot 88).

- (171) För det andra ger 2018 års dataskyddslag rätt till rättsmedel mot *the Information Commissioner* om denne inte behandlar ett klagomål från den registrerade på lämpligt sätt. Om *the Commissioner* underlåter att "gå vidare" ⁽²⁵²⁾ med ett klagomål från den registrerade har klaganden tillgång till rättsmedel, eftersom de kan ansöka hos en *First Tier Tribunal* ⁽²⁵³⁾ att den ska ålägga *the Commissioner* att vidta lämpliga åtgärder för att besvara klagomålet eller informera den klagande om hur ärendet fortskrider ⁽²⁵⁴⁾. Dessutom kan varje person som får något av de nämnda tillkännagivandena (informations-, bedömnings-, verkställighets- eller påföljdsföreläggandet) från *the Commissioner* överklaga till en *First Tier Tribunal*. Om tribunalen anser att det beslut *the Commissioner* fattar inte är förenligt med lagen eller att *the Information Commissioner* borde ha utövat sitt utrymme för skönsmässig bedömning på ett annat sätt, ska tribunalen bifalla överklagandet eller ersätta ett annat föreläggande eller beslut som *the Information Commissioner* skulle ha kunnat avge eller fatta ⁽²⁵⁵⁾.
- (172) För det tredje kan enskilda erhålla rättslig prövning av personuppgiftsansvariga och personuppgiftsbiträden direkt vid domstol. Enligt avsnitt 167 i 2018 års dataskyddslag får en registrerad lämna in en ansökan till domstolen om intrång i hans eller hennes rätt enligt dataskyddslagstiftningen och domstolen kan genom ett föreläggande begära att den personuppgiftsansvariga vidtar (eller avstår från att vidta) varje åtgärd med avseende på behandlingen för att följa 2018 års dataskyddslag. Enligt avsnitt 169 i 2018 års dataskyddslag har dessutom varje person som lidit skada till följd av en överträdelse av ett krav i dataskyddslagstiftningen (inklusive del 3 i 2018 års dataskyddslag), med undantag för brittiska dataskyddsförordningen, rätt till ersättning för denna skada från den personuppgiftsansvariga eller personuppgiftsbiträdet, utom om den personuppgiftsansvariga eller personuppgiftsbiträdet bevisar att den personuppgiftsansvariga eller personuppgiftsbiträdet inte på något sätt är ansvarig för den händelse som orsakade skadan. Med skada avses både ekonomisk förlust och skada som inte medför ekonomiska förluster, till exempel nödläge.
- (173) Slutligen kan var och en om han eller hon anser att hans eller hennes rättigheter, inklusive rätten till integritet och dataskydd, har kränkts av alla myndigheter få sin sak prövad i domstol i Förenade kungariket enligt *Human Rights Act 1998* ⁽²⁵⁶⁾ och efter att ha uttömt nationella rättsmedel kan en person, en icke-statlig organisation och grupper av enskilda få upprättelse inför Europeiska domstolen för de mänskliga rättigheterna för kränkningar av de rättigheter som garanteras enligt den europeiska konventionen om mänskliga rättigheter ⁽²⁵⁷⁾ (se skäl 111).

3.2.4.1 Prövningsmekanismer inom 2016 års lag om utredningsbefogenheter

- (174) Enskilda personer kan erhålla rättslig prövning av överträdelser av 2016 års lag om utredningsbefogenheter inför tribunalen för utredningsbefogenheter. De möjligheter till rättslig prövning som står till buds inom ramen för 2016 års lag om utredningsbefogenheter beskrivs i skälen 263–269 nedan.

⁽²⁵²⁾ I avsnitt 166 i 2018 års dataskyddslag hänvisas särskilt till följande situationer: a) *The Commissioner* underlåter att vidta lämpliga åtgärder för att besvara klagomålet, b) han eller hon underlåter att informera den klagande om hur ärendet fortskrider eller om resultatet av klagomålet före utgången av den period på 3 månader som började vid mottagandet av klagomålet eller c) om hans eller hennes behandling av klagomålet inte avslutas under den perioden inte ger klaganden sådan information under en senare period på 3 månader.

⁽²⁵³⁾ *The First Tier Tribunal* är behörig att handlägga överklaganden av beslut som fattats av statliga tillsynsorgan. När det gäller ett beslut av *the Information Commissioner* är den behöriga avdelningen "General Regulatory Chamber" som är behörig i hela Förenade kungariket.

⁽²⁵⁴⁾ Avsnitt 166 i 2018 års dataskyddslag. Exempel på framgångsrika åtgärder mot ICO vid domstolen är ett fall där ICO bekräftade mottagandet av ett klagomål från en registrerad men inte angav vilka åtgärder den avsåg att vidta och därför beordrades att inom 21 kalenderdagar bekräfta huruvida den skulle utreda klagomålen och, om så var fallet, informera klaganden om hur utredningen fortskrider minst var 21:e kalenderdag (domen har ännu inte offentliggjorts) och ett ärende där *the First Tier Tribunal* ansåg att det var oklart om det var fråga om ett svar från ICO till en klagande utgjorde "resultatet" av klagomålet (se Susan Milne/*The Information Commissioner* [2020], domen finns på följande länk: <https://informationrights.decisions.tribunals.gov.uk/DBFiles/Decision/i2730/Milne,%20S%20-%20QJ2020-0296-GDPR-V.%20051220%20Section%20166%20DPA%20-DECISION.pdf>)

⁽²⁵⁵⁾ Avsnitten 162 och 163 i 2018 års dataskyddslag.

⁽²⁵⁶⁾ Se till exempel *Brown/Commissioner of Police of the Metropolis* [2019] EWCA Civ 1724 där skadestånd på 9 000 pund utdömdes enligt dataskyddslagen från 1998 och *Human Rights Act 1998* för olagligt inhämtande och missbruk av personuppgifter och *R (on the application of Bridges)/Chief Constable of South Wales* [2020] EWCA Civ 1058 där appellationsdomstolen förklarade att det var olagligt att använda ett system för ansiktsigenkänning av walesiska polisen eftersom det stred mot artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna och den konsekvensbedömning avseende dataskydd som gjorts av den personuppgiftsansvariga inte uppfyllde 2018 års dataskyddslag.

⁽²⁵⁷⁾ I artikel 34 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna föreskrivs att "domstolen får ta emot ansökningar från personer, icke-statliga organisationer eller grupper av enskilda som påstår sig ha blivit utsatta för en kränkning från någon av de höga fördragsslutande parterna av de rättigheter som anges i konventionen eller dess protokoll. De höga fördragsslutande parterna förbinder sig att inte på något sätt hindra ett effektivt utövande av denna rättighet".

3.3 Tillgång till och användning av brittiska myndigheter för ändamål som rör nationell säkerhet

- (175) I Förenade kungarikets rättsordning är de underrättelsetjänster som har befogenhet att samla in elektronisk information som innehas av personuppgiftsansvariga eller personuppgiftsbiträden av nationella säkerhetsskäl, i situationer som är relevanta för ett adekvat scenario, *the Security Service* ⁽²⁵⁸⁾ (MI5), *the Secret Intelligence Service* ⁽²⁵⁹⁾ (SIS) och *the Government Communications Headquarters* ⁽²⁶⁰⁾ (GCHQ) ⁽²⁶¹⁾.

3.3.1 Rättsliga grunder, begränsningar och skyddsåtgärder

- (176) I Förenade kungariket definieras underrättelsetjänsternas befogenheter i 2016 års lag om utredningsbefogenheter och 2000 års lag om utredningsbefogenheter som tillsammans med 2018 års dataskyddslag fastställer det materiella och personliga tillämpningsområdet för dessa befogenheter samt begränsningar och skyddsåtgärder för utövandet av dem. Dessa befogenheter samt de begränsningar och skyddsåtgärder som är tillämpliga på dem bedöms i detalj i följande avsnitt.

3.3.1.1 Utredningsbefogenheter som utövas inom ramen för nationell säkerhet

- (177) 2016 års lag om utredningsbefogenheter utgör den rättsliga ramen för användningen av utredningsbefogenheter, dvs. befogenhet att avlyssna, få tillgång till kommunikationsuppgifter och utföra ingrepp i utrustningen. 2016 års lag om utredningsbefogenheter inför ett allmänt förbud och gör det straffbart att använda teknik som möjliggör åtkomst till kommunikationsinnehåll, åtkomst till kommunikationsuppgifter eller ingrepp i utrustning utan laglig auktoritet ⁽²⁶²⁾. Detta återspeglas i det faktum att användningen av dessa utredningsbefogenheter endast är laglig när den utförs på grundval av ett beslut eller ett tillstånd ⁽²⁶³⁾.
- (178) I 2016 års lag om utredningsbefogenheter fastställs detaljerade bestämmelser om omfattningen och tillämpningen av varje utredningsbefogenhet samt respektive begränsningar och skyddsåtgärder. Olika regler gäller beroende på vilken typ av utredningsbefogenheter det rör sig om (avlyssning av kommunikation,

⁽²⁵⁸⁾ MI5 lyder under inrikesministern. I *Security Services Act 1989* anges MI5:s uppgifter som är att skydda den nationella säkerheten (inbegripet skydd mot hot från spionage, terrorism och sabotage från verksamhet som bedrivs av utländska makter och från åtgärder som syftar till att störta eller undergräva den parlamentariska demokratin med politiska, industriella eller våldsamma medel), skydda Förenade kungarikets ekonomiska välbefinnande mot externa hot och stödja polisens och andra brottsbekämpande organs verksamhet för att förebygga och upptäcka allvarliga brott.

⁽²⁵⁹⁾ SIS lyder under utrikesministern och dess funktioner fastställs i *Intelligence Services Act 1994*. Dess uppgifter är att inhämta och tillhandahålla information om handlingar eller avsikter för personer utanför de brittiska öarna och att utföra andra uppgifter som rör dessa personers handlingar eller avsikter. Dessa funktioner kan endast utövas med hänsyn till den nationella säkerheten, till förmån för Förenade kungarikets ekonomiska välbefinnande eller till att förebygga eller upptäcka allvarliga brott.

⁽²⁶⁰⁾ GCHQ lyder under utrikesministern och dess funktioner fastställs i *Intelligence Services Act 1994*. Dessa är a) att övervaka, använda eller göra ingrepp i elektromagnetisk och annan emission och utrustning som producerar sådan emission, att erhålla och tillhandahålla information som härrör från eller rör sådana emissioner eller sådan utrustning och från krypterat material, b) ge råd och stöd om språk, inbegripet terminologi som används i tekniska frågor och kryptografi och andra frågor som rör skydd av information till försvarsmakten, till regeringen eller andra organisationer eller personer som anses lämpliga. Dessa funktioner kan endast utövas med hänsyn till den nationella säkerheten, till förmån för Förenade kungarikets ekonomiska välbefinnande i förhållande till handlingar eller avsikter för personer utanför de brittiska öarna eller till stöd för förebyggande eller upptäckt av allvarliga brott.

⁽²⁶¹⁾ Andra offentliga organ som utför uppgifter som är relevanta för den nationella säkerheten är *Defence Intelligence (DI)*, *National Security Council and Secretariat*, *Joint Intelligence Organisation* och *Joint Intelligence Committee*. Varken *Joint Intelligence Committee* eller *Joint Intelligence Organisation* kan dock utnyttja utredningsbefogenheterna inom ramen för 2016 års lag om utredningsbefogenheter medan *Defence Intelligence* har begränsade möjligheter att utöva sina befogenheter.

⁽²⁶²⁾ Förbudet gäller både offentliga och privata kommunikationsnät samt den offentliga posttjänsten när avlyssningen sker i Förenade kungariket. Förbudet gäller inte den personuppgiftsansvariga för det privata nätverket om den personuppgiftsansvariga har gett uttryckligt eller underförstått samtycke till att avlyssningen utförs (avsnitt 3 i 2016 års lag om utredningsbefogenheter).

⁽²⁶³⁾ I särskilda begränsade fall är laglig avlyssning utan beslut möjlig, dvs. när avlyssning sker med avsändarens eller mottagarens samtycke (avsnitt 44 i 2016 års lag om utredningsbefogenheter), vid begränsade administrativa ändamål eller verkställighetsändamål (avsnitten 45–48 i 2016 års lag om utredningsbefogenheter), vid vissa särskilda institutioner (avsnitten 49–51 i 2016 års lag om utredningsbefogenheter) och i enlighet med framställningar från andra länder (avsnitt 52 i 2016 års lag om utredningsbefogenheter).

inhämtande och lagring av kommunikationsuppgifter och ingrepp i utrustning)⁽²⁶⁴⁾ samt huruvida befogenheten utövas på ett visst mål eller i massomfattning. Uppgifter om tillämpningsområde, skyddsåtgärder och begränsningar för varje åtgärd enligt 2016 års lag om utredningsbefogenheter anges i ett särskilt avsnitt nedan.

- (179) Dessutom kompletteras 2016 års lag om utredningsbefogenheter med ett antal lagstadgade uppförandekoder, utfärdade av den ansvariga ministern, godkända av båda kamrarna i parlamentet⁽²⁶⁵⁾ och tillämpliga i hela landet, som ger ytterligare vägledning om hur dessa befogenheter ska användas⁽²⁶⁶⁾. Även om registrerade direkt kan förlita sig till bestämmelserna i 2016 års lag om utredningsbefogenheter för att utöva sina rättigheter, föreskriver punkt 5 i tillägg 7 till lagen att uppförandekoderna är tillåtna som bevis i civilrättsliga och straffrättsliga förfaranden och att domstolen eller tillsynsmyndigheten får ta hänsyn till bristande efterlevnad av uppförandekoderna när den avgör en relevant fråga i rättsliga förfaranden⁽²⁶⁷⁾. I samband med bedömningen av "lagstiftningens kvalitet" i Förenade kungarikets tidigare lagstiftning på övervakningsområdet, dvs. 2000 års lag om utredningsbefogenheter, bekräftade Europeiska domstolen för de mänskliga rättigheterna (stora avdelningen) uttryckligen de brittiska uppförandekodernas relevans och godtog att bestämmelserna kunde beaktas i bedömningen av förutsägbarheten hos den lagstiftning som tillåter övervakning av⁽²⁶⁸⁾.
- (180) Det bör noteras att riktade befogenheter (riktad avlyssning⁽²⁶⁹⁾, inhämtande av kommunikationsuppgifter⁽²⁷⁰⁾, lagring av kommunikationsuppgifter⁽²⁷¹⁾ och riktade ingrepp i utrustning⁽²⁷²⁾) är tillgängliga för nationella säkerhetsmyndigheter⁽²⁷³⁾ och vissa brottsbekämpande myndigheter, medan endast underrättelsetjänster får använda sig av "massbefogenheter" (dvs. massavlyssning⁽²⁷⁴⁾, massinhämtning av kommunikationsuppgifter⁽²⁷⁵⁾, massingrepp i utrustning⁽²⁷⁶⁾ och massdataset av personuppgifter⁽²⁷⁷⁾).
- (181) Vid beslut om vilken utredningsbefogenhet som ska användas måste underrättelsetjänsten uppfylla de "allmänna skyldigheter i fråga om integritet" som anges i avsnitt 2.2 a i 2016 års lag om utredningsbefogenheter vilket inbegriper en nödvändighets- och proportionalitetsprövning. Närmare bestämt ska en myndighet som har för avsikt att utnyttja en utredningsbefogenhet enligt denna bestämmelse i) överväga huruvida det som eftersträvas med

⁽²⁶⁴⁾ När det till exempel gäller tillämpningsområdet för sådana åtgärder är åtgärdens tillämpningsområde enligt delarna 3 och 4 (lagring och inhämtande av kommunikationsuppgifter) strikt begränsad till definitionen av "telekommunikationsoperatörer", vars användares uppgifter omfattas av åtgärden. Ett annat exempel är "massbefogenheter". I detta fall begränsas tillämpningsområdet för dessa befogenheter till "kommunikation som sänts eller mottagits av enskilda personer utanför den brittiska ön".

⁽²⁶⁵⁾ I tillägg 7 till 2016 års lag om utredningsbefogenheter fastställs uppförandekodernas tillämpningsområde, det förfarande som ska följas vid utfärdandet av dem, reglerna för översyn av dem och kodernas verkan.

⁽²⁶⁶⁾ Riktlinjerna för uppförandekoderna inom ramen för 2016 års lag om utredningsbefogenheter, finns på följande länk: <https://www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice>.

⁽²⁶⁷⁾ Domstolarna och tribunalerna använder uppförandekoderna för att bedöma om myndigheternas agerande är lagenligt. Se exempelvis följande: Dias/Cleveland Police, [2017] UKIPTrib15_586-CH, där tribunalen för utredningsbefogenheter (*Investigatory Powers Tribunal*) hänvisade till specifika avsnitt i uppförandekoden om kommunikationsuppgifter för att förstå definitionen av grunden "förebygga eller upptäcka brott eller förebygga störningar" som används för att ansöka om inhämtande av kommunikationsuppgifter. Koderna ingick i motiveringen för att fastställa huruvida denna grund hade använts på ett felaktigt sätt. Domstolen slog därefter fast att de omtvistade beteckningarna var rättsstridiga. Domstolarna har också utvärderat skyddsnivån i lagarna, se t.ex. *Just for Law Kids/Secretary of State for the Home Department* [2019] EWHC 1772 (Admin), där överdomstolen (High Court) fann att primär- och sekundärrätten tillsammans med den interna vägledningen gav tillräckliga garantier. Eller *R (National Council for Civil Liberties)/Secretary of State for the Home Department & Annor* [2019] EWHC 2057 (Admin) där den fann att både 2016 års lag om utredningsbefogenheter och uppförandekoden om ingrepp i utrustning innehöll tillräckliga bestämmelser om behovet av specifika fullmakter.

⁽²⁶⁸⁾ I målet *Big Brother Watch* konstaterade Europeiska domstolen för de mänskliga rättigheterna (stora avdelningen) att "IC-koden är en offentlig handling som har antagits av båda kamrarna i parlamentet och offentliggörs av regeringen på nätet och i en tryckt version, som måste beaktas både av de personer som utövar avlyssningsbefogenheter och av domstolarna (se punkterna 93–94). Till följd av detta har domstolen godtagit att dess bestämmelser får beaktas i bedömningen av förutsägbarheten hos lagen om utredningsbefogenheter (se Kennedy, citerad ovan, § 157). Domstolen godtog således att den inhemska lagstiftningen var tillräckligt 'tillgänglig' (se Europeiska domstolen för de mänskliga rättigheterna (stora avdelningen), *Big Brother Watch m.fl./United Kingdom*, ansökningar nr 58170/13, 62322/14 och 24960/15 av den 25 maj 2021, punkt 366).

⁽²⁶⁹⁾ Del 2 i 2016 års lag om utredningsbefogenheter.

⁽²⁷⁰⁾ Del 3 i 2016 års lag om utredningsbefogenheter.

⁽²⁷¹⁾ Del 4 i 2016 års lag om utredningsbefogenheter.

⁽²⁷²⁾ Del 5 i 2016 års lag om utredningsbefogenheter.

⁽²⁷³⁾ En förteckning över relevanta brottsbekämpande myndigheter som kan tillämpa riktade utredningsbefogenheter inom ramen för 2016 års lag om utredningsbefogenheter finns i fotnot (139).

⁽²⁷⁴⁾ Avsnitt 136 i 2016 års lag om utredningsbefogenheter.

⁽²⁷⁵⁾ Avsnitt 158 i 2016 års lag om utredningsbefogenheter.

⁽²⁷⁶⁾ Avsnitt 176 i 2016 års lag om utredningsbefogenheter.

⁽²⁷⁷⁾ Avsnitt 199 i 2016 års lag om utredningsbefogenheter.

beslutet, tillståndet eller föreläggandet rimligen skulle kunna uppnås med andra mindre ingripande medel, ii) huruvida den skyddsnivå som ska tillämpas vid inhämtande av information enligt beslutet, tillståndet eller föreläggandet är högre på grund av informationens särskilda känslighet, iii) allmänintresset av telekommunikations-systemens och posttjänsternas integritet och säkerhet och iv) alla andra aspekter av allmänintresset av integritetsskydd⁽²⁷⁸⁾.

(182) Det sätt på vilket dessa kriterier ska tillämpas – och det sätt på vilket deras efterlevnad bedöms som en del av den ansvariga ministerns och *the Judicial Commissioners* tillstånd att använda sådana befogenheter – specificeras närmare i de relevanta uppförandekoderna. I synnerhet måste användningen av en av dessa utredningsbefogenheter alltid stå i "proportion till vad som eftersträvas [vilket] involverar en avvägning mellan allvaret i intrånget i den personliga integriteten (och andra överväganden som anges i avsnitt 2.2) och behovet av utredningsåtgärder, operativa åtgärder eller förmågor". Detta innebär i synnerhet att det "bör erbjuda realistiska utsikter att ge den förväntade nyttan och inte vara oproportionerligt eller godtyckligt" och att "[i]nget intrång i privatlivet bör anses vara proportionerligt om den information som efterfrågas rimligen kan erhållas med andra mindre inkräktande medel"⁽²⁷⁹⁾. Närmare bestämt ska iakttagandet av proportionalitetsprincipen bedömas med beaktande av "i) omfattningen av det föreslagna intrånget i privatlivet i förhållande till vad som är avsett att uppnås, ii) hur och varför de metoder som ska antas kommer att orsaka minsta möjliga ingrepp för personen och andra, iii) huruvida verksamheten är en lämplig användning av lagen och ett rimligt sätt att, efter att ha övervägt alla rimliga alternativ, uppnå det som eftersträvas, iv) vilka andra metoder, beroende på vad som är lämpligt, som antingen inte har genomförts eller har använts men som bedöms vara otillräckliga för att uppfylla de operativa målen utan användning av den föreslagna utredningsbefogenheten"⁽²⁸⁰⁾.

(183) I praktiken, vilket de brittiska myndigheterna förklarar, säkerställer detta att en underrättelsetjänst, för det första, fastställer det operativa målet (och därmed avgränsar insamlingen, t.ex. ett internationellt terrorismbekämpningsändamål i ett specifikt geografiskt område) och, för det andra, på grundval av detta operativa mål måste överväga vilket tekniskt alternativ (t.ex. riktad avlyssning eller massavlyssning, ingrepp i utrustning, inhämtande av kommunikationsuppgifter) som är mest proportionerligt (dvs. det minst inkräktande på integriteten, jfr avsnitt 2.2 i *Investigatory Powers Act*) mot vad som är tillåtet enligt en av de lagstadgade grunderna och som därför kan uppnås.

(184) Det är värt att notera att denna hänvisning till normer för nödvändighet och proportionalitet också har noterats och välkomnats av Joseph Cannataci, FN:s särskilde rapportör för rätten till integritet, som i fråga om det system som inrättats genom 2016 års lag om utredningsbefogenheter konstaterade att "[d]e förfaranden som tillämpas både inom underrättelsetjänsterna och inom de brottsbekämpande organen förefaller kräva systematiskt att man överväger om en övervakningsåtgärd eller en övervakningsuppgift är nödvändig och proportionerlig innan den rekommenderas för godkännande samt en översyn av den på samma grunder"⁽²⁸¹⁾. Han påpekade också att han vid sitt möte med företrädare för brottsbekämpande myndigheter och nationella säkerhetsmyndigheter "hade en samsyn om att rätten till integritet måste vara en grundläggande fråga för alla beslut om övervakningsåtgärder. Alla tolkade och uppskattade nödvändigheten och proportionaliteten som de grundläggande principer som ska beaktas".

⁽²⁷⁸⁾ I uppförandekoden om avlyssning av kommunikation anges att andra delar av proportionalitetsprövningen är "i) omfattningen av det föreslagna intrånget i privatlivet i förhållande till vad som är avsett att uppnås, ii) hur och varför de metoder som ska antas kommer att orsaka minsta möjliga ingrepp för personen och andra, iii) huruvida verksamheten är en lämplig användning av lagen och ett rimligt sätt att, efter att ha övervägt alla rimliga alternativ, uppnå det som eftersträvas, iv) vilka andra metoder, beroende på vad som är lämpligt, som antingen inte har genomförts eller har använts men som bedöms vara otillräckliga för att uppfylla de operativa målen utan användning av den föreslagna utredningsbefogenheten". Uppförandekoden om avlyssning av kommunikation, punkt 4.16, finns på följande länk: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

⁽²⁷⁹⁾ Se uppförandekoden om avlyssning av kommunikation, punkterna 4.12 och 4.15, som finns på följande länk: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

⁽²⁸⁰⁾ Se uppförandekoden om avlyssning av kommunikation, punkt 4.16.

⁽²⁸¹⁾ Avslutande uppdragsrapport från den särskilda rapportören om rätten till integritet vid avslutande av hans eller hennes uppdrag i Förenade konungariket Storbritannien och Nordirland och den finns på följande länk: <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E>, punkt 1.a.

- (185) De särskilda kriterierna för utfärdande av de olika beslut samt de begränsningar och skyddsåtgärder som fastställs i 2016 års lag om utredningsbefogenheter för varje utredningsbefogenhet anges i skälen 186–243.

3.3.1.1.1 Riktad avlyssning och granskning

- (186) Det finns tre typer av beslut för riktad avlyssning: beslut om riktad avlyssning ⁽²⁸²⁾, beslut om riktad granskning och beslut om ömsesidigt bistånd ⁽²⁸³⁾. Villkoren för att erhålla sådana beslut och relevanta skyddsåtgärder anges i del 2 kapitel 1 i 2016 års lag om utredningsbefogenheter.
- (187) Ett beslut om riktad avlyssning tillåter avlyssning av de meddelanden som beskrivs i beslutet i samband med överföring och inhämtande av andra uppgifter som är relevanta för denna kommunikation ⁽²⁸⁴⁾, inbegripet sekundära uppgifter ⁽²⁸⁵⁾. Ett riktat beslut om granskning ger en person rätt att göra urvalet för granskning av avlyssnat innehåll som erhållits inom ramen för ett beslut om massavlyssning ⁽²⁸⁶⁾.
- (188) Varje beslut enligt del 2 i 2016 års lag om utredningsbefogenheter kan utfärdas av den ansvariga ministern ⁽²⁸⁷⁾ och godkännas av en *Judicial Commissioner* ⁽²⁸⁸⁾. I samtliga fall är varaktigheten för varje typ av riktat beslut begränsad till 6 månader ⁽²⁸⁹⁾ och särskilda regler gäller för ändring ⁽²⁹⁰⁾ och förnyelse av ett sådant beslut ⁽²⁹¹⁾.
- (189) Innan den ansvariga ministern utfärdar beslutet måste han eller hon göra en nödvändighets- och proportionalitetsbedömning ⁽²⁹²⁾. När det gäller ett beslut om riktad avlyssning och ett beslut om riktad undersökning bör den ansvariga ministern särskilt kontrollera om åtgärden är nödvändig på grund av nationella säkerhetsintressen, förebyggande eller avslöjande av allvarliga brott eller ett intresse för Förenade kungarikets ⁽²⁹³⁾ ekonomiska välbefinnande i den mån dessa intressen även är relevanta för den nationella säkerheten ⁽²⁹⁴⁾. Å andra sidan kan ett beslut om ömsesidigt bistånd (se skäl 139 ovan) utfärdas endast om den ansvariga ministern anser att omständigheterna är likvärdiga med dem under vilka han eller hon skulle utfärda ett beslut i syfte att förebygga och eller upptäcka allvarlig brottslighet ⁽²⁹⁵⁾.
- (190) Dessutom ska den ansvariga ministern bedöma huruvida åtgärden står i proportion till vad som är avsett att uppnås ⁽²⁹⁶⁾. Vid bedömningen av huruvida de begärda åtgärderna är proportionerliga måste hänsyn tas till de allmänna skyldigheter i fråga om personlig integritet som anges i avsnitt 2.2 i 2016 års lag om utredningsbefogenheter, särskilt behovet av att bedöma huruvida det som eftersträvas med beslutet, tillståndet eller föreläggandet

⁽²⁸²⁾ Avsnitt 15.2 i 2016 års lag om utredningsbefogenheter.

⁽²⁸³⁾ Avsnitt 15.4 i 2016 års lag om utredningsbefogenheter.

⁽²⁸⁴⁾ Avsnitt 15.2 i 2016 års lag om utredningsbefogenheter.

⁽²⁸⁵⁾ Sekundära uppgifter är uppgifter som bifogas eller logiskt förknippas med den avlyssnade kommunikationen, kan logiskt skiljas från den och skulle, om de vore åtskilda på detta sätt, inte avslöja något av vad som rimligen kan anses vara innebörden av meddelandet (i förekommande fall). Några exempel på sekundära data är routerkonfigurationer, brandväggar eller den tidsperiod under vilken en router har varit aktiv i ett nätverk som den ingår i, är kopplad till eller är logiskt förknippad med avlyssnad kommunikation. För närmare uppgifter se definitionen i avsnitt 16 i 2016 års lag om utredningsbefogenheter och uppförandekoden om avlyssning av kommunikation, punkt 2.19, se fotnot 278.

⁽²⁸⁶⁾ Denna granskning görs som ett undantag i avsnitt 152.4 i 2016 års lag om utredningsbefogenheter där det föreskrivs ett förbud mot att försöka identifiera enskilda personer som befinner sig på de brittiska öarna. Se skäl 229.

⁽²⁸⁷⁾ *The Scottish Minister* godkänner beslutet när det avser grov brottslig verksamhet i Skottland (se avsnitt 21 och avsnitt 22 i 2016 års lag om utredningsbefogenheter) medan en högre tjänsteman kan utses av den ansvariga ministern för att utfärda ett beslut om ömsesidigt bistånd när det visar sig att avlyssningen kommer att gälla en person eller lokaler utanför Förenade kungariket (avsnitt 40 i 2016 års lag om utredningsbefogenheter).

⁽²⁸⁸⁾ Avsnitten 19 och 23 i 2016 års lag om utredningsbefogenheter.

⁽²⁸⁹⁾ Avsnitt 32 i 2016 års lag om utredningsbefogenheter.

⁽²⁹⁰⁾ Avsnitt 39 i 2016 års lag om utredningsbefogenheter. Begränsade ändringar av beslut kan göras av föreskrivna personer på de villkor som anges i 2016 års lag om utredningsbefogenheter. Den person som utfärdade beslutet kan när som helst upphäva det. De ska göra detta om beslutet inte längre är nödvändig av relevanta skäl eller om det beteende som bemyndigats genom beslutet inte längre står i proportion till vad som eftersträvas.

⁽²⁹¹⁾ Avsnitt 33 i 2016 års lag om utredningsbefogenheter. Beslutet att förnya beslutet måste godkännas av en *Judicial Commissioner*.

⁽²⁹²⁾ Avsnitt 19 i 2016 års lag om utredningsbefogenheter.

⁽²⁹³⁾ När det gäller begreppet "Förenade kungarikets ekonomiska välbefinnandes intressen" när dessa intressen också är relevanta för den nationella säkerheten", ansåg Europadomstolens i målet *Big Brother Watch* (punkt 371) att detta begrepp var tillräckligt inriktat på nationell säkerhet (se fotnot 268). Domstolens slutsats i detta mål rörde tillämpningen av detta begrepp i 2000 års lag om utredningsbefogenheter, men samma begrepp används i 2016 års lag om utredningsbefogenheter.

⁽²⁹⁴⁾ Avsnitt 20.2 i 2016 års lag om utredningsbefogenheter.

⁽²⁹⁵⁾ Avsnitt 20.3 i 2016 års lag om utredningsbefogenheter.

⁽²⁹⁶⁾ Avsnitten 19.1 b, 19.2 b och 19.3 b i 2016 års lag om utredningsbefogenheter.

rimligen skulle kunna uppnås med andra mindre inkräktande medel och huruvida den skyddsnivå som ska tillämpas vid inhämtande av information enligt beslutet är högre på grund av den särskilda känsligheten hos denna information (se skäl 181 ovan).

- (191) För detta ändamål måste ministern beakta alla delar av ansökan som lämnats in av den myndighet som lämnar in begäran, särskilt de som rör de personer som ska avlyssnas och åtgärdens relevans för utredningen. Sådana inslag anges i uppförandekoden om avlyssning av kommunikation och måste beskrivas på en viss nivå av specifik karaktär ⁽²⁹⁷⁾. Dessutom krävs det i avsnitt 17 i 2016 års lag om utredningsbefogenheter att varje beslut som utfärdas enligt dess kapitel 2 ska namnge eller beskriva den specifika person eller grupp av personer, organisationer eller lokaler som ska avlyssnas (målet). Vid ett beslut om riktad avlyssning eller ett beslut om riktad granskning kan dessa även avse en grupp av personer, mer än en person eller organisation eller fler än ett komplex av lokaler (även kallat tematiskt beslut) ⁽²⁹⁸⁾. I dessa fall bör beslutet beskriva det gemensamma syftet eller den gemensamma aktiviteten eller verksamheten/utredningarna och ange eller beskriva så många av dessa personer/organisationer eller komplex av lokaler där detta rimligen är praktiskt genomförbart ⁽²⁹⁹⁾. Slutligen ska alla beslut som utfärdas enligt del 2 i 2016 års lag om utredningsbefogenheter innehålla uppgifter om adresser, nummer, apparatur, faktorer eller kombinationer av faktorer som ska användas för att identifiera kommunikationen ⁽³⁰⁰⁾. I detta avseende anges det i uppförandekoden om avlyssning att när det rör sig om beslut om riktad avlyssning och beslut om riktad granskning "måste det i beslutet specificeras (eller beskrivas) vilka faktorer eller kombinationer av faktorer som ska användas för att identifiera kommunikationen. Om kommunikationen ska identifieras med hjälp av ett telefonnummer (till exempel) måste numret specificeras genom att det i sin helhet anges. Men när mycket komplexa eller ständigt föränderliga internetväljare ska användas för att identifiera kommunikationen bör dessa valörer beskrivas så långt det är möjligt" ⁽³⁰¹⁾.
- (192) En viktig garanti i detta sammanhang är att den bedömning som den ansvariga ministern gör för att utfärda ett beslut måste godkännas av en oberoende *Judicial Commissioner* ⁽³⁰²⁾ som framför allt kontrollerar om beslutet om att godkänna husrannsakan är förenligt med nödvändighets- och proportionalitetsprinciperna ⁽³⁰³⁾ (vad gäller den ställning och roll som *the Judicial Commissioner* har, se skälen 251–256 nedan). I 2016 års lag om utredningsbefogenheter klargörs också att *the Judicial Commissioner*, när han eller hon utför en sådan kontroll, måste tillämpa samma principer som en domstol skulle tillämpa vid en ansökan om rättslig prövning ⁽³⁰⁴⁾. Detta säkerställer att efterlevnaden av nödvändighets- och proportionalitetsprinciperna systematiskt kontrolleras av ett oberoende organ i varje enskilt fall och innan tillgången till uppgifter äger rum.
- (193) I 2016 års lag om utredningsbefogenheter föreskrivs ett fåtal specifika och snäva undantag från utförandet av riktad avlyssning utan beslut. Dessa begränsade fall anges i lagen ⁽³⁰⁵⁾ och förutom det beslut som baseras på sändarens/mottagarens "samtycke", utförs de av andra personer (privata eller offentliga organ) än personer vid de nationella säkerhetsmyndigheterna. Denna typ av avlyssningar utförs dessutom för andra ändamål än insamling av "underrättelseuppgifter" ⁽³⁰⁶⁾, och i vissa fall är det mycket osannolikt att insamlingen kan ske inom ramen för ett

⁽²⁹⁷⁾ Den begärda informationen omfattar uppgifter om bakgrunden (beskrivning av personer/organisationer/uppsättningar av lokaler, den kommunikation som ska avlyssnas) och hur inhämtandet av dessa uppgifter kommer att gynna utredningen samt en beskrivning av det beteende som ska godkännas. Om det inte är möjligt att beskriva personerna/organisationen/lokalerna måste en förklaring lämnas om varför det inte var möjligt eller varför endast en allmän beskrivning gjordes (uppförandekoden om avlyssning av kommunikation, punkterna 5.32 och 5.34, se fotnot 278).

⁽²⁹⁸⁾ Avsnitt 17.2 i 2016 års lag om utredningsbefogenheter. Se även uppförandekoden för avlyssning av kommunikation, punkt 5.11 och följande, se fotnot 278.

⁽²⁹⁹⁾ Avsnitt 31.4 och 5 i 2016 års lag om utredningsbefogenheter.

⁽³⁰⁰⁾ Avsnitt 31.8 i 2016 års lag om utredningsbefogenheter.

⁽³⁰¹⁾ *Code of Practice on Interception of Communications*, punkterna 5.37 och 5.38, se fotnot 278.

⁽³⁰²⁾ Ett godkännande av en rättslig myndighet krävs inte när den ansvariga ministern anser att det finns ett brådskande behov av att utfärda beslutet (avsnitt 19.1 i 2016 års lag om utredningsbefogenheter). *The Judicial Commissioner* måste dock informeras på kort tid och måste besluta om huruvida beslutet ska godkännas eller inte. Om så inte är fallet upphör beslutet att gälla (avsnitt 24 och 25 i 2016 års lag om utredningsbefogenheter).

⁽³⁰³⁾ Avsnitt 23.1 i 2016 års lag om utredningsbefogenheter.

⁽³⁰⁴⁾ Avsnitt 23.2 i 2016 års lag om utredningsbefogenheter.

⁽³⁰⁵⁾ Se avsnitt 44–51 i 2016 års lag om utredningsbefogenheter och avsnitt 12 i *Interception Communication Code of Practice* (se fotnot 278).

⁽³⁰⁶⁾ Så är t.ex. fallet om avlyssning är nödvändig vid en psykiatrisk klinik eller i ett fängelse (för att övervaka en anhållen persons eller en patients beteende) eller av en post- eller telekommunikationsoperatör, t.ex. för att upptäcka kränkande innehåll.

”överföringsscenario” (t.ex. vid avlyssning som utförs vid en psykiatrisk klinik eller i ett fängelse). Med tanke på den typ av organ som dessa särskilda fall gäller (andra organ än nationella säkerhetsmyndigheter) är alla skyddsåtgärder i del 2 i 2018 års dataskyddslag och den brittiska dataskyddsförordningen tillämpliga, även vad gäller ICO:s tillsyn och tillgängliga rättsliga prövningsmekanismer. Utöver skyddsåtgärderna enligt 2018 års dataskyddslag föreskriver dessutom 2016 års lag om utredningsbefogenheter i vissa fall befogenheter för IPCO:s efterhandstillsyn ⁽³⁰⁷⁾.

- (194) När avlyssning utförs är ytterligare begränsningar och skyddsåtgärder tillämpliga mot bakgrund av den eller de avlyssnade personernas status ⁽³⁰⁸⁾. Avlyssning av ärenden som omfattas av rättsliga privilegier är till exempel endast tillåten om det föreligger exceptionella och tvingande omständigheter, den person som utfärdar beslutet måste ta hänsyn till allmänintresset av att ärenden som omfattas av tystnadsplikt behandlas konfidentiellt och att det finns särskilda krav för hantering, lagring och utlämnande av sådant material ⁽³⁰⁹⁾.
- (195) I 2016 års lag om utredningsbefogenheter föreskrivs dessutom särskilda skyddsåtgärder i fråga om säkerhet, lagring och utlämnande som den ansvariga ministern bör beakta innan en riktat beslut utfärdas ⁽³¹⁰⁾. I synnerhet föreskrivs i avsnitt 53.5 i 2016 års lag om utredningsbefogenheter att varje kopia av det material som samlats in inom ramen för beslutet ska förvaras på ett säkert sätt och förstöras så snart det inte längre finns några relevanta skäl att behålla det medan det i avsnitt 53.2 i 2016 års lag om utredningsbefogenheter föreskrivs att antalet personer till vilka materialet lämnas ut och i vilken utsträckning allt material lämnas ut, görs tillgängligt eller kopieras ska begränsas till vad som är absolut nödvändigt för de lagstadgade ändamålen.
- (196) När slutligen det material som har avlyssnats antingen genom ett beslut om riktad avlyssning eller genom ett beslut om ömsesidigt bistånd ska överlämnas till ett tredjeland (”utlämnanden till utlandet”) föreskrivs i 2016 års lag om utredningsbefogenheter att den ansvariga ministern ska se till att lämpliga åtgärder vidtas för att säkerställa att liknande garantier för säkerhet, lagring och utlämnande finns i det tredjelandet ⁽³¹¹⁾. Enligt avsnitt 109.2 i 2018 års dataskyddslag får underrättelsetjänster endast överföra personuppgifter utanför Förenade kungarikets territorium om överföringen är nödvändig och proportionell med hänsyn till den personuppgiftsansvarigas lagstadgade uppgifter eller för andra ändamål som anges i avsnitt 2.2 a i *Security Services Act 1989* eller avsnitten 2.2 a och 4.2 a i *Intelligence Services Act 1994* ⁽³¹²⁾. Det är viktigt att notera att dessa krav även gäller i situationer där undantaget avseende nationell säkerhet enligt avsnitt 110 i 2018 års dataskyddslag åberopas, eftersom avsnitt 109 inte anges i samma lags avsnitt 110 som en av de bestämmelser som kan upphöra att gälla om ett undantag från vissa bestämmelser krävs för att skydda den nationella säkerheten.

3.3.1.1.2 Riktat inhämtande och lagring av kommunikationsuppgifter

- (197) 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.

⁽³⁰⁷⁾ Se motsatsvis avsnitt 229.4 i lagen om utredningsbefogenheter.

⁽³⁰⁸⁾ I avsnitten 26–29 i 2016 års lag om utredningsbefogenheter införs begränsningar för att erhålla beslut om riktad avlyssning och granskning i samband med avlyssning av kommunikation som sänds av eller är avsedd för en person som är parlamentsledamot (vilket som helst av Förenade kungarikets parlament), avlyssning av saker som omfattas av rättsliga privilegier, avlyssning av kommunikation som den avlyssnande myndigheten anser kommer att vara kommunikation som innehåller konfidentiellt journalistiskt material och när syftet med beslutet är att identifiera eller bekräfta en källa till journalistisk information.

⁽³⁰⁹⁾ Avsnitt 26 i 2016 års lag om utredningsbefogenheter.

⁽³¹⁰⁾ Avsnitt 19.1 i 2016 års lag om utredningsbefogenheter.

⁽³¹¹⁾ Avsnitt 54 i 2016 års lag om utredningsbefogenheter. Skyddsåtgärder avseende utlämnande av material till utländska myndigheter beskrivs närmare i uppförandekoderna: se särskilt punkt 9.26 ff. samt punkt 9.87 i uppförandekoden om avlyssning av kommunikation och punkt 9.33 ff. samt punkt 9.41 i uppförandekoden om ingrepp i utrustning (se fotnot 278).

⁽³¹²⁾ Dessa ändamål är att säkerhetstjänsten ska förebygga eller upptäcka allvarliga brott eller straffrättsliga förfaranden (avsnitt 2.2 a i *Security Services Act 1989*), att underrättelsetjänsten ska skydda den nationella säkerheten, förebygga eller upptäcka allvarliga brott eller straffrättsliga förfaranden (avsnitt 2.2 a i *Intelligence Services Act 1994*) och att *Government Communications Headquarters* svarar för alla straffrättsliga förfaranden (avsnitt 4.2 a i *Intelligence Services Act 1994*). Se även de förklarande anmärkningarna till 2018 års dataskyddslag, som finns på följande länk: <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>.

- (198) Termen "kommunikationsuppgifter" omfattar "vem", "när", "var" och "hur" i en kommunikation men inte innehållet, dvs. vad som sades eller skrevs. Till skillnad från avlyssning syftar inhämtandet och lagringen av kommunikationsuppgifter inte till att få fram innehållet i kommunikationen utan till att erhålla information, t.ex. om abonnenten av en telefonitjänst eller en specificerad räkning. Detta kan omfatta tid och varaktighet för kommunikationen, upphovsmannens och mottagarens nummer eller e-postadress och ibland lokaliseringen av de anordningar från vilka telekommunikationen gjordes ⁽³¹³⁾.
- (199) Det bör noteras att lagring och inhämtande av kommunikationsuppgifter normalt inte gäller personuppgifter om registrerade i EU som överförs till Förenade kungariket enligt detta beslut. Skyldigheten att lagra eller lämna ut kommunikationsuppgifter enligt del 3 och 4 i 2016 års lag om utredningsbefogenheter omfattar uppgifter som samlas in av teleoperatörer i Förenade kungariket direkt från användarna av en telekommunikationstjänst ⁽³¹⁴⁾. Denna typ av "kundtillvänd" behandling omfattar vanligtvis inte en överföring på grundval av detta beslut, dvs. en överföring från en personuppgiftsansvarig/ett personuppgiftsbiträde i EU till en personuppgiftsansvarig/ett personuppgiftsbiträde i Förenade kungariket.
- (200) För fullständighetens skull analyseras dock de villkor och skyddsåtgärder som gäller för dessa system för inhämtande och lagring i följande skäl.
- (201) Som en förutsättning måste det noteras att lagringen och riktat inhämtande av kommunikationsuppgifter finns tillgängliga både för nationella säkerhetsmyndigheter och vissa brottsbekämpande myndigheter ⁽³¹⁵⁾. Villkoren för att begära lagring och/eller inhämtande av kommunikationsuppgifter kan variera beroende på grunden för att begära en sådan åtgärd, nämligen ändamål som rör nationell säkerhet eller brottsbekämpande ändamål.
- (202) I och med det nya systemet har ett allmänt krav på förhandstillstånd från ett oberoende organ införts. Kravet kommer att gälla i alla situationer där kommunikationsuppgifter lagras och/eller inhämtas (antingen för brottsbekämpande ändamål eller ändamål som rör nationell säkerhet). Efter domstolens dom i målet *Tele2/Watson* ⁽³¹⁶⁾ har dock särskilda skyddsåtgärder införts när åtgärden begärs för brottsbekämpande ändamål. När lagring eller inhämtande av kommunikationsuppgifter begärs för brottsbekämpande ändamål måste förhandstillståndet i synnerhet alltid utfärdas av *the Investigatory Power Commissioner*. Så är inte alltid fallet om åtgärden begärs för ändamål som rör nationell säkerhet, eftersom sådana typer av åtgärder i vissa fall, vilka beskrivs nedan, kan godkännas av olika "tillståndsgivande personer". I det nya systemet har tröskeln för när lagring och inhämtande av kommunikationsuppgifter kan tillåtas dessutom höjts till "grova brott" ⁽³¹⁷⁾.
-
- ⁽³¹³⁾ Kommunikationsuppgifter definieras i avsnitt 261.5 till 2016 års lag om utredningsbefogenheter. Kommunikationsuppgifter delas upp i "händelsedata" (alla data som identifierar eller beskriver en händelse, oavsett om det sker genom hänvisning till dess lokalisering, i eller med hjälp av ett telekommunikationssystem där händelsen består av en eller flera enheter som bedriver en specifik verksamhet vid en viss tidpunkt) och "enhetsuppgifter" (alla data som a) rör i) en enhet, ii) en koppling mellan en telekommunikationstjänst och en enhet eller iii) en koppling mellan någon del av ett telekommunikationssystem och en enhet som b) består av eller inkluderar data som identifierar eller beskriver en enhet (oavsett om det är med hänvisning till enhetens plats eller inte) och c) inte är händelsuppgifter).
- ⁽³¹⁴⁾ Detta följer av definitionen av kommunikationsdata i avsnitt 261.5 i 2016 års lag om utredningsbefogenheter enligt vilken kommunikationsuppgifter innehas eller erhålls av en teleoperatör och avser antingen användaren av en telekommunikationstjänst och tillhandahållandet av denna tjänst, eller omfattas av, ingår som en del av, fogas till eller logiskt förknippas med en kommunikation (se även *Code of Practice on Communications Data* som finns på följande länk https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf, punkterna 2.22–2.33). Dessutom kräver definitionen av teleoperatör i avsnitt 261.10 i 2016 års lag om utredningsbefogenheter att en teleoperatör är en person som erbjuder eller tillhandahåller en telekommunikationstjänst till personer i Förenade kungariket eller som kontrollerar eller tillhandahåller ett telekommunikationssystem som (helt eller delvis) är beläget i eller kontrolleras från Förenade kungariket. Dessa definitioner klargör att skyldigheter enligt 2016 års lag om utredningsbefogenheter inte kan åläggas teleoperatörer vilkas utrustning inte finns i eller kontrolleras från Förenade kungariket och som inte erbjuder eller tillhandahåller tjänster till personer i Förenade kungariket (se även *Code of Practice on Communications Data*, punkt 2.1). Om EU-abonnenter (oavsett om de befinner sig i EU eller i Förenade kungariket) använde sig av tjänster i Förenade kungariket skulle all kommunikation i samband med tillhandahållandet av denna tjänst samlas in direkt av tjänsteleverantören i Förenade kungariket i stället för att bli föremål för en överföring från EU.
- ⁽³¹⁵⁾ De berörda myndigheterna förtecknas i bilaga 4 till 2016 års lag om utredningsbefogenheter och omfattar polisen, underrättelsetjänsterna, vissa ministerier och regeringsministerier, *National Crime Agency*, *Her Majesty's Revenue and Customs*, *Competition and Markets Authority*, *the Information Commissioner*, ambulans, brand- och räddningstjänster samt myndigheter på området för hälsa och livsmedelssäkerhet.
- ⁽³¹⁶⁾ Förenade målen C-203/15 och C-698/15, *Tele2/Watson*, ECLI:EU:C:2016:970).
- ⁽³¹⁷⁾ Se avsnitt 61.7 b vad gäller inhämtande av kommunikationsuppgifter och avsnitt 87.10A för lagring av kommunikationsuppgifter.

i) Tillstånd för erhållande av kommunikationsuppgifter

- (203) Enligt del 3 i 2016 års lag om utredningsbefogenheter har berörda myndigheter rätt att erhålla kommunikationsuppgifter från en teleoperator eller från varje person som kan inhämta och lämna ut sådana uppgifter. Tillståndet får inte tillåta avlyssning av kommunikationsinnehållet⁽³¹⁸⁾ och upphör att gälla efter en månad⁽³¹⁹⁾ med möjlighet till förlängning med ytterligare tillstånd⁽³²⁰⁾. För inhämtande av kommunikationsdata krävs tillstånd från *the Investigatory Powers Commissioner*⁽³²¹⁾ (om dennes status och befogenheter se skälen 250–251 nedan). Så är alltid fallet om inhämtande av kommunikationsuppgifter begärs av en relevant brottsbekämpande myndighet. I avsnitt 61 i 2016 års lag om utredningsbefogenheter föreskrivs dock att när uppgifter inhämtas av hänsyn till den nationella säkerheten eller det ekonomiska välbefinnandet i Förenade kungariket, om de är relevanta för den nationella säkerheten, eller när en ansökan görs av en medarbetare i en underrättelsetjänst enligt avsnitt 61.7 b⁽³²²⁾, får inhämtandet alternativt⁽³²³⁾ godkännas av *the Investigatory Powers Commissioner* eller av en utsedd högre tjänsteman⁽³²⁴⁾. I *the Code of Practice on Communications Data* anges vidare att den utsedda handläggaren måste vara oberoende av den berörda utredningen eller insatsen och ha praktiska kunskaper om människorättsprinciper och människorättslagstiftning, särskilt principerna om nödvändighet och proportionalitet⁽³²⁵⁾. Det beslut som fattas av den utsedda tjänstemannen kommer att bli föremål för den efterhandsöversyn som *the Investigatory Powers Commissioner* utför (se skäl 254 nedan för mer information om den efterhandstillsyn *the Investigatory Powers Commissioner* utövar).
- (204) Tillståndet att inhämta kommunikationsuppgifter grundar sig på en bedömning av åtgärdens nödvändighet och proportionalitet. Närmare bestämt bedöms åtgärdens nödvändighet mot bakgrund av de skäl som anges i lagstiftningen⁽³²⁶⁾. Med tanke på att denna åtgärd är riktad måste den också vara nödvändig för en specifik utredning eller insats⁽³²⁷⁾. Ytterligare krav på bedömningen av åtgärdernas nödvändighet fastställs i uppförandekoden för kommunikationsuppgifter⁽³²⁸⁾. I denna uppförandekod föreskrivs särskilt att den ansökan som lämnas in av den begärande myndigheten ska identifiera minst tre faktorer för att motivera behovet av en sådan begäran och dessa faktorer är i) den händelse som utreds, till exempel ett brott eller en plats där en utsatt försvunnen person befinner sig, ii) den person vars uppgifter begärs, till exempel misstänkta, vittne eller försvunna personer och hur de är kopplade till händelsen och iii) de kommunikationsuppgifter som efterfrågas, till exempel telefonnummer eller IP-adress och hur dessa uppgifter är kopplade till personen och händelsen⁽³²⁹⁾.
- (205) Dessutom måste inhämtande av kommunikationsuppgifter stå i proportion till vad som eftersträvas⁽³³⁰⁾. I *Code of Practice on Communication Data* klargörs att den tillståndsgivande personen vid genomförandet av en sådan bedömning bör göra en avvägning mellan "omfattningen av ingreppet i en persons rättigheter och friheter och en specifik fördel för den utredning eller verksamhet som genomförs av en relevant myndighet i det allmänna intresse" och att med beaktande av alla överväganden i ett enskilt fall "kan ett ingrepp i en enskilds rättigheter fortfarande inte vara motiverat på grund av att den negativa inverkan på en annan enskilds eller en enskilds rättigheter är alltför allvarig". För att specifikt bedöma åtgärdens proportionalitet förtecknas i uppförandekoden

⁽³¹⁸⁾ Avsnitt 60A.6 i 2016 års lag om utredningsbefogenheter.

⁽³¹⁹⁾ Denna period förkortas till tre dagar om tillståndet ges av brådskande skäl (avsnitt 65.3 A i 2016 års lag om utredningsbefogenheter).

⁽³²⁰⁾ Enligt avsnitt 65 i 2016 års lag om utredningsbefogenheter kommer det förnyade tillståndet att gälla i en månad från och med den dag då det nuvarande tillståndet löper ut. Den som har beviljat tillståndet kan när som helst upphäva tillståndet om den anser att kraven inte längre är uppfyllda.

⁽³²¹⁾ Avsnitt 60A.1 i 2016 års lag om utredningsbefogenheter. *Office for Communications Data Authorisations* (OCDA) fullgör denna arbetsuppgift på uppdrag av *the Investigatory Powers Commissioner* (se *Communication Data Codes of Practice*, punkt 5.6).

⁽³²²⁾ Ansökan enligt avsnitt 61.7 b i 2016 års lag om utredningsbefogenheter görs för "ett tillämpligt brottsändamål" enligt avsnitt 61.7 A i 2016 års lag om utredningsbefogenheter "om kommunikationsuppgifterna helt eller delvis är uppgifter om händelser, syftet att förebygga eller upptäcka allvarlig brottslighet, i alla andra fall, syftet att förebygga eller upptäcka brott eller förebygga störningar".

⁽³²³⁾ I uppförandekoden för kommunikationsuppgifter anges följande: "Om en ansökan som rör nationell säkerhet kan göras enligt antingen avsnitt 60A eller avsnitt 61, är det de enskilda myndigheterna som avgör vilken tillståndsväg som är lämpligast i varje enskilt fall. Myndigheter som vill använda den utsedda vägen för högre tjänstemän bör ha tydliga riktlinjer för när denna tillståndsväg är lämplig" (*Code of Practice on Communication Data*, punkt 5.19 som finns på följande länk: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822817/Communications_Data_Code_of_Practice.pdf).

⁽³²⁴⁾ Avsnitt 70.3 i 2016 års lag om utredningsbefogenheter innehåller en definition av "utsedd tjänsteman" som varierar beroende på relevant myndighet (enligt bilaga 4 till 2016 års lag om utredningsbefogenheter).

⁽³²⁵⁾ Närmare uppgifter om den utsedda högre tjänstemannens oberoende ges i uppförandekoden för kommunikationsuppgifter (*Code of Practice on Communications Data*, punkterna 4.12–4.17, se fotnot 323).

⁽³²⁶⁾ Grunderna är i) nationell säkerhet, ii) förebyggande eller avslöjande av brott eller förebyggande av störningar (vid "händelsedata" endast allvarliga brott), iii) av hänsyn till Förenade kungarikets ekonomiska välbefinnande i den mån dessa intressen även är relevanta för den nationella säkerheten, iv) av hänsyn till allmän säkerhet, v) i syfte att förhindra dödsfall eller personskada eller skada på en persons fysiska eller psykiska hälsa eller för att lindra skador på en persons fysiska eller psykiska hälsa, vi) bistå vid utredningar av påstådda justitiemord eller vii) identifiera en avliden person eller person som inte kan identifiera sig på grund av ett visst villkor (avsnitt 61 (7) i 2016 års lag om utredningsbefogenheter).

⁽³²⁷⁾ Avsnitt 60A.1 b i 2016 års lag om utredningsbefogenheter.

⁽³²⁸⁾ Uppförandekoden för kommunikationsuppgifter, punkt 3.3 och följande, se fotnot 323.

⁽³²⁹⁾ Uppförandekoden för kommunikationsuppgifter, punkt 3.13, se fotnot 323.

⁽³³⁰⁾ Avsnitt 60.1 c i 2016 års lag om utredningsbefogenheter.

dessutom ett antal faktorer som bör ingå i den ansökan som den begärande myndigheten lämnar in ⁽³³¹⁾. Dessutom måste särskild hänsyn tas till vilken typ av kommunikationsuppgifter ("entitet" eller "händelsedata" ⁽³³²⁾) som ska inhämtas och företrädare måste ges åt användning av en mindre inkräktande uppgiftskategori ⁽³³³⁾. Uppförandekoden för kommunikationsuppgifter innehåller också särskilda instruktioner för tillstånd som omfattar kommunikationsuppgifter för personer i särskilda yrken (t.ex. läkare, advokater, journalister, parlamentsledamöter eller religiösa ministrar) ⁽³³⁴⁾ som omfattas av ytterligare skyddsåtgärder ⁽³³⁵⁾.

ii) *Föreläggande om lagring av kommunikationsuppgifter*

- (206) Del 4 i 2016 års lag om utredningsbefogenheter innehåller bestämmelser om lagring av kommunikationsuppgifter, särskilt de kriterier som gör det möjligt för den ansvariga ministern att utfärda ett föreläggande om lagring ⁽³³⁶⁾. De skyddsåtgärder som införs genom lagen om utredningsbefogenheter är desamma, vare sig uppgifterna lagras i brottsbekämpningssyfte eller i den nationella säkerhetens intresse.
- (207) Utfärdandet av sådana förelägganden om lagring syftar till att säkerställa att teleoperatörer under en period av högst 12 månader behåller relevanta kommunikationsuppgifter som annars skulle raderas när de inte längre behövs för affärsändamål ⁽³³⁷⁾. Europeiska domstolen för de mänskliga rättigheterna 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 som beskrivs i skälen 203–205.
- (208) Utövandet av befogenheten att ålägga att vissa uppgifter ska lagras omfattas av ett antal begränsningar och skyddsåtgärder. Närmare bestämt kan den ansvariga ministern endast utfärda ett föreläggande om lagring till en eller flera operatörer ⁽³³⁸⁾ endast om han eller hon anser att kravet på lagring av uppgifterna är nödvändigt för ett av de lagstadgade ändamålen ⁽³³⁹⁾ och står i proportion till vad som eftersträvas ⁽³⁴⁰⁾. Såsom klargörs i

⁽³³¹⁾ Denna information ska innehålla i) en översikt över hur inhämtandet av uppgifterna kommer att vara till nytta för utredningen eller verksamheten, ii) en förklaring av relevansen av de begärda tidsperioderna, inbegripet hur dessa perioder står i proportion till den händelse som utreds, iii) en förklaring av hur inkräktningsnivån är motiverad med hänsyn till den nytta som uppgifterna kommer att ge undersökningen (denna motivering bör omfatta frågan om mindre inkräktande undersökningar skulle kunna genomföras för att uppnå målet), iv) en bedömning av den enskildes rättigheter (särskilt rätten till privatliv och, i förekommande fall, yttrandefrihet) och en avvägning mellan dessa rättigheter och nyttan för utredningen och v) uppgifter om vilka säkerhetsintrång som kan uppstå och hur de begärda tidsperioderna påverkar intrång i säkerheten (*Code of Practice on Communications Data*, punkterna 3.22–3.26, se fotnot 323).

⁽³³²⁾ Se fotnot 313.

⁽³³³⁾ När mer inkräktande kommunikationsuppgifter efterfrågas (dvs. händelsedata) anges det i koden att det är lämpligare att inhämta de första enhetsuppgifterna eller att direkt förvärva händelsedata i begränsade brådskande fall (*Code of Practice on Communications Data*, punkterna 6.10–6.14, se fotnot 323).

⁽³³⁴⁾ *Code of Practice on Communications Data*, punkterna 8.8–8.44, se fotnot 323.

⁽³³⁵⁾ I riktlinjerna anges att "den tillståndsgivande personen måste vara särskilt uppmärksam när denne prövar sådana ansökningar, inbegripet ytterligare överväganden om huruvida det kan finnas oavsiktliga konsekvenser av sådana tillämpningar och om det allmänna intresset bäst tillgodoses genom tillämpningen" (punkt 8.8 i *Code of Practice on Communications Data*). Dessutom måste anteckningar föras för denna typ av ansökningar och vid nästa inspektion bör sådana ansökningar märkas för att uppmärksamma *Investigatory Powers Commissioner* (*Code of Practice on Communications Data*, punkt 8.10, se fotnot 323).

⁽³³⁶⁾ Avsnitt 87–89 i 2016 års lag om utredningsbefogenheter.

⁽³³⁷⁾ Enligt avsnitt 90 i 2016 års lag om utredningsbefogenheter kan en teleoperatör som mottar ett föreläggande om lagring begära att den utfärdande ministern ska ompröva det.

⁽³³⁸⁾ Enligt avsnitt 87.2 a i 2016 års lag om utredningsbefogenheter kan ett föreläggande om lagring dock avse "en viss operatör eller en beskrivning av operatörer".

⁽³³⁹⁾ Ändamålen är i) hänsyn till nationell säkerhet, ii) tillämpligt brottssyfte (enligt definitionen i avsnitt 87.10A i 2016 års lag om utredningsbefogenheter), iii) hänsyn till Förenade kungarikets ekonomiska välbefinnande i den mån denna hänsyn även är relevant för den nationella säkerheten, iv) hänsyn till den allmänna säkerheten, v) syftet att förhindra dödsfall, personskador eller skada på en persons fysiska eller psykiska hälsa eller att lindra skador på en persons fysiska eller psykiska hälsa eller vi) att bistå vid utredningar av påstådda felaktiga domslut (avsnitt 87 i IPA).

⁽³⁴⁰⁾ Avsnitt 87 i 2016 års lag om utredningsbefogenheter. För bedömningen av huruvida föreläggandet om lagring är proportionerligt tillämpas dessutom, enligt den relevanta uppförandekoden, kriterierna i avsnitt 2.2 i 2016 års lag om utredningsbefogenheter, särskilt kravet på att bedöma huruvida det som avses med föreläggandet rimligen skulle kunna uppnås med mindre inkräktande medel. I likhet med proportionalitetsbedömningen av inhämtandet av kommunikationsuppgifter klargörs i uppförandekoden för kommunikationsuppgifter att en sådan bedömning omfattar "avvägningen mellan omfattningen av ingreppet i en enskilds rätt till respekt för privatlivet och en särskild fördel för utredningen (*Code of Practice on Communications Data*, punkt 16.3, se fotnot 323).

själva 2016 års lag om utredningsbefogenheter ⁽³⁴¹⁾, ska den ansvariga ministern, innan han eller hon utfärdar ett föreläggande om lagring, beakta de sannolika fördelarna med föreläggandet ⁽³⁴²⁾, en beskrivning av telekommunikationstjänsterna, lämpligheten av att begränsa de uppgifter som ska lagras med hänvisning till plats eller beskrivningar av personer till vilka telekommunikationstjänster tillhandahålls ⁽³⁴³⁾, det sannolika antalet användare (om de är kända) av en telekommunikationstjänst som föreläggandet avser ⁽³⁴⁴⁾, den tekniska genomförbarheten av att följa föreläggandet och den troliga kostnaden för att följa föreläggandet och alla andra konsekvenser av föreläggandet för den teleoperatör (eller beskrivning av operatörer) som föreläggandet avser ⁽³⁴⁵⁾. I kapitel 17 i uppförandekoden för kommunikationsuppgifter beskrivs att alla förelägganden om lagring måste ange varje datatyp som ska lagras och hur denna typ av uppgifter uppfyller de nödvändiga testerna för lagring.

- (209) I samtliga fall (både för ändamål som rör nationell säkerhet och brottsbekämpande ändamål) måste ett beslut om att utfärda ett föreläggande om lagring från den ansvariga ministern godkännas av en oberoende *Judicial Commissioner* enligt det så kallade *double lock*-förfarandet. *The Judicial Commissioner* ska särskilt kontrollera om föreläggandet om lagring av relevanta kommunikationsuppgifter är nödvändigt och står i proportion till ett eller flera av de lagstadgade ändamålen ⁽³⁴⁶⁾.

3.3.1.1.3 Ingrepp i utrustning

- (210) Ingrepp i utrustning är en uppsättning tekniker som används för att erhålla en mängd olika data från utrustning ⁽³⁴⁷⁾, bl.a. datorer, surfplattor och smarttelefoner samt kablar, ledningar och lagringsanordningar ⁽³⁴⁸⁾. Ingrepp i utrustning gör det möjligt att få tillgång till både kommunikationsinnehåll och utrustningsdata ⁽³⁴⁹⁾.
- (211) I enlighet med avsnitt 13.1 i 2016 års lag om utredningsbefogenheter måste en underrättelsetjänst för att använda ingrepp i utrustning ha tillstånd i form av ett beslut inom ramen för *double lock*-förfarandet som inrättats genom 2016 års lag om utredningsbefogenheter, förutsatt att det finns en "koppling till de brittiska öarna" ⁽³⁵⁰⁾. Enligt de brittiska myndigheternas förklaringar skulle det alltid finnas en "koppling till de brittiska öarna" i situationer där

⁽³⁴¹⁾ Se avsnitt 88 i 2016 års lag om utredningsbefogenheter.

⁽³⁴²⁾ Fördelarna kan vara befintliga eller beräknade och måste avse de lagstadgade ändamål för vilka uppgifterna kan lagras (punkt 17.17 i *Code of Practice on Communications Data*, se fotnot 323).

⁽³⁴³⁾ Dessa överväganden kommer att inbegripa fastställandet av huruvida den fullständiga geografiska räckvidden för föreläggandet om lagring är nödvändig och proportionell och om det är nödvändigt och proportionerligt att inkludera eller utesluta särskilda personbeskrivningar (*Code of Practice on Communications Data*, punkt 17.17, se fotnot 323).

⁽³⁴⁴⁾ Detta kommer att hjälpa den ansvariga ministern att beakta både graden av intrång hos kunderna och de sannolika fördelarna med de uppgifter som ska lagras (punkt 17.17 i *Code of Practice on Communications Data*, se fotnot 323).

⁽³⁴⁵⁾ Avsnitt 88 i 2016 års lag om utredningsbefogenheter.

⁽³⁴⁶⁾ Avsnitt 89 i 2016 års lag om utredningsbefogenheter.

⁽³⁴⁷⁾ Enligt avsnitten 135.1 och 198.1 i 2016 års lag om utredningsbefogenheter avses med "utrustning" sådan utrustning som avger elektromagnetisk, akustisk eller annan emission samt varje anordning som kan användas i anslutning till sådan utrustning.

⁽³⁴⁸⁾ *Code of Practice on Equipment Interference* finns på följande länk: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf, punkt 2.2.

⁽³⁴⁹⁾ Utrustningsdata definieras i avsnitt 100 i 2016 års lag om utredningsbefogenheter som systemdata och data som a) omfattar, ingår som en del av, är knutna till eller logiskt förknippas med kommunikation (från avsändaren eller på annat sätt) eller någon annan information, b) logiskt kan skiljas från resten av meddelandet eller informationen och c) om den separerades på ett sådant sätt, skulle det inte avslöja något som rimligen skulle kunna anses vara innebörden (om någon) av meddelandet eller informationen.

⁽³⁵⁰⁾ För att kravet på beslut ska vara obligatoriskt krävs det också i avsnitt 13.1 i 2016 års lag om utredningsbefogenheter att underrättelsetjänstens agerande skulle utgöra ett eller flera brott enligt avsnitten 1–3A i *Computer Misuse Act 1990*, vilket skulle vara fallet i de allra flesta situationer, se riktlinjerna om ingrepp i utrustning, punkterna 3.32 och 3.6–3.9). Enligt avsnitt 13.2 i 2016 års lag om utredningsbefogenheter finns det en "koppling till brittiska öarna" om a) något av beteendet skulle äga rum på de brittiska öarna (oberoende av var utrustningen som skulle eller kan komma att utsättas för ingrepp finns placerad), b) underrättelsetjänsten tror att någon av den utrustning som skulle eller kan komma att beröras av ingreppen skulle eller kan befinna sig på de brittiska öarna vid någon tidpunkt under den tid då ingreppen äger rum eller c) ett syfte med ingreppet är att ta del av i) kommunikation som skickas av, eller till, en person som är eller som underrättelsetjänsten tror är på de brittiska öarna för tillfället, ii) privat information som avser en person som är eller som underrättelsetjänsten tror för tillfället befinner sig på de brittiska öarna eller iii) utrustningsdata som utgör en del av, eller är kopplade till, kommunikation eller privat information som omfattas av leden i) eller ii).

uppgifter överförs från Europeiska unionen till Förenade kungariket inom ramen för detta beslut och varje ingrepp i utrustning som innefattar sådana uppgifter skulle därför omfattas av kravet på obligatoriskt beslut i avsnitt 13.1 i 2016 års lag om utredningsbefogenheter ⁽³⁵¹⁾.

- (212) Reglerna för beslut om riktat ingrepp i utrustning anges i del 5 av 2016 års lag om utredningsbefogenheter. I likhet med riktad avlyssning måste riktat ingrepp i utrustning avse ett specifikt "mål" som ska uppges i beslutet ⁽³⁵²⁾. Närmare uppgifter om hur ett "mål" ska fastställas beror på vilken fråga och vilken typ av utrustning som ska påverkas. I synnerhet i avsnitt 115.3 i IPA anges vilken information som bör ingå i beslutet (t.ex. namn på personen eller organisationen, beskrivning av platsen) exempelvis beroende på om ingreppet gäller utrustning som tillhör, används eller innehas av en viss person, en organisation eller en grupp av personer, befinner sig på en viss plats och så vidare ⁽³⁵³⁾. Det är den myndighet som ansöker om ett beslut om ingrepp i utrustning som avgör för vilka syften ett beslut om ingrepp i utrustning kan utfärdas ⁽³⁵⁴⁾.
- (213) I likhet med riktad avlyssning måste den utfärdande myndigheten överväga om åtgärden är nödvändig för att uppnå ett specifikt syfte och om den står i proportion till vad som eftersträvas ⁽³⁵⁵⁾. Dessutom bör kommissionen också överväga om det finns skyddsåtgärder i fråga om säkerhet, lagring och utlämnande samt när det gäller "utlämnande till utlandet" ⁽³⁵⁶⁾ (se skäl 196).
- (214) Beslutet måste godkännas av en justitieombudsman, utom i brådskande fall ⁽³⁵⁷⁾. I det senare fallet måste en rättslig myndighet underrättas om att ett beslut har utfärdats och måste godkänna den inom tre arbetsdagar. Om *the Judicial Commissioner* vägrar att godkänna beslutet upphör beslutet att gälla och kan inte förnyas ⁽³⁵⁸⁾. *The Judicial Commissioner* är dessutom behörig att kräva att alla uppgifter som inhämtades enligt beslutet raderas ⁽³⁵⁹⁾. Den omständigheten att ett beslut utfärdades som brådskande påverkar inte tillsynen i efterhand (se skälen 244–255) eller enskilda personers möjligheter att ansöka om rättslig prövning (se skälen 260–270). Enskilda personer kan inte klagomål till ICO eller framställa krav till tribunalen för utredningsbefogenheter enligt de normala förfarandena. I samtliga fall är det kriterium som tillämpas av *the Judicial Commissioner* när han eller hon beslutar att godkänna eller avslå ett beslut nödvändighets- och proportionalitetsprövningen, som är tillämplig på begäranden om riktad avlyssning ⁽³⁶⁰⁾ (se skäl 192 ovan).

⁽³⁵¹⁾ För fullständighetens skull bör det noteras att även i situationer där det inte finns någon "koppling till de brittiska öarna" och användning av ingrepp i utrustning därför inte omfattas av kravet på obligatoriskt beslut i avsnitt 13.1 i 2016 års lag om utredningsbefogenheter bör en underrättelsetjänst som planerar att bedriva verksamhet, för vilken den kan erhålla ett beslut om massingrepp i utrustning, i princip erhålla ett sådant beslut (*as a matter of policy*) (se punkt 3.24 i *Code of Practice on Equipment Interference*). Även om ett beslut om ingrepp i utrustning enligt 2016 års lag om utredningsbefogenheter varken krävs enligt lag eller erhålls *as a matter of policy* omfattas underrättelsetjänsternas åtgärder av ett antal villkor och begränsningar enligt avsnitt 7 i *Intelligence Services Act 1994*. Detta inbegriper bland annat kravet på tillstånd från den ansvariga ministern som måste vara förvissad om att inga åtgärder går utöver vad som är nödvändigt för att utföra underrättelsetjänstens uppgifter på ett korrekt sätt.

⁽³⁵²⁾ Avsnitt 115 i 2016 års lag om utredningsbefogenheter reglerar innehållet i beslutet och anger att det måste innehålla namn på eller beskrivning av personer, organisationer, plats eller grupp av personer som utgör "målgruppen", en beskrivning av utredningens art och en beskrivning av den verksamhet för vilken utrustningen används. Den ska också innehålla en beskrivning av typen av utrustning och vilka handlingar som den person som beslutet riktar sig till har rätt att utföra.

⁽³⁵³⁾ Se även *Code of Practice on Equipment Interference*, punkt 5.7, se fotnot 348.

⁽³⁵⁴⁾ Nationella säkerhetsmyndigheter kan ansöka om ett beslut om ingrepp i utrustning när det är nödvändigt för nationella säkerhetsändamål, för att upptäcka allvarig brottslighet och/eller för att främja Förenade kungarikets ekonomiska välbefinnande, i den mån dessa hänsyn också är relevanta för den nationella säkerheten (avsnitt 102–103 i 2016 års lag om utredningsbefogenheter). Beroende på organ kan ett beslut om ingrepp i utrustning begäras för brottsbekämpande ändamål när det är nödvändigt för att upptäcka eller förebygga ett allvarligt brott eller för att förhindra dödsfall eller skada på en persons fysiska eller psykiska hälsa eller för att lindra eventuella skador på en persons fysiska eller psykiska hälsa (se avsnitt 106.1 och 106.3 i 2016 års lag om utredningsbefogenheter).

⁽³⁵⁵⁾ Avsnitt 102.1 i 2016 års lag om utredningsbefogenheter.

⁽³⁵⁶⁾ Avsnitten 129–131 i 2016 års lag om utredningsbefogenheter.

⁽³⁵⁷⁾ Avsnitt 109 i 2016 års lag om utredningsbefogenheter.

⁽³⁵⁸⁾ Avsnitt 109.4 i 2016 års lag om utredningsbefogenheter.

⁽³⁵⁹⁾ Avsnitt 110.3 b i 2016 års lag om utredningsbefogenheter. Enligt punkt 5.67 i uppförandekoden om ingrepp i utrustning avgörs brådskande omständigheter av huruvida det skulle vara rimligen genomförbart att ansöka om godkännande från *the Judicial Commissioner* om att utfärda ett beslut under den tid som finns tillgänglig för att tillgodose ett operativt eller utredningsmässigt behov. Brådskande beslut ska ingå i en eller båda följande kategorier: i) Överhängande risk för allvarlig skada – t.ex. om en person har blivit kidnappad och man gör bedömningen att personens liv är i allvarlig fara. ii) Insamling av underrättelseuppgifter eller utredningar med begränsad tid att agera – t.ex. om en sändning av klass A-narkotika som står i begrepp att föras in i Förenade kungariket och de brottsbekämpande myndigheterna vill ha täckning av personer som begår grova brott för att kunna anhålla dessa personer. Se fotnot 348.

⁽³⁶⁰⁾ Avsnitt 108 i 2016 års lag om utredningsbefogenheter.

- (215) Slutligen gäller särskilda skyddsåtgärder för riktad avlyssning även för ingrepp i utrustning när det gäller varaktighet, förnyelse och ändring av beslutet samt avlyssning av parlamentsledamöter, föremål som omfattas av rättsliga privilegier och journalistiskt material (se närmare uppgifter i skäl 193).

3.3.1.1.4 Utövande av "massbefogenheter"

- (216) Massbefogenheter regleras i del 6 av 2016 års lag om utredningsbefogenheter. Dessutom innehåller riktlinjerna för praxis mer information om användningen av massbefogenheter. Även om det inte finns någon definition i brittisk lag av "massbefogenheter" har den inom ramen för 2016 års lag om utredningsbefogenheter beskrivits som insamling och lagring av stora mängder uppgifter som regeringen inhämtat på olika sätt (dvs. befogenheter gällande massavlyssning, massinhämtande, massingrepp i utrustning och massdataset av personuppgifter) som myndigheterna därefter kan få tillgång till. Denna beskrivning förtydligas genom att den står i kontrast till vad som inte är "massbefogenhet" enligt följande: Den motsvarar inte så kallad massövervakning utan begränsningar eller skyddsåtgärder. Tvärtom innehåller den, enligt förklaringen nedan, begränsningar och skyddsåtgärder som syftar till att säkerställa att tillgång till uppgifter inte ges på ett urskillningslöst eller omotiverat sätt ⁽³⁶¹⁾. I synnerhet kan massbefogenheter endast användas om det finns en koppling mellan den tekniska åtgärd som en nationell underrättelsetjänst avser att använda och det operativa mål för vilket en sådan åtgärd begärs.
- (217) Dessutom har endast underrättelsetjänsterna tillgång till massbefogenheter och är alltid föremål för ett beslut som utfärdas av den ansvariga ministern och godkänns av en *Judicial Commissionar*. När man väljer metoder för att samla in underrättelser måste man ta hänsyn till om målet i fråga kan uppnås med hjälp av "mindre inkräktande medel" ⁽³⁶²⁾. Detta tillvägagångssätt följer av den rättsliga ram som bygger på proportionalitetsprincipen och därför prioriteras målinriktad insamling framför massinsamling.

3.3.1.1.4.1 Massavlyssning och massingrepp i utrustning

- (218) Ordningen för massavlyssning föreskrivs i del 6 kapitel 1 i 2016 års lag om utredningsbefogenheter medan massingrepp i utrustning regleras i kapitel 3 i samma del. Dessa ordningar är i stort sett desamma, så de villkor och ytterligare skyddsåtgärder som gäller för dessa beslut analyseras tillsammans.

i) Villkor och kriterier för utfärdande av beslutet

- (219) Ett beslut om massavlyssning är begränsat till avlyssning av kommunikation i samband med överföring som sänds eller tas emot av enskilda personer som befinner sig utanför de brittiska öarna ⁽³⁶³⁾, så kallad "utlandsrelaterad kommunikation" ⁽³⁶⁴⁾, samt andra relevanta uppgifter och det efterföljande urvalet för

⁽³⁶¹⁾ Enligt den rapport om massbefogenheter som lagts fram av lord David Anderson, oberoende granskare av lagstiftningen om terrorism inför godkännandet av 2016 års lag om utredningsbefogenheter bör det stå klart att insamling och lagring av uppgifter i massomfattning inte är detsamma som så kallad massövervakning. Alla rättssystem som är värda namnet kommer att innehålla begränsningar och skyddsåtgärder som är utformade just för att säkerställa att tillgång till känsliga uppgifter (...) inte ges på ett urskillningslöst eller omotiverat sätt. Sådana begränsningar och garantier finns förvisso i propositionen. Lord David Anderson, *Report of the bulk power review*, augusti 2016, punkt 1.9 (kursivering tillagd), finns på följande länk: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/546925/56730_Cm9326_WEB.PDF.

⁽³⁶²⁾ Avsnitt 2.2 i 2016 års lag om utredningsbefogenheter. Se t.ex. *Code of Practice on Bulk Acquisition of Communications Data*, punkt 4.11, som finns på följande länk: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf.

⁽³⁶³⁾ De brittiska öarna utgör Förenade kungariket, Kanalöarna och Isle of Man och definieras i tillägg 1 till *Interpretation Act 1978*, som finns på följande länk: <https://www.legislation.gov.uk/ukpga/1978/30/schedule/1>.

⁽³⁶⁴⁾ Enligt avsnitt 136 i 2016 års lag om utredningsbefogenheter avses med "utlandsrelaterad kommunikation" i) meddelanden som sänds av enskilda personer som befinner sig utanför de brittiska öarna eller ii) meddelanden som mottagits av personer som befinner sig utanför de brittiska öarna. Denna ordning, som bekräftats av de brittiska myndigheterna, omfattar även kommunikation mellan två personer som båda befinner sig utanför de brittiska öarna. I målet *Big Brother Watch m.fl. mot Förenade kungariket* (se fotnot 279), punkt 376, fann Europeiska domstolen för de mänskliga rättigheterna (stora avdelningen) i samband med en liknande begränsning av kommunikation (rörande "extern kommunikation") som kan fångas upp via massavlyssning enligt 2000 års lag om utredningsbefogenheter att begränsningen var tillräckligt avgränsad och förutsebar.

granskning av det avlyssnade materialet ⁽³⁶⁵⁾. En beslut om massingrepp i utrustning ⁽³⁶⁶⁾ gör det möjligt för mottagaren att säkra ingrepp i all utrustning i syfte att erhålla utlandsrelaterad kommunikation (däribland allt som omfattar tal, musik, ljud, visuella bilder eller data av valfri beskrivning), utrustningsdata (data som möjliggör eller underlättar funktionen för en posttjänst, ett telekommunikationssystem, telekommunikationstjänster) eller annan information ⁽³⁶⁷⁾.

- (220) Den ansvariga ministern kan utfärda ett "massbeslut" endast på begäran av en chef för en underrättelsetjänst ⁽³⁶⁸⁾. Ett beslut om att tillåta massavlyssning eller massingrepp i utrustning får endast utfärdas om det är nödvändigt för den nationella säkerhetens intresse och för ett annat syfte att förebygga eller upptäcka allvarliga brott eller vad som är bäst för Förenade kungarikets ekonomiska välbefinnande när det är relevant för den nationella säkerheten ⁽³⁶⁹⁾. I avsnitt 142.7 i 2016 års lag om utredningsbefogenheter föreskrivs dessutom att ett beslut om massavlyssning måste anges mer detaljerat än en enkel hänvisning till "vad som är bäst för den nationella säkerheten", "Förenade kungarikets ekonomiska välbefinnande" och "förebyggande och bekämpning av grov brottslighet" och en koppling mellan den åtgärd som ska begäras och ett eller flera operativa syften som måste ingå i beslutet måste fastställas.
- (221) Valet av operativt syfte är ett resultat av en process i flera lager. I avsnitt 142.4 föreskrivs att de operativa syften som anges i beslutet ska anges i en förteckning som förs av cheferna för underrättelsetjänsterna eftersom de anser att det är fråga om operativa ändamål för vilka avlyssnat innehåll eller sekundära uppgifter som erhållits i samband med beslut om massavlyssning kan väljas ut för granskning. Förteckningen över operativa ändamål ska godkännas av ministern. En ansvariga ministern får ge ett sådant godkännande endast om han eller hon är förvissad om att det operativa syftet är mer detaljerat än de allmänna grunderna för beviljande av tillstånd (nationell säkerhet eller nationell säkerhet och ekonomiskt välbefinnande eller förhindrande av allvarlig brottslighet) ⁽³⁷⁰⁾. Vid utgången av varje relevant tremånadersperiod ska ministern lämna en kopia av förteckningen över operativa ändamål till parlamentets underrättelse- och säkerhetsutskott. Slutligen måste premiärministern se över förteckningen över operativa syften minst en gång om året ⁽³⁷¹⁾. *High Court* har påpekat att "dessa inte ska behandlas som obetydliga skyddsåtgärder eftersom de tillsammans bygger upp en invecklad uppsättning metoder för ansvarsskyldighet som inbegriper såväl parlamentet som regeringsledamöter på högsta nivå" ⁽³⁷²⁾.
- (222) Sådana operativa syften begränsar också omfattningen av urvalet av avlyssningsmaterial för granskningsfasen. Urvalet för granskning av eventuellt material som samlats in inom ramen för "massbeslutet" måste motiveras mot bakgrund av det/de operativa syftet/syften. Enligt de brittiska myndigheternas förklaring innebär detta att de praktiska arrangemangen för granskning måste bedömas av den ansvariga ministern redan i samband med beslutet, med tillräckligt detaljerade uppgifter för att uppfylla de lagstadgade skyldigheterna enligt avsnitten 152 och 193 i 2016 års lag om utredningsbefogenheter ⁽³⁷³⁾. De uppgifter som lämnas till den ansvariga ministern i samband med dessa arrangemang skulle till exempel behöva innehålla information (i förekommande fall) om hur filtreringsarrangemangen kan variera under den tid som ett beslut kommer att ha verkan ⁽³⁷⁴⁾. För närmare uppgifter om processen och de skyddsåtgärder som tillämpas under filtrerings- och granskningsfaserna, se skäl 229 nedan.

⁽³⁶⁵⁾ Avsnitt 136.4 i 2016 års lag om utredningsbefogenheter. Enligt de förklaringar som lämnats av den brittiska regeringen kan massavlyssning till exempel användas för att identifiera tidigare okända hot mot landets nationella säkerhet, genom filtrering och analys av avlyssnat material för att identifiera kommunikation av underrättelsevärde (*UK Explanatory Framework* avsnitt H: *National security* s. 27–28, se fotnot 29). Som de brittiska myndigheterna har förklarat kan sådana instrument användas för att fastställa kopplingar mellan kända personer av intresse och för att söka efter spår av verksamhet hos personer som kanske ännu inte är kända men som under en utredning dyker upp och för att identifiera aktivitetsmönster som kan tyda på ett hot mot Förenade kungariket.

⁽³⁶⁶⁾ I enlighet med avsnitt 13.1 i 2016 års lag om utredningsbefogenheter kräver en underrättelsetjänsts användning av ingrepp i utrustning ett tillstånd genom ett beslut enligt 2016 års lag om utredningsbefogenheter förutsatt att det finns en "koppling till de brittiska öarna", se skäl 211.

⁽³⁶⁷⁾ Avsnitt 176 i 2016 års lag om utredningsbefogenheter. Ett beslut om massingrepp i utrustning får inte ge tillstånd till ett beteende som (om det inte sker med lagligt stöd) skulle utgöra olaglig avlyssning (utom i samband med lagrad kommunikation). Enligt *UK Explanatory Framework* kan den information som erhålls vara nödvändig för att identifiera personer av intresse och skulle vanligen vara lämpliga storskaliga insatser (*UK Explanatory Framework*, avsnitt H: *National security* s. 28, se fotnot 29).

⁽³⁶⁸⁾ Avsnitten 138.1 och 178.1 i 2016 års lag om utredningsbefogenheter.

⁽³⁶⁹⁾ Avsnitten 138.2 och 178.2 i 2016 års lag om utredningsbefogenheter.

⁽³⁷⁰⁾ Enligt de brittiska myndigheternas förklaringar kan exempelvis ett operativt syfte begränsa åtgärdens omfattning till förekomsten av ett hot i ett visst geografiskt område.

⁽³⁷¹⁾ Avsnitt 142.4–10 i 2016 års lag om utredningsbefogenheter.

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

⁽³⁷³⁾ I avsnitten 152 och 193 i 2016 års lag om utredningsbefogenheter föreskrivs att a) urvalet för granskning görs endast för de operativa syften som anges i beslutet, b) urvalet för granskning är nödvändigt och proportionerligt under alla omständigheter och c) urvalet för granskning inte strider mot förbudet mot att välja ut material och identifiera meddelanden som har skickats av eller är avsedda för personer som är kända för att befinna sig på de brittiska öarna vid den tidpunkten.

⁽³⁷⁴⁾ Se uppförandekoden om avlyssning av kommunikation, punkt 6.6, se fotnot 278.

- (223) En massbefogenhet kan endast godkännas om den står i proportion till vad som eftersträvas⁽³⁷⁵⁾. Enligt *Code of Practice on Interception* innebär varje proportionalitetsbedömning en avvägning mellan allvaret i intrånget i den personliga integriteten (och andra överväganden som anges i avsnitt 2.2) och behovet av utredningsåtgärder, operativa åtgärder eller förmågor. Det godkända beteendet bör erbjuda en realistisk möjlighet att uppnå den förväntade nyttan och bör inte vara oproportionerligt eller godtyckligt⁽³⁷⁶⁾. Som redan nämnts innebär detta i praktiken att proportionalitetstestet baseras på ett avvägningstest mellan vad som eftersträvas ("operativt syfte/operativa syften") och tillgängliga tekniska alternativ (t.ex. riktad eller massavlyssning, ingrepp i utrustningen, inhämtande av kommunikationsuppgifter) med företräde för de minst inkräktande medlen (se skälen 181 och 182 ovan). Om mer än en åtgärd är lämplig för målet måste de mindre inkräktande åtgärderna föredras.
- (224) Ytterligare en garanti för bedömningen av den begärda åtgärdens proportionalitet säkerställs genom det faktum att ministern måste få den relevanta information som behövs för att kunna göra sin bedömning på ett korrekt sätt. I synnerhet krävs det enligt uppförandekoden om avlyssning och uppförandekoden om ingrepp i utrustning att den ansökan som lämnas in av den berörda myndigheten ska innehålla uppgifter om bakgrunden till ansökan, beskrivning av den kommunikation som ska avlyssnas och de teleoperatörer som är skyldiga att bistå, en beskrivning av det beteende som ska godkännas, de operativa ändamålen och en förklaring till varför beteendet är nödvändigt och proportionerligt⁽³⁷⁷⁾.
- (225) Slutligen är det viktigt att den ansvariga ministerns beslut att utfärda beslutet måste godkännas av en oberoende *Judicial Commissioner* som bedömer huruvida den föreslagna åtgärden är nödvändig och proportionerlig med tillämpning av samma principer som en domstol skulle använda i en ansökan om rättslig prövning⁽³⁷⁸⁾. *The Judicial Commissioner* kommer närmare bestämt att granska den ansvariga ministerns slutsatser om huruvida beslutet är nödvändigt och huruvida beteendet är proportionerligt mot bakgrund av de principer som fastställs i avsnitt 2.2 i 2016 års lag om utredningsbefogenheter (allmänna skyldigheter i fråga om integritet). *The Judicial Commissioner* kommer också att granska ministerns slutsatser om huruvida vart och ett av de operativa syften som anges i beslutet är ett syfte för vilket urvalet är eller kan vara nödvändigt. Om *the Judicial Commissioner* vägrar att godkänna beslutet att utfärda ett beslut om husrannsakan kan den ansvariga ministern antingen i) godta beslutet och därför inte utfärda beslutet om husrannsakan eller ii) hänskjuta ärendet till den utredande myndigheten för beslut (såvida inte den utredande myndigheten har fattat det ursprungliga beslutet)⁽³⁷⁹⁾.

ii) Ytterligare skyddsåtgärder

- (226) Genom 2016 års lag om utredningsbefogenheter infördes ytterligare begränsningar för varaktigheten, förnyelse och ändring av ett "massbeslut". Beslutet ska ha en giltighetstid på högst sex månader och varje beslut om att förnya eller ändra (med undantag för mindre ändringar) beslutet måste också godkännas av en *Judicial Commissioner*⁽³⁸⁰⁾. I uppförandekoden om avlyssning av kommunikation och i uppförandekoden om ingrepp i utrustning anges att en ändring av de operativa syftena med beslutet betraktas som en betydande ändring av beslutet⁽³⁸¹⁾.

⁽³⁷⁵⁾ Avsnitten 138.1 b och c och 178 b och c i 2016 års lag om utredningsbefogenheter.

⁽³⁷⁶⁾ *Code of Practice on Interception of Communications*, punkt 4.10, se fotnot 278.

⁽³⁷⁷⁾ *Code of Practice on Interception of Communications*, punkt 6.20, se fotnot 278, och *Code of Practice on Equipment Interference*, punkt 6.13, se fotnot 348.

⁽³⁷⁸⁾ Avsnitten 138.1 g och 178.1 f i 2016 års lag om utredningsbefogenheter. Europeiska domstolen för de mänskliga rättigheterna har slagit fast att förhandstillstånd från ett oberoende organ är en särskilt viktig skyddsåtgärd mot missbruk i samband med massavlyssning. Europeiska domstolen för de mänskliga rättigheterna (stora avdelningen), *Big Brother Watch m.fl./Förenade kungariket* (se fotnot 269), punkterna 351 och 352. Det är viktigt att tänka på att denna dom avsåg den tidigare rättsliga ramen (2000 års lag om utredningsbefogenheter), som inte innehöll alla skyddsåtgärder (bland annat förhandstillstånd från en oberoende *Judicial Commissioner*) som infördes genom 2016 års lag om utredningsbefogenheter.

⁽³⁷⁹⁾ Avsnitt 159.3 och 4 i 2016 års lag om utredningsbefogenheter.

⁽³⁸⁰⁾ Avsnitten 143–146 och 184–188 i 2016 års lag om utredningsbefogenheter. Vid en brådskande ändring kan den ansvariga ministern göra ändringen utan godkännande men måste underrätta *the Commissioner* och han eller hon måste sedan besluta om huruvida ändringen ska godkännas eller avslås (avsnitt 147 i 2016 års lag om utredningsbefogenheter). Besluten måste annulleras, om beslutet inte längre är nödvändigt eller proportionerligt, eller om granskningen av avlyssnat innehåll, metadata eller andra data som erhållits inom ramen för beslutet inte längre är nödvändig för något av de operativa ändamål som anges i beslutet (avsnitt 148 och 189 i 2016 års lag om utredningsbefogenheter).

⁽³⁸¹⁾ *Code of Practice on Interception of Communications*, punkt 6.44–6.47, se fotnot 278, och *Code of Practice on Equipment Interference*, punkt 6.48, se fotnot 348.

- (227) I likhet med vad som föreskrivs för riktad avlyssning föreskrivs i del 6 i 2016 års lag om utredningsbefogenheter att den ansvariga ministern ska se till att det finns gällande bestämmelser om lagring och utlämnande av material som erhållits i enlighet med beslutet ⁽³⁸²⁾ samt om utlämnande utomlands ⁽³⁸³⁾. I synnerhet föreskrivs i avsnitten 150.5 och 191.5 i 2016 års lag om utredningsbefogenheter att varje kopia av sådant material som samlats in enligt beslutet ska förvaras på ett säkert sätt och förstöras så snart det inte längre finns några relevanta skäl för att behålla det medan det i avsnitten 150.2 och 191.2 krävs att antalet personer till vilka materialet lämnas ut och i vilken omfattning materialet lämnas ut görs tillgängligt eller kopieras ska begränsas till vad som är absolut nödvändigt för de lagstadgade ändamålen ⁽³⁸⁴⁾.
- (228) När slutligen det material som har avlyssnats antingen genom en massavlyssning eller ett massingrepp i utrustning ska överlämnas till tredjeland ("utlämnande till utlandet") föreskrivs i 2016 års lag om utredningsbefogenheter att den ansvariga ministern ska se till att lämpliga åtgärder vidtas för att säkerställa att liknande skyddsåtgärder för säkerhet, lagring och utlämnande finns i det tredjelandet ⁽³⁸⁵⁾. I avsnitt 109 i 2018 års dataskyddslag fastställs dessutom särskilda krav för underrättelsetjänsters internationella överföringar av personuppgifter till tredjeländer eller internationella organisationer. Enligt dessa bestämmelser får personuppgifter inte överföras till ett land eller territorium utanför Förenade kungariket eller till en internationell organisation om inte överföringen är nödvändig och proportionell med hänsyn till den personuppgiftsansvarigas lagstadgade uppgifter eller för andra ändamål som anges i avsnitt 2.2 a i *Security Services Act 1989* eller avsnitten 2.2 a och 4.2 a i *Intelligence Services Act 1994* ⁽³⁸⁶⁾. Det är viktigt att notera att dessa krav även gäller i situationer där undantaget avseende nationell säkerhet enligt avsnitt 110 i 2018 års dataskyddslag åberopas, eftersom avsnitt 109 inte anges i samma lags avsnitt 110 som en av de bestämmelser som kan upphöra att gälla om ett undantag från vissa bestämmelser krävs för att skydda den nationella säkerheten.
- (229) När beslutet har godkänts och uppgifterna har samlats in i massomfattning kommer uppgifterna att bli föremål för ett urval innan de granskas. Urvals- och granskningsfasen är föremål för ytterligare ett proportionalitetstest som utförs av analytikern och som på grundval av de operativa syften som ingår i beslutet (och eventuellt befintliga filtreringsarrangemang) definierar urvalskriterierna. Enligt avsnitt 152 och 193 i IPA måste ministern vid utfärdandet av beslutet se till att det finns arrangemang som garanterar att urvalet av materialet endast sker för de angivna operativa ändamålen och att det är nödvändigt och proportionerligt under alla omständigheter. I detta avseende klargjorde de brittiska myndigheterna att det material som massavlyssnats först och främst väljs ut genom automatisk filtrering i syfte att göra sig av med uppgifter som sannolikt inte är av nationellt säkerhetsintresse. Filtren kommer att variera från tid till annan (allteftersom mönstren, typerna och protokollen för Internettrafik ändras) och kommer att bero på tekniken och det operativa sammanhanget. Efter denna fas kan uppgifterna väljas ut för granskning endast om de är relevanta för de operativa syften som anges i beslutet ⁽³⁸⁷⁾. De skyddsåtgärder som föreskrivs i 2016 års lag om utredningsbefogenheter vad gäller granskning av insamlat material är tillämpliga på alla typer av uppgifter (både avlyssnat innehåll och sekundära uppgifter) ⁽³⁸⁸⁾. I avsnitten 152 och 193 i 2016 års lag om utredningsbefogenheter föreskrivs även ett allmänt förbud mot att välja ut material för granskning som avser samtal som sänds av eller är avsedda för personer som befinner sig på de brittiska öarna. Om myndigheterna vill granska sådant material ska de lämna in en begäran om ett beslut om en riktad granskning enligt del 2 och del 4 i 2016 års lag om utredningsbefogenheter utfärdad av den ansvariga ministern och godkänd av en *Judicial Commissioner* ⁽³⁸⁹⁾. Om en person avsiktligt väljer ut avlyssnat innehåll för granskning i strid med kraven i lagstiftningen ⁽³⁹⁰⁾ begår han eller hon ett brott ⁽³⁹¹⁾.

⁽³⁸²⁾ Avsnitt 156 i 2016 års lag om utredningsbefogenheter.

⁽³⁸³⁾ Avsnitten 150 och 191 i 2016 års lag om utredningsbefogenheter.

⁽³⁸⁴⁾ I målet *Big Brother Watch m.fl. mot Förenade kungariket* (se fotnot 268) upprätthöll Europeiska domstolen för de mänskliga rättigheterna (stora avdelningen) systemet med ytterligare skyddsåtgärder för lagring, tillgång och utlämnande som föreskrevs i 2000 års lag om utredningsbefogenheter, se punkterna 392–394 och 402–405. Samma system med skyddsåtgärder föreskrivs i 2016 års lag om utredningsbefogenheter.

⁽³⁸⁵⁾ Avsnitten 151 och 192 i 2016 års lag om utredningsbefogenheter.

⁽³⁸⁶⁾ För ytterligare information om dessa ändamål, se fotnot 312.

⁽³⁸⁷⁾ I koderna om avlyssning av kommunikation anges följande: "Dessa behandlingssystem behandlar data från de kommunikationslänkar eller signaler som den avlyssnande myndigheten har valt att avlyssna. En viss filtrering tillämpas sedan på trafiken på dessa länkar och signaler som är utformad för att välja typer av kommunikation av potentiellt underrättelsevärde samtidigt som man bortser från de typer av kommunikation som minst sannolikt är av underrättelsevärde. Till följd av denna filtrering, som kommer att variera mellan olika behandlingssystem, kommer en betydande del av kommunikationen på dessa länkar och signaler att kasseras automatiskt. Ytterligare komplicerade sökningar kan sedan göras för att ta fram ytterligare meddelanden som sannolikt har störst underrättelsevärde och som rör myndighetens lagstadgade uppgifter. Dessa meddelanden kan sedan väljas ut för granskning för ett eller flera av de operativa syften som anges i beslutet om villkoren för nödvändighet och proportionalitet är uppfyllda. Endast poster som inte har filtrerats kan väljas ut för granskning av behöriga personer" (*Codes of practice on interception of communications*, punkt 6.6, se fotnot 278).

⁽³⁸⁸⁾ Se avsnitt 152.1 a och b i 2016 års lag om utredningsbefogenheter, där det anges att granskning av båda typerna av uppgifter (avlyssnat innehåll och sekundära uppgifter) endast får utföras för ett uttryckligt ändamål och måste vara nödvändig och proportionerlig under alla omständigheter.

⁽³⁸⁹⁾ Denna typ av beslut krävs inte om uppgifter som rör personer som befinner sig på de brittiska öarna utgör "sekundära uppgifter" (se avsnitt 152.1 c i 2016 års lag om utredningsbefogenheter).

⁽³⁹⁰⁾ Avsnitten 152 och 193 i 2016 års lag om utredningsbefogenheter.

⁽³⁹¹⁾ Avsnitten 155 och 196 i 2016 års lag om utredningsbefogenheter.

- (230) Analytikerns bedömning av urvalet av materialet är föremål för en efterhandsöversyn av *the Investigatory Powers Commissioner* som utvärderar efterlevnaden av de särskilda skyddsåtgärder som fastställs i 2016 års lag om utredningsbefogenheter för granskningsfasen ⁽³⁹²⁾ (se även skäl 229). *The Investigatory Powers Commissioner* måste övervaka (bland annat genom revisioner, inspektioner och utredningar) myndigheternas utövande av de utredningsbefogenheter som nämns i 2016 års lag om utredningsbefogenheter ⁽³⁹³⁾. I detta avseende klargörs det i uppförandekoden om avlyssning av kommunikation och uppförandekoden om ingrepp i utrustning att myndigheten måste föra register för efterföljande granskningar och revisioner och i dessa register ska anges varför behöriga personers tillgång till materialet är nödvändig och proportionell och de tillämpliga operativa ändamålen ⁽³⁹⁴⁾. I sin årsrapport för 2018 drar IPCO ⁽³⁹⁵⁾ slutsatsen att analytikernas motiveringar för granskningen av visst material som samlats in i massomfattning uppfyllde kraven på proportionalitet genom att tillhandahålla tillräckliga uppgifter om skälen till deras "frågor" i förhållande till det syfte som skulle uppnås ⁽³⁹⁶⁾. I sin rapport om massbefogenheter från 2019 uttryckte IPCO klart sin avsikt att fortsätta inspektionerna av massavlyssningar, inklusive en detaljerad granskning av urvals- och sökkriterierna ⁽³⁹⁷⁾. IPCO kommer även att fortsätta att noggrant och från fall till fall kontrollera valet av övervakningsåtgärder (riktade åtgärder eller massåtgärder) i samband med handläggning av ansökningar om betyg enligt *double lock*-förfarandet och vid inspektioner ⁽³⁹⁸⁾. Kommissionen kommer vederbörligen att beakta denna ytterligare övervakning när den övervakar detta beslut enligt skälen 281–284.

3.3.1.1.4.2 Massinhämtande av kommunikationsuppgifter

- (231) Kapitel 2 i del 6 i 2016 års lag om utredningsbefogenheter reglerar beslut om massinhämtande som ger mottagaren rätt att kräva att en teleoperatör lämnar ut eller erhåller eventuella kommunikationsuppgifter som operatören förfogar över. Dessa beslut godkänner också att den begärande myndigheten väljer ut uppgifterna för den fortsatta fasen av granskningen. Precis som när det gäller riktad lagring och inhämtande av kommunikationsuppgifter (se skäl 199) rör det mesta massinhämtande av kommunikationsuppgifter normalt inte personuppgifter om registrerade i EU som överförs till Förenade kungariket enligt detta beslut. Skyldigheten att lämna ut kommunikationsuppgifter enligt kapitel 2 i del 6 i 2016 års lag om utredningsbefogenheter omfattar uppgifter som samlas in av teleoperatörer i Förenade kungariket direkt från användarna av en telekommunikationstjänst ⁽³⁹⁹⁾. Denna typ av "kundtillvänd" behandling omfattar vanligtvis inte en överföring på grundval av detta beslut, dvs. en överföring från en personuppgiftsansvarig/ett personuppgiftsbiträde i EU till en personuppgiftsansvarig/ett personuppgiftsbiträde i Förenade kungariket.
- (232) För fullständighetens skull beskrivs dock de villkor och skyddsåtgärder som gäller för massinhämtande av kommunikationsuppgifter nedan.

⁽³⁹²⁾ Avsnitten 152 och 193 i 2016 års lag om utredningsbefogenheter.

⁽³⁹³⁾ Avsnitt 229 i 2016 års lag om utredningsbefogenheter.

⁽³⁹⁴⁾ *Code of Practice on Interception of Communications*, punkt 6.74, se fotnot 278 och *Code of Practice on Equipment Interference*, punkt 6.78, se fotnot 348.

⁽³⁹⁵⁾ IPCO har bildats enligt avsnitt 238 i 2016 års lag om utredningsbefogenheter för att förse *the Investigatory Powers Commissioner* med nödvändig personal, logi, utrustning och andra hjälpmedel och tjänster som krävs för att de ska kunna utföra sina uppgifter (se skäl 251).

⁽³⁹⁶⁾ I *IPCO Annual Report 2018* angavs att de motiveringar som gjorts av analytiker vid *Government Communications Headquarters* uppfyllde den standard som krävs och att analytikerna tog tillräcklig hänsyn till proportionaliteten i deras förfrågningar om massuppgifter. *Annual Report of the Investigatory Powers Commissioner 2018*, punkt 6.22, se fotnot 464.

⁽³⁹⁷⁾ *Annual Report of the Investigatory Powers Commissioner 2019*, punkt 7.6, se fotnot 463.

⁽³⁹⁸⁾ *Annual Report of the Investigatory Powers Commissioner 2019*, punkt 10.22, se fotnot 463.

⁽³⁹⁹⁾ Detta följer av definitionen av kommunikationsuppgifter i avsnitt 261.5 i 2016 års lag om utredningsbefogenheter enligt vilken kommunikationsuppgifter innehas eller erhålls av en teleoperatör och avser antingen användaren av en telekommunikationstjänst och tillhandahållandet av denna tjänst eller ingår i, ingår som en del av, läggs till eller logiskt förknippas med en kommunikation (se även *Code of Practice on Bulk Acquisition of Communications Data*, som finns på följande länk: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf punkterna 2.15 till 2.22). Dessutom kräver definitionen av teleoperatör i avsnitt 261.10 i 2016 års lag om utredningsbefogenheter att en teleoperatör är en person som erbjuder eller tillhandahåller en telekommunikationstjänst till personer i Förenade kungariket eller som kontrollerar eller tillhandahåller ett telekommunikationssystem som (helt eller delvis) är beläget i eller kontrolleras från Förenade kungariket. Dessa definitioner klargör att skyldigheter enligt 2016 års lag om utredningsbefogenheter inte kan åläggas teleoperatörer vars utrustning inte finns i eller kontrolleras från Förenade kungariket och som inte erbjuder eller tillhandahåller tjänster till personer i Förenade kungariket (se även *Code of Practice on Bulk Acquisition of Communications Data*, punkt 2.2). Om EU-abonnenter (oavsett om de befinner sig i EU eller i Förenade kungariket) använde sig av tjänster i Förenade kungariket skulle all kommunikation i samband med tillhandahållandet av denna tjänst samlas in direkt av tjänsteleverantören i Förenade kungariket i stället för att bli föremål för en överföring från EU.

- (233) 2016 års lag om utredningsbefogenheter ersätter den lagstiftning om massinhämtande av kommunikationsuppgifter som var föremål för EU-domstolens dom i målet *Privacy International*. Den lagstiftning som var i fråga i det målet upphävdes och det nya systemet innehåller särskilda villkor och garantier för att en sådan åtgärd ska kunna godkännas.
- (234) I synnerhet kräver 2016 års lag om utredningsbefogenheter, till skillnad från det tidigare systemet enligt vilket den ansvariga ministern hade full handlingsfrihet när det gäller att godkänna åtgärden ⁽⁴⁰⁰⁾, att den ansvariga ministern endast ska utfärda ett beslut om åtgärden är nödvändig och proportionerlig. Detta innebär i praktiken att det bör finnas en koppling mellan tillgången till uppgifterna och det eftersträvade målet ⁽⁴⁰¹⁾. Närmare bestämt måste den ansvariga ministern bedöma om det finns ett samband mellan den begärda åtgärden och ett eller flera "operativa ändamål" som anges i beslutet (se skäl 219) med avseende på proportionalitetsbedömningen och i den relevanta uppförandekoden anges att "ministern måste beakta huruvida det som avses med beslutet rimligen skulle kunna uppnås med andra mindre inkräktande medel (avsnitt 2.2 a i lagen). Till exempel inhämtande av den begärda informationen genom en mindre inkräktande befogenhet, till exempel riktat inhämtande av kommunikationsuppgifter" ⁽⁴⁰²⁾.
- (235) För att göra en sådan bedömning kommer den ansvariga ministern att förlita sig på uppgifter som underrättelsetjänsterna ⁽⁴⁰³⁾ är skyldiga att lämna i sin ansökan, till exempel skälen till att åtgärden anses nödvändig på grund av en av de lagstadgade grunderna och skälen till att det som eftersträvas inte rimligen skulle kunna uppnås med andra, mindre inkräktande medel ⁽⁴⁰⁴⁾. Dessutom begränsar de operativa ändamålen det område inom vilket de uppgifter som erhållits inom ramen för beslutet kan väljas ut för granskning ⁽⁴⁰⁵⁾. Enligt den relevanta uppförandekoden ska de operativa ändamålen beskriva ett tydligt krav och vara tillräckligt detaljerade för att övertyga den ansvariga ministern om att inhämtade uppgifter endast får väljas ut för granskning av särskilda skäl ⁽⁴⁰⁶⁾. Den ansvariga ministern måste nämligen, innan beslutet godkänns, se till att det finns särskilda arrangemang för att säkerställa att endast det material som har bedömts vara nödvändigt för ett operativt ändamål och ett lagstadgat syfte väljs ut för granskningen och att det bör vara proportionerligt och nödvändigt under alla omständigheter. Detta särskilda krav, som återspeglas i avsnitten 158 och 172 ⁽⁴⁰⁷⁾ i 2016 års lag om utredningsbefogenheter, när det gäller förhandsbedömningen av nödvändigheten och proportionaliteten för de kriterier som används för urvalet utgör en annan viktig nyhet i den ordning som infördes genom 2016 års lag om utredningsbefogenheter jämfört med den tidigare ordningen.
- (236) Genom 2016 års lag om utredningsbefogenheter infördes också en skyldighet för den ansvariga ministern att se till att vissa begränsningar finns vad gäller säkerhet, lagring och utlämnande är begränsade innan beslut om massinhämtande av kommunikationsuppgifter utfärdas ⁽⁴⁰⁸⁾. Vad gäller utlämnande till utlandet gäller de skyddsåtgärder som beskrivs i skäl 227 även i detta sammanhang för massavlyssning och massgrepp i utrustning ⁽⁴⁰⁹⁾. Ytterligare begränsningar fastställs i lagstiftningen om giltighetstid ⁽⁴¹⁰⁾, förnyelse ⁽⁴¹¹⁾ och ändring av "massbesluten" ⁽⁴¹²⁾.
- (237) Det är viktigt att den ansvariga ministern innan beslutet utfärdas måste få ett godkännande av en *Judicial Commissioner* på samma sätt som gäller för övriga massbefogenheter ⁽⁴¹³⁾. Detta är ett centralt inslag i den ordning som infördes genom 2016 års lag om utredningsbefogenheter.

⁽⁴⁰⁰⁾ I avsnitt 94.1 i *Telecommunication Act 1984* föreskrevs att den ansvariga ministern kunde utfärda "allmänna anvisningar som enligt den ansvariga ministern framstår som nödvändiga eller lämpliga med hänsyn till den nationella säkerheten (...)" (se fotnot 451).

⁽⁴⁰¹⁾ Se *Privacy International*, punkt 78.

⁽⁴⁰²⁾ Se *Code of Practice on Bulk Acquisition of Communications Data*, punkt 4.11 (se fotnot 399).

⁽⁴⁰³⁾ Ett beslut om massinhämtande får endast begäras av cheferna för underrättelsetjänster som är i) generaldirektören för säkerhetstjänsten, ii) chefen för underrättelsetjänsten eller iii) chefen för *Government Communications Headquarters* (se avsnitten 158 och 263 i 2016 års lag om utredningsbefogenheter).

⁽⁴⁰⁴⁾ *Code of Practice on Bulk Acquisition of Communications Data*, punkt 4.5 (se fotnot 399).

⁽⁴⁰⁵⁾ Enligt avsnitt 161 i 2016 års lag om utredningsbefogenheter ska de operativa syften som anges i beslutet vara de som anges i en förteckning som förs av cheferna för underrättelsetjänsterna (nedan kallad förteckningen över operativa ändamål) eftersom de anser att de är operativa ändamål för vilka kommunikationsuppgifter som erhålls genom beslut om massinhämtande kan väljas ut för granskning.

⁽⁴⁰⁶⁾ *Code of Practice on Bulk Acquisition of Communications Data*, punkt 6.6 (se fotnot 399).

⁽⁴⁰⁷⁾ Enligt avsnitt 172 i 2016 års lag om utredningsbefogenheter ska särskilda skyddsåtgärder införas för filtrerings- och urvalsfasen för granskning av kommunikation som inhämtats i massomfattning. Dessutom är en avsiktlig granskning i strid med dessa skyddsåtgärder också ett brott (se avsnitt 173 i 2016 års lag om utredningsbefogenheter).

⁽⁴⁰⁸⁾ Avsnitt 171 i 2016 års lag om utredningsbefogenheter.

⁽⁴⁰⁹⁾ Avsnitt 171.9 i 2016 års lag om utredningsbefogenheter.

⁽⁴¹⁰⁾ Avsnitt 162 i 2016 års lag om utredningsbefogenheter.

⁽⁴¹¹⁾ Avsnitt 163 i 2016 års lag om utredningsbefogenheter.

⁽⁴¹²⁾ Avsnitten 164–166 i 2016 års lag om utredningsbefogenheter.

⁽⁴¹³⁾ Avsnitt 159 i 2016 års lag om utredningsbefogenheter.

- (238) *The Investigatory Powers Commissioner* utför en efterhandsöversyn av granskningsförfarandet över det material (kommunikationsuppgifter) som inhämtats i massomfattning (se skäl 254 nedan). I 2016 års lag om utredningsbefogenheter infördes i detta avseende ett krav på att underrättelseanalytikern måste registrera skälen till att den föreslagna granskningen är nödvändig och proportionerlig för ett bestämt operativt syfte innan han eller hon väljer ut de uppgifter som ska granskas⁽⁴¹⁴⁾. I IPCO:s årsrapport 2019 konstaterades med avseende på *Government Communications Headquarters* och säkerhetstjänsten MI5:s praxis att "den avgörande roll som data från masskommunikationsuppgifter spelar för den verksamhet som bedrivs vid *Government Communications Headquarters* var väl förankrad i det arbete som vi inspekterade. Vi bedömde de begärda uppgifternas art och de angivna underrättelsekraven och var övertygade om att dokumentationen visade att deras tillvägagångssätt var nödvändigt och proportionerligt"⁽⁴¹⁵⁾. MI5:s registrerade motiveringar var av god standard och uppfyllde principerna om nödvändighet och proportionalitet"⁽⁴¹⁶⁾.

3.3.1.1.4.3 Lagring och granskning av massdataset av personuppgifter

- (239) Genom beslut om massdataset av personuppgifter⁽⁴¹⁷⁾ får underrättelsetjänster tillstånd får lagra och undersöka dataset som innehåller personuppgifter som rör ett antal enskilda personer. Enligt de brittiska myndigheternas förklaringar kan analysen av sådana dataset vara "det enda sättet för UKIC att gå vidare med utredningar och identifiera terrorister från mycket begränsade ledande underrättelser eller när deras kommunikation avsiktligt har dolts"⁽⁴¹⁸⁾. Det finns två typer av beslut enligt följande: "Typbeslut om massdataset av personuppgifter"⁽⁴¹⁹⁾ som avser en viss kategori av dataset, dvs. dataset som liknar varandra i fråga om innehåll och föreslagen användning och som tar upp liknande överväganden som exempelvis graden av intrång och känslighet och proportionaliteten i användningen av uppgifterna, vilket gör det möjligt för den ansvariga ministern att beakta nödvändigheten och proportionaliteten av att samla in alla uppgifter inom den relevanta typen vid en enda tidpunkt. Till exempel kan ett typbeslut om massdataset av personuppgifter omfatta resedataset som avser liknande rutter⁽⁴²⁰⁾. "specifika beslut om massdataset av personuppgifter"⁽⁴²¹⁾ avser i stället ett specifikt dataset, till exempel ett dataset av en ny eller ovanlig typ av information som inte omfattas av en befintlig typ av beslut om massdataset av personuppgifter eller ett dataset som rör specifika typer av personuppgifter⁽⁴²²⁾ och därför kräver ytterligare skyddsåtgärder⁽⁴²³⁾. Bestämmelserna i 2016 års lag om utredningsbefogenheter gällande massdataset av personuppgifter tillåter att sådana dataset granskas och lagras endast om det är nödvändigt och proportionerligt att göra detta⁽⁴²⁴⁾ och i enlighet med de allmänna skyldigheterna i fråga om integritet⁽⁴²⁵⁾.
- (240) Befogenheten att utfärda ett beslut om massdataset av personuppgifter omfattas av *double lock*-förfarandet där bedömningen av åtgärdens nödvändighet och proportionalitet görs först av den ansvariga ministern och därefter av *the Judicial Commissioner*⁽⁴²⁶⁾. Den ansvariga ministern är skyldig att beakta arten och omfattningen av den typ av beslut som begärs, vilken kategori av uppgifter det rör sig om och antalet enskilda massdataset av personuppgifter som sannolikt omfattas av den specifika typen av beslut⁽⁴²⁷⁾. Enligt vad som anges i uppförandekoden för underrättelsetjänsters lagring och användning av massdataset av personuppgifter ska detaljerade register föras och omfattas av revision av *the Investigatory Powers Commissioner*⁽⁴²⁸⁾. Att lagra och granska massdataset av personuppgifter utanför begränsningarna i 2016 års lag om utredningsbefogenheter är ett brott⁽⁴²⁹⁾.

⁽⁴¹⁴⁾ IPCO Annual Report 2019, punkt 8.6, se fotnot 463.

⁽⁴¹⁵⁾ IPCO Annual Report 2019, punkt 10.4, se fotnot 463.

⁽⁴¹⁶⁾ IPCO Annual Report 2019, punkt 8.37, se fotnot 463.

⁽⁴¹⁷⁾ Avsnitt 200 i 2016 års lag om utredningsbefogenheter.

⁽⁴¹⁸⁾ UK Explanatory Framework for Adequacy Discussions, avsnitt H: National Security, s. 34, se fotnot 29.

⁽⁴¹⁹⁾ Avsnitt 204 i 2016 års lag om utredningsbefogenheter.

⁽⁴²⁰⁾ Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets, punkt 4.7, som finns på följande länk: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715478/Bulk_Personal_Datasets_Code_of_Practice.pdf.

⁽⁴²¹⁾ Avsnitt 205 i 2016 års lag om utredningsbefogenheter.

⁽⁴²²⁾ Till exempel känsliga personuppgifter, se avsnitt 202 i 2016 års lag om utredningsbefogenheter och *the Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets*, punkterna 4.21 och 4.12, se fotnot 469.

⁽⁴²³⁾ En ansökan om ett specifikt beslut om massdataset av personuppgifter måste bedömas individuellt av den ansvariga ministern, dvs. med avseende på en specifik datauppsättning. Underrättelsetjänsten är enligt avsnitt 205 i lagen om utredningsbefogenheter skyldig att i sin ansökan om specifika massdataset av personuppgifter inkludera en detaljerad förklaring av arten och omfattningen av det aktuella materialet och en förteckning över de "operativa syften" för vilka den berörda underrättelsetjänsten vill granska massdataset av personuppgifter (där underrättelsetjänsten ansöker om ett beslut om lagring och granskning, snarare än enbart lagring). Vid utfärdandet av ett typbeslut om massdataset av personuppgifter beaktar sekreteraren i stället hela kategorin av dataset samtidigt.

⁽⁴²⁴⁾ Avsnitten 204 och 205 i 2016 års lag om utredningsbefogenheter.

⁽⁴²⁵⁾ Avsnitt 2 i 2016 års lag om utredningsbefogenheter.

⁽⁴²⁶⁾ Avsnitten 204 och 205 i 2016 års lag om utredningsbefogenheter.

⁽⁴²⁷⁾ Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets, punkt 5.2, se fotnot 420.

⁽⁴²⁸⁾ Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets, punkterna 8.1–8.15, se fotnot 420.

⁽⁴²⁹⁾ UK Explanatory Framework for Adequacy Discussions, avsnitt H: National Security, s. 34, se fotnot 29.

3.3.2 Vidare användning av de insamlade uppgifterna

- (241) Personuppgifter som behandlas enligt del 4 i 2018 års dataskyddslag får inte behandlas på ett sätt som är oförenligt med det syfte för vilket de samlades in ⁽⁴³⁰⁾. 2018 års dataskyddslag föreskriver att den personuppgiftsansvariga får behandla uppgifterna för ett annat ändamål än det för vilket uppgifterna samlades in om det är förenligt med det ursprungliga ändamålet och förutsatt att den personuppgiftsansvariga enligt lag har rätt att behandla uppgifterna och att behandlingen är nödvändig och proportionerlig ⁽⁴³¹⁾. I *Security Services Act 1989* och *Intelligence Services Act 1994* anges dessutom att cheferna för underrättelsetjänsterna är skyldiga att se till att ingen information erhålls eller röjs utom i den mån det är nödvändigt för att myndigheten ska kunna fullgöra sina uppgifter på ett korrekt sätt eller för de andra begränsade och specifika ändamål som anges i de relevanta bestämmelserna ⁽⁴³²⁾.
- (242) I avsnitt 109 i 2018 års dataskyddslag fastställs dessutom särskilda krav för underrättelsetjänsters internationella överföring av personuppgifter till tredjeländer eller internationella organisationer. Enligt denna bestämmelse får personuppgifter inte överföras till ett land eller territorium utanför Förenade kungariket eller till en internationell organisation om inte överföringen är nödvändig och proportionell med hänsyn till den personuppgiftsansvarigas lagstadgade uppgifter eller för andra ändamål som anges i avsnitt 2.2 a i *Security Services Act 1989* eller avsnitten 2.2 a och 4.2 a i *Intelligence Services Act 1994* ⁽⁴³³⁾. Det är viktigt att notera att dessa krav även gäller i situationer där undantaget avseende nationell säkerhet enligt avsnitt 110 i 2018 års dataskyddslag åberopas, eftersom avsnitt 109 inte anges i samma lags avsnitt 110 som en av de bestämmelser som kan upphöra att gälla om ett undantag från vissa bestämmelser krävs för att skydda den nationella säkerheten.
- (243) Såsom ICO framhåller i sin vägledning om underrättelsetjänsters behandling av personuppgifter omfattas underrättelsetjänster när de utbyter uppgifter med ett underrättelseorgan i ett tredjeland, utöver skyddsåtgärderna enligt avsnitt 4 i 2018 års dataskyddslag, även av skyddsåtgärder enligt andra lagstiftningsåtgärder som är tillämpliga på dem, i syfte att säkerställa att personuppgifter inhämtas, utbyts och hanteras på ett lagligt och ansvarsfullt sätt ⁽⁴³⁴⁾. Exempelvis fastställs i 2016 års lag om utredningsbefogenheter ytterligare skyddsåtgärder när det gäller överföring till tredjeland av material som samlats in genom riktad avlyssning ⁽⁴³⁵⁾, riktade ingrepp i utrustning ⁽⁴³⁶⁾, massavlyssning ⁽⁴³⁷⁾, massinhämtande av kommunikationsuppgifter ⁽⁴³⁸⁾ och massingrepp i utrustning ⁽⁴³⁹⁾ (så kallade utlämnanden till utlandet). I synnerhet måste den myndighet som utfärdar beslutet se till att det finns gällande arrangemang för att säkerställa att det tredjeland som mottar uppgifterna begränsar antalet personer som ser materialet, omfattningen av utlämnandet och antalet kopior av allt material till det minimum som krävs för de godkända ändamål som anges i 2016 års lag om utredningsbefogenheter ⁽⁴⁴⁰⁾.

3.3.3 Tillsyn

- (244) Statliga myndigheters tillträde för ändamål som rör nationell säkerhet övervakas av ett antal olika organ. *The Information Commissioner* övervakar behandlingen av personuppgifter mot bakgrund av 2018 års dataskyddslag (för mer information om dennes oberoende, utnämningssfunktion och befogenheter, se skälen 85–98) medan oberoende och rättslig tillsyn av användningen av utredningsbefogenheter inom ramen för 2016 års lag om utredningsbefogenheter tillhandahålls av *the Investigatory Powers Commissioner*. *The Investigatory Powers Commissioner* övervakar både

⁽⁴³⁰⁾ Avsnitt 87.1 i 2018 års dataskyddslag.

⁽⁴³¹⁾ Avsnitt 87.3 i 2018 års dataskyddslag. Personuppgiftsansvariga kan undantas från denna princip enligt avsnitt 110 i 2018 års dataskyddslag i den mån ett sådant undantag krävs för att skydda den nationella säkerheten men ett sådant undantag måste bedömas från fall till fall och kan endast åberopas i den mån tillämpningen av en viss bestämmelse skulle få negativa konsekvenser för den nationella säkerheten (se skäl 132). De nationella säkerhetscertifikaten för underrättelsetjänsterna i Förenade kungariket (finns på följande länk: <https://ico.org.uk/about-the-ico/our-information/national-security-certificates/>) täcker inte avsnitt 87.3 i 2018 års dataskyddslag. Eftersom all behandling för ett annat ändamål måste vara tillåten enligt lag måste underrättelsetjänsterna dessutom ha en tydlig rättslig grund för den vidare behandlingen.

⁽⁴³²⁾ För ytterligare information om dessa ändamål, se fotnot 312.

⁽⁴³³⁾ Se fotnot 312.

⁽⁴³⁴⁾ *ICO guidance on intelligence services processing* (se fotnot 161).

⁽⁴³⁵⁾ Avsnitt 54 i 2016 års lag om utredningsbefogenheter.

⁽⁴³⁶⁾ Avsnitt 130 i 2016 års lag om utredningsbefogenheter.

⁽⁴³⁷⁾ Avsnitt 151 i 2016 års lag om utredningsbefogenheter.

⁽⁴³⁸⁾ Avsnitt 171.9 i 2016 års lag om utredningsbefogenheter.

⁽⁴³⁹⁾ Avsnitt 192 i 2016 års lag om utredningsbefogenheter.

⁽⁴⁴⁰⁾ Åtgärderna ska omfatta åtgärder för att säkerställa att varje exemplar av materialet lagras på ett säkert sätt så länge det bevaras. Det material som erhållits med stöd av ett beslut och eventuella kopior av detta material ska förstöras så snart det inte längre finns någon relevant grund för att behålla det (se avsnitten 150.2, 150.5 och 151.2 i 2016 års lag om utredningsbefogenheter). Det är värt att nämna att liknande skyddsåtgärder som föreskrevs enligt den tidigare rättsliga ramen (2000 års lag om utredningsbefogenheter) ansågs överensstämma med de krav som Europeiska domstolen för de mänskliga rättigheterna (stora avdelningen) har fastställt för utbyte av material som inhämtats genom massavlyssning med utländska stater eller internationella organisationer (Europeiska domstolen för de mänskliga rättigheterna (stora avdelningen), *Big Brother Watch m.fl./Förenade kungariket* (se fotnot 279), punkterna 362 och 399).

brottsbekämpande och nationella säkerhetsmyndigheters användning av utredningsbefogenheter enligt 2016 års lag om utredningsbefogenheter. Den politiska tillsynen garanteras av parlamentets utskott för underrättelsetjänsten (*Intelligence Service Committee*).

3.3.3.1 Tillsyn enligt del 4 i dataskyddslagen

- (245) Underrättelsetjänsternas behandling av personuppgifter enligt del 4 i 2018 års dataskyddslag övervakas av *the Information Commissioner* ⁽⁴⁴¹⁾.
- (246) De allmänna arbetsuppgifter som *the Information Commissioner* har vad gäller underrättelsetjänsters behandling av personuppgifter enligt del 4 i 2018 års dataskyddslag fastställs i tillägg 13 till 2018 års dataskyddslag. Uppgifterna omfattar, men är inte begränsade till, övervakning och efterlevnad av del 4 i 2018 års dataskyddslag, främjande av allmänhetens medvetenhet, rådgivning till parlamentet, regeringen och andra institutioner om lagstiftningsåtgärder och administrativa åtgärder, främjande av personuppgiftsansvarigas och personuppgiftsbiträdens medvetenhet om sina skyldigheter, tillhandahållande av information till registrerade om utövande av den registrerades rättigheter, genomförande av utredningar osv.
- (247) *The Commissioner* har, liksom för del 3 i 2018 års dataskyddslag, befogenhet att underrätta personuppgiftsansvariga om en påstådd överträdelse och utfärda varningar om att en behandling sannolikt kommer att strida mot reglerna och utfärda reprimander när överträdelsen bekräftas. Han eller hon kan också utfärda förelägganden om verkställighet och påföljder för överträdelser av vissa bestämmelser i lagen ⁽⁴⁴²⁾. I motsats till vad som gäller för andra delar av 2018 års dataskyddslag kan dock *the Commissioner* inte utfärda ett bedömningsföreläggande till ett nationellt säkerhetsorgan ⁽⁴⁴³⁾.
- (248) I avsnitt 110 i 2018 års dataskyddslag föreskrivs dessutom ett undantag från användningen av vissa av de befogenheter *the Commissioner* har när detta krävs för att skydda den nationella säkerheten. Detta inbegriper de befogenheter *the Commissioner* har att utfärda (alla typer av) förelägganden enligt dataskyddslagen (information, bedömning, verkställighet och påföljder), befogenhet att utföra inspektioner i enlighet med internationella skyldigheter, befogenheter för tillträde och inspektion samt regler om brott ⁽⁴⁴⁴⁾. Enligt skäl 126 gäller dessa undantag endast om det är nödvändigt och proportionerligt samt från fall till fall.
- (249) ICO och brittiska underrättelsetjänster har undertecknat ett samförståndsavtal ⁽⁴⁴⁵⁾ som fastställer en ram för samarbete i ett antal frågor, bland annat anmälningar om personuppgiftsbrott och hantering av klagomål från registrerade. Det föreskrivs särskilt att ICO, efter att ha mottagit ett klagomål, ska bedöma om tillämpningen av eventuella undantag för nationell säkerhet har använts på lämpligt sätt. Svar på ICO frågor i samband med granskningen av enskilda klagomål måste lämnas inom 20 arbetsdagar av den berörda underrättelsetjänsten med hjälp av lämpliga säkra kanaler om det rör sig om sekretessbelagd information. Från april 2018 till dags dato har ICO mottagit 21 klagomål från enskilda personer om underrättelsetjänsterna. Varje klagomål bedömdes och resultatet meddelades den registrerade ⁽⁴⁴⁶⁾.

⁽⁴⁴¹⁾ Avsnitt 116 i 2018 års dataskyddslag.

⁽⁴⁴²⁾ I enlighet med punkt 2 i tillägg 13 till 2018 års dataskyddslag kan förelägganden om verkställighet och påföljder utfärdas till en personuppgiftsansvarig eller ett personuppgiftsbiträde i samband med överträdelser av kapitel 2 i del 4 i 2018 års dataskyddslag (principer för behandling), en bestämmelse i del 4 i 2018 års dataskyddslag som ger den registrerade rättigheter, ett krav på att meddela ett personuppgiftsbrott till *the Commissioner* enligt avsnitt 108 i 2018 års dataskyddslag och principerna för överföring av personuppgifter till tredjeländer, länder som inte omfattas av konventionen och internationella organisationer i avsnitt 109 i 2018 års dataskyddslag (för ytterligare information om verkställighets- och påföljdsförelägganden hänvisas till skäl 92).

⁽⁴⁴³⁾ Enligt avsnitt 147.6 i 2018 års dataskyddslag får *the Information Commissioner* inte utfärda ett bedömningsföreläggande till ett organ som anges i avsnitt 23.3 i *Freedom of Information Act 2000*. Detta inbegriper säkerhetstjänsten (MI5), underrättelsetjänsten (MI6) och underrättelseorganet Government Communications Headquarter (GCHQ).

⁽⁴⁴⁴⁾ Följande bestämmelser kan undantas: Avsnitt 108 (meddelande till *the Commissioner* om personuppgiftsbrott), avsnitt 119 (inspektion i enlighet med internationella förpliktelser). Avsnitten 142–154 och tillägg 15 (förelägganden och befogenheter för tillträde och inspektion från *the Commissioner*). Avsnitten 170–173 (personuppgiftsbrott). Dessutom när det gäller underrättelsetjänsternas behandling i tillägg 13 (andra allmänna uppgifter för *the Commissioner*), punkt 1 a och g samt punkt 2.

⁽⁴⁴⁵⁾ *Memorandum of Understandings between Information Commission's Office and the UK Intelligence Community*, se fotnot 165.

⁽⁴⁴⁶⁾ I sju av dessa fall rädde ICO klaganden att ta upp frågan med den personuppgiftsansvariga (detta är fallet när en person har tagit upp en fråga med ICO men borde ha tagit upp frågan med den personuppgiftsansvariga först), i ett av dessa fall gav ICO allmänna råd till den personuppgiftsansvariga (detta används när den personuppgiftsansvarigas åtgärder inte verkar ha brutit mot lagstiftningen men en förbättring av rutinerna kunde ha förhindrat problemet som tagits upp med ICO) och i de övriga 13 fallen krävdes ingen åtgärd av den personuppgiftsansvariga (detta används när problem tas upp av den individ som 2018 års dataskyddslag gäller för eftersom han eller hon är bekymrad över behandlingen av personuppgifter men baserat på den information som tillhandahålls verkar det inte som om den personuppgiftsansvariga har brutit mot lagstiftningen).

3.3.3.2 Översyn av användningen av utredningsbefogenheter inom ramen för 2016 års lag om utredningsbefogenheter

- (250) Enligt del 8 i 2016 års lag om utredningsbefogenheter utövas tillsynen över användningen av utredningsbefogenheter av *the Investigatory Powers Commissioner*. *The Investigatory Powers Commissioner* består av andra rättsliga *Judicial Commissioners* som tillsammans kallas *Judicial Commissioners* ⁽⁴⁴⁷⁾. I 2016 års lag om utredningsbefogenheter fastställs garantier som skyddar *Judicial Commissioners* oberoende. *Judicial Commissioners* måste inneha eller ha innehaft ett högt domarämbete (dvs. de måste vara eller ha varit ledamöter av överdomstolarna) ⁽⁴⁴⁸⁾ och de har, i egenskap av domare, en oberoende ställning i förhållande till regeringen ⁽⁴⁴⁹⁾. Enligt avsnitt 227 i 2016 års lag om utredningsbefogenheter är det premiärministern som utser IPC och så många *Judicial Commissioners* som han eller hon anser vara nödvändiga. Alla *Commissioners*, vare sig där är aktiva eller tidigare verksamma inom rättsväsendet, får endast utses på grundval av en gemensam rekommendation från de tre *Chief Justices for England & Wales, Scotland and Northern Ireland* och *Lord Chancellor* ⁽⁴⁵⁰⁾. Den ansvarige ministern måste förse *the Investigatory Powers Commissioner* med personal, inkvartering, utrustning och andra faciliteter och tjänster ⁽⁴⁵¹⁾. Mandatperiod för en *Commissioner* är tre år och de kan utnämnas på nytt ⁽⁴⁵²⁾. Som en ytterligare garanti för deras oberoende kan *Judicial Commissioners* endast avsättas enligt stränga villkor med en hög tröskel antingen av premiärministern under de särskilda omständigheter som anges på ett uttömmande sätt i avsnitt 228.5 i 2016 års lag om utredningsbefogenheter (t.ex. konkurs eller fängelse) eller om båda kamrarna har antagit en resolution om att godkänna avsättningen ⁽⁴⁵³⁾.
- (251) *The Investigatory Powers Commissioner* och *the Judicial Commissioners* består i sina roller av IPCO. IPCO:s personal består av en grupp inspektörer, intern juridisk och teknisk expertis och en teknisk rådgivande panel som ska ge expertråd. Liksom är fallet för de individuella *Judicial Commissioners* skyddas oberoendet för IPCO. IPCO är ett "organ på armlängds avstånd" inom inrikesministeriet, dvs. det får finansiering från inrikesministeriet men utför sina uppgifter självständigt ⁽⁴⁵⁴⁾.
- (252) *Judicial Commissioners* huvuduppgifter anges i avsnitt 229 i 2016 års lag om utredningsbefogenheter ⁽⁴⁵⁵⁾. I synnerhet har *Judicial Commissioners* omfattande befogenheter att förhandsgodkänna, vilket är en del av de garantier som införts i Förenade kungarikets rättsliga ram genom 2016 års lag om utredningsbefogenheter. Beslut i samband med riktad avlyssning, ingrepp i utrustning, masdataset av personuppgifter, massinhämtande av kommunikationsuppgifter samt förelägganden om lagring av kommunikationsuppgifter måste alla godkännas av *Judicial Commissioners* ⁽⁴⁵⁶⁾. *The Investigatory Powers Commissioner* måste också alltid förhandsgodkänna inhämtande av kommunikationsuppgifter för brottsbekämpande ändamål ⁽⁴⁵⁷⁾. Om en *Commissioner* vägrar att godkänna ett beslut kan den ansvariga ministern överklaga till *the Investigatory Powers Commissioner*, vars beslut är slutgiltigt.

⁽⁴⁴⁷⁾ I enlighet med avsnitten 227.7 och 8 i 2016 års lag om utredningsbefogenheter är *Investigatory Powers Commissioner* en *Judicial Commissioner* och *Investigatory Powers Commissioner* och övriga *Judicial Commissioners* kallas gemensamt för *Judicial Commissioners*. För närvarande finns det 15 *Judicial Commissioners*.

⁽⁴⁴⁸⁾ Enligt avsnitt 60.2 i del 3 i 2005 års lag om reform av författningen (*Constitutional Reform Act 2005*) avses med "högt uppsatt domarämbete" ämbetet som domare vid någon av domstolarna i) Högsta domstolen ii) Appellationsdomstolen i England och Wales. iii) Överdomstolen (High Court) i England och Wales. iv) Court of Session. v) Appellationsdomstolen i Nordirland. (vi) Överdomstolen (High Court) i Nordirland eller som en Lord of Appeal in Ordinary.

⁽⁴⁴⁹⁾ Rättsväsendets oberoende grundar sig på konvention och har fått ett brett erkännande sedan 1701 *Act of Settlement*.

⁽⁴⁵⁰⁾ Avsnitt 227.3 i 2016 års lag om utredningsbefogenheter. *Judicial Commissioners* måste också rekommenderas av *the Investigatory Powers Commissioner*, avsnitt 227.4 e i 2016 års lag om utredningsbefogenheter.

⁽⁴⁵¹⁾ Avsnitt 238 i 2016 års lag om utredningsbefogenheter.

⁽⁴⁵²⁾ Avsnitt 227.2 i 2016 års lag om utredningsbefogenheter.

⁽⁴⁵³⁾ Avsättningen är identisk med avsättningen för andra domare i Förenade kungariket (se t.ex. avsnitt 11.3 i *Senior Courts Act 1981* och avsnitt 33 i 2005 års lag om reform av författningen som också kräver en resolution efter godkännande av båda kamrarna i parlamentet). Hittills har ingen *Judicial Commissioner* avsatts.

⁽⁴⁵⁴⁾ Ett organ på armlängds avstånd är en organisation eller byrå som får finansiering från en regering men som kan agera självständigt (för en definition och mer information om ett organ på armlängds avstånd, se kansliets handbok om klassificeringen av offentliga organ, som finns på följande länk: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/519571/Classification-of-Public-Bodies-Guidance-for-Departments.pdf och den första rapporten från sammanträdesperioden 2014–2015 från Public Administration Select Committee of the House of Commons som finns på följande länk: <https://publications.parliament.uk/pa/cm201415/cmselect/cmpubadm/110/110.pdf>)

⁽⁴⁵⁵⁾ Enligt avsnitt 229 i 2016 års lag om utredningsbefogenheter har *the Judicial Commissioner* omfattande tillsynsbefogenheter som även omfattar tillsyn av lagring och utlämnande av uppgifter som samlats in av underrättelsetjänsterna.

⁽⁴⁵⁶⁾ Beslut om godkännande av beslut av den ansvariga ministern att utfärda ett beslut är en fråga för *the Judicial Commissioners* själva. Om en *Commissioner* vägrar att godkänna ett beslut kan den ansvariga ministern överklaga till *the Investigatory Powers Commissioner*, vars beslut är slutgiltigt.

⁽⁴⁵⁷⁾ *Investigatory Powers Commissions* tillstånd begärs alltid när kommunikationsuppgifter inhämtas för brottsbekämpande ändamål (avsnitt 60A i 2016 års lag om utredningsbefogenheter). Om kommunikationsuppgifter inhämtas med hänsyn till den nationella säkerheten kan tillståndet beviljas av *the Investigatory Powers Commissioner* eller, alternativt, av en utsedd högre tjänsteman vid den berörda myndigheten (se avsnitten 61 och 61A i 2016 års lag om utredningsbefogenheter och skäl 203 ovan).

- (253) FN:s särskilda rapportör för rätten till integritet välkomnade varmt inrättandet av *Judicial Commissioners* i 2016 års lag om utredningsbefogenheter, eftersom "alla mer känsliga eller inkräktande begäranden om att genomföra övervakning måste godkännas av både en minister och IPCO". Han betonade särskilt att denna del av domstolsprövningen [genom den roll som *the Investigatory Powers Commissioner* har] med hjälp av en grupp erfarna inspektörer och tekniska experter med bättre resurser är en av de viktigaste nya skyddsåtgärder som införts genom lagen om utredningsbefogenheter, som ersatte ett tidigare splittrat system av tillsynsmyndigheter och kompletterar den roll som parlamentets underrättelse- och säkerhetsutskott och tribunalen för utredningsbefogenheter spelar ⁽⁴⁵⁸⁾.
- (254) Dessutom har *the Investigatory Powers Commissioner* befogenhet att i efterhand, inklusive genom revisioner, inspektioner och utredningar, övervaka ⁽⁴⁵⁹⁾ användningen av utredningsbefogenheter enligt 2016 års lag om utredningsbefogenheter och vissa andra befogenheter och funktioner som föreskrivs i relevant lagstiftning ⁽⁴⁶⁰⁾. Resultaten av denna efterhandskontroll ingår i den rapport som *the Investigatory Powers Commissioner* årligen ska utarbeta och lägga fram för premiärministern ⁽⁴⁶¹⁾ och som ska offentliggöras och läggas fram för parlamentet ⁽⁴⁶²⁾. Rapporten innehåller relevant statistik och information om underrättelsetjänsters och brottsbekämpande myndigheters användning av utredningsbefogenheter samt införandet av skyddsåtgärder i samband med föremål som omfattas av rättsliga privilegier, konfidentiellt journalistiskt material och källor till journalistisk information, information om de arrangemang som vidtagits och de operativa ändamål som används i samband med "massbeslut". I *IPCO Annual Report* anges slutligen vilka områdesrekommendationer som har lämnats till myndigheter och hur de har åtgärdats ⁽⁴⁶³⁾.
- (255) I enlighet med avsnitt 231 i 2016 års lag om utredningsbefogenheter ska *the Investigatory Powers Commissioner*, om han eller hon får kännedom om ett relevant fel som begåtts av myndigheter vid utövandet av sina utredningsbefogenheter, informera den berörda personen om han eller hon anser att felet är allvarligt och det ligger i allmänhetens intresse att personen informeras ⁽⁴⁶⁴⁾. I avsnitt 231 i 2016 års lag om utredningsbefogenheter anges särskilt att *the Investigatory Powers Commissioner*, när en person informeras om ett misstag, ska lämna information om eventuella rättigheter som han eller hon har att vända sig till tribunalen för utredningsbefogenheter och lämna sådana uppgifter som *the Commissioner* anser vara nödvändiga för utövandet av dessa rättigheter och det finns ett allmänintresse av att informationen lämnas ut ⁽⁴⁶⁵⁾.

⁽⁴⁵⁸⁾ *End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion Of his Mission to the United Kingdom of Great Britain and Northern Ireland* (se fotnot 281).

⁽⁴⁵⁹⁾ Avsnitt 229 i 2016 års lag om utredningsbefogenheter. *Judicial Commissioners* utrednings- och informationsbefogenheter anges i avsnitt 235 i 2016 års lag om utredningsbefogenheter.

⁽⁴⁶⁰⁾ Detta inbegriper övervakningsåtgärder inom ramen för 2000 års lag om utredningsbefogenheter, utövandet av funktioner enligt del 3 i polislagen från 1997 (bemyndigande av åtgärder i fråga om egendom) och ministerns utövande av funktioner enligt avsnitten 5–7 i *Intelligence Services Act 1994* (beslut om ingrepp för trådlös telegrafi, tillträde och ingrepp i egendom) (avsnitt 229 i 2016 års lag om utredningsbefogenheter).

⁽⁴⁶¹⁾ Avsnitt 230 i 2016 års lag om utredningsbefogenheter. *The Investigatory Powers Commissioner* för utredningsbefogenheter kan också på eget initiativ rapportera till premiärministern i alla frågor som rör hans eller hennes uppdrag. *The Investigatory Powers Commissioner* måste också rapportera till premiärministern på dennes begäran och premiärministern kan ge honom eller henne i uppdrag att se över underrättelsetjänstens eventuella funktioner.

⁽⁴⁶²⁾ Vissa delar kan uteslutas om publiceringen skulle strida mot den nationella säkerheten.

⁽⁴⁶³⁾ I *IPCO Annual report 2019* (punkt 6.38) nämns till exempel att MI5 rekommenderades att ändra sin policy för lagring av massdataset av personuppgifter eftersom man borde ha tagit hänsyn till proportionaliteten i lagringen på alla områden som rör innehav av massdataset av personuppgifter och för varje massdataset av personuppgifter som innehas. I slutet av 2018 var IPCO inte nöjd med att denna rekommendation följdes och i 2019 års rapport förklarades att MI5 nu inför en ny process för att uppfylla detta krav. I årsrapporten för 2019 (punkt 8.22) nämns också att GHQ fick en rad rekommendationer om redovisningen av proportionaliteten i deras förfrågningar om massuppgifter. I rapporten bekräftas att förbättringar har gjorts på detta område i slutet av 2018. Årsrapport från IPCO för 2019 finns på följande länk: https://www.ipco.org.uk/docs/IPC%20Annual%20Report%202019_Web%20Accessible%20version_final.pdf. Dessutom avslutas varje inspektion som IPCO utför av en myndighet med en rapport med rekommendationer till följd av inspektionen som lämnas till den berörda myndigheten. IPCO inleder därefter varje efterföljande inspektion med en granskning av eventuella tidigare rekommendationer från den senaste inspektionen och överväger i den nya inspektionsrapporten om de tidigare rekommendationerna har genomförts eller håller på att genomföras.

⁽⁴⁶⁴⁾ Ett fel betraktas som "allvarligt" om *the Commissioner* anser att det har vållat den berörda personen betydande skada eller skada (avsnitt 231.2 i 2016 års lag om utredningsbefogenheter). Under 2018 rapporterades 22 fel, varav åtta bedömdes allvarliga och ledde till information till den berörda personen. Se årsrapport från IPCO 2018, bilaga C (se <https://www.ipco.org.uk/docs/IPC%20Annual%20Report%202018%20final.pdf>). Under 2019 ansågs 14 fel vara allvarliga. *Annual Report of the Investigatory Powers Commissioner Office 2019*, bilaga C, se fotnot 463.

⁽⁴⁶⁵⁾ I avsnitt 231 i 2016 års lag om utredningsbefogenheter anges att *the Investigatory Powers Commissioner*, när han eller hon informerar en person om ett misstag, ska lämna sådana uppgifter som *the Commissioner* anser vara nödvändiga för utövandet av dessa rättigheter, särskilt med hänsyn till i vilken utsträckning utlämnandet av uppgifterna skulle strida mot allmänintresset eller inverka menligt på förebyggande eller avslöjande av allvarlig brottslighet, Förenade kungarikets ekonomiska välbefinnande eller den fortsatta tjänsteutövningen av någon av underrättelsetjänsterna.

3.3.3.3 Parlamentarisk tillsyn av underrättelsetjänster

- (256) Den parlamentariska tillsyn som utförs av underrättelse- och säkerhetsutskottet har sin rättsliga grund i *Justice and Security Act 2013* (JSA 2013) ⁽⁴⁶⁶⁾. Genom lagen inrättas underrättelse- och säkerhetsutskottet i det brittiska parlamentet. Sedan 2013 har underrättelse- och säkerhetsutskottet fått större befogenheter, bland annat tillsyn över säkerhetstjänsternas operativa verksamhet. Enligt avsnitt 2 i *Justice and Security Act 2013* har underrättelse- och säkerhetsutskottet till uppgift att övervaka de nationella säkerhetsorganens utgifter, administration, politik och verksamhet. I *Justice and Security Act 2013* anges att underrättelse- och säkerhetsutskottet kan genomföra utredningar i operativa frågor som inte rör pågående insatser ⁽⁴⁶⁷⁾. I det samförståndsavtal som premiärministern och underrättelse- och säkerhetsutskottet ⁽⁴⁶⁸⁾ kommit överens om anges i detalj vilka faktorer som ska beaktas när man överväger om en verksamhet inte är en del av en pågående insats ⁽⁴⁶⁹⁾. Underrättelse- och säkerhetsutskottet kan också uppmanas att utreda pågående insatser av premiärministern och kan granska information som tillhandahålls frivilligt av organen.
- (257) Enligt bilaga 1 till *Justice and Security Act 2013* får underrättelse- och säkerhetsutskottet begära att cheferna för någon av de tre underrättelsetjänsterna lämnar ut all slags information. Myndigheten ska göra sådan information tillgänglig, såvida inte den ansvariga ministern lägger in sitt veto mot den ⁽⁴⁷⁰⁾. Enligt de förklaringar som lämnats av de brittiska myndigheterna undanhålls i praktiken mycket lite information från underrättelse- och säkerhetsutskottet ⁽⁴⁷¹⁾.
- (258) Underrättelse- och säkerhetsutskottet består av ledamöter som tillhör någon av parlamentets kammare och utses av premiärministern efter samråd med oppositionsledaren ⁽⁴⁷²⁾. Underrättelse- och säkerhetsutskottet ska lämna en årlig rapport till parlamentet om fullgörandet av sina uppgifter och andra rapporter som den anser lämpliga ⁽⁴⁷³⁾. Dessutom har underrättelse- och säkerhetsutskottet rätt att var tredje månad få en förteckning över de operativa ändamål som används för att undersöka material som erhållits i massomfattning ⁽⁴⁷⁴⁾. Premiärministern delger underrättelse- och säkerhetsutskottet de utredningar, inspektioner eller revisioner som görs av *the Investigatory Power Commissioner* när frågan om rapporterna är relevant för utskottets lagstadgade befogenheter ⁽⁴⁷⁵⁾. Slutligen kan utskottet be *the Investigatory Powers Commissioner* att göra en utredning och *the Commissioner* måste informera underrättelse- och säkerhetsutskottet om huruvida en sådan utredning ska genomföras ⁽⁴⁷⁶⁾.
- (259) Underrättelse- och säkerhetsutskottet bidrog också till utkastet till 2016 års lag om utredningsbefogenheter, vilket resulterade i ett antal ändringar som nu återspeglas i 2016 års lag om utredningsbefogenheter ⁽⁴⁷⁷⁾. I synnerhet rekommenderade underrättelse- och säkerhetsutskottet en förstärkning av integritetsskyddet genom att införa en

⁽⁴⁶⁶⁾ Som de brittiska myndigheterna förklarade utvidgade *Justice and Security Act* ansvarsområde för underrättelse- och säkerhetsutskottet till att omfatta en roll när det gäller att övervaka underrättelsegemenskapen utöver de tre myndigheterna och möjliggöra en retroaktiv översyn av myndigheternas operativa verksamhet i frågor av stort nationellt intresse.

⁽⁴⁶⁷⁾ Avsnitt 2 i JSA 2013.

⁽⁴⁶⁸⁾ Samförståndsavtal mellan premiärministern och underrättelse- och säkerhetsutskottet, finns på följande länk: <http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf>

⁽⁴⁶⁹⁾ Samförståndsavtal mellan premiärministern och underrättelse- och säkerhetsutskottet, punkt 14, se fotnot 468.

⁽⁴⁷⁰⁾ Den ansvariga ministern får endast lägga in veto mot utlämnande av uppgifter på följande två grunder: Uppgifterna är känsliga och bör inte lämnas ut till underrättelse- och säkerhetsutskottet med hänsyn till den nationella säkerheten. Om den ansvariga ministern anmodades att inkomma med den till ett av underhusets särskilda utskott, skulle den ansvariga ministern (av skäl som inte är begränsade till den nationella säkerheten) anse att det var lämpligt att inte göra det (tillägg 1 punkt 4.2 i *Justice and Security Act 2013*).

⁽⁴⁷¹⁾ *UK Explanatory Framework for Adequacy Discussions*, avsnitt H: *National Security*, s. 43, se fotnot 31.

⁽⁴⁷²⁾ Avsnitt 1 i JSA 2013. Ministrar kan inte bli ledamöter. Ledamöterna innehar sin ställning i underrättelse- och säkerhetsutskottet under parlamentets hela mandatperiod för vilket de har utnämnts. De kan avsättas genom ett beslut av det parlament för vilket de utnämnts om de upphör att vara parlamentsledamot eller utnämns till minister. En ledamot kan också avgå.

⁽⁴⁷³⁾ Utskottets betänkanden och uttalanden finns på följande webbadress: <https://isc.independent.gov.uk/publications/>. År 2015 utfärdade underrättelse- och säkerhetsutskottet en rapport om integritet och säkerhet: *A modern and transparent legal framework* (se: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf) där den granskade den rättsliga ramen för de övervakningstekniker som används av underrättelsetjänsterna och utfärdade en rad rekommendationer som sedan övervägdes och integrerades i utkastet till lag om utredningsbefogenheter som omvandlades till lag, 2016 års lag om utredningsbefogenheter. Regeringens svar på rapporten om personlig integritet och säkerhet finns på följande länk: https://b1cba9b3-a-5e6631fd-s-sites.google.com/a/independent.gov.uk/isc/files/20151208_Privacy_and_Security_Government_Response.pdf

⁽⁴⁷⁴⁾ Avsnitten 142, 161 och 183 i 2016 års lag om utredningsbefogenheter.

⁽⁴⁷⁵⁾ Avsnitt 234 i 2016 års lag om utredningsbefogenheter.

⁽⁴⁷⁶⁾ Avsnitt 236 i 2016 års lag om utredningsbefogenheter.

⁽⁴⁷⁷⁾ Parlamentets underrättelse- och säkerhetsutskottet, *Report on the draft Investigatory Powers Bill* finns på följande länk: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20160209_ISC_Rpt_IPBillweb.pdf

uppsättning integritetsskydd som omfattar alla utredningsbefogenheter ⁽⁴⁷⁸⁾. Det föreslog också ändringar av den föreslagna kapaciteten när det gäller ingrepp i utrustning, massdatat av personuppgifter och kommunikationsuppgifter samt begärde andra specifika ändringar för att stärka begränsningarna och skyddsåtgärderna för användningen av utredningsbefogenheter ⁽⁴⁷⁹⁾.

3.3.4 Prövningsmöjligheter

- (260) När det gäller statlig åtkomst för ändamål som rör nationell säkerhet måste de registrerade ha möjlighet att väcka talan vid en oberoende och opartisk domstol för att få tillgång till sina personuppgifter eller för att få dessa uppgifter rättade eller raderade ⁽⁴⁸⁰⁾. Ett sådant rättsligt organ måste särskilt ha befogenhet att anta bindande beslut om underrättelsetjänsten ⁽⁴⁸¹⁾. I Förenade kungariket ger ett antal möjligheter till rättslig prövning, vilket förklaras i skälen 261–271, en möjlighet för registrerade att utnyttja och erhålla sådana rättsmedel.

3.3.4.1 Prövningsmekanismer enligt del 4 i dataskyddslagen

- (261) Enligt avsnitt 165 i 2018 års dataskyddslag har den registrerade rätt att lämna in ett klagomål till *the Information Commissioner* om den registrerade anser att det föreligger en överträdelse av del 4 i 2018 års dataskyddslag i samband med personuppgifter som rör honom eller henne. *The Information Commissioner* har befogenhet att bedöma om den personuppgiftsansvariga och personuppgiftsbiträdet efterlever 2018 års dataskyddslag och kräva att de vidtar nödvändiga åtgärder. Enligt del 4 i 2018 års dataskyddslag har enskilda dessutom rätt att ansöka hos *High Court* (eller *Court of Session in Scotland*) om ett föreläggande om att den personuppgiftsansvariga ska iakttä rätten till tillgång till uppgifter ⁽⁴⁸²⁾, invända mot behandling ⁽⁴⁸³⁾ och rättelse eller radering ⁽⁴⁸⁴⁾.
- (262) Enskilda har också rätt att från den personuppgiftsansvariga eller personuppgiftsbiträdet begära ersättning för skada till följd av överträdelse av ett krav i del 4 i 2018 års dataskyddslag ⁽⁴⁸⁵⁾. Med skada avses både ekonomisk förlust och skada som inte medför ekonomiska förluster, till exempel nödläge ⁽⁴⁸⁶⁾.

3.3.4.2 Prövningsmekanismer inom 2016 års lag om utredningsbefogenheter

- (263) Enskilda personer kan erhålla rättslig prövning av överträdelser av 2016 års lag om utredningsbefogenheter inför tribunalen för utredningsbefogenheter.
- (264) Tribunalen för utredningsbefogenheter inrättas av 2000 års lag om utredningsbefogenheter och är oberoende av den verkställande makten ⁽⁴⁸⁷⁾. I enlighet med avsnitt 65 i 2000 års lag om utredningsbefogenheter utses tribunalens ledamöter av drottningen för en femårsperiod. En ledamot i tribunalen kan avsättas från sitt ämbete av drottningen efter en framställning ⁽⁴⁸⁸⁾ från båda kamrarna i parlamentet ⁽⁴⁸⁹⁾.

⁽⁴⁷⁸⁾ Dessa allmänna skyldigheter i fråga om personlig integritet anges nu i avsnitt 2.2 i 2016 års lag om utredningsbefogenheter, där det föreskrivs att en myndighet som agerar enligt 2016 års lag om utredningsbefogenheter ska ta hänsyn till om det som avses med beslutet, tillståndet eller föreläggandet rimligen skulle kunna uppnås med andra mindre inkräktande medel, 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, det allmänna intresset för integritet och säkerhet i fråga om telekommunikationssystem och andra posttjänster och alla andra aspekter av allmänt intresse när det gäller skyddet av integriteten.

⁽⁴⁷⁹⁾ På begäran av underrättelse- och säkerhetsutskottet kan till exempel antalet dagar ett "brådskande" beslut kan vara på plats innan *the Judicial Commissioner* måste godkänna det ha minskat från fem till tre arbetsdagar och utskottet fick befogenhet att hänskjuta ärenden till *the Investigatory Powers Commissioner* för undersökning.

⁽⁴⁸⁰⁾ Schrems II, punkt 194.

⁽⁴⁸¹⁾ Schrems II, punkt 197.

⁽⁴⁸²⁾ Avsnitt 94.11 i 2018 års dataskyddslag.

⁽⁴⁸³⁾ Avsnitt 99.4 i 2018 års dataskyddslag.

⁽⁴⁸⁴⁾ Avsnitt 100.1 i 2018 års dataskyddslag.

⁽⁴⁸⁵⁾ I avsnitt 169 i 2018 års dataskyddslag tilläts anspråk från "en person som lider skada på grund av överträdelse av ett krav i dataskyddslagstiftningen". Enligt de uppgifter som lämnats av de brittiska myndigheterna är det i praktiken troligt att ett anspråk eller ett klagomål mot underrättelsetjänsterna kommer att framställas till tribunalen för utredningsbefogenheter som har en omfattande behörighet som kan ge ersättning/skadestånd och när ett yrkande inte medför några kostnader.

⁽⁴⁸⁶⁾ Avsnitt 169.5 i 2018 års dataskyddslag.

⁽⁴⁸⁷⁾ Enligt bilaga 3 till 2000 års lag om utredningsbefogenheter måste ledamöterna ha särskild erfarenhet inom rättsväsendet och kunna återutnännas.

⁽⁴⁸⁸⁾ Framställningen utgörs av en *address* som en motion som lagts fram för parlamentet och som syftar till att göra monarken medveten om parlamentets yttranden i en viss fråga.

⁽⁴⁸⁹⁾ Tillägg 3 punkt 1.5 till 2000 års lag om utredningsbefogenheter.

- (265) Enligt avsnitt 65 i 2000 års lag om utredningsbefogenheter är tribunalen det lämpliga rättsliga organet för klagomål från en person som lidit skada på grund av handlingar inom ramen för 2016 års lag om utredningsbefogenheter, 2000 års lag om utredningsbefogenheter eller valfritt agerande från underrättelsetjänsternas sida ⁽⁴⁹⁰⁾.
- (266) För att väcka talan vid tribunalen för utredningsbefogenheter ("obligatoriska krav") enligt avsnitt 65 i 2000 års lag om utredningsbefogenheter måste en enskild tro ⁽⁴⁹¹⁾ att en underrättelsetjänst har agerat med avseende på honom, hans egendom, alla meddelanden som skickats av eller till honom eller som är avsedda för honom eller hans användning av posttjänster, telekommunikationstjänster eller telekommunikationssystem" ⁽⁴⁹²⁾. Dessutom är klaganden skyldig att tro att beteendet har ägt rum under "omständigheter mot vilka talan kan väckas" ⁽⁴⁹³⁾ eller "har utförts av underrättelsetjänsterna eller för deras räkning" ⁽⁴⁹⁴⁾. Eftersom denna "övertygelse" i synnerhet har tolkats ganska brett ⁽⁴⁹⁵⁾, omfattas ett mål vid tribunalen av låga obligatoriska krav.
- (267) När tribunalen för utredningsbefogenheter prövar ett klagomål som ingetts till dem är det tribunalens uppgift att undersöka huruvida de personer som anklagas i klagomålet har handlat i förhållande till den klagande samt att utreda vilken myndighet som påstås ha gjort sig skyldig till överträdelse och huruvida det påstådda beteendet har ägt rum ⁽⁴⁹⁶⁾. När tribunalen prövar ett mål ska den tillämpa samma principer för att avgöra målet som en domstol skulle tillämpa vid en ansökan om rättslig prövning ⁽⁴⁹⁷⁾. Dessutom är mottagarna av besluten eller föreläggandena enligt 2016 års lag om utredningsbefogenheter och alla andra personer som tjänstgör under kronan och som är anställda av polisen eller *the Police Investigations and Review Commissioner* skyldiga att lämna ut eller till tribunalen lämna ut alla handlingar och all information som tribunalen kan behöva för att kunna utöva sin behörighet ⁽⁴⁹⁸⁾.
- (268) Tribunalen för utredningsbefogenheter ska underrätta den klagande om huruvida det har fällt ett utslag till hans eller hennes fördel eller inte ⁽⁴⁹⁹⁾. Enligt avsnitten 67.6 och 67.7 i 2000 års lag om utredningsbefogenheter är tribunalen behörig att besluta om interimistiska åtgärder och att meddela sådan ersättning eller andra förelägganden som den finner lämpliga. Detta kan innebära ett beslut om att ogiltigförklara eller upphäva varje beslut eller tillstånd

⁽⁴⁹⁰⁾ Avsnitt 65.5 i 2000 års lag om utredningsbefogenheter.

⁽⁴⁹¹⁾ När det gäller standarden på "testet av övertygelsen", se målet Human Rights Watch/Secretary of State [2016] UKIPTrib15_165-CH, punkt 41. I detta mål fann tribunalen för utredningsbefogenheter, genom att hänvisa till rättspraxis från Europeiska domstolen för de mänskliga rättigheterna, att det lämpliga testet är huruvida det, med avseende på den påstådda övertygelsen att något beteende som omfattas av underavsnitt 68.5 i 2000 års lag om utredningsbefogenheter har utförts av någon underrättelsetjänst eller för dess räkning, finns någon grund för en sådan övertygelse, så att den enskilde kan hävda att han eller hon har utsatts för en överträdelse på grund av blotta förekomsten av hemliga åtgärder eller lagstiftning som medger hemliga åtgärder, endast om han eller hon kan visa att det finns en risk för att han eller hon utsätts för denna typ av åtgärder på grund av hans eller hennes personliga situation.

⁽⁴⁹²⁾ Avsnitt 65.4 a i 2000 års lag om utredningsbefogenheter.

⁽⁴⁹³⁾ Sådana omständigheter avser myndigheters agerande med myndighetsutövning (t.ex. ett beslut, ett tillstånd/ett föreläggande om inhämtande av meddelanden osv.) eller om omständigheterna är sådana (oavsett om det finns en sådan myndighet eller inte) att det inte skulle ha varit lämpligt att beteendet ägde rum utan det eller åtminstone utan att vederbörlig hänsyn hade tagits till huruvida en sådan befogenhet borde ha sökts. Ett agerande som har godkänts av en *Judicial Commissioner* anses ha ägt rum under omständigheter mot vilka talan kan väckas (avsnitt 65 (7ZA) i 2000 års lag om utredningsbefogenheter) medan andra handlingar som äger rum med tillstånd av en person som innehar ett domarämbete inte anses ha ägt rum under omständigheter mot vilka talan kan väckas (avsnitten 65.7 och 8 i 2000 års lag om utredningsbefogenheter).

⁽⁴⁹⁴⁾ Enligt de uppgifter som lämnats av de brittiska myndigheterna visar den låga tröskeln för att lämna in ett klagomål att det inte är ovanligt att tribunalen i sin undersökning fastställer att klaganden i själva verket aldrig varit föremål för en utredning av en myndighet. I den senaste statistiska rapporten från tribunalen för utredningsbefogenheter anges att under 2016 mottog tribunalen 209 klagomål, varav 52 % ansågs vara av okynneskaraktär eller förargelseväckande och 25 % fick ett "obestämt" resultat. De brittiska myndigheterna förklarade att detta antingen innebär att ingen hemlig verksamhet/inga dolda befogenheter har använts i förhållande till klaganden eller att dold teknik användes och tribunalen fastställde att verksamheten var laglig. Dessutom uteslöts 11 % från jurisdiktion, drogs tillbaka eller var inte giltiga, 5 % uteslöts för sent, 7 % konstaterades vara till klagandens fördel. *Statistical Report of the Investigatory Powers Tribunal 2016* finns på följande länk: <https://www.ipt-uk.com/docs/IPT%20Statistical%20Report%202016.pdf>

⁽⁴⁹⁵⁾ Se målet Human Rights Watch/Secretary of State [2016] UKIPTrib15_165-CH. I detta fall fann tribunalen för utredningsbefogenheter, genom att hänvisa till rättspraxis från Europeiska domstolen för de mänskliga rättigheterna, att det lämpliga kriteriet för att anta att ett beteende som omfattas av underavsnitt 68.5 i 2000 års lag om utredningsbefogenheter har utförts av någon underrättelsetjänst eller för dess räkning är huruvida det finns någon grund för en sådan övertygelse, inbegripet det faktum att en enskild kan hävda att han eller hon har utsatts för en överträdelse på grund av blotta förekomsten av hemliga åtgärder eller lagstiftning som medger hemliga åtgärder endast om han eller hon kan visa att han eller hon på grund av sin personliga situation riskerar att utsättas för sådana åtgärder (se Human Rights Watch/Secretary of State, punkt 41).

⁽⁴⁹⁶⁾ Avsnitt 67.3 i 2000 års lag om utredningsbefogenheter.

⁽⁴⁹⁷⁾ Avsnitt 67.2 i 2000 års lag om utredningsbefogenheter.

⁽⁴⁹⁸⁾ Avsnitten 68.6–7 i 2000 års lag om utredningsbefogenheter.

⁽⁴⁹⁹⁾ Avsnitt 68.4 i 2000 års lag om utredningsbefogenheter.

och ett beslut om att förstöra alla register över uppgifter som erhållits i samband med utövandet av befogenheter som erhållits genom ett beslut, ett tillstånd eller ett föreläggande eller på annat sätt innehas av en myndighet med avseende på en person ⁽⁵⁰⁰⁾. Enligt avsnitt 67A i 2000 års lag om utredningsbefogenheter kan ett avgörande från tribunalen överklagas med förbehåll för tribunalens eller den relevanta appellationsdomstolens tillstånd.

- (269) Slutligen är det värt att notera att den roll som spelas av tribunalen för utredningsbefogenheter har diskuterats i samband med rättsliga förfaranden vid Europeiska domstolen för de mänskliga rättigheterna vid flera tillfällen, särskilt i målet *Kennedy/United Kingdom* ⁽⁵⁰¹⁾ och mer nyligen i målet *Big Brother Watch m.fl./United Kingdom* ⁽⁵⁰²⁾, där domstolen förklarade att domstolen för utredningsbefogenheter erbjöd ett gedigen rättsmedel för alla som misstänkte att hans eller hennes kommunikation hade avlyssnats av underrättelsetjänsterna ⁽⁵⁰³⁾.

3.3.4.3 Andra tillgängliga rättsliga prövningsmekanismer

- (270) Enligt skälen 109–111 finns rättsmedel enligt *Human Rights Act 1998* och genom Europeiska domstolen för de mänskliga rättigheterna ⁽⁵⁰⁴⁾ också på området nationell säkerhet. I avsnitt 65.2 i 2000 års lag om utredningsbefogenheter föreskrivs att tribunalen för utredningsbefogenheter har exklusiv behörighet att pröva alla anspråk i lagen om mänskliga rättigheter i förhållande till underrättelsetjänsterna ⁽⁵⁰⁵⁾. Detta innebär, som överdomstolen (High Court) har påpekat, att "huruvida det har förekommit ett brott mot *Human Rights Act* i ett enskilt fall är något som i princip kan tas upp och avgöras av en oberoende tribunal som kan få tillgång till allt relevant material, inbegripet hemligt material. [...] Vi har också i detta sammanhang i åtanke att tribunalen själv nu kan överklaga till en lämplig appellationsdomstol (i England och Wales är det appellationsdomstolen (Court of Appeal)) och att högsta domstolen nyligen har beslutat att domstolen i princip kan bli föremål för domstolsprövning, se *R (Privacy International)/Investigatory Powers Tribunal* [2019] UKSC 22, [2019] 2 WLR 1219" ⁽⁵⁰⁶⁾.
- (271) Av ovanstående följer att när brittiska brottsbekämpande myndigheter eller nationella säkerhetsmyndigheter får åtkomst till personuppgifter som omfattas av detta beslut regleras sådan åtkomst av lagar som fastställer villkoren för åtkomst och säkerställer att åtkomst och vidare användning av uppgifterna begränsas till vad som är nödvändigt och står i proportion till det mål som eftersträvas med brottsbekämpning eller nationell säkerhet. För sådan åtkomst krävs dessutom i de flesta fall förhandstillstånd från ett rättsligt organ, genom godkännande av ett beslut eller en utlämnandeorder och under alla omständigheter av oberoende tillsyn. När myndigheter har fått åtkomst till uppgifterna omfattas behandlingen av dem, inbegripet ytterligare delning och vidareöverföring, av särskilda dataskyddsgarantier enligt del 3 i 2018 års dataskyddslag i enlighet med bestämmelserna i direktiv (EU) 2016/680 för behandling som utförs av brottsbekämpande myndigheter och del 4 i 2018 års dataskyddslag för behandling som utförs av underrättelsetjänster. Slutligen åtnjuter registrerade på detta område effektiva administrativa och rättsliga prövningsrättigheter, inbegripet rätten att få tillgång till sina uppgifter eller rättelse eller radering av sådana uppgifter.
- (272) Med tanke på betydelsen av sådana villkor, begränsningar och skyddsåtgärder för ändamålen med detta beslut kommer kommissionen noggrant att övervaka tillämpningen och tolkningen av Förenade kungarikets beslut om regeringens tillgång till personuppgifter. Övervakningen kommer att omfatta relevant utveckling i fråga om lagstiftning, reglering och rättspraxis samt ICO:s och andra tillsynsmyndigheters verksamheter på detta område.

⁽⁵⁰⁰⁾ Ett exempel på tillämpningen av dessa befogenheter är *Liberty & Others/Security Services, SIS, GCHQ*, [2015] UKIP Trib 13_77-H_2. Tribunalen uttalade sig till förmån för två klagande på grund av att deras kommunikation i det ena fallet låg utanför de gränser som fastställts och, i det andra, på grund av att granskningsförfarandet inte följdes på det sätt som föreskrivs i interna regler som gäller för *Government Communications Headquarter*. I det första målet ålade domstolen underrättelsetjänsterna att förstöra de meddelanden som behållits längre än den relevanta tidsfristen. I det andra fallet utfärdades inte något beslut om förstöring på grund av att kommunikationen inte lagats.

⁽⁵⁰¹⁾ *Kennedy*, se fotnot 129.

⁽⁵⁰²⁾ Europeiska domstolen för de mänskliga rättigheterna, *Big Brother Watch m.fl./Förenade kungariket* (se fotnot 268), punkterna 413–415.

⁽⁵⁰³⁾ Europeiska domstolen för de mänskliga rättigheterna, *Big Brother Watch*, punkt 425.

⁽⁵⁰⁴⁾ Såsom exempelvis framgår av en färsk dom från Europeiska domstolen för de mänskliga rättigheterna i målet *Big Brother Watch m.fl./Förenade kungariket* (se fotnot 279) blir det på detta sätt möjligt för internationella domstolar att på ett ändamålsenligt sätt kontrollera – liknande den kontroll som EU-medlemsstaterna är föremål för – myndigheters efterlevnad av de grundläggande rättigheterna i samband med tillgång till personuppgifter. Verkställandet av domar från Europeiska domstolen för de mänskliga rättigheterna är dessutom föremål för Europarådets tillsyn.

⁽⁵⁰⁵⁾ I målet *Belhaj & others* [2017] UKSC 3 grundades fastställandet av att avlyssningen av sekretesskyddat material var olaglig direkt på artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (se avgörande 11).

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

Särskild uppmärksamhet kommer också att ägnas Förenade kungarikets verkställande av relevanta domar från Europeiska domstolen för de mänskliga rättigheterna, inklusive åtgärder som anges i de "åtgärdsplaner" och "åtgärdsrapporter" som lämnas till ministerkommittén i samband med övervakningen av domstolens beslut.

4. SLUTSATS

- (273) Kommissionen anser att den brittiska dataskyddsförordningen och 2018 års dataskyddslag säkerställer en skyddsnivå för personuppgifter som överförs från Europeiska unionen som i allt väsentligt motsvarar den som garanteras genom förordning (EU) 2016/679.
- (274) 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.
- (275) 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.
- (276) Mot bakgrund av slutsatserna i detta beslut bör det därför beslutas att Förenade kungariket säkerställer 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.
- (277) Denna slutsats grundar sig på både Förenade kungarikets relevanta inhemska system och dess internationella åtaganden, särskilt anslutningen till den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna och hänvändelse till 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.

5. EFFEKTERNA AV DETTA BESLUT OCH DATASKYDDSMYNDIGHETERNAS ÅTGÄRDER

- (278) 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.
- (279) 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 detta beslut får överföringar från en personuppgiftsansvarig eller ett personuppgiftsbiträde i Europeiska unionen till personuppgiftsansvariga eller personuppgiftsbiträden i Förenade kungariket ske utan ytterligare tillstånd.
- (280) Det bör erinras om att enligt artikel 58.5 i förordning (EU) 2016/679, och såsom domstolen förklarade i Schrems-domen ⁽⁵⁰⁷⁾, 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 EU-domstolen ⁽⁵⁰⁸⁾.

⁽⁵⁰⁷⁾ Schrems-målet, punkt 65.

⁽⁵⁰⁸⁾ Schrems-målet, 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."

6. ÖVERVAKNING, TILLFÄLLIGT UPPHÄVANDE, UPPHÄVANDE ELLER ÄNDRING AV DETTA BESLUT

- (281) Enligt artikel 45.4 i förordning (EU) 2016/679 ska kommissionen fortlöpande övervaka relevant utveckling i Förenade kungariket efter antagandet av detta beslut för att bedöma om det fortfarande säkerställer en väsentligen likvärdig skyddsnivå. En sådan övervakning är särskilt viktig i detta fall, eftersom Förenade kungariket kommer att administrera, tillämpa och verkställa ett nytt system för dataskydd som inte längre omfattas av unionsrätten och som kan komma att utvecklas. I detta avseende kommer särskild uppmärksamhet att ägnas 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 detta beslut, 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 kommer utveckling av rättspraxis och ICO:s och andra oberoende organs tillsyn ligga till grund för kommissionens övervakning.
- (282) 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 detta beslut, liksom om eventuella förändringar av praxis i samband med behandling av personuppgifter som bedöms i 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 281.
- (283) 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.
- (284) Om tillgänglig information, särskilt information från övervakningen av detta beslut eller från Förenade kungarikets eller medlemsstaternas myndigheter, visar att den skyddsnivå som Förenade kungariket erbjuder kanske inte längre är adekvat, bör kommissionen informera de behöriga brittiska myndigheterna om detta och begära att lämpliga åtgärder vidtas inom en angiven tidsram, som får vara högst tre månader. Vid behov kan denna tidsram förlängas med en angiven tidsperiod, med beaktande av den aktuella frågan och/eller de åtgärder som ska vidtas. 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.
- (285) 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.
- (286) 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 konstaterandet om adekvat skyddsnivå endast till uppgiftsöverföringar för vilka en adekvat skyddsnivå fortfarande säkerställs.
- (287) 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 tillfälligt upphäver, upphäver eller ändrar beslutet.

7. GILTIGHETSTID OCH FÖRLÄNGNING AV DETTA BESLUT

- (288) Kommissionen måste ta hänsyn till att Förenade kungariket, i och med att övergångsperioden enligt utträdesavtalet löper ut och så snart övergångsbestämmelsen i artikel 782 i handels- och samarbetsavtalet mellan EU och Förenade kungariket upphör att gälla, kommer att administrera, tillämpa och verkställa ett nytt system för dataskydd jämfört med det system som gällde när landet var bundet av EU-lagstiftningen. Detta kan särskilt omfatta ändringar eller ändringar av ramen för dataskydd som bedöms i detta beslut, liksom annan relevant utveckling.

- (289) Det är därför lämpligt att föreskriva att detta beslut ska tillämpas under en period av fyra år från och med dess ikraftträdande.
- (290) 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

- (291) Europeiska dataskyddsstyrelsen offentliggjorde sitt yttrande ⁽⁵⁰⁹⁾, vilket har beaktats vid utarbetandet av detta beslut.
- (292) 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.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

1. Vid tillämpningen av artikel 45 i förordning (EU) 2016/679 säkerställer Förenade kungariket en adekvat skyddsnivå för personuppgifter som överförs från Europeiska unionen till Förenade kungariket inom tillämpningsområdet för förordning (EU) 2016/679.
2. Detta beslut omfattar inte personuppgifter som överförs för Förenade kungarikets invandringskontroll eller som på annat sätt omfattas av undantaget från vissa registrerade rättigheter i fråga om upprätthållandet av en effektiv invandringskontroll enligt artikel 4.1 i tillägg 2 till 2018 års dataskyddslag.

Artikel 2

Närhelst de behöriga tillsynsmyndigheterna i medlemsstaterna, i syfte att skydda enskilda personer med avseende på behandlingen av deras personuppgifter, utövar sina befogenheter enligt artikel 58 i förordning (EU) 2016/679 med avseende på uppgiftsöverföringar som omfattas av det tillämpningsområde som anges i artikel 1, ska den berörda medlemsstaten utan dröjsmål underrätta kommissionen därom.

Artikel 3

1. Kommissionen ska fortlöpande övervaka tillämpningen av den rättsliga ram som ligger till grund för detta beslut, inbegripet de villkor enligt vilka vidare överföring genomförs, individuella rättigheter utövas och brittiska myndigheter har tillgång till uppgifter som överförs på grundval av detta beslut, i syfte att bedöma om Förenade kungariket fortsatt säkerställer en adekvat skyddsnivå i den mening som avses i artikel 1.
2. Medlemsstaterna och kommissionen ska underrätta varandra om fall där *the Information Commissioner* eller någon annan behörig brittisk myndighet underlåter att säkerställa att den rättsliga ram som ligger till grund för detta beslut efterlevs.
3. Medlemsstaterna och kommissionen ska underrätta varandra om alla indikationer på att de brittiska myndigheternas ingripanden i enskildas rätt till skydd av sina personuppgifter går utöver vad som är absolut nödvändigt eller att det inte finns något effektivt rättsligt skydd mot sådana ingrepp.
4. Om kommissionen har indikationer på att en adekvat skyddsnivå inte längre säkerställs ska kommissionen underrätta de behöriga myndigheterna i Förenade kungariket och får tillfälligt upphäva, upphäva eller ändra detta beslut.

⁽⁵⁰⁹⁾ Yttrande 14/2021 om Europeiska kommissionens utkast till genomförandebeslut enligt förordning (EU) 2016/679 om adekvat skydd av personuppgifter i Förenade kungariket, som finns tillgängligt på följande länk: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-142021-regarding-european-commission-draft_en.

5. Kommissionen får tillfälligt upphäva, upphäva eller ändra detta beslut om den brittiska regeringens bristande samarbete hindrar kommissionen från att avgöra om konstaterandet i artikel 1.1 påverkas.

Artikel 4

Detta beslut ska upphöra att gälla den 27 juni 2025, såvida det inte förlängs i enlighet med det förfarande som avses i artikel 93.2 i direktiv (EU) 2016/679.

Artikel 5

Detta beslut riktar sig till medlemsstaterna.

Utfärdat i Bryssel den 28 juni 2021.

På kommissionens vägnar

Didier REYNERS

Ledamot av kommissionen
