

# Opinion of the Board (Art. 70.1.s)



**Yttrande 14/2021 om Europeiska kommissionens utkast till  
genomförandebeslut enligt förordning(EU) 2016/679 om  
adekvat skydd av personuppgifter i Förenade kungariket**

**Antaget den 13 april 2021**

Translations proofread by EDPB Members.  
This language version has not yet been proofread.

## INNEHÅLL

|                                                                                                                                                                                    |    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 1. SAMMANFATTNING .....                                                                                                                                                            | 4  |
| 1.1. Konvergensområden .....                                                                                                                                                       | 5  |
| 1.2. Utmaningar.....                                                                                                                                                               | 5  |
| 1.2.1. Allmänt .....                                                                                                                                                               | 5  |
| 1.2.2. Allmänna dataskyddsaspekter .....                                                                                                                                           | 6  |
| 1.2.3. Om offentliga myndigheters tillgång till uppgifter som överförts till Förenade kungariket.....                                                                              | 8  |
| 1.3 Slutsats .....                                                                                                                                                                 | 10 |
| 2. INLEDNING .....                                                                                                                                                                 | 11 |
| 2.1 Förenade kungarikets dataskyddsram.....                                                                                                                                        | 11 |
| 2,2. Omfattning av EDPB:s bedömning .....                                                                                                                                          | 11 |
| 2.3 Allmänna kommentarer och frågor .....                                                                                                                                          | 13 |
| 2.3.1. Internationella åtaganden som Förenade kungariket har inlett.....                                                                                                           | 13 |
| 2.3.2. Eventuella kommande skillnader i Förenade kungarikets dataskyddsram .....                                                                                                   | 13 |
| 3. ALLMÄNNA DATASKYDDASPEKTER.....                                                                                                                                                 | 15 |
| 3.1 Innehåll.....                                                                                                                                                                  | 15 |
| 3.1.1 Rätt till tillgång, rättelse, radering och invändningar .....                                                                                                                | 16 |
| 3.1.2. Begränsningar av vidare överföring.....                                                                                                                                     | 21 |
| 3,2. Förfarande- och verkställandemekanismer .....                                                                                                                                 | 29 |
| 3.2.1 Oberoende behörig tillsynsmyndighet .....                                                                                                                                    | 29 |
| 3.2.2. Befintligheten av ett dataskyddssystem som säkerställer en god nivå av efterlevnad.....                                                                                     | 30 |
| 3.2.3. Systemet för skydd av personuppgifter måste ge stöd och hjälp till registrerade i deras utövande av sina rättigheter samt tillhandahålla lämpliga prövningsmekanismer ..... | 30 |
| 4. FÖRENADE KUNGARIKETS MYNDIGHETERS TILLGÅNG TILL OCH ANVÄNDNING AV PERSONUPPGIFTER SOM ÖVERFÖRTS FRÅN EU.....                                                                    | 30 |
| 4,1. Förenade kungarikets myndigheters tillgång till och användning av personuppgifter för brottsbekämpande ändamål .....                                                          | 30 |
| 4.1.1. Rättsliga grunder och tillämpliga begränsningar och skyddsåtgärder.....                                                                                                     | 31 |
| 4.1.2. Vidare användning av information som samlas in för brottsbekämpningsändamål (skäl 140–154) .....                                                                            | 33 |
| 4.1.3. Tillsyn.....                                                                                                                                                                | 35 |
| 4,2. Allmän rättslig ram för dataskydd på området nationell säkerhet .....                                                                                                         | 35 |
| 4.2.1. Nationella säkerhetscertifikat.....                                                                                                                                         | 35 |

|                                                                                                                                              |    |
|----------------------------------------------------------------------------------------------------------------------------------------------|----|
| 4.2.2. Rätten till rättelse och radering.....                                                                                                | 36 |
| 4.2.3. Undantag som rör den nationella säkerheten.....                                                                                       | 36 |
| 4,3. Förenade kungarikets offentliga myndigheters åtkomst och användning för ändamål som rör den nationella säkerheten .....                 | 37 |
| 4.3.1. Rättsliga grunder, begränsningar och skyddsåtgärder – Utredningsbefogenheter som utövas inom ramen för nationell säkerhet .....       | 37 |
| 4.3.2. Ytterligare användning av den information som samlas in för ändamål som rör nationell säkerhet och utlämnande till andra länder ..... | 47 |
| 4.3.3. Tillsyn.....                                                                                                                          | 51 |
| 4.3.4. Prövningsmöjligheter .....                                                                                                            | 52 |

## Europeiska dataskyddsstyrelsen har antagit följande yttrande

med beaktande av artikel 70.1 s i 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*),

med beaktande av avtalet om Europeiska ekonomiska samarbetsområdet (nedan kallat *EES*), särskilt bilaga XI och protokoll 37, ändrat genom gemensamma EES-kommitténs beslut nr 154/2018 av den 6 juli 2018<sup>1</sup>,

med beaktande av artiklarna 12 och 22 i arbetsordningen.

## HÄRIGENOM FÖRESKRIVS FÖLJANDE.

### 1. SAMMANFATTNING

1. Europeiska kommissionen godkände sitt utkast till genomförandebeslut (nedan kallat *utkast till beslut*) om adekvat skydd av personuppgifter i Förenade kungariket enligt den allmänna dataskyddsförordningen den 19 februari 2021<sup>2</sup>. Efter detta inledde Europeiska kommissionen sitt förfarande för formellt antagande.
2. Samma datum bad Europeiska kommissionen om ett yttrande från Europeiska dataskyddsstyrelsen (nedan kallad *EDPB*)<sup>3</sup>. EDPB:s bedömning av adekvat skyddsnivå i Förenade kungariket har gjorts mot bakgrund av undersökningen av själva utkastet till beslutet, samt mot bakgrund av analysen av den dokumentation som tillgängliggjorts av Europeiska kommissionen.
3. EDPB inriktade sig på att bedöma både de allmänna aspekterna av utkastet till beslut och offentliga myndigheters tillgång till personuppgifter som överförts från EES för brottsbekämpande ändamål och nationell säkerhet, inbegripet de rättsmedel som finns tillgängliga för enskilda personer inom EES. EDPB har också bedömt huruvida de skyddsåtgärder som föreskrivs i Förenade kungarikets rättsliga ram har införts och är effektiva.
4. Som främsta referens har EDPB använt referensramen för adekvat skyddsnivå inom ramen för den allmänna dataskyddsförordningen<sup>4</sup> som antogs i februari 2018 samt EDPB:s rekommendationer 02/2020 om europeiska nödvändiga garantier för övervakningsåtgärder<sup>5</sup>.

---

<sup>1</sup> Hänvisningar till "medlemsstater" i detta yttrande ska förstås som hänvisningar till "medlemsstater i EES".

<sup>2</sup> Se Europeiska kommissionens pressmeddelande, *Skydd av personuppgifter: EU-kommissionen inleder förfarande rörande flödet av personuppgifter till Storbritannien*, den 19 februari 2021, [https://ec.europa.eu/commission/presscorner/detail/sv/ip\\_21\\_661](https://ec.europa.eu/commission/presscorner/detail/sv/ip_21_661).

<sup>3</sup> Se ovan.

<sup>4</sup> Se artikel 29-arbetsgruppen, referensramen för adekvat skyddsnivå, som antogs den 28 november 2017, senast ändrad och antagen den 6 februari 2018, WP254 rev.01 (godkänd av EDPB, [https://edpb.europa.eu/node/1491\\_sv](https://edpb.europa.eu/node/1491_sv)), (nedan kallad *referensramen för adekvat skyddsnivå inom ramen för den allmänna dataskyddsförordningen*).

<sup>5</sup> Se EDPB:s rekommendationer 02/2020 om europeiska nödvändiga garantier för övervakningsåtgärder, antagna den 10 november 2020, [https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees\\_sv](https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_sv).

## 1.1. Konvergensområden

5. EDPB:s främsta mål är att lämna ett yttrande till Europeiska kommissionen om adekvat skyddsnivå för enskilda personer i Förenade kungariket. Det är viktigt att erkänna att EDPB inte förväntar sig att den rättsliga ramen i Förenade kungariket ska spegla den europeiska dataskyddslagstiftningen.
6. EDPB påminner emellertid om att det för att upprätthålla en adekvat skyddsnivå krävs enligt artikel 45 i allmänna dataskyddsförordningen vid brottsbekämpning och enligt rättspraxis från Europeiska unionens domstol (nedan kallad *EU-domstolen*) att tredjelandets lagstiftning ska vara samordnad med de väsentliga principerna som anges i allmänna dataskyddsförordningen vid brottsbekämpning. Förenade kungarikets dataskyddsram bygger till stor del på EU:s rättsliga ramar för skydd av personuppgifter (särskilt den allmänna dataskyddsförordningen och Europaparlamentets och rådets direktiv (EU) 2016/680, nedan kallat *EU:s brottsbekämpningsdirektiv*), vilket beror på att Förenade kungariket var medlem i EU fram till den 31 januari 2020. I Förenade kungarikets dataskyddslag från 2018 (*Data Protection Act 2018*), som trädde i kraft den 23 maj 2018 och upphävde den brittiska dataskyddslagen från 1998, preciseras tillämpningen av den allmänna dataskyddsförordningen i Förenade kungarikets lagstiftning ytterligare. Den införlivar också EU-direktivet om brottsbekämpning samt beviljar befogenheter och ålägger skyldigheter för den nationella tillsynsmyndigheten för dataskydd, den brittiska dataskyddsmyndigheten *Information Commissioner's Office*. EDPB erkänner därför att Förenade kungariket till största delen återspeglar den allmänna dataskyddsförordningen i sin dataskyddsram.
7. **När EDPB har analyserat lagstiftningen och praxis i ett tredjeland som har varit medlem i EU tills nyligen är det uppenbart att det finns många aspekter som är likvärdiga.**
8. När det gäller dataskydd noterar EDPB att det finns en tydlig samordning mellan ramen för den allmänna dataskyddsförordningen och den rättsliga ramen i Förenade kungariket när det gäller vissa viktiga bestämmelser som till exempel koncept (dvs. *personuppgifter*, *behandling av personuppgifter*, *personuppgiftsansvarig*), grunder för laglig och rättvis behandling för berättigade ändamål, ändamålsbegränsning, uppgifternas kvalitet och proportionalitet, lagring av uppgifter, säkerhet och konfidentialitet, transparens, särskilda kategorier av uppgifter, direkt saluföring, automatiserat beslutsfattande och profilering.

## 1.2. Utmaningar

9. Förenade kungariket var fram till nyligen medlem av EU. EDPB har därför vid sin analys av landets lagstiftning och praxis konstaterat många aspekter som är i stort sett likvärdiga. Samtidigt har EDPB, både med hänsyn till sin roll i processen för att anta ett beslut om adekvat skyddsnivå och med hänsyn till tidsbegränsningarna, beslutat att rikta sin uppmärksamhet på de aspekter som man anser behöver undersökas närmare och granskas mer i detalj.
10. Trots detta kvarstår utmaningar, och EDPB anser att följande punkter bör utvärderas ytterligare för att säkerställa att en väsentligen likvärdig skyddsnivå uppnås och att de bör övervakas noga i Förenade kungariket av Europeiska kommissionen.

### 1.2.1. Allmänt

11. Den första utmaningen, som är allmän, gäller övervakningen av utvecklingen av det brittiska rättssystemet om dataskydd som helhet. Förenade kungarikets regering har uppgett sin avsikt att utveckla en separat och oberoende politik för dataskydd och att man möjligen vill avvika från EU:s dataskyddslagstiftning. Sådana politiska förklaringar har ännu inte genomförts inom Förenade

kungarikets rättsliga ram. Denna eventuella framtida **skillnad kan emellertid skapa risker när det gäller bibehållandet av den skyddsnivå som tillhandahålls personuppgifter som överförs från EU. Kommissionen uppmanas därför att noga övervaka en sådan utveckling från och med ikraftträdandet av dess beslut om adekvat skyddsnivå och att vidta nödvändiga åtgärder, bland annat genom att ändra och/eller tillfälligt upphäva beslutet vid behov.**

### 1.2.2. Allmänna dataskyddsaspekter

12. För det första är det så kallade **invandringsundantaget**, som fastställs i **bilaga 2 till 2018 års dataskyddslag, del 1, punkt 4, "brett" formulerat**. Det gäller i synnerhet även om personuppgifter inte samlas in för invandringskontroll av en personuppgiftsansvarig, utan görs tillgängliga för en annan personuppgiftsansvarig som behandlar sådana personuppgifter för invandringskontroll.
13. EDPB uppmanar Europeiska kommissionen att kontrollera läget i målet *Open Rights Group & Anor, R (on the Application of) mot Minister for the Home Department & Anor* [2019] EWHC 2562 (Admin) och att, eftersom denna dom inte är slutgiltig (*res judicata*), kontrollera om den bekräftas eller ses över genom överklagandedomen, och beakta eventuella uppdateringar i detta avseende och ange det i beslutet. **EDPB uppmanar också kommissionen att i beslutet om adekvat skyddsnivå lämna ytterligare information om invandringsundantaget<sup>6</sup>, särskilt när det gäller nödvändigheten och proportionaliteten av ett sådant brett undantag i brittisk lagstiftning, i synnerhet med beaktande av den breda omfattningen av tillämpningen av personlig obehörighet**. Samtidigt uppmanar EDPB Europeiska kommissionen att vidare undersöka om det finns eller kommer att införas ytterligare skyddsåtgärder i Förenade kungarikets rättsliga ram, till exempel i form av rättsligt bindande instrument som skulle komplettera invandringsundantaget genom att förbättra dess förutsebarhet och öka skyddet för de registrerade, samtidigt som det skulle möjliggöra en bättre och snabb bedömning och övervakning av nödvändighets- och proportionalitetskraven.
14. För det andra, även om EDPB erkänner att Förenade kungariket till största delen har speglat kapitel V i sin dataskyddsram, har EDPB identifierat vissa aspekter av Förenade kungarikets rättsliga ram **när det gäller vidareöverföringar** som kan undergräva skyddsnivån för personuppgifter som överförs från EES.
15. Enligt artikel 44 i den allmänna dataskyddsförordningen<sup>7</sup> ska överföringar och vidareöverföringar av personuppgifter endast ske om skyddsnivån för fysiska personer som garanteras av den allmänna dataskyddsförordningen inte undergrävs. **Detta innebär att inte bara den brittiska lagstiftningen ska vara "väsentligen likvärdig" EU-lagstiftningen när det gäller behandling av personuppgifter som överförs till Förenade kungariket enligt det framtida beslutet om adekvat skyddsnivå, utan också att de regler som är tillämpliga i Förenade kungariket när det gäller vidareöverföring av dessa**

---

<sup>6</sup> Också som ett resultat av den pågående översynen av användningen av det invandringsundantag som avses på s. 5 i Förenade kungarikets *Explanatory Framework for Adequacy Discussions, Section E3: Schedule 2 Restrictions*, 13 mars 2020.

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/872232/E - Narrative on Restrictions.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf).

<sup>7</sup> "Överföring av personuppgifter som är under behandling eller är avsedda att behandlas efter det att de överförts till ett tredjeland eller en internationell organisation får bara ske under förutsättning att den personuppgiftsansvarige och personuppgiftsbiträdet, med förbehåll för övriga bestämmelser i denna förordning, uppfyller villkoren i detta kapitel, inklusive för vidare överföring av personuppgifter från tredjelandet eller den internationella organisationen till ett annat tredjeland eller en annan internationell organisation. Alla bestämmelser i detta kapitel ska tillämpas för att säkerställa att den nivå på skyddet av fysiska personer som säkerställs genom denna förordning inte undergrävs."

**uppgifter till tredjeländer ska säkerställa att en väsentligen likvärdig skyddsnivå kommer att fortsätta att tillhandahållas.**

16. Även om EDPB noterar Förenade kungarikets förmåga att enligt sin rättsliga ram erkänna territorier som har en adekvat uppgiftsskyddsnivå sett till Förenade kungarikets dataskyddsram vill EDPB betona att dessa territorier kanske inte för närvarande omfattas av ett beslut om adekvat skyddsnivå som utfärdats av Europeiska kommissionen där man säkerställer en skyddsnivå som är likvärdig med det skydd som garanteras i EES. Detta kan innebära eventuella risker i det skydd av personuppgifter som tillhandahålls från EES, särskilt om Förenade kungarikets dataskyddsram avviker från EU:s regelverk. Dessutom har Förenade kungariket redan erkänt att de tredjeländer som åtnjuter ett beslut om adekvat skyddsnivå av Europeiska kommissionen enligt direktiv 95/46/EG<sup>8</sup> är adekvata, medan kommissionen snart kommer att se över dessa resultat, och slutsatserna av denna översyn är ännu inte kända.
17. **I situationerna ovan bör Europeiska kommissionen fullgöra sin övervakande roll, och om en likvärdig skyddsnivå för de personuppgifter som överförs från EES inte kan upprätthållas, bör Europeiska kommissionen beakta en ändring av beslutet om adekvat skyddsnivå så att det även inbegriper särskilda specifika skyddsåtgärder för uppgifter som överförs från EES och/eller att upphäva beslutet om adekvat skyddsnivå.**
18. **När det gäller internationella avtal mellan Förenade kungariket och tredjeländer** uppmanas Europeiska kommissionen att undersöka samspelet mellan Förenade kungarikets dataskyddsram och dess internationella åtaganden, utöver avtalet om tillgång till elektroniska uppgifter för att motverka grov brottslighet som ingåtts mellan Förenade kungariket och Amerikas förenta stater<sup>9</sup> (nedan kallat *CLOUD-avtalet*), särskilt för att säkerställa kontinuiteten i skyddsnivån när personuppgifter överförs från EU till Förenade kungariket på grundval av Förenade kungarikets beslutet om adekvat skyddsnivå och sedan överförs vidare till andra tredjeländer. För att hela tiden kunna övervaka situationen och vidta åtgärder om så krävs, om ingående av internationella avtal mellan Förenade kungariket och tredjeländer innebär risker för att nivån på skyddet av personuppgifter i EU kan undermineras.
19. Vidare uppmanas Europeiska kommissionen att övervaka om CLOUD-avtalet säkerställer lämpliga ytterligare skyddsåtgärder, med beaktande av känsligheten hos de berörda uppgiftskategorierna och kraven som endast avser överföringen av elektronisk bevisning direkt av tjänsteleverantörer snarare än mellan myndigheter, och även att bedöma under vilka omständigheter skyddsåtgärder kan tillhandahållas genom ett lämpligt genomförande av anpassningen av paraplyavtalet mellan EU och Förenta staterna<sup>10</sup>.
20. EDPB noterar även att vidareöverföringar också kan ske från Förenade kungariket till ett annat tredjeländ på grundval av **överföringsverktyg i enlighet med Förenade kungarikets tillämpliga**

---

<sup>8</sup> Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (EGT L 281, 23.11.1995, s. 31).

<sup>9</sup> Se avtalet mellan Förenade konungariket Storbritannien och Nordirlands regering och Amerikas förenta staters regering om tillgång till elektroniska uppgifter för bekämpning av allvarliga brott, Washington DC, Förenta staterna, den 3 oktober 2019, <https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-counteracting-serious-crime-cs-usa-no62019>.

<sup>10</sup> Se avtalet mellan Amerikas förenta stater och Europeiska unionen om skydd av personuppgifter i samband med förebyggande, utredning, avslöjande och lagföring av brott, december 2016 (nedan kallat *paraplyavtalet*), [https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=LEGISSUM%3A3104\\_8](https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=LEGISSUM%3A3104_8).

**dataskyddslagstiftning**<sup>11</sup>. Efter Schrems II<sup>12</sup> uppmanar EDPB Europeiska kommissionen att i sitt beslut om adekvat skyddsnivå försäkra sig om att nödvändiga skyddsåtgärder kommer att införas på ett effektivt sätt, även med beaktande av lagstiftningen i det mottagande tredjelandet.

21. När det gäller avsaknaden av **skydd enligt artikel 48 i den allmänna dataskyddsförordningen** uppmanar EDPB kommissionen att tillhandahålla ytterligare garantier och specifika hänvisningar till den brittiska lagstiftningen som säkerställer att skyddsnivån enligt den brittiska rättsliga ramen i allt väsentligt motsvarar den skyddsnivå som garanteras inom EES.
22. Vad gäller **förfarande- och verkställandemekanismer** noterar EDPB att det finns en oberoende tillsynsmyndighet och att den fungerar effektivt; befintligheten av ett system som säkerställer en god nivå av efterlevnad och ett system för tillgång till lämpliga prövningsmekanismer som ger enskilda personer inom EES möjlighet att utöva sina rättigheter och söka gottgörelse utan att stöta på besvärliga hinder för administrativ och rättslig prövning är centrala element i en ram för dataskydd som är förenlig med den europeiska lagstiftningen.
23. EDPB erkänner att Förenade kungariket i de flesta delar har återspeglat de relevanta bestämmelserna i den allmänna dataskyddsförordningen i den brittiska allmänna dataskyddsförordningen och i 2018 års dataskyddslag. Kommissionen uppmanas dock att kontinuerligt övervaka utvecklingen av Förenade kungarikets rättsliga ram och praxis, som kan leda till skadliga effekter på dessa områden.

#### 1.2.3. Om offentliga myndigheters tillgång till uppgifter som överförts till Förenade kungariket

24. EDPB noterar de betydande förändringar i Förenade kungarikets rättsliga ram som är tillämpliga på säkerhets- och underrättelsebyråer, särskilt när det gäller avlyssning och förvärv av kommunikationsuppgifter. EDPB förstår att dessa förändringar bland annat är ett svar på de förfaranden som inletts vid EU-domstolen och Europeiska domstolen för de mänskliga rättigheterna och deras senaste domar i detta sammanhang.
25. EDPB välkomnar särskilt att Förenade kungariket har inrättat domstolen med utredningsbefogenheter (*Investigatory Powers Tribunal*). Domstolen med utredningsbefogenheter är inte bara behörig att pröva mål som rör brottsbekämpande myndigheters användning av utredningsbefogenheter, utan även av underrättelsetjänsters användning av sådana befogenheter. EDPB förstår därför att domstolen med utredningsbefogenheter fungerar som en riktig domstol i den mening som avses i artikel 47 i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad *EU-stadgan*).
26. Vidare noterar EDPB att införandet av "justitieombudsmän" i 2016 års lag om utredningsbefogenheter (nedan kallad *IPA 2016*) är en betydande förbättring. EDPB förstår att en viktig funktion för justitieombudsmännen är att i enskilda fall förhandsgodkänna olika övervakningsåtgärder, däribland riktad avlyssning och massinsamling av kommunikationsuppgifter (så kallat dubbellåsningsförfarande).
27. För att bedöma om denna ytterligare tillsynsnivå är effektiv anser EDPB dock att det är nödvändigt att ytterligare klargöra de scenarier för vilka en laglig avlyssning utan godkännande från ombudsmannen för utredningsbefogenheter (*Investigatory Powers Commissioner*) eller

---

<sup>11</sup> Se artiklarna 46 och 47 i den allmänna dataskyddsförordningen.

<sup>12</sup> Se Schrems II.

justitieombudsmännen är möjlig, och uppmanar Europeiska kommissionen att ytterligare bedöma och visa att även i fall där dubbellåsningförfarandet inte är tillämpligt, föreskriver den brittiska rättsliga ramen lämpliga skyddsåtgärder, inbegripet möjligheter till översyn och prövning *ex post* för individer, och att den därmed säkerställer en skyddsnivå som är likvärdig med den som tillhandahålls i EU.

28. EDPB uppmanar dessutom Europeiska kommissionen att ytterligare bedöma under vilka förhållanden brådskande åtgärder kan åberopas, och att tillhandahålla förtydliganden om de möjliga sätten att utöva rättigheter för de registrerade och om de möjligheter till prövning som erbjuds dem i samband med utrustningsstörning, särskilt vid undantag från förfarandet med dubbelspärning.
29. EDPB anser dessutom att det finns ett behov av ytterligare klargöranden och bedömning av avlyssningar i bulk, i synnerhet när det gäller val och tillämpning av väljarna, för att klargöra i vilken utsträckning tillgången till personuppgifter är förenlig med den tröskel som fastställts av EU-domstolen, och vilka skyddsåtgärder som finns för att skydda de grundläggande rättigheterna för enskilda personer vars uppgifter avlyssnas i detta sammanhang, inbegripet när det gäller lagringsperioder för uppgifter. En oberoende bedömning från de behöriga brittiska tillsynsmyndigheterna skulle vara särskilt användbar. EDPB understryker också att det förefaller vara desto mer kritiskt att "utomeuropeisk kommunikation" som faller inom ramen för massavlyssningsmetoder tycks innebära att uppgifter direkt kan avlyssnas och samlas in i bulk inom EU av Förenade kungariket, inbegripet uppgifter som transiteras mellan EU och Förenade kungariket, vilket skulle omfattas av förslaget till beslut. Med tanke på hur viktig denna aspekt är uppmanar EDPB kommissionen att noga övervaka utvecklingen i detta avseende.
30. Fortfarande när det gäller massavlyssning framhåller EDPB den konsekventa bedömning som Europeiska domstolen för de mänskliga rättigheterna och EU-domstolen har gjort, och påminner om de farhågor som uttryckts i fråga om sekundära uppgifter, som bör omfattas av särskilda skyddsåtgärder på grund av deras känslighet. EDPB uppmanar därför Europeiska kommissionen att noggrant bedöma om de skyddsåtgärder som föreskrivs i brittisk lagstiftning för sådana kategorier av personuppgifter säkerställer en skyddsnivå som i allt väsentligt är likvärdig med den som garanteras inom EES.
31. I detta sammanhang är EDPB medveten om att 2016 års rapport från underrättelse- och säkerhetskommittén om användningen av bulkbefogenheter<sup>13</sup> rör praxis inom den tidigare rättsliga ramen, som senare ersattes av IPA 2016. EDPB ser dock ett behov av ytterligare oberoende bedömning av och tillsyn över användningen av verktyg för automatiserad behandling av de behöriga brittiska tillsynsmyndigheterna, och uppmanar kommissionen att ytterligare bedöma denna fråga och de skyddsåtgärder som i detta sammanhang skulle och/eller skulle kunna erbjudas registrerade i EES.
32. EDPB delar åsikt med ombudsmannen för utredningsbefogenheter att ytterligare översyn och övervakning behövs för att säkerställa att de skyddsåtgärder som i praktiken tillämpas av behöriga myndigheter på området nationell säkerhet och underrättelser för att avhjälpa brister i tillämpningen av relevant lagstiftning upprätthålls och kommer att fortsätta att förbättras. EDPB välkomnar också det faktum att ombudsmannen för utredningsbefogenheter följaktligen genomförde en översyn av sin strategi för inspektion av massavlyssning 2019, som innehöll en noggrann översyn av de tekniskt

---

<sup>13</sup> Se *Report of the bulk powers review* från Independent Review of Terrorism Legislation, augusti 2016, <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf>.

*komplexa sätt på vilka massavlyssning faktiskt genomförs och åtog sig att inkludera en detaljerad granskning av de väljare och sökkriterier som Europeiska domstolen för de mänskliga rättigheterna hänvisade till ovan i inspektionerna av massavlyssning från och med 2020. Med tanke på vikten av denna aspekt är EDPB bekymrad över att en detaljerad granskning av urvals- och sökkriterierna ännu inte har gjorts av ombudsmannen för utredningsbefogenheter, och uppmanar kommissionen att noga övervaka utvecklingen i detta avseende, särskilt eftersom den konkreta utformningen av denna tillsyn fortfarande måste klargöras.*

33. EDPB understryker att när det gäller utomeuropeiska upplysningar kan tillämpningen av det nationella säkerhetsundantag som föreskrivs i brittisk lagstiftning leda till att det inte finns några skyddsåtgärder som säkerställer att principerna om ändamålsbegränsning, nödvändighet och proportionalitet också respekteras eller förutser att tillräckliga rättigheter för individer, tillsyn och prövning också skulle tillhandahållas eller respekteras i det tredjeland som är bestämmelseland. EDPB rekommenderar därför kommissionen att ytterligare undersöka de övergripande skyddsåtgärder som föreskrivs i brittisk lag när det gäller utlämnande till andra länder, särskilt mot bakgrund av tillämpningen av undantag för nationell säkerhet.
34. EDPB är slutligen oroad över andra former av informationsutbyte och information, på grundval av andra instrument, särskilt de olika internationella avtal som Förenade kungariket har ingått med andra tredjeländer, särskilt eftersom allmänheten fortfarande inte har tillgång till dessa instrument, t.ex. kommunikationsunderrättelseavtalet mellan Förenade kungariket och Förenta staterna. Effekten av ett sådant avtal skulle kunna leda till ett kringgående av de säkerhetsgarantier som fastställts i samband med tillgång till och användning av personuppgifter för ändamål som rör nationell säkerhet. EDPB anser också att man för att kunna ingå bilaterala eller multilaterala avtal med tredjeländer för att samarbeta på underrättelseområdet, där man tillhandahåller en rättslig grund för direkt avlyssning och inhämtning eller överföring av personuppgifter till dessa länder, också kan påverka villkoren för vidare delning av inhämtad information i större utsträckning, eftersom sådana avtal sannolikt kommer att påverka Förenade kungarikets rättsliga ram för dataskydd så som den bedömts.

### 1.3 Slutsats

35. EDPB anser att den brittiska bedömningen av adekvat skyddsnivå är unik på grund av Förenade kungarikets tidigare status som EU-medlemsstat. Dessutom skulle det också vara det första beslutet om adekvat skyddsnivå som inbegriper en tidsbegränsningsklausul.
36. EDPB konstaterar därför att det finns många områden av konvergens mellan Förenade kungariket och EU:s dataskyddsramar. Samtidigt och efter en noggrann analys av Europeiska kommissionens utkast till beslut och Förenade kungarikets dataskyddslagstiftning har EDPB identifierat ett antal utmaningar som granskas utförligt i detta yttrande. I detta sammanhang vill EDPB betona Europeiska kommissionens avgörande roll i övervakningen av all relevant utveckling i Förenade kungariket.
37. Mot bakgrund av ovanstående rekommenderar EDPB kommissionen att ta itu med de utmaningar som tas upp i detta yttrande. EDPB uppmanar också kommissionen att noga övervaka all relevant utveckling i Förenade kungariket som kan påverka den väsentliga likvärdigheten av skyddsnivån för personuppgifter och att vid behov vidta lämpliga åtgärder.

## 2. INLEDNING

### 2.1 Förenade kungarikets dataskyddsram

38. Den brittiska ramen för dataskydd bygger till stor del på EU:s ram för dataskydd (särskilt den allmänna dataskyddsförordningen och LED-direktivet), vilket beror på att Förenade kungariket var medlem i EU fram till den 31 januari 2020. Den brittiska dataskyddslagen från 2018, som trädde i kraft den 23 maj 2018 och upphävde den brittiska dataskyddslagen från 1998, specificerar dessutom tillämpningen av den allmänna dataskyddsförordningen i brittisk lagstiftning, utöver att införliva EU:s direktiv om brottsbekämpning, och beviljar befogenheter och åläggande av skyldigheter för den nationella tillsynsmyndigheten för dataskydd, den brittiska dataskyddsmyndigheten.
39. Enligt vad som anges i skäl 12 i Europeiska kommissionens utkast till beslut antog Förenade kungarikets regering *European Union (Withdrawal) Act 2018* som införlivade direkt tillämplig unionslagstiftning i Förenade kungarikets lagstiftning. Enligt den här lagen har Förenade kungarikets ministrar befogenhet att införa sekundärlagstiftning, via rättsliga instrument, för att införa nödvändiga ändringar av bibehållen EU-lagstiftning till följd av Förenade kungarikets utträde ur unionen för att passa det inhemska sammanhanget.
40. Därmed består den gällande rättsliga ramen för Förenade kungariket i slutet av övergångsperioden<sup>14</sup> av följande:
- Förenade kungarikets allmänna dataskyddsförordning som införlivats i Förenade kungarikets lagstiftning enligt *European Union (Withdrawal) Act 2018*, och som ändrats genom 2019 års förordningar om uppgiftsskydd, integritet och elektronisk kommunikation (ändringar etc.) (EU Exit) 2019,
  - 2018 års dataskyddslag som ändrats genom 2019 års förordningar om uppgiftsskydd, integritet och elektronisk kommunikation (ändringar etc.) (EU Exit) 2020, och
  - IPA 2016.

(tillsammans utgör de "Förenade kungarikets dataskyddsram").

### 2.2. Omfattning av EDPB:s bedömning

41. Europeiska kommissionens utkast till beslut är resultatet av en bedömning av Förenade kungarikets dataskyddsram, följt av diskussioner med regeringen i Förenade kungariket. Enligt artikel 70.1 s i den allmänna dataskyddsförordningen förväntas EDPB lämna ett oberoende yttrande över Europeiska kommissionens resultat, identifiera brister i ramen för adekvat skyddsnivå om sådana finns, samt sträva efter att ge förslag till åtgärder.
42. Så som anges i referensramen för adekvat skyddsnivå inom ramen för den allmänna dataskyddsförordningen, ska "informationen som lämnas av kommissionen vara uttömmande och göra det möjligt för Europeiska dataskyddsstyrelsen att göra en egen bedömning av skyddsnivån för uppgifter i tredjelandet"<sup>15</sup>.

---

<sup>14</sup> Övergångsperioden gäller till den 31 december 2020. Därefter gäller inte EU:s lagstiftning i Förenade kungariket. "Övergångsperioden" gäller som längst till den 30 juni 2021, och avser tilläggsperioden då överföring av personuppgifter från EES till Förenade kungariket inte betraktas som en överföring.

<sup>15</sup> Se WP254 rev.01, s. 3.

43. I detta avseende bör det noteras att EDPB endast till viss del tagit emot dokument i tid som är relevanta för att undersöka Förenade kungarikets rättsliga ram. EDPB tog emot en stor del av Förenade kungarikets lagstiftning som det hänvisas till i utkastet till beslutet via länkar som fanns i utkastet. Europeiska kommissionen kunde inte ge EDPB någon skriftlig förklaring och åtaganden från Förenade kungariket om utbyten mellan myndigheterna i Förenade kungariket och Europeiska kommissionen under detta arbete<sup>16</sup>.
44. Mot bakgrund av informationen ovan och på grund av den begränsade tidsramen (två månader) som EDPB har för att anta detta yttrande har EDPB valt att fokusera på några särskilda punkter som presenterades i utkastet till beslutet för att lämna en analys och ett yttrande för dessa.
45. När EDPB har analyserat lagstiftningen och praxis i ett tredjeland som har varit medlem i EU tills nyligen är det uppenbart att det finns många aspekter som är likvärdiga. EDPB har för att kunna anta beslut om adekvat skyddsnivå och analysera den mängd lagar och praxis som krävs beslutat att fokusera på de delar som var i störst behov av en översyn. Dessutom omfattar en mycket viktig del av analysen, i linje med EU-domstolens rättspraxis, det rättsliga systemet för tillgång till de personuppgifter som överförs till Förenade kungariket för nationella säkerhetsändamål och praxis för den nationella säkerhetsapparaten i Förenade kungariket. Man måste dock komma ihåg att nationell säkerhet naturligtvis är ett rättsligt och praktiskt område där medlemsstaternas lagstiftning inte är harmoniserad på EU-nivå och därför kan skilja sig åt.
46. EDPB beaktade den tillämpliga ramen om europeiskt dataskydd, inklusive artiklarna 7, 8 och 47 i EU-stadgan som var för sig skyddar rätten till privat- och familjeliv, rätten till skydd av personuppgifter och rätten till ett effektivt rättsmedel och en rättvis rättegång, samt artikel 8 i Europeiska konventionen om de mänskliga rättigheterna som skyddar rätten till privat- och familjeliv. Utöver detta beaktade EDPB kraven enligt direktivet om uppgiftsskydd samt relevant rättspraxis.
47. Målet med åtgärden är att lämna ett yttrande till Europeiska kommissionen så att de kan bedöma adekvat skyddsnivå i Förenade kungariket. Begreppet "adekvat skyddsnivå" som fanns med redan i direktiv 95/46/EG har vidareutvecklats av EU-domstolen. Det är i detta sammanhang viktigt att påminna om den princip som fastställdes av EU-domstolen i Schrems I-målet, närmare bestämt att medan skyddsnivån i tredjelandet måste vara väsentligen likvärdig med den som garanteras inom EU gäller att "de medel som detta tredjeland använder för att säkerställa en sådan skyddsnivå kan skilja sig från dem som används inom unionen"<sup>17</sup>. Därför är målet inte att punkt för punkt efterlikna EU-

---

<sup>16</sup> Avseende artikel 48 i den allmänna dataskyddsförordningen (fotnot 78 i utkastet till beslut); förbättrade skyddsåtgärder och säkerhetsåtgärder som tillämpas av personuppgiftsansvariga vid behandling i samband med landets säkerhet (fotnot 64 i utkastet till beslut); kravet att personuppgiftsansvarig ska överväga om det finns ett behov av att från fall till fall förlita sig på undantaget även om ett nationellt säkerhetsintyg har utfärdats (skäl 126 och fotnot 172 i utkastet till beslut); det faktum att skyddet enligt paraplyavtalet mellan EU och Förenta staterna kommer att gälla all personlig information som tas fram eller bevaras enligt CLOUD-avtalet, oavsett vilken typ av organ som framställer begäran, när det gäller detaljerna för det konkreta genomförandet av dataskyddsåtgärder som fortfarande är föremål för diskussioner mellan Förenade kungariket och Förenta staterna, försäkran om att Förenade kungarikets myndigheter endast kommer att låta detta avtal träda i kraft när man är säker på att genomförandet är förenligt med dataskyddsstandarderna för alla uppgifter som begärs enligt detta avtal (skäl 153 i utkastet till beslut); situationer där uppgifter överförs från EU till Förenade kungariket inom ramen för detta utkast till beslut, och det faktum att det alltid skulle finnas en "anslutning till de brittiska öarna" och eventuell utrustningsstörning som omfattar sådana uppgifter skulle därför omfattas av kravet på obligatorisk garanti i avsnitt 13.1 i IPA 2016 (skäl 206 i utkastet till beslut); och de exempel på operativa syften som anges (skäl 216 och fotnot 369 i utkastet till beslut).

<sup>17</sup> Se domstolens dom av den 6 oktober 2015 i mål C-362/14, Maximilian Schrems/Data Protection Commissioner, (nedan kallad *Schrems I*), ECLI:EU:C:2015:650, punkterna 73 och 74.

lagstiftningen utan att fastställa de grundläggande och avgörande kraven i denna lagstiftning som undersöks. Adekvat skyddsnivå kan uppnås genom en kombination av rättigheter för de registrerade och skyldigheter för de som behandlar personuppgifter, eller som utövar kontroll över sådan behandling, och övervakning av oberoende organ. Bestämmelser om skydd av personuppgifter är dock endast effektiva om de är verkställbara och följs i praktiken. Det är därför nödvändigt att inte bara se till innehållet i bestämmelserna för överföring av personuppgifter till ett tredjeland eller en internationell organisation utan också till de mekanismer som har inrättats för att säkerställa att dessa bestämmelser är verkningsfulla. Effektiva verkställighetsmekanismer är av avgörande betydelse för att få verkningsfulla bestämmelser om skydd av personuppgifter<sup>18</sup>.

## 2.3 Allmänna kommentarer och frågor

### 2.3.1. Internationella åtaganden som Förenade kungariket har inlett

48. Enligt artikel 45.2 c i den allmänna dataskyddsförordningen samt i referensramen för adekvat skyddsnivå inom ramen för den allmänna dataskyddsförordningen<sup>19</sup> ska Europeiska kommissionen vid bedömning av adekvat skyddsnivå i ett tredjeland bland annat beakta de internationella åtaganden som tredjelandet har inlett, eller andra krav som uppkommit på grund av tredjelandets deltagande i multilaterala eller regionala system, särskilt med hänsyn till skydd av personuppgifter, samt genomförandet av sådana krav. Dessutom bör tredjelandets anslutning till Europarådets konvention av den 28 januari 1981 om skydd för fysiska personer vid automatiserad databehandling av personuppgifter (nedan kallad *konvention 108*)<sup>20</sup> och dess tilläggsprotokoll<sup>21</sup> beaktas.
49. **I detta avseende välkomnar EDPB det faktum att Förenade kungariket har följt Europakonventionen och tillhör jurisdiktionen för Europeiska domstolen för de mänskliga rättigheterna. Dessutom följer Förenade kungariket även konvention 108 och dess tilläggsprotokoll. Man har även undertecknat konvention 108+<sup>22</sup> 2018 och arbetar för närvarande med dess ratificering.**

### 2.3.2. Eventuella kommande skillnader i Förenade kungarikets dataskyddsram

50. Som nämns i skäl 281 i utkastet till förslag måste Europeiska kommissionen beakta att Förenade kungariket, i slutet av den övergångsperiod som föreskrivs i enligt utträdesavtalet<sup>23</sup> och så snart överbrygningsperioden upphör att gälla enligt artikel FINPROV.10A i handels- och samarbetsavtalet mellan EU och Förenade kungariket<sup>24</sup>, kommer att administrera och tillämpa egna system för dataskydd, vilket särskilt kan inbegripa ändringar i dataskyddsramen som bedömts i utkastet till beslut, samt annan relevant utveckling.

---

<sup>18</sup> Se WP254 rev.01, s. 2.

<sup>19</sup> Se WP254 rev.01, s. 2.

<sup>20</sup> Se *Konvention om skydd för enskilda vid automatisk databehandling av personuppgifter*, konvention 108, 28 januari 1981.

<sup>21</sup> Se tilläggsprotokollet om ändring av konventionen om skydd för enskilda vid automatisk databehandling av personuppgifter, om tillsynsmyndigheter och gränsöverskridande dataflöden, som öppnades för undertecknande den 8 november 2001.

<sup>22</sup> Se protokollet om ändring av konventionen om skydd för enskilda vid automatisk databehandling av personuppgifter (*konvention 108+*), den 18 maj 2018.

<sup>23</sup> Se avtalet om Förenade konungariket Storbritannien och Nordirlands utträde ur Europeiska unionen och Europeiska atomenergigemenskapen (EUT L 29, 31.1.2020, s. 7).

<sup>24</sup> Se avtalet om handel och samarbete 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).

51. Europeiska kommissionen har därför beslutat om att införa en tidsbegränsningsklausul i sitt utkast till beslut<sup>25</sup>, med ett utgångsdatum som är fyra år efter dess ikraftträdande.
52. Det är viktigt att notera att möjligheten för Förenade kungarikets ministrar och statssekreterare att införa sekundärlagstiftning efter övergångsperiodens slut kan leda till betydande skillnader mellan Förenade kungarikets dataskyddsram och unionens dataskyddsram i framtiden.
53. Förenade kungarikets regering har också angett sin avsikt att utveckla en separat och oberoende politik för uppgiftsskydd, vilket kan leda till skillnader gentemot EU:s dataskyddslagstiftning<sup>26</sup>. Denna avsikt omfattar införlivandet av aspekter av personuppgifter i handelsavtal<sup>27</sup>, en praxis som innebär en risk för att den skyddsnivå för personuppgifter som Förenade kungariket föreskriver sänks<sup>28</sup>.
54. Förenade kungariket har möjlighet att ändra bibehållen EU-rättspraxis när övergångsperioden har passerat och när landets högsta domstol inte längre är bunden till bibehållen EU-rättspraxis<sup>29</sup> eftersom Förenade kungariket sedan slutet av överbrygningsperioden inte längre omfattas av domstolens rättspraxis eftersom det redan finns fastslagna domar från domstolen som betraktas som bibehållen EU-rättspraxis i Förenade kungarikets rättsliga ramverk inte kan gälla Förenade kungariket längre.
55. **Med beaktande av de risker som finns med att Förenade kungarikets dataskyddsram skiljer sig från EU:s regelverk när övergångsperioden har passerat välkomnar EDPB beslutet som fattats av Europeiska kommissionen att införa en tidsbegränsningsklausul under fyra år för utkastet till beslut. EDPB vill emellertid betona vikten av Europeiska kommissionens övervakande roll<sup>30</sup>.**

---

<sup>25</sup> Se artikel 4 i utkastet till beslutet. Se även skäl 282 i utkastet till beslutet.

<sup>26</sup> Förenade kungarikets nationella datastrategi (senast uppdaterad den 9 december 2020, <https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy>) omfattar följande som ett av sina uppdrag: Att kämpa för det internationella dataflödet. Informationsflödet över gränserna underblåser globala affärsverksamheter, leveranskedjor och handel, vilket ger tillväxt över hela världen. Det spelar också en bredare samhällsroll. Överföringen av personuppgifter säkerställer att folk får sina löner utbetalda och hjälper människor att på avstånd kommunicera med nära och kära. Och, som coronaviruspandemin har visat, kan utbyte av hälsouppgifter bidra till viktig vetenskaplig forskning om sjukdomar och förena länder i deras svar på globala hälsokriser. **Efter att ha lämnat EU kommer Förenade kungariket att kämpa för de fördelar som kan erhållas med hjälp av data.** Vi kommer att främja bästa inhemska praxis och samarbeta med internationella partner för att se till att uppgifterna inte felaktigt begränsas av nationella gränser och fragmenterade regleringssystem så att de kan användas till sin fulla potential. (understrykning tillagd).

<sup>27</sup> Ibid. Underlätta gränsöverskridande dataflöden: **Vi kommer att arbeta globalt för att undanröja onödiga hinder för internationella dataflöden. Vi kommer att enas om ambitiösa databestämmelser i våra handelsförhandlingar och använda vår nya oberoende position i Världshandelsorganisationen för att påverka handelsreglerna för data till det bättre. Vi kommer att undanröja hinder för internationella dataöverföringar** vilket stöder tillväxt och innovation, bland annat genom att utveckla en ny brittisk kapacitet som tillhandahåller nya och innovativa mekanismer för internationella dataöverföringar. Vi kommer också att samarbeta med partner i G20 för att skapa interoperabilitet mellan nationella datasystem för att minimera friktionen vid överföring av data mellan olika länder. (understrykning tillagd).

<sup>28</sup> Se Europaparlamentets resolution av den 12 december 2017 *En digital handelsstrategi* (2017/2065(INI)), avsnitt V, där det betonas att "[s]kyddet av personuppgifter [inte] är [...] förhandlingsbart i [EU]-handelsavtal", som finns på [https://www.europarl.europa.eu/doceo/document/TA-8-2017-0488\\_SV.pdf](https://www.europarl.europa.eu/doceo/document/TA-8-2017-0488_SV.pdf). Se även Europaparlamentets resolution av den 25 mars 2021 om kommissionens utvärderingsrapport om genomförandet av den allmänna dataskyddsförordningen två år efter dess tillämpning, punkt 28 i vilken följande anges: "stöder kommissionens praxis att behandla dataskydd och flöden av personuppgifter separat från handelsavtal", [https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111\\_SV.html](https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_SV.html).

<sup>29</sup> Se avsnitt 6.3 till 6.6 i *EU (Withdrawal) Act 2018*.

<sup>30</sup> Se artikel 45.4 i den allmänna dataskyddsförordningen.

Europeiska kommissionen bör övervaka relevant utveckling i Förenade kungariket som kan påverka den väsentliga likvärdigheten när det gäller skydd av personuppgifter som överförts enligt Förenade kungarikets beslut om adekvat skyddsnivå på regelbunden och permanent basis från beslutets ikraftträdande. Dessutom bör Europeiska kommissionen vidta lämpliga åtgärder genom att dra tillbaka, ändra eller upphäva beslutet om adekvat skyddsnivå, baserat på de specifika omständigheter som råder, om Europeiska kommissionen efter att beslutet om adekvat skyddsnivå har antagits får indikationer på att en adekvat skyddsnivå inte längre kan säkerställas i Förenade kungariket.

56. EDPB kommer att göra sitt bästa för att informera Europeiska kommissionen om relevanta åtgärder som medlemsstaternas dataskyddsmyndigheter inom den kommersiella eller offentliga sektorn har vidtagit, särskilt när det gäller klagomål som lämnats in av de registrerade i EES om överföringen av personuppgifter från EES till Förenade kungariket.

### 3. ALLMÄNNA DATASKYDDASPEKTER

#### 3.1 Innehåll

57. Kapitel 3 i referensramen för adekvat skyddsnivå inom ramen för den allmänna dataskyddsförordningen är avsett för "de innehållsmässiga principerna". Ett tredjelandssystem måste innehålla dem för att dess dataskyddsnivå ska anses vara likvärdig med den som garanteras inom EU. EDPB konstaterar att Förenade kungariket inte har någon kodifierad konstitution eftersom det inte finns något gemensamt dokument som fastställer dess grundläggande bestämmelser. Rätten till respekt för privatlivet och familjelivet (och rätten till uppgiftsskydd som en del av denna rätt) och rätten till en rättvis rättegång<sup>31</sup> ingår dock i lagen om mänskliga rättigheter från 1998, och det konstitutionella värdet av denna stadga har erkänts av brittiska domstolar. 1998 års lag om mänskliga rättigheter införlivar också rättigheterna i Europakonventionen<sup>32</sup>. Dessutom anges det, mycket viktigt, i 1998 års lag om mänskliga rättigheter att alla offentliga myndigheters åtgärder måste vara förenliga med Europakonventionen<sup>33</sup>.
58. Utöver strukturella och formalistiska skillnader mellan Förenade kungarikets lagstiftning och EU:s lagstiftning noterar EDPB, som man kan förvänta sig, att Förenade kungarikets dataskyddsstrategi liknar den i EU, eftersom Förenade kungariket var medlem i EU fram till den 31 januari 2020. Därför är många innehållsmässiga principer anpassade till den allmänna dataskyddsförordningen, och ger därmed en skyddsnivå som är likvärdig med den som EU tillhandahåller. EDPB har beslutat att inte vidareutveckla analysen av de innehållsmässiga principer som överensstämmer med EU:s lagstiftning och är nöjd med den analys som Europeiska kommissionen tillhandahållit i sitt utkast till beslut. Sådana innehållsmässiga principer är till exempel följande: koncept (t.ex. *personuppgifter*), *behandling av personuppgifter*, *personuppgiftsansvarig*), grunder för laglig och rättvis behandling för berättigade ändamål, ändamålsbegränsning, uppgifternas kvalitet och proportionalitet, lagring av uppgifter, säkerhet och konfidentialitet, transparens, särskilda kategorier av uppgifter, direkt saluföring, automatiserat beslutsfattande och profilering. EDPB noterar vidare att det i den brittiska allmänna dataskyddsförordningen och 2018 års dataskyddslag ingår innehållsmässiga principer som går längre än vad som krävs enligt referensramen för adekvat skyddsnivå inom ramen för den allmänna dataskyddsförordningen och återspeglar principerna i den allmänna

<sup>31</sup> Se artiklarna 6 och 8 i Europakonventionen (bilaga 1 till lagen om mänskliga rättigheter från 1998).

<sup>32</sup> Mer information finns i skälen 8-10 i utkastet till beslut.

<sup>33</sup> Se avsnitt 6 i lagen om mänskliga rättigheter från 1998.

dataskyddsförordningen, och därmed förhöjer den skyddsnivå som föreskrivs i Förenade kungariket. Sådana innehållsmässiga principer är till exempel de som rör underrättelser om personuppgiftsincidenter, dataskyddsombudet, konsekvensbedömningar avseende dataskydd och inbyggt dataskydd och dataskydd som standard.

59. Som nämndes i inledningen vill EDPB dock i detta yttrande särskilt ta upp vissa punkter där Europeiska dataskyddsstyrelsen är bekymrad och vill begära förtydliganden från Europeiska kommissionen.

### 3.1.1 Rätt till tillgång, rättelse, radering och invändningar

60. Det så kallade invandringsundantaget, som fastställs i **bilaga 2 i 2018 års dataskyddslag, del 1**, punkt 4, gör det möjligt för registeransvariga som deltar i "invandringskontroll" att inte tillämpa vissa registrerades rättigheter enligt 2018 års dataskyddslag om detta sannolikt skulle *påverka upprätthållandet av effektiv invandringskontroll eller utredning eller upptäckt av verksamhet som skulle undergräva upprätthållandet av effektiv invandringskontroll*.
61. Som kommissionen erkände i sitt utkast till beslut<sup>34</sup> och som hänvisades till i yttrandet från Europaparlamentets utskott för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor om ingående på EU:s vägnar av handels- och samarbetsavtalet mellan EU och Förenade kungariket<sup>35</sup>, är detta undantag **"brett" formulerat**. Förordningen gäller följande rättigheter: rätten till information, rätten till åtkomst, rätten till radering, rätten till begränsad behandling och rätten att protestera.
62. Det är dessutom viktigt att notera att detta undantag även gäller om personuppgifter inte samlas in av en personuppgiftsansvarig (*personuppgiftsansvarig 1*) för invandringskontroll, men görs tillgängliga för en annan personuppgiftsansvarig (*personuppgiftsansvarig 2*) som behandlar sådana personuppgifter för invandringskontroll (t.ex. Förenade kungarikets inrikesministeriet)<sup>36</sup>.

---

<sup>34</sup> Se skälen 62–65 i utkastet till beslut.

<sup>35</sup> I detta hänseende, när det gäller den **breda formuleringen** i invandringsundantaget, se yttrandet från utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor om ingående på unionens vägnar av avtalet om handel och samarbete mellan Europeiska unionen och Europeiska atomenergigemenskapen, å ena sidan, och Förenade konungariket Storbritannien och Nordirland, å andra sidan, och avtalet mellan Europeiska unionen och Förenade konungariket Storbritannien och Nordirland om skydd av säkerhetsskyddsklassificerade EU-uppgifter (2020/0382(NLE)), 5 februari 2021, [https://www.europarl.europa.eu/doceo/document/LIBE-AL-680848\\_SV.pdf](https://www.europarl.europa.eu/doceo/document/LIBE-AL-680848_SV.pdf), punkt 10: "Parlamentet erinrar i detta hänseende om sina resolutioner från februari och juni 2020, där man framhåller det **allmänna och breda undantaget** för behandling av personuppgifter för immigrationsändamål i Förenade kungarikets dataskyddslag", och punkt 11: "anser att det **allmänna och breda undantaget** för behandling av personuppgifter för immigrationsändamål i Förenade kungarikets dataskyddslag [...] måste ändras innan ett giltigt beslut om adekvat skyddsnivå kan utfärdas" (betoning tillagd).

<sup>36</sup> Se exemplet i den brittiska dataskyddsmyndighetens *Guide to the General Data Protection Regulation (GDPR)*, v. 1 januari 2021, s. 307 (understrykning tillagd): *En privat organisation (personuppgiftsansvarig 1) varnar inrikesministeriet (personuppgiftsansvarig 2) för en anställd som tros ha lämnat in falska handlingar för att styrka sin identitet och sina kvalifikationer för att få ett jobb. Arbetsgivaren förser inrikesministeriet med relevant information. Individens rätt att få information om att hans eller hennes personuppgifter har överförts till inrikesministeriet är begränsad i den mån det sannolikt skulle skada utredningen.*

**Arbetsgivaren är därför inte skyldig att informera personen om att hans eller hennes information har överförts till inrikesministeriet, och inrikesministeriet är i sin tur inte skyldigt att förse personen med ett integritetsmeddelande som informerar denna person om att det nu behandlar hans eller hennes personuppgifter. Undantaget gäller båda personuppgiftsansvariga i samma utsträckning.**

63. I *Open Rights Group & Anor, R (on the Application Of) mot Minister of State for the Home Department & Anor* [2019] EWHC 2562 (Admin) (3 oktober 2019) ifrågasatte sökandena lagenligheten hos invandringsundantaget eftersom det stred mot artikel 23 i den allmänna dataskyddsförordningen och var oförenligt med de rättigheter som garanteras i artiklarna 7 och 8 i EU-stadgan om integritet och skydd av personuppgifter. Högsta domstolen i England och Wales (nedan kallad *högsta domstolen*) övervägde huruvida invandringsundantaget i punkt 4 i del 1 i bilaga 2 till 2018 års dataskyddslag är lagenligt och drog slutsatsen att så var fallet.
64. Högsta domstolen menade särskilt att
- [...] undantaget för invandring uppenbart är en fråga av 'viktigt allmänintresse' och som syftar till ett legitimt mål[...], punkt 30;
  - undantaget för invandring uppfyller kraven för att en åtgärd ska vara 'i enlighet med lagen. [...], punkt 38;
  - Undantaget för invandring får endast tillämpas om och i den utsträckning som efterlevnaden av 'de angivna bestämmelserna i den allmänna dataskyddsförordningen' **sannolikt skulle inverka menligt** på upprätthållandet av en effektiv invandringskontroll eller utredandet och upptäckandet av verksamhet som skulle kunna undergräva upprätthållandet av en effektiv invandringskontroll. Orden 'sannolikt skulle inverka menligt', inom ramen för 1998 års dataskyddslag (som var föregångaren till 2018 års dataskyddslag), tolkades i betydelsen 'en mycket betydande och tungt vägande risk för menlig inverkan på det specifika allmänintresset'. Graden av risk måste vara sådan att det 'mycket väl kan' uppstå en menlig inverkan på dessa intressen, även om risken är långt ifrån att vara mer sannolik än osannolik, punkt 39 (fetstil tillagd).
65. Det bör noteras att detta domslut är, så vitt EDPB vet, inte slutgiltigt och har överklagats.
66. Så som anges i EDPB *Guidelines 10/2020 on restrictions under Article 23 GDPR* (inte översatta till svenska)<sup>37</sup> [...] inom ramen för GDPR ska begränsningar **införas i en lagstiftningsåtgärd, omfatta ett begränsat antal av de registrerades rättigheter och/eller den personuppgiftsansvariges skyldigheter** vilka anges i artikel 23 i den allmänna dataskyddsförordningen, **ske med respekt för andemeningen i de grundläggande rättigheterna och friheterna i fråga och utgöra en nödvändig och proportionell åtgärd** i ett demokratiskt samhälle i syfte att säkerställa ett av de skäl som fastställs i artikel 23.1 i den allmänna dataskyddsförordningen [...] <sup>38</sup>.
67. EDPB erinrar också om att det i skäl 41 till den allmänna dataskyddsförordningen anges att "[n]är det i denna förordning hänvisas till en **rättslig grund eller lagstiftningsåtgärd**, innebär detta inte

---

*Den anställda begär dock en kopia av sina personuppgifter från inrikesministeriet som nu undersöker dem. Inrikesministeriet kan förlita sig på undantaget för att undanhålla en del av sina uppgifter om utlämnandet av uppgifter sannolikt skulle inverka menligt på undersökningen. Om den anställda gör en liknande begäran till sin arbetsgivare skulle denna också kunna tillämpa undantaget i samma utsträckning.*

*Med andra ord, vilket klargörs på sidan 300: I de flesta fall kommer inrikesministeriet, eller en av dess byråer och entreprenörer, att vara den registeransvariga som tillämpar detta undantag. Det är dock viktigt att notera att tillämpningen av detta undantag inte bara är begränsad till inrikesministeriet. Det kan också vara relevant för andra registeransvariga, såsom arbetsgivare, universitet och polisen, som samarbetar med inrikesministeriet i invandringsfrågor.*

<sup>37</sup> Se EDPB *Guidelines 10/2020 on restrictions under Article 23 GDPR*, version 1.0, antagna den 15 december 2020, som för närvarande slutförs efter offentligt samråd, [https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-102020-restrictions-under-article-23\\_sv](https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-102020-restrictions-under-article-23_sv).

<sup>38</sup> Se EDPB *Guidelines 10/2020 on restrictions under Article 23 GDPR*, punkt 9, s. 5.

nödvändigtvis en lagstiftningsakt antagen av ett parlament, utan att detta påverkar krav som uppställs i den konstitutionella ordningen i den berörda medlemsstaten. En sådan rättslig grund eller lagstiftningsåtgärd bör dock vara **tydlig och precis och dess tillämpning bör vara förutsägbar för personer som omfattas av den**, i enlighet med rättspraxis vid Europeiska unionens domstol [...] och Europeiska domstolen för de mänskliga rättigheterna.” (fetstil tillagd).

68. Men Europeiska domstolen för de mänskliga rättigheterna specificerade att *[v]idare, när det gäller formuleringarna 'med stöd av lag' och 'föreskrivna i lag' som finns med i artiklarna 8 till 11 i Europakonventionen, konstaterar [Europeiska domstolen för de mänskliga rättigheterna] att den alltid har förstått termen 'lagen' i dess 'substantiella' betydelse och inte i den 'formella' betydelsen. Den har omfattat både 'skriven lag', vilket omfattar lagtexter från lägre prioriterade stadgar och lagstiftningsåtgärder vidtagna av professionella lagstiftande organ med självständiga lagstiftande befogenheter som delegerats till dem av parlamentet, samt oskriven lag. 'Lag' måste förstås som att det omfattar både skriven rätt och 'lag' som stiftats av domstolen<sup>39</sup>, i Guidelines 10/2020 on restrictions under Article 23 GDPR erinrar man om att [i] enlighet med rättspraxis från Europeiska unionens domstol, ska alla lagstiftningsåtgärder som antas på grundval av artikel 23.1 i den allmänna dataskyddsförordningen, särskilt, **uppfylla de särskilda krav som fastställs i artikel 23.2 i den allmänna dataskyddsförordningen**. I artikel 23.2 i den allmänna dataskyddsförordningen anges att de lagstiftningsåtgärder som innebär begränsningar av de registrerades rättigheter och den personuppgiftsansvariges skyldigheter ska innehålla **specifika bestämmelser åtminstone, när så är relevant, avseende flera kriterier som anges nedan**. I regel ska alla de krav som anges nedan **ingå i den lagstiftningsåtgärd som innebär begränsningar i enlighet med artikel 23 [i] den allmänna dataskyddsförordningen**<sup>40</sup>.*
69. Man kan i detta hänseende notera att **undantaget för invandring** i sig självt **inte innehåller följande aspekter som anges i artikel 23.2 i den allmänna dataskyddsförordningen**:
- "skyddsåtgärder för att förhindra missbruk eller olaglig tillgång eller överföring" d),

---

<sup>39</sup> Se Europeiska domstolen för de mänskliga rättigheterna, Sanoma Uitgevers B.V./The Netherlands, 14 september 2010, EC:ECHR:2010:0914JUD003822403, punkt 83.

<sup>40</sup> Se EDPB Guidelines 10/2020 on restrictions under Article 23 GDPR, punkterna 45 och 46, s. 11. Enligt artikel 52.3 i EU-stadgan "[i] den mån som denna stadga omfattar rättigheter som motsvarar sådana som garanteras av europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna ska de ha samma innebörd och räckvidd som i konventionen. Denna bestämmelse hindrar inte unionsrätten från att tillförsäkra ett mer långtgående skydd.". Angående begreppet "**föreskriven i lag**" enligt artikel 52.1 i EU-stadgan, ska de kriterier som utarbetats av Europeiska domstolen för de mänskliga rättigheterna användas så som det föreslås i flera förslag till avgöranden från EU-domstolens generaladvokat, se bland annat förslagen till avgörande i de förenade målen C-203/15 och C-698/15, Tele2 Sverige AB, ECLI:EU:C:2016:572, punkterna 137–154, och i mål C-70/10, Scarlet Extended, ECLI:EU:C:2011:255, punkterna 88–114. Därmed kan man hänvisa till, bland annat, Europeiska domstolen för de mänskliga rättigheternas avgörande i Weber and Saravia/Germany, punkt 84: *Domstolen upprepar att uttrycket "med stöd av lag" enligt artikel 8 § 2 [i Europakonventionen] kräver, för det första, att den ifrågasatta åtgärden har någon grund i den inhemska lagstiftningen. Vi hänvisar även till kvaliteten hos lagen i fråga och kräver att den ska vara tillgänglig för den berörda personen som därutöver måste kunna förutse dess konsekvenser för honom eller henne, samt förenlig med rättsstatsprincipen.* (fetstil tillagd).

Se även skäl 41 i den allmänna dataskyddsförordningen: "En sådan rättslig grund eller lagstiftningsåtgärd bör dock vara **tydlig och precis** och dess tillämpning bör vara **förutsägbar för personer som omfattas av den**, i enlighet med rättspraxis vid Europeiska unionens domstol [...] och Europeiska domstolen för de mänskliga rättigheterna." (fetstil tillagd).

- "den personuppgiftsansvarige eller kategorierna av personuppgiftsansvariga" e)<sup>41</sup>,
- "riskerna för de registrerades rättigheter och friheter" g),
- "de registrerades rätt att bli informerade om begränsningen, såvida detta inte kan inverka menligt på begränsningen" h).

70. Den brittiska dataskyddsmyndighetens *Guide to the General Data Protection Regulation (GDPR)*<sup>42</sup>, som innehåller ett kapitel om "undantaget för invandring" erbjuder tydliggöranden om undantaget för invandring men **kan inte** i sig tillhandahålla bindande regler som kompletterar det. Dessutom är frågan om "kvaliteten hos lagen" särskilt relevant med tanke på vikten av de begränsade rättigheterna och undantagets omfattning<sup>43</sup>.

<sup>41</sup> Se ovannämnda mål från Överdomstolen, punkt 54: *I min mening finns det inget som är olagligt med att undantaget för invandring finns tillgängligt för alla personuppgiftsansvariga som behandlar personuppgifter i de angivna syftena. Som de svarande påpekar så skulle undantaget för invandring bli verkningslöst utan punkterna 4.3–4 i fall där man erhållit uppgifter från tredje parter (så som en lokal myndighet eller den brittiska skatte- och tullmyndigheten) i syfte att upprätthålla effektiv invandringskontroll. (fetstil tillagd), därmed bekräftar man den generella tillämpningen av begränsningarna.*

<sup>42</sup> Den brittiska dataskyddsmyndighetens *Guide to the General Data Protection Regulation (GDPR)*, v 01 januari 2021, s. 299–307.

<sup>43</sup> Se punkt 57 i det tidigare nämnda målet från Överdomstolen: *Herr Knight informerar mig om att kommissionären håller på att slutföra vägledningen för undantaget, men den kommer att ha "lagstadgad" status endast i den betydelsen att den utfärdats med stöd av kommissionärens befogenheter i enlighet med artikel 57.1 i den allmänna dataskyddsförordningen. Den kommer inte att någon rättslig status i enlighet med 2018 års dataskyddslag.*

Resonemanget bakom att man inför juridiskt bindande vägledning med stöd av den brittiska dataskyddsmyndigheten beskrivs särskilt i punkterna 56–60 i domen:

56. Slutligen, vänder jag mig till kommissionärens inlaga om att utan medföljande lagstadgad vägledning som kan tillhandahålla skyddsåtgärder gällande betydelsen och tillämpningen av undantaget för invandring så skulle undantaget inte utgöra en proportionerlig tillämpning av artikel 23.1 i den allmänna dataskyddsförordningen. Herr Knight menar att när bestämmelsen åtföljs av sådan vägledning så är den proportionerlig.

57. Herr Knight informerar mig om att kommissionären håller på att slutföra vägledningen för undantaget, men den kommer att ha "lagstadgad" status endast i den betydelsen att den utfärdats med stöd av kommissionärens befogenheter i enlighet med artikel 57.1 i den allmänna dataskyddsförordningen. Den kommer inte att någon rättslig status i enlighet med 2018 års dataskyddslag. Jag förstår även att inrikesministeriet har utarbetat ett utkast till interna riktlinjer gällande undantaget för invandring (se [22] ovan). I praktiken är riktlinjer som utfärdats av kommissionären inflytelserika oavsett vilken rättslig grund de har. Dock har kommissionären ingen befogenhet att utfärda en "bindande" vägledning av den sort som den Högsta domstolen hade i åtanke i målet rörande *Christian Institute* (punkterna [101] och [107]). Det verkar som att primärlagstiftning skulle krävas om det skulle bedömas nödvändigt att det finns vägledning rörande undantaget för invandring som har samma status som de förfaranderegler som fastställs på sidorna [avsnitt 121–124 i 2018 års dataskyddslag](#).

58. I sina argument för lagstadgad vägledning framhåller Herr Knight att det sammanhang i vilket användningen av undantaget för invandring kommer att uppstå av nödvändighet ramar in frågorna om nödvändigheten och proportionaliteten i att det finns och används. Han drar uppmärksamheten till särskilt två frågor i det rättsliga sammanhanget. För det första, de personuppgifter som undantaget för invandring tillämpas på är i sig sådana att de troligtvis omfattar de särskilda kategorier av personuppgifter som beskrivs i artikel 9.1 i den allmänna dataskyddsförordningen (dvs. uppgifter som "avslöjar ras eller etniskt ursprung"). Sådana uppgifter identifieras i den allmänna dataskyddsförordningen eftersom de kräver en högre skyddsnivå ([Yttrande 1/15 \[2019\] 3 C.M.L.R. 25](#) punkt [141]). För det andra, så är det en grundläggande tes inom dataskyddslagstiftning att den registrerades rätt till tillgång är av stor vikt i egenskap av att det är inkörsporten till att kunna utöva de andra rättigheter som registrerade personer har tillgång till (se [YS/Minister voor Immigratie, Integratie en Asiel \(C-141/12\) EU:C:2014:2081; \[2015\] 1 C.M.L.R. 18](#) punkt [44]).

71. I ännu högre grad så innebär **"inverkanstestet"** inte att man fastställer några skyddsåtgärder för att förhindra missbruk eller olaglig tillgång eller överföring, och som skulle kunna tillämpas av till exempel inrikesministeriet.
72. Mot bakgrund av allt det som beskrivits ovan, påpekar EDPB att ytterligare klargöranden kring tillämpningen av undantaget för invandring krävs.
73. Vidare påpekar EDPB avsaknaden av ett juridiskt bindande instrument som klargör undantaget för invandring när det gäller att överväga om det i huvudsak motsvarar artikel 23 i den allmänna dataskyddsförordningen och artiklarna 7 och 8 i EU-stadgan om de grundläggande rättigheterna. Samtidigt anser EDPB att nödvändigheten och proportionaliteten för den personkrets som omfattas av tillämpningsområdet för undantaget för invandring måste bevisas ytterligare av Europeiska kommissionen, med stöd av bevismaterial.
74. Slutligen, uppmanar EDPB Europeiska kommissionen att kontrollera det aktuella läget i förfarandet **Open Rights Group & Anor, R (On the Application Of) mot Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin)** som det hänvisas till ovan, eftersom detta inte är en slutlig dom (*res judicata*), för att kontrollera om avgörandet i första instans bekräftats eller omprövats, så att man kan ta hänsyn till eventuella uppdateringar i detta hänseende och specificera det i beslutet om adekvat skyddsnivå. EDPB uppmanar också Europeiska kommissionen att tillhandahålla ytterligare information om nödvändigheten och proportionaliteten för undantaget för invandring, särskilt med hänsyn till den breda omfattningen av tillämpningen med hänsyn till personkretsen.
75. Samtidigt anmodar EDPB Europeiska kommissionen att vidare undersöka huruvida det finns ytterligare skyddsåtgärder inom ramen för Förenade kungarikets rättsliga ram eller om sådan skulle kunna planeras, till exempel med hjälp av juridiskt bindande instrument som skulle komplettera undantaget för invandring och öka dess förutsägbarhet och dess skyddsåtgärder för de registrerade, vilket också skulle möjliggöra en bättre och snabbare bedömning och övervakning av nödvändighets- och proportionalitetskraven.

---

59. Herr Knight identifierar fyra punkter av praktisk natur. För det första, när personuppgiftsansvariga inte förklarar för de registrerade att de förlitat sig på ett lagstadgat undantag och inte heller tillhandahåller en bred sammanfattning av skälen till detta, så kommer den registrerade att vara omedveten om att undantaget har tillämpats och har därmed ingen möjlighet att bestrida det. För det andra kommer de registrerade att vara särskilt beroende av att de personuppgiftsansvariga tillämpar undantaget med försiktighet och bara i den mån den är nödvändig. Även om alla registrerade har rätt att klaga till kommissionären gällande tillämpningen av undantaget eller att väcka talan inför domstol, så är det troligt att den registrerade är omedveten om sina rättigheter och saknar medel för att vidta rättsliga åtgärder, i situationer där det behövs en snabb och korrekt efterlevnad av rättigheterna i fråga om uppgiftsskydd. För det tredje, som invandrare befinner sig den registrerade troligen i en utsatt position. För det fjärde, det här är inte en abstrakt fråga mot bakgrund av den svarandes bevis gällande användningen av undantaget för invandring (se [4] ovan).

60. Herr Knight menar att det finns en nära parallell mellan föreliggande bestridande av undantaget för invandring och domstolens resonemang i målet [Christian Institute \[2016\] UKSC 51](#). Som med [Christian Institute](#), framhåller han, är undantaget för invandring brett, det använder odefinierade termer, tillämpar en låg tröskel, det är föremål för kontroller som inte är uppenbara på bestämmelsens yta och det tillämpas på en bred uppsättning sammanhang och rättigheter. Till skillnad från [Christian Institute](#) finns det när det gäller undantaget för invandring ingen offentligt tillgänglig vägledning och ännu mindre av en lagstadgad status som man måste ta hänsyn till.

### 3.1.2. Begränsningar av vidare överföring

76. I artikel 44 i den allmänna dataskyddslagen fastställs att överföring och vidare överföring av personuppgifter bara får ske om den nivå på skyddet av fysiska personer som säkerställs genom den allmänna dataskyddsförordningen inte undergrävs. Därför ska personuppgifter som överförs från EES till Förenade kungariket på grundval av beslutet om adekvat skyddsnivå åtnjuta en skyddsnivå som i huvudsak motsvarar den som tillhandahålls inom ramen för EU:s dataskyddsram. **Det betyder att Förenade kungarikets lagstiftning inte bara ska vara "i huvudsak ska motsvara" EU-lagstiftningen när det gäller behandling av personuppgifter som överförs till Förenade kungariket i enlighet med utkastet till beslut, utan de regler som är tillämpliga i Förenade kungariket när det gäller vidare överföring av dessa personuppgifter till tredje land ska också säkerställa att en skyddsnivå som i huvudsak motsvarar den inom EES fortsätter att tillhandahållas.**
77. Därmed är det viktigt att all vidare överföring från Förenade kungariket till ett annat tredjeland av personuppgifter från EES skyddas ordentligt med skyddsåtgärder, eller utförs i enlighet med reglerna för undantag<sup>44</sup> för att säkerställa en kontinuitet av det skydd som tillhandahålls i EU-lagstiftningen. **Och om sådant skydd inte kan tillhandahållas, så ska ingen överföring av personuppgifter från EES äga rum.**
78. EDPB erkänner att Förenade kungariket till största delen har speglat kapitel V i den allmänna dataskyddsförordningen i den brittiska allmänna dataskyddsförordningen (artiklarna 44–49) och i 2018 års dataskyddslag<sup>45</sup>. **Men EDPB har identifierat vissa aspekter i Förenade kungarikets rättsliga ram när det gäller vidare överföring som kan undergräva skyddsnivån för personuppgifter som överförs från EES.**
79. **Den första utmaningen** som EDPB har identifierat har att göra med Förenade kungarikets erkännande, i enlighet med det förfarande som utarbetats i 2018 års dataskyddslag, av tredjeländer, internationella organisationer och territorier<sup>46</sup> som adekvata mottagare. Vidare överföring av personuppgifter från EES kan komma att ske från Förenade kungariket till andra tredjeländer, på grundval av Förenade kungarikets framtida möjlig förordning rörande adekvat skyddsnivå<sup>47</sup>.
80. Mer specifikt, har Förenade kungarikets minister befogenhet att som förklaras i skäl 77 i utkastet till beslut, erkänna att ett tredjeland (eller ett territorium eller ett område i ett tredjeland), en internationell organisation eller en beskrivning av ett sådant land, territorium, område eller organisation har en adekvat skyddsnivå för personuppgifter efter samråd med den brittiska dataskyddsmyndigheten<sup>48</sup>. När Förenade kungarikets inrikesminister bedömer adekvat skyddsnivå ska denne beakta samma delar som Europeiska kommissionen ska bedöma enligt artikel 45.2 a–c i den allmänna dataskyddsförordningen, som tolkas tillsammans med skäl 104 i den allmänna dataskyddsförordningen och bibehållen EU-rättspraxis. Detta innebär att man vid bedömning av ett tredjelands adekvata skyddsnivå tillämpar relevanta standarder för om det berörda tredjelandet kan säkerställa en skyddsnivå som "i huvudsak motsvarar" det skydd som garanteras i Förenade

<sup>44</sup> Se artikel 49 i den brittiska allmänna dataskyddsförordningen.

<sup>45</sup> Se avsnitt 17A, 17B, 17C och 18 i 2018 års dataskyddslag.

<sup>46</sup> Se avsnitt 17 i 2018 års dataskyddslag.

<sup>47</sup> Förenade kungarikets motsvarighet till ett beslut om adekvat skyddsnivå i enlighet med den allmänna dataskyddsförordningen.

<sup>48</sup> Se avsnitt 182.2 i 2018 års dataskyddslag. Se även samförståndsavtalet om den brittiska dataskyddsmyndighetens roll med hänsyn till nya bedömningar om adekvat skyddsnivå i Förenade kungariket, <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/03/secretary-of-state-for-the-department-for-dcms-and-the-information-commissioner-sign-memorandum-of-understanding/>.

kungariket. Även om EDPB noterar Förenade kungarikets förmåga att enligt den brittiska allmänna dataskyddsförordningen erkänna territorier som har en adekvat skyddsnivå sett till Förenade kungarikets dataskyddsråd vill EDPB betona att dessa senare territorier kanske inte för närvarande omfattas av ett beslut om adekvat skyddsnivå som utfärdats av Europeiska kommissionen där man erkänner en skyddsnivå som ”i huvudsak motsvarar” det skydd som garanteras i EU. Detta kan innebära eventuella risker i det skydd av personuppgifter som tillhandahålls från EES, särskilt om Förenade kungarikets dataskyddsråd avviker från EU:s regelverk i framtiden. Det bör noteras att EU-domstolens vägledande mål Schrems II i juli 2020<sup>49</sup> innebar att beslutet om den amerikanska skölden för skydd av privatlivet ogiltigförklarades eftersom den amerikanska rättsliga ramen inte kunde anses tillhandahålla en skyddsnivå som i huvudsak motsvarar skyddet i EU. De redan antagna domarna från EU-domstolen som betraktas som bibehållen rättspraxis i Förenade kungarikets rättsliga ram kan emellertid inte vara bindande för Förenade kungariket längre, särskilt eftersom Förenade kungariket kan ändra bibehållen unionslagstiftning när överbrygningsperioden har löpt ut, och när landets högsta domstol inte längre är bunden till någon bibehållen EU-rättspraxis<sup>50</sup>.

81. **EDPB uppmanar Europeiska kommissionen att noga övervaka Förenade kungarikets bedömningsprocesser och kriterier för adekvat skyddsnivå avseende andra tredjeländer, särskilt med hänsyn till de tredjeländer som inte erkänns ha en adekvat skyddsnivå enligt EU:s allmänna dataskyddslag. Om Europeiska kommissionen inte finner att en skyddsnivå som i huvudsak motsvarar skyddsnivån i EU inte kan garanteras i ett tredjeland som anses ha en adekvat skyddsnivå uppmanar EDPB kommissionen att vidta de åtgärder som krävs för att till exempel ändra Förenade kungarikets beslut om adekvat skyddsnivå så att det inbegriper särskilda skyddsåtgärder för personuppgifter som kommer från EES, och/eller beakta upphävandet av Förenade kungarikets beslut om adekvat skyddsnivå i de fall där personuppgifter som överförts från EES till Förenade kungariket omfattas av vidare överföring till det berörda tredjelandet mot bakgrund av Förenade kungarikets förordning om adekvat skyddsnivå.**
82. **Den andra utmaningen** har att göra med den kommande översynen av de redan befintliga besluten om adekvat skyddsnivå som utfärdats av Europeiska kommissionen i enlighet med direktiv 95/46/EG. Efter denna översyn kan Europeiska kommissionen komma att besluta att vissa länder som fram till nu har haft ett beslut om adekvat skyddsnivå inte längre tillhandahåller en skyddsnivå som i huvudsak motsvarar den inom EES, med hänsyn till nuvarande EU-lagstiftning och nyare rättspraxis. Förenade kungariket har emellertid, i enlighet med vad som fastställs i bilaga 21, punkt 4 i 2018 års dataskyddslag, redan erkänt att dessa länder tillhandahåller en adekvat skyddsnivå. Även om Förenade kungarikets inrikesminister måste göra en översyn av dessa konstateranden om adekvat skyddsnivå inom en period på fyra år, så noterar Europeiska kommissionen i sitt utkast till beslut att dessa konstateranden om adekvat skyddsnivå inte automatiskt kommer att upphöra om Förenade kungarikets inrikesminister inte utför den översyn som krävs inom den föreskrivna fyraårsperioden<sup>51</sup>.
83. **EDPB uppmanar Europeiska kommissionen att övervaka huruvida något land som, efter att EU-översynen av de redan befintliga besluten om adekvat skyddsnivå är slutförd, inte längre bedöms tillhandahålla en adekvat skyddsnivå fortfarande bedöms göra det av Förenade kungariket. Om detta skulle vara fallet, uppmanar EDPB Europeiska kommissionen att, på grundval av skälen 277–280 i utkastet till beslut vidta lämpliga åtgärder för att åtgärda situationen, till exempel genom att**

---

<sup>49</sup> Se Schrems II.

<sup>50</sup> Se avsnitt 6.3 till 6.6 i EU (Withdrawal) Act 2018.

<sup>51</sup> Se skäl 82 i utkastet till beslut.

**ändra beslutet om adekvat skyddsnivå för att lägga till specifika krav för personuppgifter som kommer från EES och/eller genom att upphäva beslutet om adekvat skyddsnivå, om personuppgifter som överförts från EES till Förenade kungariket är föremål för vidare överföring till tredjelandet i fråga. EDPB uppmanar Europeiska kommissionen att fortsätta denna övervakning under giltighetstiden för beslutet om adekvat skyddsnivå gällande Förenade kungariket.**

84. **Den tredje utmaningen** har att göra med vidare överföring av personuppgifter från EES till länder som saknar en adekvat skyddsnivå på grundval av de överföringsverktyg som beskrivs i artiklarna 46 och 47 i den brittiska allmänna dataskyddsförordningen. Även om den brittiska allmänna dataskyddsförordningen innehåller samma överföringsverktyg som den allmänna dataskyddsförordningen, så understryker EDPB behovet av att säkerställa att de skyddsåtgärder de omfattar tillhandahåller ett effektivt skydd i tredjelandet, särskilt sett till Schrems II-domen.
85. Efter domen i målet Schrems II, där EU-domstolen påminner om att det skydd som ges till personuppgifter inom EU alltid måste följa med uppgifterna, har EDPB redan antagit inledande rekommendationer om kompletterande åtgärder<sup>52</sup> för att vid behov stödja exportörer i arbetet med att säkerställa att registrerade personer ges en skyddsnivå som i huvudsak motsvarar den som garanteras inom EU.
86. Enligt EU-domstolen är uppgiftsutförare ansvariga för att verifiera, från fall till fall och där det är lämpligt i samarbete med uppgiftsinföraren i tredjelandet, om landets lag eller praxis inkräktar på effektiviteten hos de lämpliga skyddsåtgärder som ingår i överföringsverktygen i artikel 46 i den allmänna dataskyddsförordningen<sup>53</sup>. När då är fallet ska uppgiftsutförarna genomföra kompletterande åtgärder som fyller dessa luckor i skyddet och höja det till den nivå som krävs enligt unionsrätten.
87. **EDPB uppmanar Europeiska kommissionen att, för att säkerställa kontinuiteten i skyddet, i utkastet till beslut införliva försäkringar om att när de överföringsverktyg som föreskrivs i artiklarna 46 och 47 i den brittiska allmänna dataskyddsförordningen används av uppgiftsutförare i Förenade kungariket för vidare överföring till andra tredjeländer av uppgifter som överförts från EES så bedömer dessa uppgiftsutförare från fall till fall dataskyddsramen i tredjelandet. Och om det är nödvändigt vidtar de lämpliga åtgärder för att säkerställa en effektiv respekt för de skyddsåtgärder som ingår i det valda överföringsverktyget för att säkerställa en skyddsnivå som i huvudsak motsvarar den som garanteras inom EU. Utan dessa försäkringar, betonar EDPB att det finns en risk att den skyddsnivå som i huvudsak motsvarar den som garanteras inom EU riskerar att urvattnas genom att vidare överföring sker från Förenade kungariket.**
88. **Den fjärde utmaningen** som har att göra med vidare överföring rör de internationella överenskommelser som ingåtts, eller som ingås i framtiden av Förenade kungariket och den möjliga direkta tillgång till personuppgifter från EES som dessa överenskommelser ger myndigheter i tredjeland/-länder som är parter i dessa avtal. EDPB känner stark oro för det redan ingångna CLOUD-avtalet och Europeiska kommissionen erkänner denna utmaning samt betonar att *ett möjligt ikraftträdande av avtalet kan komma att påverka den skyddsnivå som bedömts i detta beslut*<sup>54</sup>.

---

<sup>52</sup> Se EDPB:s rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överensstämmelsen med EU-nivån för skydd av personuppgifter, antagna 10 november 2020, som för närvarande slutförs efter offentligt samråd, [https://edpb.europa.eu/sites/default/files/consultation/edpb\\_recommendations\\_202001\\_supplementarymeasures\\_transfer\\_tools\\_sv.pdf](https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasures_transfer_tools_sv.pdf).

<sup>53</sup> Se Schrems II, punkt 134.

<sup>54</sup> Se skäl 153 i utkastet till beslut.

Utifrån den överenskommelsen, när den träder i kraft, skulle personuppgifter som överförs från EES till Förenade kungariket i enlighet med utkastet till beslut sedan omfattas av bestämmelserna i denna överenskommelse där man fastställer villkoren för direkt tillgång för amerikanska myndigheter, vilket påverkar Förenade kungarikets dataskyddsram och däribland bestämmelserna rörande vidare överföring. Därmed kan den skyddsnivå som tillhandahålls för de uppgifter som överförs från EES komma att påverkas avsevärt av bestämmelserna i denna överenskommelse som ingåtts med Förenta staterna och inverka på skyddsnivån för sådana uppgifter. EDPB noterar i det här sammanhanget att Europeiska kommissionen hänvisar till förklaringar som givits av Förenade kungarikets myndigheter i skäl 153 till utkastet till beslut, utan att citera eller tillhandahålla någon konkret skriftlig försäkran eller åtagande och man pekar inte heller på någon specifik rättslig bestämmelse i Förenade kungarikets lagstiftning som skulle ge verkan åt sådana förklaringar.

89. EDPB har tidigare påtalat denna oro i ett brev adresserat till Europaparlamentet daterat 15 juni 2020<sup>55</sup>. EDPB har betonat att på grundval av *EU:s regelverk på dataskyddsområdet, och särskilt den allmänna dataskyddsförordningen och dataskyddsdirektivet för brottsbekämpning* så har EDPB reservationer när det gäller huruvida skyddsåtgärderna i överenskommelsen för tillgång till personuppgifter i Förenade kungariket skulle vara giltiga under vissa förutsättningar som kräver upplysningsskyldigheter gentemot Förenta staterna, samt när det gäller huruvida dessa skyddsåtgärder är tillräckliga sett till EU-standarden så att den skyddsnivå som tillhandahålls av EU inte undergrävs.
90. Vidare kan bestämmelserna i CLOUD-avtalet avsevärt inverka på de materiella och formella villkoren enligt vilka myndigheter i Förenta staterna kan ges direkt tillgång personuppgifter som innehas av personuppgiftsansvariga eller personuppgiftsbiträden i Förenade kungariket och därmed påverka den skyddsnivå som garanteras enligt Förenade kungarikets lagstiftning. För att tillhandahålla en skyddsnivå som i huvudsak motsvarar den som garanteras enligt EU-lagstiftningen är det till exempel avgörande att skyddsåtgärderna i enlighet med en sådan överenskommelse omfattar ett obligatorisk rättsligt tillstånd, som en nödvändig garanti för tillgången till metadata och innehållsdata. Utifrån sin preliminära bedömning kan EDPB, även om man noterar att det i överenskommelsen hänvisas till nationell lagstiftning, inte identifiera någon sådan tydlig bestämmelse i den överenskommelse som ingåtts mellan Förenade kungariket och Förenta staterna<sup>56</sup>.
91. Även om Europeiska kommissionen lyfter fram att uppgifter som erhållits inom ramen för denna överenskommelse ska åtnjuta likvärdigt skydd som det som tillhandahålls av de specifika skyddsåtgärderna i det så kallade paraplyavtalet mellan EU och Förenta staterna, finns det en oro hos EDPB gällande huruvida införlivandet av dessa skyddsåtgärder i CLOUD-avtalet genom enbart en hänvisning som tillämpas i tillämpliga delar skulle uppfylla kriterierna för tydliga, precisa och tillgängliga regler när det gäller tillgången till personuppgifter, eller om det i tillräcklig utsträckning skulle inbegripa att sådana skyddsåtgärder är effektiva och ger möjlighet att väcka talan enligt Förenade kungarikets lagstiftning.
92. **EDPB rekommenderar därför att Europeiska kommissionen klargör hur och på grundval av vilket rättsligt instrument likvärdigt skydd som de specifika skyddsåtgärderna i paraplyavtalet mellan EU**

---

<sup>55</sup> Se EDPB:s svar till parlamentsledamöterna Sophie in't Veld och Moritz Körner rörande överenskommelsen mellan Förenta staterna och Förenade kungariket inom ramen för *US Cloud Act*, antaget den 15 juni 2020, [https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_letter\\_out\\_2020-0054-uk-usagreement.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0054-uk-usagreement.pdf).

<sup>56</sup> Se det ovannämnda brevet från EDPB.

**och Förenta staterna skulle ges verkan och vara av bindande karaktär i enlighet med Förenade kungarikets lagstiftning.**

93. EDPB noterar också att bestämmelserna i CLOUD-avtalet när de jämförs med avsnitt 3 i *US CLOUD Act*<sup>57</sup> väcker frågor rörande den faktiska tillämpningen av de skyddsåtgärder som erbjuds i överenskommelsen för Förenta staternas brottsbekämpande myndigheters tillgång till personuppgifter i Förenade kungariket som behandlas av leverantörer av elektroniska kommunikationstjänster eller fjärrdatatjänster (nedan kallat *CSPs*) som faller under amerikansk jurisdiktion. Om en CSP som är belägen i Förenade kungariket skulle omfattas av amerikansk lagstiftning (t.ex. för att det är ett dotterbolag till ett amerikanskt företag), är det ännu inte fastställt huruvida de amerikanska myndigheterna skulle vara bundna att förlita sig på CLOUD-avtalet för att få uppgifterna. Eftersom Europeiska kommissionen påpekar att *[s]ärskild uppmärksamhet ska riktas mot tillämpningen och anpassningen av skydden i paraplyavtalet till den specifika typ av överföringar som omfattas av överenskommelsen mellan Förenade kungariket och Förenta staterna*, betonar EDPB att på grundval av dess preliminära bedömning så är det oklart huruvida de skyddsåtgärder som ingår i CLOUD-avtalet, och därför de som tillhandahålls av paraplyavtalet mellan EU och Förenta staterna, skulle vara tillämpliga på alla, om några, av de förfrågningar om tillgång till personuppgifter som riktas till Förenade kungariket från amerikanska myndigheter inom ramen för *US CLOUD Act*.
94. Det kan komma andra framtida internationella överenskommelser eller åtaganden med tredjeländer som Förenade kungariket kan komma att ingå i framtiden och som skulle vara tillämpliga på personuppgifter som överförs från EES till Förenade kungariket i enlighet med utkastet till beslut<sup>58</sup>. Beroende på bestämmelserna i dessa överenskommelser och tillämpningen av specifika skyddsåtgärder kan dessa internationella överenskommelser, i och med att de påverkar Förenade kungarikets dataskyddsram, också avsevärt komma att påverka de materiella och formella villkoren för tredjeländers myndigheters tillgång till personuppgifter i Förenade kungariket. Det här är särskilt fallet när det gäller utkastet till det andra tilläggsprotokollet till Europarådets konvention om it-brottslighet (nedan kallat *Budapestkonventionen*) som för närvarande förhandlas fram av parterna in konventionen, vilka omfattar flera länder utanför EU. Utkastet till protokollet omfattar faktiskt flera klausuler som godtyckligt kan aktiveras av parterna, till exempel gällande valet att bevilja tillgång till innehållsdata eller inte. Även om alla EU:s medlemsstater skulle aktivera klausulerna i enlighet med EU:s regler för skydd av personuppgifter, så har ingen garanti lämnats gällande Förenade kungariket, som skulle kunna avvika avsevärt från den skyddsnivå som då skulle erbjudas inom EU. Ett annat exempel på de problem som beskrivs ovan är överenskommelsen mellan Förenade kungariket och Japan om ett omfattande ekonomiskt partnerskap<sup>59</sup> (*CEPA*), Förenade kungarikets första handelsavtal efter Brexit som trädde i kraft den 1 januari 2021<sup>60</sup> och som omfattar bestämmelser kring personuppgifter<sup>61</sup>. EDPB noterar vidare att Förenade kungariket även den 1

---

<sup>57</sup> Se *US CLOUD Act*, <https://www.congress.gov/bill/115th-congress/senate-bill/2383/text>.

<sup>58</sup> Se rubrik 2.3.3 ovan.

<sup>59</sup> Se Förenade kungariket/Japan: *Agreement for a Comprehensive Economic Partnership [CS Japan No.1/2020]*, <https://www.gov.uk/government/publications/uk-japan-agreement-for-a-comprehensive-economic-partnership-cs-japan-no12020>.

<sup>60</sup> Se Förenade kungarikets vägledning om Förenade kungarikets handelsavtal med länder utanför EU, <https://www.gov.uk/guidance/uk-trade-agreements-with-non-eu-countries>.

<sup>61</sup> I enlighet med artikel 8.80, punkt 5 i *CEPA*, åtar sig parterna att uppmuntra utvecklingen av mekanismer för att främja kompatibilitet mellan deras olika rättsliga strategier för skydd av (person)uppgifter. I enlighet med artikel 8.84, åtar sig parterna att inte förbjuda eller begränsa gränsöverskridande överföringar av information med elektroniska medel, däribland personlig information, när denna aktivitet utförs i samband med att en person som omfattas av *CEPA* bedriver affärsverksamhet.

februari 2021 formellt tillkännagav sin begäran om att gå med i det övergripande och progressiva avtalet för Stillehavspartnerskapet ("CPTPP") som omfattar Partnerskapsavtalet för Stillehavsområdet (TPP)<sup>62</sup>.

95. EDPB noterar att, förutom CLOUD-avtalet, så behandlas inte de överenskommelser som nämns ovan i utkastet till beslut.
96. **EDPB uppmanar Europeiska kommissionen att**
- undersöka samspelet mellan Förenade kungarikets dataskyddsram och dess internationella åtaganden, bortom CLOUD-avtalet, framför allt för att säkerställa kontinuitet i skyddsnivån i fall av vidare överföring till andra tredjeländer av personuppgifter som överförs från EES till Förenade kungariket på grundval av Förenade kungarikets beslut om adekvat skyddsnivå, och att regelbundet övervaka och vidta åtgärder där så krävs när det gäller andra internationella överenskommelser som ingåtts mellan Förenade kungariket och tredjeländer som riskerar att underminera skyddsnivån av personuppgifter som tillhandahålls i EU,
  - förse EDPB med skriftliga åtaganden från myndigheter i Förenade kungariket och identifiera specifika bestämmelser i Förenade kungarikets lagstiftning, när det gäller förklaringen rörande den möjliga tillämpningen och genomförandet av CLOUD-avtalet så som det beskrivs i skäl 153 i utkastet till beslut,
  - i detta sammanhang övervaka huruvida CLOUD-avtalet, utöver de skyddsåtgärder som skulle kunna tillhandahållas i och med en lämplig tillämpning av anpassningen av paraplyavtalet mellan EU och Förenta staterna, säkerställer lämpliga ytterligare skyddsåtgärder så att man tar hänsyn till känsligheten hos uppgifterna i fråga och de unika kraven på överföring av elektroniska bevis direkt från CSPs snarare än mellan myndigheter.
  - bedöma inverkan och de potentiella riskerna med de bestämmelser kring personuppgifter som ingår i de internationella avtal som nyligen undertecknats av Förenade kungariket, så som CEPA.
97. **Den femte utmaningen** som identifierats har att göra med tillämpningen av undantagen för överföring av personuppgifter till ett tredjeland. Även om de tillgängliga undantaget enligt den brittiska allmänna dataskyddsförordningen är desamma som de som tillhandahålls i den allmänna dataskyddsförordningen, så är det viktigt att den brittiska dataskyddsmyndigheten tillämpar och fortsätter att tillämpa en tolkning gällande användningen av dessa undantag som stämmer överens med den som finns i den allmänna dataskyddsförordningen. Om så inte är fallet, eller om Förenade kungariket avviker från den här tolkningen i framtiden, finns det en risk för att skyddsnivån för de uppgifter som överförs från EES till tredjeländer via Förenade kungariket kan komma att undergrävas.
98. **EDPB uppmanar Europeiska kommissionen att, som en del av dess övervakningsarbete, specifikt kontrollera att Förenade kungarikets tolkning av användningen av undantag fortsätter att stämma överens med EU:s tolkning. Om en annan tolkning av användningen av undantag däremot skulle följas av Förenade kungariket och därmed undergräva skyddsnivån, så är det mycket viktigt att Europeiska kommissionen vidtar nödvändiga åtgärder genom att ändra beslutet om adekvat skyddsnivå för att säkerställa att den skyddsnivå som tillhandahålls för personuppgifter från EES**

---

<sup>62</sup> I enlighet med artikel 14.11 punkt 2 i TPP, ska var och en av parterna tillåta gränsöverskridande överföring av information med elektroniska medel, däribland personlig information, när denna aktivitet utförs i samband med att en person som omfattas bedriver affärsverksamhet.

som överförs till Förenade kungariket inte sedan kommer att undergrävas när dessa uppgifter överförs vidare från Förenade kungariket till tredjeländer på grundval av en annan tolkning av undantagen.

99. **Den sjätte utmaningen**, den sista i detta avsnitt, har att göra med frånvaron av det skydd som fastställs i artikel 48 i den allmänna dataskyddsförordningen i Förenade kungarikets dataskyddsram.
100. Europeiska kommissionen klargör i sitt utkast till beslut att i frånvaron av förordningar om adekvat skyddsnivå eller lämpliga skyddsåtgärder, kan en överföring bara ske på grundval av de undantag som fastställs i artikel 49 i den brittiska allmänna dataskyddsförordningen *med undantag för artikel 48 i förordning (EU) 2016/679 som Förenade kungariket har valt att inte införliva i den brittiska allmänna dataskyddsförordningen*.<sup>63</sup> Frånvaron i Förenade kungarikets dataskyddsram av en bestämmelse som i huvudsak motsvarar artikel 48 i den allmänna dataskyddsförordningen, när det gäller överföring eller utlämnande, efter ett domslut från en domstol eller ett beslut fattat av en administrativ myndighet i ett annat tredjeländ, kan ge upphov till rättslig osäkerhet gällande huruvida skyddsnivån för personuppgifter som överförs från EES till Förenade kungariket i enlighet med utkastet till beslut skulle påverkas väsentligt.
101. I sin referensram för adekvat skyddsnivå inom ramen för den allmänna dataskyddsförordningen påpekar EDPB att, när det gäller vidare överföring, *[ska] ytterligare överföring som utförs av den ursprungliga mottagaren av den ursprungliga uppgiftsöverföringen [...] bara vara tillåten när den ytterligare mottagaren också omfattas av regler som erbjuder en adekvat skyddsnivå och följer de relevanta instruktionerna när denne behandlar personuppgifter på den personuppgiftsansvariges vägnar*<sup>64</sup>. Vidare understryker EDPB att *den ursprungliga mottagaren av uppgifter som överförts från EU ska ansvara för att lämpliga skyddsåtgärder tillhandahålls för vidare överföring i avsaknad av ett beslut om adekvat skyddsnivå. Sådan vidare överföring av uppgifter får bara ske i begränsade och specificerade syften och så länge det finns en rättslig grund för den behandlingen*<sup>65</sup>. Som en del av kapitel V i den allmänna dataskyddsförordningen, måste man fullt ut ta hänsyn till artikel 48 när man bedömer huruvida Förenade kungarikets rättsliga ram säkerställer en skyddsnivå som i huvudsak motsvarar den inom EES i detta hänseende<sup>66</sup>.
102. EDPB betonar i detta sammanhang rättspraxis från EU-domstolen när det gäller risken för missbruk eller olaglig tillgång och användning av uppgifter och framhåller särskilt *vad gäller den nivå för skyddet av grundläggande fri- och rättigheter som garanteras inom unionen måste en unionslagstiftning som innebär ett ingrepp i de grundläggande rättigheter som garanteras av artiklarna 7 och 8 i stadgan, enligt domstolens fasta praxis, föreskriva tydliga och precisa bestämmelser som reglerar räckvidden och tillämpligheten av en åtgärd och slå fast minimikrav, så att de personer vilkas personuppgifter berörs har tillräckliga garantier som möjliggör ett effektivt skydd av deras uppgifter mot risker för missbruk och otillåten åtkomst eller användning. Behovet av sådana garantier är av än större betydelse när personuppgifterna är föremål för automatisk behandling och risken för otillåten åtkomst till uppgifterna är stor*<sup>67</sup>.

---

<sup>63</sup> Se fotnot 78 i utkastet till beslut.

<sup>64</sup> Se WP254 rev.01, s. 6.

<sup>65</sup> Se WP254 rev.01, s. 6.

<sup>66</sup> Se artikel 44 i den allmänna dataskyddsförordningen, sista meningen, särskilt: "Alla bestämmelser i detta kapitel ska tillämpas för att säkerställa att den nivå på skyddet av fysiska personer som säkerställs genom denna förordning inte undergrävs."

<sup>67</sup> Se Schrems I, punkt 91.

103. EDPB noterar i detta hänseende att, utifrån den information som finns tillgänglig i utkastet till beslut, föreskrivs inte tydligt i Förenade kungarikets dataskyddsram att ett domstolsbeslut eller beslut från myndigheter i tredjeland där det krävs att en personuppgiftsansvarig eller ett personuppgiftsbiträde överför eller lämnar ut personuppgifter får erkännas eller genomföras på något som helst sätt endast om det grundar sig på en internationell överenskommelse som gäller mellan det begärande tredjelandet och Förenade kungariket. Artikel 48 i den allmänna dataskyddsförordningen är en mycket viktig bestämmelse i kapitel V i den allmänna dataskyddsförordningen eftersom den kräver att en överföring eller ett utlämnande av personuppgifter efter ett domslut eller ett beslut från en administrativ myndighet i ett tredjeland får erkännas eller genomföras endast om det grundar sig på en internationell överenskommelse som gäller mellan det begärande tredjelandet och unionen eller en medlemsstat, utan att detta påverkar andra grunder för överföring enligt kapitel V i den allmänna dataskyddsförordningen. EDPB erinrar om att *en begäran från en utländsk myndighet inte i sig själv utgör en rättslig grund för en överföring. Ordern kan endast erkännas "om den grundar sig på en internationell överenskommelse, såsom ett avtal om ömsesidig rättslig hjälp, som gäller mellan det begärande tredjelandet och unionen eller en medlemsstat"*<sup>68</sup>. Det är därför avgörande att bestämmelser som i huvudsak motsvarar detta kan identifieras i Förenade kungarikets lagstiftning.
104. I utkastet till beslut rapporterar Europeiska kommissionen om förklaringar från myndigheterna i Förenade kungariket enligt vilka en utländsk begäran om uppgifter i enlighet med common law eller lag är ogenomförbar om det saknas en internationell överenskommelse och alla överföringar av uppgifter på begäran av en utländsk domstol eller administrativ myndighet kräver ett överföringsverktyg så som en förordning om adekvat skyddsnivå eller lämpliga skyddsåtgärder, förutom om ett undantag i enlighet med artikel 49 i den brittiska allmänna dataskyddsförordningen är tillämpligt. EDPB har emellertid inte fått tillgång till utbytena mellan Europeiska kommissionen och myndigheterna i Förenade kungariket<sup>69</sup> i denna fråga och kan därför inte analysera och göra en oberoende bedömning av huruvida de garantier som tillhandahållits av myndigheterna i Förenade kungariket är tillräckliga för att säkerställa en skyddsnivå som i huvudsak motsvarar de skyddsåtgärder som ingår i artikel 48 i den allmänna dataskyddsförordningen.
105. **EDPB uppmanar Europeiska kommissionen att tillhandahålla ytterligare försäkringar och specifika hänvisningar till Förenade kungarikets lagstiftning som säkerställer att skyddsnivån i enlighet med Förenade kungarikets rättsliga ram i huvudsak motsvarar den som garanteras inom EES. EDPB uppmanar därför Europeiska kommissionen att tillhandahålla skriftliga förklaringar och åtaganden från Förenade kungarikets myndigheter rörande tillämpningen av skydd som i huvudsak motsvarar det som tillhandahålls av artikel 48 i den allmänna dataskyddsförordningen.**
106. EDPB anser att identifieringen av bestämmelser i Förenade kungarikets lagstiftning som säkerställer en skyddsnivå som i huvudsak motsvarar de skyddsåtgärder som ingår i artikel 48 i den allmänna dataskyddsförordningen blir ännu viktigare mot bakgrund av de frågor som tidigare väckts kring begäranden om tillgång till uppgifter i Förenade kungariket från myndigheter i Förenta staterna eller andra tredjeländer, och med hänsyn till att i och med beslutet om adekvat skyddsnivå så kan personuppgifter överföras från EES till Förenade kungariket utan några ytterligare garantier eller bindande åtaganden från mottagaren när det gäller begäranden om tillgång till uppgifter från andra tredjeländers myndigheter.

---

<sup>68</sup> Se bilagan till EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection, antagen den 10 juli 2019, [https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act\\_sv](https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_sv).

<sup>69</sup> Se fotnot 78 i utkastet till beslut.

## 3.2. Förfarande- och verkställandemekanismer

107. På grundval av de kriterier som fastställs i referensramen för adekvat skyddsnivå inom ramen för den allmänna dataskyddsförordningen, har EDPB analyserat följande aspekter i Förenade kungarikets dataskyddsram så som de behandlas i utkastet till beslut: befintligheten av en effektivt fungerande oberoende tillsynsmyndighet, befintligheten av ett system som säkerställer en god nivå av efterlevnad och ett system för tillgång till lämpliga prövningsmöjligheter som förser enskilda personer i EU med möjligheter att utöva sina rättigheter och söka prövning utan att stöta på betungande hinder för administrativ och rättslig prövning.

### 3.2.1 Oberoende behörig tillsynsmyndighet

108. EDPB välkomnar Europeiska kommissionens insatser för att göra en omfattande utredning av inrättandet, funktionen och befogenheterna för Förenade kungarikets tillsynsmyndighet i kapitel 2.6 i utkastet till beslut. I Förenade kungariket har *Information Commissioner* till uppgift att ansvara för översyn och efterlevnad av den brittiska allmänna dataskyddsförordningen och 2018 års dataskyddslag. Enligt bilaga 12 till 2018 års dataskyddslag är *Information Commissioner* en "Corporation Sole", dvs. en separat juridisk person som består av en enda person, med stöd av den brittiska dataskyddsmyndigheten.
109. När det gäller informationskommissionärens oberoende, understryker EDPB att artikel 51 i den brittiska allmänna dataskyddsförordningen inte innehåller ett uttryckt klagande av att informationskommissionären är en oberoende offentlig myndighet så som det fastställs i artikel 51 i den allmänna dataskyddsförordningen gällande tillsynsmyndigheter. EDPB erkänner trots det att den brittiska allmänna dataskyddsförordningen i sin artikel 52 på ett liknande sätt speglar motsvarande regler gällande oberoende som de som fastställs i artikel 52.1–3 i den allmänna dataskyddsförordningen.
110. Vidare påpekar EDPB att artikel 52 i den brittiska allmänna dataskyddsförordningen inte innehåller skyldigheter motsvarande artikel 52.4–6 i den allmänna dataskyddsförordningen som uttryckligen säkerställer att respektive tillsynsmyndighet förfogar över de resurser som behövs för att myndigheten ska kunna utföra sina uppgifter och utöva sina befogenheter. EDPB erkänner emellertid att 2018 års dataskyddslag innehåller bestämmelser som syftar till att säkerställa lämplig finansiering av den brittiska dataskyddsmyndigheten<sup>70</sup>, samt den omständighet att den brittiska dataskyddsmyndigheten för närvarande är en av de största tillsynsmyndigheterna när man jämför med tillsynsmyndigheter inom EU/EES. Eftersom en kontinuerlig tilldelning av lämpliga resurser, särskilt när det gäller personal och budget<sup>71</sup>, är absolut nödvändigt för att säkerställa en väl fungerande tillsynsmyndighet som kan utföra alla uppgifter den tilldelats och eftersom det också nyligen har flaggats av Europaparlamentet som något av stor vikt<sup>72</sup>, bedömer EDPB det som avgörande att man riktar särskild uppmärksamhet på den framtida utvecklingen på det här området.
111. **EDPB uppmanar därför Europeiska kommissionen att observera alla utvecklingar gällande tilldelningen av resurser till den brittiska dataskyddsmyndigheten, som skulle kunna ha en skadlig effekt på ett riktigt utförande av den brittiska dataskyddsmyndighetens uppgifter.**

<sup>70</sup> Se avsnitt 137, 138, 182 och bilaga 12 punkt 9 i 2018 års dataskyddslag.

<sup>71</sup> Se WP254 rev.01, s. 7.

<sup>72</sup> Europaparlamentets resolution av den 25 mars 2021 om kommissionens utvärderingsrapport om genomförandet av den allmänna dataskyddsförordningen två år efter dess tillämpning, punkt 15, [https://www.europarl.europa.eu/doceo/document/B-9-2021-0211\\_SV.html](https://www.europarl.europa.eu/doceo/document/B-9-2021-0211_SV.html).

### 3.2.2. Befintligheten av ett dataskyddssystem som säkerställer en god nivå av efterlevnad

112. I utkastet till beslut görs en omfattande undersökning av de befogenheter som den brittiska dataskyddsmyndigheten förfogar över i enlighet med artikel 58 i den brittiska allmänna dataskyddsförordningen och 2018 års dataskyddslag för att säkerställa övervakning och efterlevnad av lagstiftningen. EDPB erkänner att artikel 58 i den brittiska allmänna dataskyddsförordningen nära speglar motsvarande regler gällande tillsynsmyndigheters befogenheter i artikel 58 i den allmänna dataskyddsförordningen. När det gäller befogenheten att påföra administrativa sanktionsavgifter beroende på omständigheterna i det enskilda fallet, innehåller artikel 83 i den brittiska allmänna dataskyddsförordningen liknande bestämmelser och högsta totalbelopp som de som fastställs i artikel 83 i den allmänna dataskyddsförordningen. Därmed anser EDPB att Förenade kungarikets rättsliga ram inom det här området för närvarande är i linje med de standarder som fastställs i relevant EU-lagstiftning. I det hänseendet lyfter EDPB emellertid fram att befintligheten av *effektiva* sanktioner spelar en viktig roll i säkerställandet av respekt för reglerna<sup>73</sup>.
113. **Mot bakgrund av ovanstående, uppmanar EDPB Europeiska kommissionen att övervaka effektiviteten hos sanktioner och relevanta åtgärder i Förenade kungarikets dataskyddsram.**

### 3.2.3. Systemet för skydd av personuppgifter måste ge stöd och hjälp till registrerade i deras utövande av sina rättigheter samt tillhandahålla lämpliga prövningsmekanismer

114. En effektiv tillsynsmekanism, som möjliggör oberoende utredning av klagomål så att man kan identifiera och bestraffa överträdelser av registrerades rättigheter i praktiken, samt en effektiv administrativ och rättslig prövning (som omfattar gottgörelse för skador som skett som ett resultat av olaglig behandling av registrerades personuppgifter) är viktiga inslag i bedömningen av huruvida ett dataskyddssystem tillhandahåller en adekvat skyddsnivå.
115. EDPB välkomnar att den brittiska dataskyddsmyndigheten tillhandahåller omfattande information och vägledning på sin webbplats, som syftar till att öka medvetenheten hos personuppgiftsansvariga och personuppgiftsbiträden om deras skyldigheter och förpliktelser samt till att stödja registrerade så att de är informerade om sina personuppgiftsrättigheter och kan göra sina rättigheter gällande i enlighet med den brittiska allmänna dataskyddsförordningen och 2018 års dataskyddslag.
116. **Trots det aktuella läget så uppmuntrar EDPB Europeiska kommissionen att kontinuerligt observera den nivå av stöd som den brittiska dataskyddsmyndigheten tillhandahåller specifikt till enskilda personer vars personuppgifter har överförts till Förenade kungariket inom ramen för Förenade kungarikets beslut om adekvat skyddsnivå, för att hjälpa dem att utöva sina rättigheter i enlighet med Förenade kungarikets dataskyddssystem.**

## 4. FÖRENADE KUNGARIKETS MYNDIGHETERS TILLGÅNG TILL OCH ANVÄNDNING AV PERSONUPPGIFTER SOM ÖVERFÖRTS FRÅN EU

### 4.1. Förenade kungarikets myndigheters tillgång till och användning av personuppgifter för brottsbekämpande ändamål

---

<sup>73</sup> Se WP254 rev.01, s. 7.

#### 4.1.1. Rättsliga grunder och tillämpliga begränsningar och skyddsåtgärder

117. När det gäller den bedömning som gjorts av Europeiska kommissionen och som dokumenteras i skäl 132 och framåt i utkastet till beslut **gällande tillgång för brottsbekämpande ändamål**, tillhandahåller Europeiska kommissionen nyanserad och detaljerad information och når generellt sett begripliga slutsatser. Därför avstår EDPB från att upprepa de flesta av faktiska fynden och bedömningarna i detta yttrande. Det finns emellertid vissa fall där beskrivningen av fakta eller förklaringen av slutsatserna inte är tillräckliga för att EDPB ska kunna tillägna sig dem.

##### 4.1.1.1 Användningen av samtycke

118. EDPB noterar att Europeiska kommissionen i skäl 184 i utkastet till beslut<sup>74</sup> hävdar att **användningen av samtycke** inte är relevant när det gäller adekvat skyddsnivå, eftersom det vid överföringen inte rör sig om uppgifter inhämtats direkt från den registrerade av en myndighet för brottsbekämpning i Förenade kungariket mot bakgrund av samtycke. Därmed bedöms inte användningen av samtycke som rättslig grund i polisarbete av Europeiska kommissionen.
119. I detta avseende erinrar EDPB om att artikel 45.2 a i den allmänna dataskyddsförordningen kräver en bedömning av många olika delar som inte är begränsade till överföringssituationen, inklusive *rättsstatsprincipen, respekten för de mänskliga rättigheterna och de grundläggande friheterna, relevant lagstiftning, både allmän och sektoriell, inbegripet allmän och sektoriell, inbegripet [...] straffrätt.*
120. EDPB noterar att, också på grundval av den information som Europeiska kommissionen tillhandahåller i skäl 38 i sitt utkast till genomförandebeslut enligt Europaparlamentets och rådets direktiv (EU) 2016/680 om adekvat skydd av personuppgifter i Förenade kungariket, att användningen av samtycke, som anges i Förenade kungarikets system inom ramen för brottsbekämpning alltid skulle innebära ett krav på rättslig grund att utgå från. Detta innebär att även om polisen har lagstadgade befogenheter att behandla uppgifterna under en utredning kan de under särskilda omständigheter (till exempel för att ta DNA-prov) anse det vara lämpligt att inhämta den registrerades samtycke.
121. **EDPB uppmanar Europeiska kommissionen att i beslutet om adekvat skyddsnivå införa sin analys av den möjliga användningen av samtycke i ett brottsbekämpningssammanhang, så som det beskrivs i utkastet till genomförandebeslut enligt Europaparlamentets och rådets direktiv (EU) 2016/680 direktiv om adekvat skydd av personuppgifter i Förenade kungariket.**

##### 4.1.1.2 Husrannsakan och utlämnandeorder

122. EDPB har inga synpunkter på polisens bevisupptagning genom husrannsakan och utlämnandeorder i allmänhet, men det står genom skäl 136 i beslutsutkastet klart att Europeiska kommissionen i sina överväganden om brottsbekämpande myndigheters åtkomst har inriktat sig på polisen. Andra brottsbekämpande myndigheters behandling av personuppgifter har granskats i mindre utsträckning.
123. Till exempel anges på sida 11 i Förenade kungarikets förklarande ram för diskussioner om adekvat skyddsnivå, avsnitt F: brottsbekämpning<sup>75</sup>, att **den nationella brottsmyndigheten** kan vara en

<sup>74</sup> Se sidan 37 i utkastet till beslut.

<sup>75</sup> Se Förenade kungarikets regerings förklarande ram för diskussioner om adekvat skyddsnivå, avsnitt F: brottsbekämpning, 13 mars 2020, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/872237/F\\_-\\_Law\\_Enforcement\\_.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf).

brottsbekämpande myndighet av särskilt intresse, som bland annat har en bredare funktion som omfattar kriminalunderrättelser. Den nationella brottsmyndighetens uppdrag inbegriper sammanställande av underrättelser från en mängd olika källor för att maximera analysen, bedömningen och de taktiska möjligheterna, inklusive från teknisk avlyssning av kommunikation, brottsbekämpande partner i Förenade kungariket och i andra länder samt säkerhets- och underrättelseorgan<sup>76</sup>. Den nationella brottsmyndigheten är också en viktig partner för internationella parter på brottsbekämpningsområdet och spelar en central roll vid utbytet av kriminella underrättelser<sup>77</sup>.

124. EDPB noterar dessutom det faktum att regeringens kommunikationshögkvarter (nedan kallat *Government Communications Headquarters – GCHQ*), vars verksamhet normalt omfattas av tillämpningsområdet för del 4 i 2018 års dataskyddslag, dvs. nationell säkerhet, även får aktiv roll i arbetet med att minska de effekter som den allvarliga och organiserade brottsligheten orsakar samhället och ekonomin i Förenade kungariket. GCHQ bedriver ett nära samarbete med inrikesministeriet, den nationella brottsmyndigheten, skatteverket samt andra regeringsorgan<sup>78</sup>. Dess verksamheter omfattar kampen mot sexuella övergrepp mot barn; bedrägerier; andra typer av ekonomisk brottslighet, inklusive penningtvätt; brottslig användning av teknik; it-brottslighet; organiserad brottslighet med koppling till immigration, inklusive människosmuggling; samt smuggling av narkotika, vapen och annan olaglig smuggling.
125. **EDPB uppmanar Europeiska kommissionen att komplettera sin analys med en analys av de organ som arbetar med brottsbekämpning och som tycks har gjort insamling och analys av uppgifter, inklusive personuppgifter, till ett fokusområde för sin dagliga verksamhet, särskilt den nationella brottsmyndigheten. Dessutom uppmanar EDPB kommissionen att titta närmare på organ som GCHQ, vars verksamhet både avser brottsbekämpning och nationell säkerhet, och på den rättsliga ram som är tillämplig på dessa i samband med behandlingen av personuppgifter.**

#### 4.1.1.3 Utredningsbefogenheter för brottsbekämpningsändamål

126. I kapitel 4 i referensramen för adekvat skyddsnivå inom ramen för den allmänna dataskyddsförordningen, "Grundläggande garantier i **tredjeländer för brottsbekämpande myndigheters** och nationella säkerhetsmyndigheters åtkomst för att begränsa ingreppen i de

---

<sup>76</sup> Se den nationella brottsmyndighetens webbplats, *Intelligence: enhancing the picture of serious organised crime affecting the UK*, <https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work/intelligence-enhancing-the-picture-of-serious-organised-crime-affecting-the-uk>.

<sup>77</sup> Samtidigt som inte alla underrättelser som behandlas av den nationella brottsmyndigheten utgörs av personuppgifter kan en betydande andel vara personliga uppgifter och de verksamheter som beskrivs här skiljer sig från vanligt polisarbete, vilket innebär att en bedömning av de brottsbekämpande myndigheternas tillgång till personuppgifter i Förenade kungariket skulle vara ofullständig utan en genomgripande bedömning av den nationella brottsmyndighetens verksamhet. Rimligtvis bör det säkerställas att dataskyddsprinciperna har samma betydelse för samtliga berörda brottsbekämpande myndigheter, vilket därmed lyfter fram särskilt uppgiftsinriktade myndigheter som den nationella brottsmyndigheten. I avsnittet "blicken mot framtiden" fortsätter förklaringen: *Vi letar hela tiden efter nya möjligheter att samla in, utveckla och förbättra de traditionella kapaciteterna för att kunna öka mängden tillgängliga underrättelser och kvaliteten på dessa, både i Förenade kungariket och utomlands. Som en del av detta utvecklar vi den nya nationella kapaciteten för datautnyttjande och använder de befogenheter som myndigheten tilldelats genom Crime and Courts Act för att koppla samman, ge åtkomst till och utnyttja data som innehåller av regeringen. [...] Allt detta kommer att öka vår förmåga och flexibilitet när det gäller att bemöta nya hot och arbeta proaktivt, för att samla in och analysera information och underrättelser om nya hot så att vi kan vidta åtgärder innan hoten blir verklighet.*

<sup>78</sup> Se GCHQ:s webbplats, *Mission, Serious and Organised Crime*, <https://www.gchq.gov.uk/section/mission/serious-crime>.

grundläggande rättigheterna” påminner EDPB om att *i detta sammanhang konstaterade också domstolen att det tidigare Safe Harbor-beslutet ”inte [innehåller] något konstaterande beträffande förekomsten i Förenta staterna av regler som antagits av staten och som syftar till att begränsa eventuella ingrepp i de grundläggande rättigheterna för personer vilkas personuppgifter överförs från unionen till Förenta staterna, **ingrepp som statliga organ kan vara tillåtna att göra när de görs i ett legitimt syfte, såsom nationell säkerhet***<sup>79</sup>. I denna referensram uppger EDPB att de **fyra europeiska nödvändiga garantierna**<sup>80</sup> **måste respekteras innan åtkomst till uppgifter kan beviljas, oavsett om ändamålet avser nationell säkerhet eller brottsbekämpning, av alla tredjeländer för att skyddsnivån ska anses adekvat, i synnerhet måste nödvändigheten och proportionaliteten med avseende på de eftersträfvade legitima syftena styrkas.**

127. I detta avsnitt av beslutsutkastet konstaterar Europeiska kommissionen (i skäl 139) att *eftersom de utredningsbefogenheter som anges i IPA 2016 är desamma som de som nationella säkerhetsmyndigheter har tillgång till beskrivs de villkor, begränsningar och skyddsåtgärder som gäller för sådana befogenheter i detalj i avsnittet om Förenade kungarikets offentliga myndigheters åtkomst till och användning av personuppgifter för ändamål som rör den nationella säkerheten*. Det följer dock av EU-domstolens rättspraxis att när man tillämpar nödvändighets- och proportionalitetstestet på medlemsstatslagstiftning som tillåter att offentliga myndigheter lagrar och ges åtkomst till personuppgifter, att de legitima målen, såsom nationell säkerhet eller kampen mot allvarlig brottslighet, skiljer sig åt, och att vissa medlemsstater därför kanske kan rättfärdiga en viss typ av ingrepp trots att andra inte kan det<sup>81</sup>.
128. EDPB skulle därför välkomna en specifik bedömning i beslutet av nödvändigheten och proportionaliteten hos de villkor, begränsningar och skyddsåtgärder som beskrivs i skäl 174 och följande – ett avsnitt om åtgärder som vidtas för att uppnå nationella säkerhetsmål – när det gäller tillämpningen av dessa villkor, begränsningar och skyddsåtgärder i samband med en åtgärd som har som mål att bekämpa brott. EDPB uppmanar därmed kommissionen att ytterligare förklara huruvida den beskrivna lagringen av personuppgifter och åtkomsten till dessa för brottsbekämpningsändamål är tillräckligt begränsad för att säkerställa en skyddsnivå som i huvudsak är likvärdig med den som garanteras inom EU.

#### 4.1.2. Vidare användning av information som samlas in för brottsbekämpningsändamål (skäl 140–154)

129. EDPB noterar att Förenade kungarikets dataskyddsram innehåller skyddsåtgärder och begränsningar som liknar de i unionsrätten när det gäller vidare användning av information som samlas in för brottsbekämpningsändamål.

##### 4.1.2.1 Vidare användning för andra brottsbekämpningsändamål

130. I 2018 års dataskyddslag föreskrivs att personuppgifter som samlats in av en behörig myndighet för brottsbekämpningsändamål får behandlas ytterligare (antingen av den ursprungliga personuppgiftsansvarige eller av en annan personuppgiftsansvarig) för andra brottsbekämpningsändamål, förutsatt att den personuppgiftsansvarige har rätt att enligt lag behandla uppgifter för det andra ändamålet och att behandlingen är nödvändig och proportionell med avseende på det ändamålet. Kommissionen noterar att alla skyddsåtgärder som föreskrivs i del

<sup>79</sup> Se WP254 rev. 01, s. 9.

<sup>80</sup> Se EDPB:s rekommendationer 02/2020 om europeiska nödvändiga garantier för övervakningsåtgärder.

<sup>81</sup> Se EU-domstolens dom i de förenade målen C-511/18, C-512/18 och C-520/18, La Quadrature du Net m. fl., 6 oktober 2020, ECLI:EU:C:2020:791.

3 i 2018 års dataskyddslag är tillämpliga på den behandling som utförs av den mottagande myndigheten. EDPB belyser dock att i del 3 i 2018 års dataskyddslag fastställs i avsnitt 44.4, 45.4, 48.3 och 68.7 möjligheten att begränsa registrerades rättigheter, och i avsnitt 79 föreskrivs möjligheten att utfärda certifikat som styrker att en begränsning är en nödvändig och proportionerlig åtgärd för att skydda den nationella säkerheten. **EDPB rekommenderar därför att Europeiska kommissionen fortsätter att bedöma den möjliga inverkan av sådana begränsningar på skyddsnivån för personuppgifter med avseende på vidare användning av den information som samlas in. På samma sätt bör ytterligare förklaringar också lämnas med avseende på Förenade kungarikets rättsliga ram som tillåter sådant vidare utbyte, i synnerhet 2017 års lag om den digitala ekonomin (*Digital Economy Act 2017*) och 2013 års lag om brottslighet och domstolsväsendet (*Crime and Courts Act 2013*), som tillåter att information utbyts med den nationella brottsmyndigheten.**

#### 4.1.2.2 Vidare användning för andra ändamål än brottsbekämpning inom Förenade kungariket

131. I 2018 års dataskyddslag föreskrivs också att personuppgifter som samlas in för brottsbekämpningsändamål får behandlas för ett ändamål som inte rör brottsbekämpning när behandlingen tillåts enligt lag. I detta fall utgör avsnitt 19 i 2008 års lag om terrorismbekämpning (*Counter-Terrorism Act 2008*) den rättsliga grunden för ett sådant utbyte. I detta avseende noterar EDPB att tillämpningsområdet för och bestämmelserna i avsnitt 19 i 2008 års lag om terrorismbekämpning inte utvärderas fullt ut i Europeiska kommissionens bedömning, och kan innebära en mer omfattande vidare användning, särskilt när det gäller avsnitt 19.2, där det anges att *information som någon av underrättelsetjänsterna har inhämtat i anslutning till utövandet av någon av dess funktioner kan användas av den tjänsten för att utöva tjänstens andra funktioner*.
132. EDPB noterar också att kommissionens hänvisning till det faktum att behöriga myndigheter är offentliga myndigheter som måste agera i enlighet med Europakonventionen, inklusive artikel 8 i denna, vilket därmed säkerställer att allt datautbyte mellan brottsbekämpande myndigheter och underrättelsetjänsterna följer dataskyddslagstiftningen, liksom Europakonventionen, skulle kunna styrkas ytterligare genom identifiering av de relevanta lagar och förordningar i Förenade kungarikets rättsordning som fastställer dessa begränsningar på ett klart och tydligt sätt.

#### 4.1.2.3 Vidare användning i samband med vidare överföring utanför Förenade kungariket

133. Medan Europeiska kommissionen har hänvisat till det faktum att CLOUD-avtalet mellan Förenade kungariket och Förenta staterna kan påverka vidare överföringar till Förenta staterna från tjänsteleverantörer i Förenade kungariket betonar EDPB även att detta avtals ikraftträdande även kan påverka vidare användning av den information som samlas in genom vidare överföring från brottsbekämpande myndigheter i Förenade kungariket, särskilt när det gäller utfärdandet och överföringen av beslut enligt artikel 5 i nämnda avtal.
134. I ett bredare perspektiv anser EDPB också att ingåendet av framtida bilaterala avtal med tredjeländer för ändamål som rör samarbete inom brottsbekämpning, som ger en rättslig grund för överföringen av personuppgifter till dessa länder, också väsentligen kan komma att påverka villkoren för vidare användning av den inhämtade informationen, eftersom sådana avtal kan påverka Förenade kungarikets bedömda dataskyddsram. EDPB rekommenderar därför att kommissionen bedömer denna fråga närmare, fastställer om internationella avtal existerar och klargör huruvida bestämmelserna i dessa avtal kan påverka tillämpningen av Förenade kungarikets dataskyddslag, och föreskriver ytterligare begränsningar eller undantag när det gäller vidare användning och utlämnande av information som samlats in för brottsbekämpningsändamål i andra länder. EDPB anser att denna information och bedömning är avgörande för att möjliggöra en genomgripande

bedömning av den skyddsnivå som säkerställs genom Förenade kungarikets rättsliga ram och praxis för utlämnande och vidare användning i andra länder.

#### 4.1.3. Tillsyn

135. EDPB noterar att tillsynen av brottsbekämpande myndigheter säkerställs genom en kombination av olika ombudsmän, utöver den brittiska dataskyddsmyndigheten. I bedömningarna av utkastet till adekvat skyddsnivå nämns ombudsmannen för utredningsbefogenheter, ombudsmannen med ansvar för lagring och användning av biometriska uppgifter och ombudsmannen med ansvar för övervakningskameror. I detta avseende ska det noteras att EU-domstolen upprepade gånger har betonat behovet av oberoende tillsyn. Ombudsmannen för utredningsbefogenheter har en särskild betydelse i frågor som rör åtkomsten till personuppgifter som överförs till Förenade kungariket. EDPB tolkar det som att ombudsmannen för utredningsbefogenheter är en så kallad justitieombudsman, i likhet med andra justitieombudsmän, som ska betraktas mot bakgrund av kapitlet om nationell säkerhet, och att dessa justitieombudsmän är oberoende på samma sätt som domare, även när de agerar i egenskap av ombudsmän. När det gäller ombudsmannen för utredningsbefogenheter förklarar Europeiska kommissionen i skäl 245 i beslutsutkastet att denne agerar oberoende enligt "principen om armlängds avstånd" samtidigt som denne finansieras av inrikesministeriet.
136. EDPB har i beslutsutkastet inte hittat några uppgifter som antyder att oberoendet hos ombudsmannen med ansvar för lagring och användning av biometriska uppgifter eller ombudsmannen med ansvar för övervakningskameror borde bedömas.
137. **Europeiska kommissionen uppmanas att bedöma justitieombudsmännens oberoende närmare, även i fall där ombudsmannen inte (längre) arbetar som domare, samt att bedöma oberoendet hos ombudsmannen med ansvar för lagring och användning av biometriskt material och ombudsmannen med ansvar för övervakningskameror.**

## 4.2. Allmän rättslig ram för dataskydd på området nationell säkerhet

### 4.2.1. Nationella säkerhetscertifikat

138. Enligt avsnitt 111 i 2018 års dataskyddslag kan personuppgiftsansvariga ansöka om nationella säkerhetscertifikat som utfärdas av en minister, kabinettmedlem, statsåklagaren eller generaladvokaten för Skottland som intygar att undantagen från kraven och skyldigheterna i del 4–6 i 2018 års dataskyddslag är åtgärder som är nödvändiga och proportionella för att skydda den nationella säkerheten. Dessa certifikat har för avsikt att ge personuppgiftsansvariga större rättssäkerhet och kommer att vara avgörande bevis för att den nationella säkerheten är tillämplig när personuppgifter behandlas. Det bör emellertid nämnas att dessa certifikat inte krävs för att förlita sig på undantag som rör den nationella säkerheten, utan att de istället motsvarar en insynsåtgärd<sup>82</sup>.
139. Av avsnitt 17 och 18 i bilaga 20 till 2018 års dataskyddslag drar EDPB slutsatsen att ett nationellt säkerhetscertifikat som utfärdats enligt 1998 års dataskyddslag (nedan kallat *äldre certifikat*) hade en utökad verkan när det gäller behandlingen av personuppgifter enligt 2018 års dataskyddslag fram

---

<sup>82</sup> Se 2018 års dataskyddslag från inrikesministeriet, *National Security Certificates Guidance*, augusti 2020, punkt 4, s. 3, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/910279/Data\\_Protection\\_Act\\_2018\\_-\\_National\\_Security\\_Certificates\\_Guidance.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf).

till den 25 maj 2019. Fram till detta datum behandlades äldre certifikat, såvida de inte ersattes eller återkallades, som om de hade utfärdats enligt 2018 års dataskyddslag.

140. När ett nationellt säkerhetscertifikat enligt 1998 års dataskyddslag inte uttryckligen har någon sista giltighetsdag tolkar EDPB det som att ett sådant certifikat kommer att fortsätta att vara giltigt för behandling enligt 1998 års dataskyddslag, såvida inte certifikatet återkallas eller upphävs<sup>83</sup>. Även om det skydd som ges genom de äldre certifikaten är begränsat till behandlingen av personuppgifter enligt 1998 års dataskyddslag noterar EDPB att nya nationella säkerhetscertifikat kan utfärdas enligt 1998 års dataskyddslag för personuppgifter som behandlades enligt den dataskyddslagen<sup>84</sup>.
141. **För tydlighetens skull uppmanar EDPB Europeiska kommissionen att i sitt beslutsutkast förtydliga att nationella säkerhetscertifikat fortfarande kan utfärdas enligt 1998 års dataskyddslag. EDPB uppmanar dessutom kommissionen att i sitt beslutsutkast beskriva tillsynsmekanismerna och möjligheterna till prövning när det gäller certifikat som utfärdats enligt 1998 års dataskyddslag. EDPB uppmanar slutligen kommissionen att i sitt beslutsutkast inkludera antalet befintliga certifikat som har utfärdats enligt 1998 års dataskyddslag och att övervaka denna fråga noggrant.**

#### 4.2.2. Rätten till rättelse och radering

142. När det gäller rätten till rättelsen och radering noterar EDPB att i enlighet med avsnitt 100 och 149 i 2018 års dataskyddslag har registrerade möjlighet att vända sig till High Court (Court of Session i Skottland) för att uppmana en personuppgiftsansvarig att rätta eller radera deras uppgifter utan otillbörligt dröjsmål.
143. **EDPB betonar att utövandet av registrerades rättigheter måste säkerställas på ett effektivt sätt. EDPB uppmanar därför Europeiska kommissionen att i sitt beslutsutkast att beskriva hur avsnitt 100 i 2018 års dataskyddslag fungerar i praktiken, och att övervaka tillämpningen av detta avsnitt noggrant.**

#### 4.2.3. Undantag som rör den nationella säkerheten

144. EDPB önskar uppmärksamma avsnitt 110 i 2018 års dataskyddslag, och i synnerhet bilaga 11, som anger i vilka specifika situationer underrättelsetjänsterna får avvika från vissa dataskyddsprinciper, inklusive med anknytning till registrerades rättigheter, och inte skyldiga att meddela personuppgiftsintrång till den brittiska dataskyddsmyndigheten<sup>85</sup>.
145. **EDPB uppmanar Europeiska kommissionen att ytterligare förklara undantagens omfattning eftersom EDPB undrar om alla undantag som tas upp i bilaga 11 till 2018 års dataskyddslag är relevanta för underrättelsetjänsternas arbete, och huruvida de säkerställer likvärdighet med nödvändighets- och proportionalitetsprincipen. EDPB uppmanar i synnerhet kommissionen att lämna ytterligare förtydliganden om under vilka omständigheter en underrättelsetjänst kan förlita sig på avsnitt 10 i bilaga 11 till 2018 års dataskyddslag, där det anges att *de angivna***

---

<sup>83</sup> Se 2018 års dataskyddslag från inrikesministeriet, *National Security Certificates Guidance*, augusti 2020, s. 5.

<sup>84</sup> Se 2018 års dataskyddslag från inrikesministeriet, *National Security Certificates Guidance*, augusti 2020, punkt 8, s. 5.

<sup>85</sup> Dessa ändamål rör förebyggande och upptäckt av "brott", "information som måste lämnas ut enligt lag etc. eller i samband med rättsliga förfaranden", "parlamentariskt privilegium", "rättsliga förfaranden", "hedersbetyg och titlar", "försvarsmakten", "ekonomiskt välmående", "juristprivilegium", "förhandlingar", "konfidentiella hänvisningar som lämnas av personuppgiftsansvariga", "prov och betyg", "forskning och statistik" och "arkivering i allmänhetens intresse".

***bestämmelserna inte är tillämpliga på personuppgifter som består av register över den personuppgiftsansvariges avsikter med avseende några förhandlingar med den registrerade i den utsträckningen att tillämpningen av de angivna bestämmelserna sannolikt skulle skada förhandlingarna.***

#### 4.3. Förenade kungarikets offentliga myndigheters åtkomst och användning för ändamål som rör den nationella säkerheten

146. Rent allmänt är EDPB medveten om att staterna har ett stort utrymme för skönsmässig bedömning i frågor som rör den nationella säkerheten, vilket också erkänns av Europeiska domstolen för de mänskliga rättigheterna. EDPB påminner också om att, vilket understryks i dess uppdaterade rekommendationer om europeiska nödvändiga garantier för övervakningsåtgärder<sup>86</sup>, det i artikel 6.3 i fördraget om Europeiska unionen fastställs att de grundläggande rättigheter som nämns i Europakonventionen ska ingå i EU-rätten som allmänna principer. Såsom EU-domstolen dock påminner om i sin rättspraxis utgör den sistnämnda, så länge EU inte har anslutit sig till det, ett rättsligt instrument som har införlivats formellt i EU-rätten<sup>87</sup>. Därmed måste skyddsnivån för de grundläggande rättigheter som krävs i artikel 45 i den allmänna dataskyddsförordningen fastställas på grundval av bestämmelserna i den förordningen, jämförda med de grundläggande rättigheter som tas upp i EU-stadgan. Enligt artikel 52.3 i EU-stadgan ska dock de rättigheter som ingår i denna och som motsvarar de rättigheter som garanteras genom Europakonventionen ha samma innebörd och räckvidd som i Europakonventionen. Därmed, vilket EU-domstolen påminner om, måste rättspraxis från Europeiska domstolen för de mänskliga rättigheterna betraktas som lägsta tillåtna skyddsnivå vid tolkningen av motsvarande rättigheter i EU-stadgan<sup>88</sup>. Enligt den sista meningen i artikel 52.3 i EU-stadgan hindrar dock "[d]enna bestämmelse [...] inte unionsrätten från att tillförsäkra ett mer långtgående skydd".
147. I bedömningen nedan har EDPB därför tagit hänsyn till rättspraxis från Europeiska domstolen för de mänskliga rättigheterna, i den mån som EU-stadgan, enligt EU-domstolens tolkning, inte föreskriver en högre skyddsnivå med andra krav än rättspraxis från Europeiska domstolen för de mänskliga rättigheterna.

##### 4.3.1. Rättsliga grunder, begränsningar och skyddsåtgärder – Utredningsbefogenheter som utövas inom ramen för nationell säkerhet

###### 4.3.1.1 Allmänna anmärkningar

148. EDPB erinrar om att IPA 2016 är en ny lag som rör ändringar av flera bestämmelser i *Intelligence Services Act* från 1994. I lagen anges i vilken utsträckning vissa utredningsbefogenheter får användas för att göra ingrepp i privatlivet<sup>89</sup>. Trots två rapporter från ombudsmannen för utredningsbefogenheter, vilka innehåller användbar information om tillämpningen av denna nya rättsliga ram, finns det fortfarande ingen översyn av vissa aspekter, särskilt när det gäller de urvals- och sökkriterier som används.

<sup>86</sup> Se EDPB:s rekommendationer 02/2020 om europeiska nödvändiga garantier för övervakningsåtgärder.

<sup>87</sup> Se Schrems II, punkt 98.

<sup>88</sup> Se EU-domstolens dom i de förenade målen C-511/18, C-512/18 och C-520/18, *La Quadrature du Net* m.fl., 6 oktober 2020, ECLI:EU:C:2020:791, punkt 124.

<sup>89</sup> Se avsnitt 1 i IPA 2016.

149. Som en allmän anmärkning om IPA 2016 och dess tillämpningsområde framhåller Europeiska dataskyddsstyrelsen dessutom följande fyra punkter:
150. När det gäller den **första punkten** vill Europeiska dataskyddsstyrelsen, med hänsyn till lagens särdrag, understryka två aspekter.
151. Europeiska dataskyddsstyrelsen noterar för det första att lagstiftningen hänvisar till breda ändamål för att använda de förfaranden som föreskrivs i IPA 2016 och inte till de kategorier av enskilda personer som kan beröras av insamlingen av uppgifter på grundval av delarna 2–7 i IPA 2016. I detta avseende påminner Europeiska dataskyddsstyrelsen om att det bör finnas en koppling mellan de personkategorier som kan bli föremål för övervakningsåtgärder och de ändamål som eftersträvas med lagstiftningen för att fastställa lagens personkrets.
152. Vidare betonar Europeiska dataskyddsstyrelsen även att definitionerna av "teleoperatörer", "teletjänster" och "telekommunikationssystem", i vilka lagens tillämpningsområde fastställs, också är mycket breda och i viss mån otydliga. Europeiska dataskyddsstyrelsen framhåller att dessa begrepp, inom ramen för IPA 2016, måste tolkas på ett mycket bredare sätt än enligt lagstiftningen om telekommunikationer, såsom de definieras i exempelvis den europeiska kodexen för elektronisk kommunikation<sup>90</sup>. Europeiska dataskyddsstyrelsen noterar att definitionerna av "teletjänster" och "telekommunikationssystem" i lagen anses vara avsiktligt breda, så att de förblir relevanta för ny teknik. Definitionen av en teleoperatör är också mycket bred och skulle exempelvis kunna omfatta onlinebaserade videospel med chattfunktion eller andra webbplatser som endast innehåller sådana chattfönster<sup>91</sup>.
153. Dessutom, även om förfaranden och tillsyn när det gäller bedömningen av nödvändigheten och proportionaliteten av insamling och tillgång till uppgifter i allmänhet tillhandahålls, är kriterierna för att genomföra en sådan bedömning inte fastställda i själva lagen. Ytterligare uppgifter finns i andra dokument, t.ex. uppförandekoder.
154. Såsom det framgår av Europeiska dataskyddsstyrelsens rekommendationer 02/2020 om europeiska nödvändiga garantier för övervakningsåtgärder har EU-domstolen angett att "kravet på att samtliga begränsningar i utövandet av grundläggande rättigheter ska vara föreskrivna i lag, innebär att den rättsliga grund som gör ingreppet i rättigheterna möjligt i sig ska definiera räckvidden av begränsningen i utövandet av den aktuella rättigheten<sup>92</sup>". Närmare bestämt klargjorde Europeiska unionens domstol att *[f]ör att kravet på proportionalitet ska vara uppfyllt måste det i lagstiftning föreskrivas klara och precisa bestämmelser som reglerar räckvidden och tillämpningen av den aktuella åtgärden samt anges minimikrav, så att de personer vars personuppgifter berörs har*

---

<sup>90</sup> Se artikel 2.5 i den europeiska kodexen för elektronisk kommunikation, i vilken exempelvis "interpersonell kommunikationstjänst" definieras som "en tjänst som vanligen tillhandahålls mot ersättning och som möjliggör direkt interpersonellt och interaktivt informationsutbyte via elektroniska kommunikationsnät mellan ett begränsat antal personer, varigenom de personer som inleder eller deltar i kommunikationen bestämmer vem eller vilka som ska vara mottagare av denna; den inbegriper inte tjänster som möjliggör interpersonell och interaktiv kommunikation enbart som en extrafunktion av mindre betydelse som är direkt kopplad till en annan tjänst".

<sup>91</sup> Se inrikesministeriets *Code of practice on the interception of communications*, mars 2018, punkt 2.5 och följande, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/715480/Interception\\_of\\_Communications\\_Code\\_of\\_Practice.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf).

<sup>92</sup> Se Schrems II, punkt 175, och nämnda mål, samt domstolens dom av den 6 oktober 2020 i mål C-623/17, Privacy International/Secretary of State for Foreign and Commonwealth Affairs m.fl., ECLI:EU:C:2020:790 (nedan kallad *Privacy International*), punkt 65.

*tillräckliga garantier för att uppgifterna på ett effektivt sätt är skyddade mot riskerna för missbruk. Denna lagstiftning ska vara rättsligt bindande enligt nationell rätt och i synnerhet ange under vilka omständigheter och på vilka villkor en åtgärd avseende behandling av sådana uppgifter får vidtas, vilket säkerställer att ingreppet begränsas till vad som är strängt nödvändigt.*<sup>93</sup>

155. Europeiska domstolen för de mänskliga rättigheterna betonade också att lagen måste vara tillräckligt tydlig ”så att medborgarna får en tillfredsställande indikation på de omständigheter enligt vilka och villkoren för när offentliga myndigheter har rätt att tillgripa sådana åtgärder”<sup>94</sup>.
156. **Europeiska dataskyddsstyrelsen uppmanar därför Europeiska kommissionen att ytterligare bedöma dessa aspekter när det gäller den relevanta lagstiftningens precision, tydlighet och fullständighet samt att tillhandahålla ytterligare uppgifter för att visa att den ger en skyddsnivå som i allt väsentligt motsvarar den som säkerställs inom EU med avseende på de rättsliga förhållandena. Europeiska dataskyddsstyrelsen betonar även att breda definitioner också bör bedömas i förhållande till avlyssningsåtgärdernas proportionalitet.**
157. Dessutom, även om flera av de behöriga underrättelsetjänstmyndigheternas interna koder delvis utvecklar några av dessa aspekter, till exempel när det gäller att bedöma huruvida insamlingen av uppgifter är nödvändig och proportionerlig, betonar Europeiska dataskyddsstyrelsen att EU-domstolens krav när det gäller lagstiftningens karaktär innebär att de centrala delarna, bland annat att enskilda personer ska kunna göra dem gällande i samband med domstolsprövning, måste anges i den lagstiftning där bindande rättigheter föreskrivs<sup>95</sup>. I punkt 6 i bilaga 7 till IPA 2016 anges att domstolar (och tillsynsmyndigheter) *får beakta en persons underlåtenhet att ta hänsyn till en kod vid fastställandet av en fråga i ett sådant förfarande* utan att klargöra huruvida enskilda personer kan åberopa en överträdelse av koderna inför domstol (eller tillsynsmyndigheter). Dessutom hänvisar de uppgifter som hittills lämnats i utkastet till beslut antingen till att Europeiska domstolen för de mänskliga rättigheterna erkänner att reglerna i dessa koder är förutsebara<sup>96</sup>, snarare än ”bindande” i domstol, vilket krävs av EU-domstolen, eller till det faktum att brittiska domstolar i vissa mål har hänvisat till koder, medan möjligheten för enskilda personer att åberopa de rättigheter som härrör från koderna inte anges i något av de nämnda målen. **Om man drar slutsatsen att det i Förenade kungarikets lagstiftning inte i tillräcklig utsträckning anges under vilka omständigheter och på vilka villkor en åtgärd får vidtas samt att dessa element faktiskt tillhandahålls genom underrättelsetjänstmyndigheternas interna koder, uppmanar Europeiska dataskyddsstyrelsen följaktligen Europeiska kommissionen att ytterligare bedöma huruvida de begränsningar och skyddsåtgärder som föreskrivs i underrättelsetjänstmyndigheternas olika interna koder kan åberopas av enskilda personer inför domstol och verkställas.**
158. **Den andra punkten** gäller det faktum att bestämmelserna om riktad insamling och lagring av kommunikationsuppgifter å ena sidan och bulkinsamling å andra sidan, antingen i IPA 2016 eller i

---

<sup>93</sup> Se *Privacy International*, punkt 68.

<sup>94</sup> Se Europeiska domstolen för de mänskliga rättigheterna, *Zakharov/Ryssland*, 4 december 2015, CE:ECHR:2015:1204JUD004714306, punkt 229.

<sup>95</sup> I detta avseende ansåg EU-domstolen till exempel att PPD-28 i Förenta staterna inte uppfyllde kraven, även om det också innehöll vissa begränsningar när det gäller bulkinsamling, se *Schrems II*, punkt 181.

<sup>96</sup> Se Europeiska domstolen för de mänskliga rättigheterna, *Big Brother Watch m.fl./Förenade kungariket*, 13 september 2018, ECLI:CE:ECHR:2018:0913JUD005817013 (nedan kallad *Big Brother Watch*), punkt 325: *Eftersom IC-koden är en offentlig handling, med förbehåll för godkännande från båda kamrarna i parlamentet, och måste beaktas både av dem som utövar avlyssningsuppdrag och av domstolar, har domstolen uttryckligen godtagit att dess bestämmelser skulle kunna beaktas vid bedömningen av huruvida Ripa-ordningen är förutsebar.*

annan lagstiftning som exempelvis i *Intelligence Services Act* från 1994 eller *Regulation of Investigatory Powers Act* från 2000, även kommer att tillämpas när det gäller uppgifter som överförs från EU till Förenade kungariket. När det gäller bulkinsamling understryker EDPB att enligt de relevanta bestämmelserna i Förenade kungarikets lagstiftning tillåts insamling av uppgifter utanför Förenade kungariket. På så sätt skulle uppgifter som befinner sig i transit kunna överföras från EES till Förenade kungariket på grundval av beslutet om adekvat skyddsnivå<sup>97</sup>. Dessutom konstaterar Europeiska dataskyddsstyrelsen att Europeiska kommissionen anger att *[d]et bör noteras att lagring och insamling av kommunikationsuppgifter normalt inte avser personuppgifter om registrerade i EU, vilka överförs enligt detta beslut till Förenade kungariket. Skyldigheten att lagra eller lämna ut kommunikationsuppgifter enligt delarna 3 och 4 i IPA 2016 omfattar uppgifter som samlas in av teleoperatörer i Förenade kungariket direkt från användarna av en telekommunikationstjänst*.<sup>98</sup> Europeiska dataskyddsstyrelsen betonar likväl att det saknas tydlighet när det gäller det faktum att endast dessa operatörers verksamhetsställen i Förenade kungariket kan ta emot sådana förfrågningar från behöriga brittiska myndigheter eftersom det enligt den definition av teleoperatörer som anges i avsnitt 261.10 i IPA 2016 krävs 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) styrs från Förenade kungariket". Följaktligen skulle personuppgifter om registrerade i EES faktiskt kunna beröras, till exempel när det gäller uppgifter som samlats in eller genererats av en brittisk teleoperatörs verksamhetsställe inom EES och som överförs till samma operatörs verksamhetsställe i Förenade kungariket på grundval av beslutet om adekvat skyddsnivå (för kommersiella ändamål), och sedan samlas in inom Förenade kungariket av de behöriga offentliga myndigheterna.

159. **Europeiska dataskyddsstyrelsen anser därför att bedömningen av dessa bestämmelser också är relevant för att bedöma den brittiska rättsliga ramens adekvata skyddsnivå och uppmanar Europeiska kommissionen att klargöra denna aspekt och ytterligare bedöma i vilken utsträckning detta är fallet. Europeiska dataskyddsstyrelsen uppmanar i synnerhet Europeiska kommissionen att klargöra att den förstår räckvidden av denna lagstiftning, inbegripet vad begreppet "användare av telekommunikationstjänster" omfattar, samt huruvida uppgifter från teleföretags verksamhetsställen utanför Förenade kungariket skulle kunna begäras, i den mån uppgifter om registrerade i EES berörs, med tanke på den mycket breda definitionen av teleoperatörer.**
160. **Den tredje punkten** avser förfarandet med "dubbla lås". Europeiska dataskyddsstyrelsen noterar att ett nytt förfarande med "dubbla lås" infördes i IPA 2016. Trots detta förstår Europeiska dataskyddsstyrelsen också att även om insamling av eller åtkomst till uppgifter för ändamål som avser nationell säkerhet eller underrättelse i princip endast kan ske med ett tillstånd som beviljats av en justitieombudsman, föreskrivs i IPA 2016 att *i särskilda begränsade fall är laglig avlyssning utan tillstånd möjlig och det krävs endast förhandsgodkännande från de behöriga IC-myndigheterna själva [se nedan avsnittet om tillsyn], bland annat för avlyssning i enlighet med utländska förfrågningar (avsnitt 52 i IPA 2016)*. Såsom understryks nedan sammanfaller detta också med Europeiska dataskyddsstyrelsen oro, särskilt när det gäller utlämnande av uppgifter utanför EU. Dessutom noterar Europeiska dataskyddsstyrelsen också att ett undantag från förfarandet med dubbla lås även är möjligt när det gäller utrustningsstörning, antingen riktad eller i bulk, och att justitieombudsmannen endast har rätt att godkänna att bulkstillstånd förnyas efter en inledande

---

<sup>97</sup> Se punkt 183 och följande i Schrems II om bedömningen av en lagstiftning som gör det möjligt att få åtkomst till uppgifter som befinner sig i transit mellan EU och ett tredjeland inom ramen för ett beslut om adekvat skyddsnivå.

<sup>98</sup> Se skäl 196 i utkastet till beslut.

period på högst sex månader. **Europeiska dataskyddsstyrelsen uppmanar Europeiska kommissionen att ytterligare bedöma och visa att Förenade kungarikets rättsliga ram, även i fall där förfarandet med dubbla lås inte är tillämpligt, tillhandahåller lämpliga skyddsåtgärder, bland annat genom effektiv efterhandstillsyn och prövningsmöjligheter som erbjuds enskilda personer, för att säkerställa att skyddsnivån i allt väsentligt är likvärdig med den som tillhandahålls inom EU (se även avsnitt 4.3.3 om tillsyn).**

161. Även om förfarandet med "dubbla lås" faktiskt har införts genom IPA 2016 oroas Europeiska dataskyddsstyrelsen fortfarande över vissa inslag i den nya lagstiftningen. Efter presentationen av motsvarande avsnitt i utkastet till beslut har Europeiska dataskyddsstyrelsen analyserat följande typer av insamling och tillgång till uppgifter i samma ordning som kommissionen presenterat. Ordningsföljden för de faktorer som bedöms nedan återspeglar därför inte en hierarki när det gäller graden av oro hos Europeiska dataskyddsstyrelsen.

#### 4.3.1.2 Riktat inhämtande och lagring av kommunikationsuppgifter

162. Europeiska dataskyddsstyrelsen noterar att det finns två tjänstemän som kan bevilja riktade tillstånd för inhämtande av kommunikationsuppgifter: utanordnaren vid *Office for Communications Data Authorisations* (nedan kallad *ombudsmannen för utredningsbefogenheter*), en utsedd högre tjänsteman (en person som innehar ett föreskrivet ämbete eller rang vid en relevant offentlig myndighet), därjämte en justitieombudsmans godkännande i vissa fall. Det är dock fortfarande oklart för EDPB, enligt lagen och den relevanta koden, exakt vilken tjänsteman som beviljar vilken typ av riktat inhämtande av kommunikationsuppgifter och i vilken utsträckning en utsedd tjänsteman skulle vara tillräckligt oberoende<sup>99</sup>.
163. **Europeiska dataskyddsstyrelsen uppmanar därför Europeiska kommissionen att ytterligare bedöma denna aspekt och lämna tydligare förklaringar om dessa frågor.**
164. När det gäller meddelandet om krav på lagring av kommunikationsuppgifter noterar Europeiska dataskyddsstyrelsen också att sådana meddelanden kan riktas till en "beskrivning av aktörer". Detta begrepp förefaller innebära att flera aktörer samtidigt kan uppmanas att lagra uppgifter. Syftet med inhämtandet avser nämligen inte antalet aktörer, utan namnet på eller beskrivningen av de personer, organisationer, platser eller grupper av personer som utgör "målet", en beskrivning av utredningens art och en beskrivning av den verksamhet för vilken utrustningen används. EDPB betonar därför att meddelandet, beroende på hur många operatörer som berörs av en sådan "beskrivning av operatörer", kan vara bredare än vad förfarandet för riktad lagring kan tyckas innebära. **EDPB uppmanar Europeiska kommissionen att ytterligare bedöma denna aspekt samt att lämna ytterligare försäkringar om att även när meddelanden riktar sig till flera operatörer är de begränsade till vad som är strängt nödvändigt och proportionerligt.**

#### 4.3.1.3 Utrustningsinterferens

165. EDPB noterar att i brådskande fall kan "utrustningsstörning" utgöra undantag från förfarandet med dubbla lås<sup>100</sup>. Europeiska dataskyddsstyrelsen är därför oroad över att de ändamål för vilka sådan utrustningsstörning kan krävas är breda och att kriterierna för skyndsamhet (i vilket fall justitieombudsmannen inte är skyldig att tillhandahålla ett förhandstillstånd efter en bedömning av huruvida utrustningsstörningen är nödvändig och proportionerlig) fortfarande är oklara. Eftersom tillståndet i den senare situationen "upphör att påverka och kanske inte förnyas" i fall där

---

<sup>99</sup> Se även bedömningen av förfarandet med dubbla lås och justitieombudsmannens oberoende nedan.

<sup>100</sup> Se avsnitt 109 i IPA 2016.

justitieombudsmannen inte godkänner utrustningsstörning i efterhand, förstår Europeiska dataskyddsstyrelsen att de uppgifter som samlats in under tiden fortfarande är lagligt insamlade. För att dessa uppgifter ska raderas kan ett särskilt beslut utfärdas av justitieombudsmannen<sup>101</sup>.

166. **Europeiska dataskyddsstyrelsen uppmanar Europeiska kommissionen att ytterligare bedöma på vilka villkor skyndsamhet kan åberopas samt att klargöra hur berörda registrerade kan utöva sina rättigheter och vilka möjligheter till rättslig prövning de erbjuds i samband med utrustningsstörningsverksamhet, särskilt när detta sker i skyndsamma fall som leder till undantag från förfarandet med dubbla lås.**

#### 4.3.1.4 Massavlyssning av uppgifter från bärare

167. Såsom det anges i rapporten om översyn av bulkbefogenheter<sup>102</sup> *involverar massavlyssning vanligtvis insamling av kommunikationer som befinner sig i transit hos särskilda bärare (kommunikationslänkar)*. I det officiella faktabladet om IPA 2016 anges att "massavlyssning" är förfarandet för att samla in en mängd kommunikationer vartefter särskilda kommunikationer väljs ut för att avläsas, övervakas eller avlyssnas när det är nödvändigt och proportionerligt. Europeiska dataskyddsstyrelsen noterar att "massavlyssning" av uppgifter faktiskt innebär att uppgifter samlas in redan innan filtrering av väljare (antingen enkelt i samband med övervakning av enskilda personer som redan är kända för att utgöra ett hot, eller komplicerat i samband med identifiering av nya hot och av tidigare okända personer av intresse).
168. Inhämtandet av mängddata om kommunikation var också en av de frågor som prövades av EU-domstolen i målet Privacy International, vilket resulterade i en dom från stora avdelningen av den 6 oktober 2020 (utöver huruvida datainsamlingen utfördes inom ramen för unionsrätten, även för nationella säkerhetsändamål). IPA 2016 ersätter den lagstiftning som var föremål för denna dom.
169. Europeiska dataskyddsstyrelsen noterar att i och med införlivandet av IPA 2016 i Förenade kungarikets lagstiftning krävs nu ett tillstånd för massavlyssning. Förfarandet för att utfärda detta tillstånd bygger på fastställandet av "operativa ändamål". Förteckningen över dessa operativa ändamål upprättas av underrättelsetjänsternas chefer och godkänns sedan av ministern. Detta beslut godkänns i sin tur av en oberoende justitieombudsman som ska pröva huruvida tillståndet är nödvändigt och proportionerligt med avseende på de operativa ändamålen. Europeiska dataskyddsstyrelsen förstår att justitieombudsmannen inte har befogenhet att bedöma de operativa ändamålen i sig, utan huruvida tillståndet är nödvändigt och proportionerligt med avseende på de operativa ändamål som anges i tillståndet. Den parlamentariska underrättelse- och säkerhetskommittén får en kopia av förteckningen var tredje månad och premiärministern ser över förteckningen över dessa operativa ändamål minst en gång om året.
170. På grundval av de uppgifter som Europeiska kommissionen lämnade i utkastet till beslut förefaller det dock svårt att bedöma omfattningen av de operativa ändamål som anges i förteckningen och huruvida insamlingen av de uppgifter som tillåts uppnår det tröskelvärde som fastställts av EU-domstolen (t.ex. att begränsa insamlingen av uppgifter till ett geografiskt område kan vara lika snävt som ett fåtal gator eller som att samla in uppgifter från hela EES).
171. EDPB understryker dessutom att uppgifter som massinsamlas kan lagras under långa perioder (för att vara tillgängliga för ytterligare åtkomst för granskning). EDPB noterar att det i avsnitt 150, punkterna 5 och 6 i IPA 2016 endast föreskrivs att kopior av insamlade uppgifter ska förstöras, och

<sup>101</sup> Se avsnitt 110, underavsnitt 3 b i IPA 2016.

<sup>102</sup> Se *Report of the bulk powers review* från Independent Review of Terrorism Legislation, augusti 2016.

endast om lagringen av dem inte är nödvändig eller sannolikt inte kommer att bli nödvändig, av hänsyn till den nationella säkerheten eller av andra skäl som omfattas av avsnitt 138.2 i IPA 2016, eller om lagringen inte är nödvändig för flera andra ändamål<sup>103</sup>. EDPB betonar att dessa skäl förefaller mycket breda, och i vart fall nämns endast kopior av de uppgifter som erhålls.

172. Vidare noterar EDPB att IPA 2016 i brådskande fall också medger ändring av warranter utan förhandsgodkännande av en justitieombudsman, och att om den justitieombudsman som i ett sådant fall rådfrågades i efterhand inom tre arbetsdagar efter ändringen vägrar godkänna ändringen bör warranterna ha verkan som om ändringen inte hade gjorts, men de uppgifter som samlats in däremellan har fortfarande samlats in lagligt<sup>104</sup>. För att dessa uppgifter ska raderas kan ett särskilt beslut utfärdas av justitieombudsmannen<sup>105</sup>.
173. **EDPB uppmanar därför kommissionen att ytterligare klargöra och bedöma massavlyssningar, särskilt när det gäller urval och tillämpning av selektorer inom ramen för dessa förfaranden för massavlyssning, för att klargöra i vilken utsträckning tillgången till personuppgifter uppfyller det tröskelvärde som fastställts av EU-domstolen (se även avsnitt 4.3.1.7 nedan, särskilt om tillsynen över selektorerna) och vilka åtgärder som finns på plats för att skydda de grundläggande rättigheterna för personer vars uppgifter är föremål för intrång i detta sammanhang, inbegripet när det gäller lagringstiden för uppgifter. En oberoende bedömning av behöriga brittiska tillsynsmyndigheter skulle vara särskilt användbar.**
174. EDPB understryker också att det förefaller särskilt kritiskt att "utrikesrelaterad kommunikation" som omfattas av massavlyssning verkar innebära att uppgifter direkt kan fångas upp och massinsamlas inom EES av Förenade kungariket, inbegripet uppgifter som överförs mellan EES och Förenade kungariket och som skulle omfattas av tillämpningsområdet för utkastet till beslut (se avsnitt 4.3.2 nedan om ytterligare användning av den information som samlas in för ändamål som rör nationell säkerhet och utlämnande till andra länder).

#### 4.3.1.5 Skydd och skyddsåtgärder för sekundärdata

175. EDPB är vidare oroad över att Förenade kungarikets relevanta lagstiftning om massavlyssning inte ger samma skyddsnivå för alla kommunikationsdata. "Sekundärdata", som kan erhållas med en warrant för inhämtning av mängddata, är enligt avsnitt 137 i IPA 2016 både "systemdata", som omfattas av, ingår som en del av, bifogas eller logiskt förknippas med kommunikationen (antingen av avsändaren eller på annat sätt), och "identifieringsuppgifter", som omfattas av, ingår som en del av, bifogas eller logiskt förknippas med kommunikationen (antingen av avsändaren eller på annat sätt), kan särskiljas logiskt från resten av kommunikationen och, om de skulle särskiljas på detta sätt, inte skulle avslöja något av vad som rimligen kan anses vara kommunikationens budskap (om ett sådant finns), utan hänsyn till ett eventuellt budskap som härrör från den faktiska kommunikationen eller från uppgifter som rör översändandet av kommunikationen<sup>106</sup>.
176. EDPB noterar att dessa "sekundärdata", även kallade "metadata"<sup>107</sup>, som massinsamlas inte verkar omfattas av samma skyddsåtgärder som data som samlas in med en riktad warrant, utan även som

<sup>103</sup> Se underavsnitten 3 och 6 i avsnitt 150 i IPA 2016.

<sup>104</sup> Se avsnitt 147 i IPA 2016 (del 6 kapitel I).

<sup>105</sup> Se avsnitt 181 underavsnitt 3 b i IPA 2016.

<sup>106</sup> "Systemdata" och "identifieringsuppgifter" definieras i avsnitt 263 i IPA 2016.

<sup>107</sup> Se *Report of the bulk powers review* från Independent Review of Terrorism Legislation, augusti 2016.

<sup>108</sup> Se avsnitt 152 underavsnitt 1 c och underavsnitt 3 och därpå följande avsnitt i IPA 2016.

innehållsdata som massinsamlas. EDPB konstaterar att urvalet av avlyssnat innehåll omfattas av fler skyddsåtgärder<sup>108</sup> än urvalet av sekundärdata<sup>109</sup>.

177. Dessutom betonar EDPB att både Europeiska domstolen för de mänskliga rättigheterna<sup>110</sup> och EU-domstolen<sup>111</sup> har ifrågasatt det faktum att sådana data är mindre känsliga än andra, i synnerhet mindre känsliga än innehållsdata. I uppförandekoden om avlyssning anges som exempel på "sekundärdata" (båda "systemdata", såsom routerkonfigurationer, e-postadresser eller användar-ID, men även alternativa kontokoder, liksom "identifieringsuppgifter", såsom platsen för ett möte i en kalender, fotoinformation, t.ex. tid, datum och plats då bilden togs). **EDPB betonar därför Europeiska domstolen för de mänskliga rättigheternas och EU-domstolens konsekventa bedömning och erinrar om de farhågor som uttryckts när det gäller sekundärdata, som bör omfattas av särskilda skyddsåtgärder på grund av deras känslighet. EDPB uppmanar därför kommissionen att noggrant bedöma huruvida de skyddsåtgärder som föreskrivs i brittisk lag för en sådan kategori av personuppgifter säkerställer en skyddsnivå som i allt väsentligt är likvärdig med den som garanteras i EU.**

#### 4.3.1.6 Automatiserad behandling av kommunikationsdata

178. EDPB noterar att underrättelsetjänster inte bara använder enkla eller komplexa selektorer för att filtrera de uppgifter som massinsamlas, utan att de också kan förlita sig på andra automatiserade behandlingsverktyg för att analysera *stora mängder information, vilket gör det möjligt för organen att även hitta kopplingar, mönster, associationer eller beteenden som kan påvisa ett allvarligt hot som kräver utredning*, enligt rapporten från underrättelse- och säkerhetskommittén (*Intelligence and Security Committee*) 2015<sup>112</sup>. **EDPB är medveten om att denna offentliga rapport rör praxis enligt den tidigare rättsliga ramen, som senare ersattes av IPA 2016. EDPB ser dock ett behov av ytterligare oberoende bedömning av och tillsyn över användningen av verktyg för automatiserad behandling av de behöriga brittiska tillsynsmyndigheterna, och uppmanar kommissionen att**

<sup>108</sup> Se avsnitt 152 underavsnitt 1 c och underavsnitt 3 och därpå följande avsnitt i IPA 2016.

<sup>109</sup> Se avsnitt 152 underavsnitt 1 a och b i IPA 2016.

<sup>110</sup> Se Europeiska domstolen för de mänskliga rättigheterna, Big Brother Watch, punkt 357, med hänskjutning till stora avdelningen: *Även om domstolen inte betvivlar att relaterade kommunikationsdata är ett viktigt verktyg för underrättelsetjänsterna i kampen mot terrorism och grov brottslighet anser den följaktligen inte att myndigheterna har uppnått en rimlig balans mellan konkurrerande offentliga och privata intressen genom att i sin helhet undanta dem från de skyddsåtgärder som ska tillämpas på sökning och granskning av innehåll. Domstolen föreslår inte att relaterade kommunikationsdata endast bör vara tillgängliga för att avgöra om en person befinner sig på de brittiska öarna eller inte, eftersom detta skulle kräva tillämpning av strängare standarder för relaterade kommunikationsdata än vad som gäller för innehåll, men det bör ändå finnas tillräckliga skyddsåtgärder för att säkerställa att undantaget för relaterade kommunikationsdata från kraven i avsnitt 16 i RIPA begränsas till vad som är nödvändigt för att fastställa huruvida en person för tillfället befinner sig på de brittiska öarna.*

<sup>111</sup> Se EU-domstolen, Privacy International, punkt 71: "Det ingrepp som överföring av trafik- och lokaliseringssuppgifter till säkerhets- och underrättelsetjänsterna utgör i den rätt som är stadfäst i artikel 7 i stadgan måste betraktas som synnerligen allvarligt, bland annat med hänsyn till att den information som dessa uppgifter kan innehålla är känslig och i synnerhet till att det utifrån uppgifterna är möjligt att kartlägga de berörda personerna, då sådan information är lika känslig som själva innehållet i kommunikationerna. Det kan dessutom ge de berörda personerna en känsla av att deras privatliv står under ständig övervakning (se, analogt, dom av den 8 april 2014, Digital Rights Ireland m.fl., C-293/12 och C-594/12, EU:C:2014:238, punkterna 27 och 37, och dom av den 21 december 2016, Tele2, C-203/15 och C-698/15, EU:C:2016:970, punkterna 99 och 100)."

<sup>112</sup> Se Intelligence and Security Committee, *Privacy and Security: A modern and transparent legal framework*, 2015, punkt 18, s. 13, [https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312\\_ISC\\_PSRptweb.pdf](https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf).

**ytterligare bedöma denna fråga och de skyddsåtgärder som i detta sammanhang skulle och/eller skulle kunna erbjudas registrerade i EES.**

#### 4.3.1.7 Efterlevnadsrisker och oförenliga metoder hos behöriga underrättelsetjänster

179. EDPB noterar att detaljerade tillsynsrapporter finns tillgängliga. De tillför värdefulla aspekter när det gäller vad de bedömer som positiv efterlevnadspraxis, samt de efterlevnadsrisker och oförenliga metoder som identifierats.
180. I detta avseende framgår det av ombudsmannen för utredningsbefogenheter i dess rapport för 2019 att flera aspekter som rör de olika behöriga myndigheternas tillämpning av den rättsliga ramen har avslöjat en del (risker för) bristande efterlevnad från de behöriga myndigheternas sida.
181. För det första har EDPB noterat att kriterierna för att klassificera ett dataset som mängddata om personuppgifter eller som riktade data inte alltid verkar vara tydliga för MI5 och SIS själva, särskilt för MI5, vilket kan leda till att lämpliga skyddsåtgärder inte tillämpas på datan<sup>113</sup>. I sin rapport från 2019 föreslog ombudsmannen för utredningsbefogenheter att *denna fråga bör lösas som en prioriterad fråga*<sup>114</sup>. Även när det gäller mängddata om personuppgifter noterar EDPB att även om klassificeringen av mängddata om personuppgifter förefaller vara tillfredsställande (men ännu inte har granskas av ombudsmannen för utredningsbefogenheter) för GCHQ gav det särskilda teamets interna efterlevnadskontroll av warranter i mars 2019 upphov till allvarliga farhågor, eftersom 50 % av de motiveringar för warranter för inhämtning av mängddata som granskades av GCHQ:s efterlevnadsgrupp inte uppfyllde kraven. Enligt ombudsmannen för utredningsbefogenheter hade efterlevnadsgruppen börjat undersöka problemet och omskola personalen för att förbättra standarden. Den uppdaterade utbildningen om bestämmelserna i IPA 2016 och den ytterligare utbildning som tillhandahålls av nätverk för politik och efterlevnad har förbättrat GCHQ:s efterlevnad på detta område. Ombudsmannen för utredningsbefogenheter förväntar sig inte en försämring av denna standard vid framtida kontroller, men kommer att fortsätta att noggrant granska detta område<sup>115</sup>. **EDPB delar därför uppfattningen att kommissionen behöver se över och övervaka dessa aspekter ytterligare som en del av bedömningen av skyddsnivån för att säkerställa att denna standard förbättras, vilket betonas i en rapport från ombudsmannen för utredningsbefogenheter, och påminner om att genomförandet och den konkreta tillämpningen av den rättsliga ramen också ska beaktas i enlighet med artikel 45 i dataskyddsförordningen vid bedömningen av ett tredjelands väsentliga likvärdighet.**

---

<sup>113</sup> Se 2019 års rapport från ombudsmannen för utredningsbefogenheter av den 15 december 2020, punkt 8.39, [https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPC-Annual-Report-2019\\_Web-Accessible-version\\_final.pdf](https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPC-Annual-Report-2019_Web-Accessible-version_final.pdf): Vi har noterat den positiva utvecklingen av [Bulk Oversight Panel (BOP)] och noterar dess inverkan på hanteringen av intern efterlevnad. Vi fortsätter att sträva efter större tydlighet när det gäller det förfarande som MI5 använder för att utföra inledande undersökningar av nya dataset för att bättre förstå beslut om att klassificera ett dataset som mängddata om personuppgifter eller, till exempel, som riktade data. Vi var bekymrade över en olöst åtgärd i BOP:s protokoll för att åtgärda diskrepanser mellan fördelningen av mängddata om personuppgifter mellan MI5 och SIS. På grund av de olika användningsområdena för uppgifterna och de olika delar av uppgifter som innehas är det möjligt att båda organen innehar samma dataset, eller versioner av det, och att det lagligen kan kategoriseras som mängddata av den ena och som riktade data av den andra. Det finns en risk för att om ett av organen felaktigt har klassificerat datainnehavet som riktat skulle dessa data lagras utan en lämplig warrant och kanske inte omfattas av lämpliga skyddsåtgärder.

<sup>114</sup> Se 2019 års rapport från ombudsmannen för utredningsbefogenheter, punkt 8.39.

<sup>115</sup> Se 2019 års rapport från ombudsmannen för utredningsbefogenheter, punkt 10.48.

182. Mer allmänt betonar EDPB de punkter som ombudsmannen för utredningsbefogenheter delar när det gäller de ”uppgiftsbaserade sökningar” som leds av tjänstemän vid MI5 – som gör det möjligt för en utredare att göra mer än en sökning i de stora samlingar mängddata om personuppgifter som de har tillgång till – och de *allvarliga efterlevnadsrisker som är förknippade med vissa teknikmiljöer som används av MI5*, när det gäller var uppgifterna lagrades i miljön, vem som hade tillgång till dem, i vilken utsträckning de kopierades eller delades, de raderingsförfaranden som tillämpades på dem samt lagringsperioderna. Även om ombudsmannen för utredningsbefogenheter anger att åtgärder har vidtagits och garantier införts förblir vissa av dem manuella och leds av enskilda personer, men betonar att det är mycket viktigt att *MI5 fortsätter att upprätthålla dessa nya förfaranden och tillhandahåller tillräckliga resurser för att de ska kunna fungera effektivt. Om MI5 identifierar en ökning av bristande efterlevnad*<sup>116</sup> förväntar sig ombudsmannen för utredningsbefogenheter att detta kommer att meddelas den så snart som möjligt. **EDPB uppmanar därför kommissionen att noga övervaka dessa aspekter i framtiden.**
183. När det gäller GCHQ förstår EDPB också av rapporten från ombudsmannen för utredningsbefogenheter att, när det gäller insatser som genomförs inom ramen för warranter för inhämtning av mängddata, *kvaliteten på ansökningar om internt godkännande varierade, och vi konstaterade att det fanns utrymme för förbättringar när det gäller utformningen av sådana tillämpningar*<sup>117</sup> och att förklaringarna till användningen av allmänna deskriptorer ibland var alltför allmänna och ottydliga när det gäller riktad utrustningsstörning<sup>118</sup>. EDPB noterade även att ombudsmannen för utredningsbefogenheter i samband med massutrustningsstörning rekommenderar att *ansökningar konsekvent och uttryckligen bör ange kopplingen mellan målet och det stadseenliga syftet och underrättelsekraven*<sup>119</sup> och att *alla ansökningar tydligt bör ta upp potentialen för oavsiktlig insamling av information och relevanta riskreducerande åtgärder vid bedömning av proportionaliteten*<sup>120</sup>. Ombudsmannen för utredningsbefogenheter betonade även att trots framstegen *finns det fortfarande utrymme för förbättring*<sup>121</sup> och att ytterligare uppmärksamhet kommer att krävas i framtiden.
184. När det gäller systemet för massavlyssning enligt *Regulation of Investigatory Powers Act 2000* (nedan kallad *RIPA 2000*), som sedan dess har ersatts av bestämmelser i IPA 2016, erinrar EDPB om att den otillräckliga tillsynen, både över urvalet av internetbärare för avlyssning och över filtreringen, sökningen och urvalet av avlyssnad kommunikation för granskning, var en av de centrala aspekter som Europeiska domstolen för de mänskliga rättigheterna ansåg vara oförenlig med artikel 8 i Europakonventionen med avseende på den tidigare lagstiftningen om de brittiska myndigheternas undersökningsbefogenheter inom ramen för nationell säkerhet i målet *Big Brother Watch*, som nu hänskjutits till den stora avdelningen. **EDPB uppmanar kommissionen att kontrollera statusen för förfarandena, beakta dessa aspekter och ange dem i beslutet om adekvat skyddsnivå om kommissionen antar detta.**
185. I detta mål var Europeiska domstolen för de mänskliga rättigheterna *inte övertygad om att de skyddsmekanismer som styr urvalet av bärare som ska avlyssnas och urvalet av avlyssnat material för granskning är tillräckligt robusta för att ge tillräckliga garantier mot missbruk. Det mest oroande är dock att det saknas robust, oberoende tillsyn över selektorerna och de sökkriterier som används*

<sup>116</sup> Se 2019 års rapport från ombudsmannen för utredningsbefogenheter, punkt 8.52.

<sup>117</sup> Se 2019 års rapport från ombudsmannen för utredningsbefogenheter, punkt 10.2.

<sup>118</sup> Se 2019 års rapport från ombudsmannen för utredningsbefogenheter, punkterna 10.16 och 10.17.

<sup>119</sup> Se 2019 års rapport från ombudsmannen för utredningsbefogenheter, punkt 10.23.

<sup>120</sup> Se 2019 års rapport från ombudsmannen för utredningsbefogenheter, punkt 10.23.

<sup>121</sup> Se 2019 års rapport från ombudsmannen för utredningsbefogenheter, punkt 10.23.

för att filtrera avlyssnad kommunikation.<sup>122</sup> Ombudsmannen för utredningsbefogenheter betonade att denna slutsats följde en liknande rekommendation från underrättelse- och säkerhetskommittén i *Privacy and Security: A modern and transparent legal framework report* från mars 2015<sup>123</sup>. EDPB välkomnar att ombudsmannen för utredningsbefogenheter följaktligen genomförde en översyn av sin metod för inspektion av massavlyssning under 2019, som inbegrep en noggrann översyn av de tekniskt komplicerade sätt på vilka massavlyssning faktiskt genomförs<sup>124</sup> och åtog sig att inkludera en ingående granskning av de selektorer och sökkriterier som Europeiska domstolen för de mänskliga rättigheterna hänvisar till ovan<sup>125</sup> i inspektionerna av massavlyssning från och med 2020. Med tanke på betydelsen av denna aspekt är EDPB oroad över att ombudsmannen för utredningsbefogenheter ännu inte har gjort någon ingående granskning av selektorerna och sökkriterierna, och uppmanar kommissionen att noga övervaka utvecklingen i detta avseende, särskilt eftersom det konkreta formatet för en sådan tillsyn ännu inte har klargjorts<sup>126</sup>.

#### 4.3.2. Ytterligare användning av den information som samlas in för ändamål som rör nationell säkerhet och utlämnande till andra länder

186. När det gäller ytterligare användning av den information som samlas in för ändamål som rör nationell säkerhet hänvisar kommissionen i sin bedömning till avsnitt 87.1 i 2018 års dataskyddslag, där det föreskrivs att *personuppgifter som samlas in på detta sätt inte får behandlas på ett sätt som är oförenligt med det ändamål för vilket de samlas in*. EDPB påpekar dock att denna bestämmelse kan omfattas av undantag för nationell säkerhet i enlighet med avsnitt 110 i 2018 års dataskyddslag. EDPB noterar vidare att det i lagstiftningen föreskrivs en möjlighet till "utlämnande till andra länder", oavsett om det gäller riktad avlyssning och granskning, riktat förvärv och lagring av kommunikationsdata, riktad utrustningsstörning eller massavlyssning och massutrustningsstörning.

##### 4.3.2.1 Ytterligare användning, utlämnande till andra länder och den tillämpliga rättsliga ramen i Förenade kungariket

187. Kommissionen har identifierat del 4 i 2018 års dataskyddslag, särskilt avsnitt 109, som relevanta bestämmelser som fastställer särskilda krav för ytterligare användning av den information som samlas in, särskilt underrättelsetjänsters internationella överföring av personuppgifter till tredjeländer eller internationella organisationer. EDPB noterar dock att avsnitt 110 i 2018 års dataskyddslag föreskriver ett undantag för nationell säkerhet, där det anges att vissa bestämmelser i 2018 års dataskyddslag inte är tillämpliga om undantag från dessa bestämmelser krävs för att skydda den nationella säkerheten. De berörda bestämmelserna som eventuellt inte är tillämpliga inbegriper kapitel 2 i del 4 i 2018 års dataskyddslag avseende principerna för dataskydd, inbegripet ändamålsbegränsning, samt kapitel 3 i del 4 i 2018 års dataskyddslag avseende registrerades rättigheter. Avsnitt 109 i 2018 års dataskyddslag, jämfört med avsnitt 110 i 2018 års dataskyddslag och de villkor enligt vilka det tillämpas, kan leda till att en underrättelsetjänsts internationella överföring av personuppgifter till ett tredjeland äger rum utan tillämpning av bestämmelser som rör principerna för dataskydd och den registrerades rättigheter.
188. Som kommissionen har konstaterat måste ett sådant undantag bedömas från fall till fall och kan endast åberopas i den mån tillämpningen av en viss bestämmelse skulle få negativa konsekvenser

<sup>122</sup> Se Europeiska domstolen för de mänskliga rättigheterna, Big Brother Watch, punkt 347.

<sup>123</sup> Se 2019 års rapport från ombudsmannen för utredningsbefogenheter, punkt 10.28.

<sup>124</sup> Se 2019 års rapport från ombudsmannen för utredningsbefogenheter, punkt 10.28.

<sup>125</sup> Se 2019 års rapport från ombudsmannen för utredningsbefogenheter, punkt 10.28.

<sup>126</sup> Se 2019 års rapport från ombudsmannen för utredningsbefogenheter, punkt 10.28: *det exakta formatet för denna inspektion har ännu inte fastställts*.

för den nationella säkerheten. Utfärdandet av ett nationellt certifikat för de brittiska underrättelsetjänsterna syftar till att intyga att ett undantag krävs för specificerade personuppgifter som behandlas i syfte att skydda den nationella säkerheten. EDPB noterar dock att det brittiska inrikesministeriet i sin vägledning för nationella säkerhetscertifikat enligt 2018 års dataskyddslag klargör att *det är viktigt att redan från början notera att ett certifikat inte krävs för att åberopa undantaget för nationell säkerhet. Faktum är att personuppgiftsansvariga i de flesta fall själva kommer att avgöra huruvida undantaget för nationell säkerhet är tillämpligt.*<sup>127</sup> I det brittiska inrikesministeriets vägledning noteras vidare att *nationella säkerhetscertifikat kan tillämpas på personuppgifter som särskilt kan identifieras eller omfatta en bredare kategori av personuppgifter. De kan tillämpas både i förhand och i efterhand.*<sup>128</sup> Undantaget för nationell säkerhet kan därför tillämpas i samband med en underrättelsetjänsts internationella överföring av personuppgifter till ett tredjeland i avsaknad av ett nationellt säkerhetscertifikat.

189. EDPB noterar vidare att det i det nationella säkerhetscertifikatet DPA/S27/Security<sup>129</sup> till och med den 24 juli 2024 föreskrivs att personuppgifter som behandlas *på uppdrag av, på begäran av eller med hjälp av säkerhetstjänsten* och *när sådan behandling är nödvändig för att underlätta ett korrekt utförande av säkerhetstjänstens uppgifter enligt avsnitt 1 i Security Service Act 1989* undantas från motsvarande bestämmelser i brittisk lag till kapitel V i dataskyddsförordningen när det gäller överföring av personuppgifter till tredjeländer eller internationella organisationer. Även om det i andra nationella säkerhetscertifikat som är allmänt tillgängliga inte föreskrivs något undantag från bestämmelserna i avsnitt 109 i 2018 års dataskyddslag bör det erinras om att en del av eller hela texten i ett nationellt säkerhetscertifikat kan nekas om dess offentliggörande skulle strida mot den nationella säkerheten, strida mot allmänintresset eller äventyra någon persons säkerhet.
190. Vid bedömningen av utkastet till beslut i förhållande till dessa bestämmelser konstaterar EDPB i allmänhet att skyddsåtgärderna för dessa utlämnanden endast omfattar kravet att mottagaren av uppgifterna ska respektera kraven på datasäkerhet, omfattningen av utlämnandet begränsat till vad som är nödvändigt, lagringen av uppgifter och begränsningen av tillgången till uppgifter till ett begränsat antal personer. **Därför understryker EDPB att när det gäller utlämnande till andra länder kan tillämpningen av det undantag för nationell säkerhet som föreskrivs i brittisk lag leda till situationer där skyddsåtgärder som säkerställer att principerna om ändamålsbegränsning, nödvändighet och proportionalitet samt rättigheterna för enskilda, rätten till tillsyn och rätten till prövning inte skulle tillhandahållas eller respekteras till fullo i det mottagande tredjelandet.** EDPB rekommenderar därför kommissionen att ytterligare undersöka de övergripande skyddsåtgärder som föreskrivs i brittisk lag när det gäller utlämnande till andra länder, särskilt mot bakgrund av tillämpningen av undantag för nationell säkerhet.

#### 4.3.2.2 Utlämnade till andra länder och utbyte av underrättelser inom ramen för internationellt samarbete

191. EDPB noterar också att kommissionen, som en del av sin bedömning av adekvat skyddsnivå, inte beaktade befintliga internationella avtal som ingåtts mellan Förenade kungariket och tredjeländer

<sup>127</sup> Se 2018 års dataskyddslag från inrikesministeriet, *National Security Certificates guidance*, augusti 2020, punkt 3, s. 3.

<sup>128</sup> Se 2018 års dataskyddslag från inrikesministeriet, *National Security Certificates guidance*, augusti 2020, punkt 5, s. 4.

<sup>129</sup> Se DPA/S27/Security Service, avsnitt 27 i 2018 års dataskyddslag, *Certificate of the Secretary of State*, 24 juli 2019, <https://ico.org.uk/media/about-the-ico/documents/nscs/2615660/nsc-part-2-mi5-201908.pdf>.

eller internationella organisationer som kan innehålla särskilda bestämmelser om underrättelsetjänsters internationella överföring av personuppgifter till tredjeländer.

192. EDPB betonar också att kommissionens bedömning huvudsakligen bygger på bedömningen av del 4 i 2018 års dataskyddslag och är särskilt oroad över att IPA 2016 fokuserar på "begäranden" om utbyte av underrättelser med utländska partner, men inte tar upp andra former av utbyte av underrättelser. EDPB noterar i detta avseende att kommissionens utkast till beslut inte hänvisar till eller bedömer kopplingen mellan Förenade kungarikets rättsliga ram och avtalet mellan Förenade kungariket och Förenta staterna om underrättelseverksamhet (*UK-US Communication Intelligence Agreement*). I ett uttalande nyligen för att uppmärksamma detta avtals 75-årsdag konstaterade Förenta staternas nationella säkerhetsorgan (NSA) att detta partnerskap gör det möjligt *att dela information mellan de två organen i så stor utsträckning som möjligt, med minimala begränsningar* och att *detta banbrytande dokument skapade riktlinjer och förfaranden för anställda inom underrättelsetjänsten i Förenade kungariket och Förenta staterna för utbyte av kommunikation, översättning, analys och information om kodknäckning*<sup>130</sup>. Detta avtal lade också grunden för andra underrättelsepartnerskap med Australien, Kanada och Nya Zeeland.
193. Att detta avtal och dess särskilda bestämmelser är hemliga innebär en allvarlig utmaning i fråga om klarhet och förutsebarhet i lagstiftningen när det gäller fortsatt användning och utlämnande till andra länder av information som samlas in av brittiska myndigheter för ändamål som rör nationell säkerhet. I detta sammanhang påminner EDPB om att EU-domstolen, när det gäller den skyddsnivå som garanteras inom EU, har betonat att lagstiftning som innebär ingrepp i den grundläggande rätten till skydd av personuppgifter måste "föreskriva tydliga och precisa bestämmelser som reglerar räckvidden och tillämpligheten av en åtgärd och slå fast minimikrav, så att de personer vilkas personuppgifter berörs har tillräckliga garantier som möjliggör ett effektivt skydd av deras uppgifter mot risker för missbruk och otillåten åtkomst eller användning. Behovet av sådana garantier är av än större betydelse när personuppgifterna är föremål för automatisk behandling och risken för otillåten åtkomst till uppgifterna är stor"<sup>131</sup>. EDPB anser därför att kommissionen bör beakta effekterna av avtalet mellan Förenade kungariket och Förenta staterna som en del av sin bedömning av adekvat skyddsnivå.
194. Europeiska domstolen för de mänskliga rättigheterna har i första avsnittet av sin dom av den 13 september 2018 i målet Big Brother Watch gjort en bedömning av Förenade kungarikets system för utbyte av underrättelser och särskilt avtalet mellan Förenade kungariket och Förenta staterna. Europeiska domstolen för de mänskliga rättigheterna konstaterade att *den rättsliga ram som gör det möjligt för Förenade kungarikets underrättelsetjänster att begära avlyssnat material från utländska underrättelsetjänster ingår inte i RIPA. Enligt avtalet mellan Förenade kungariket och Förenta staterna av den 5 mars 1946 tillåts särskilt utbyte av material mellan Förenta staterna och Förenade kungariket*<sup>132</sup> och det anses att det finns *en rättslig grund för att begära underrättelser från utländska underrättelseorgan, och att denna lag är tillräckligt tillgänglig*<sup>133</sup>. Även om Europeiska domstolen för de mänskliga rättigheterna har konstaterat att ingen överträdelse har skett av artikel 8<sup>134</sup> i Europakonventionen när det gäller systemet för utbyte av underrättelser noterar EDPB att denna

---

<sup>130</sup> Se NSA:s pressmeddelande, *GCHQ and NSA Celebrate 75 Years of Partnership*, 5 februari 2021, <https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2494453/gchq-and-nsa-celebrate-75-years-of-partnership/>.

<sup>131</sup> Se Schrems I, punkt 91.

<sup>132</sup> Se Europeiska domstolen för de mänskliga rättigheterna, Big Brother Watch, punkt 425.

<sup>133</sup> Se Europeiska domstolen för de mänskliga rättigheterna, Big Brother Watch, punkt 427.

<sup>134</sup> Se Europeiska domstolen för de mänskliga rättigheterna, Big Brother Watch, punkt 448.

dom nu har hänskjutits till den stora avdelningen, som ännu inte har fattat ett beslut. EDPB noterar också att domare Koskelo i sitt delvis instämmande och delvis avvikande yttrande, till vilket domare Turković anslöt sig<sup>135</sup>, kom fram till att artikel 8 i Europakonventionen har överträtts när det gäller systemet för utbyte av underrättelser, och konstaterade att *det är lätt att instämma i principen att varje arrangemang enligt vilket underrättelser från avlyssnad kommunikation inhämtas via utländska underrättelsetjänster, oavsett om det sker på grundval av begäranden om att utföra sådan avlyssning eller att sprida dess resultat, inte bör innebära att de garantier som måste finnas för all övervakning genom inhemska myndigheter kringgås (se punkterna 216, 423 och 447). Varje annat tillvägagångssätt skulle i själva verket vara orealistiskt.*

195. Som framhållits i flera rapporter från medier och icke-statliga organisationer<sup>136137</sup> är den senaste offentliggjorda versionen av avtalet mellan Förenade kungariket och Förenta staterna från 1956, och sedan dess har kommunikationstekniken och signalspaningens karaktär förändrats avsevärt. Medierapporter har till exempel visat att data som passerar genom undervattenskablar som slutar i Förenade kungariket fångas upp av GCHQ och görs tillgängliga för NSA<sup>138</sup>.
196. För EDPB är en nyckelfråga när det gäller utbyte av underrättelser huruvida avsnitt 109 i 2018 års dataskyddslag och bestämmelserna i IPA 2016 fortfarande är tillämpliga när brittiska underrättelsetjänster agerar i enlighet med avtalet mellan Förenade kungariket och Förenta staterna. En annan viktig aspekt som ska bedömas är huruvida bestämmelserna eller den faktiska tillämpningen av detta avtal påverkar skyddsnivån för personuppgifter som överförs från EES till Förenade kungariket eller möjliggör direkt åtkomst till och direkt förvärv av personuppgifter för underrättelsetjänster i tredjeländer.
197. Följaktligen är EDPB, utöver de reservationer som uttryckts i fråga om ”utlämnande till andra länder” på grundval av del 4 i 2018 års dataskyddslag och dess tillhörande undantag för nationell säkerhet, samt begäranden inom ramen för IPA 2016, **oroad över andra former av informationsutbyte och utlämnande, på grundval av andra instrument, särskilt de olika internationella avtal som Förenade kungariket ingått med andra tredjeländer, i synnerhet när dessa instrument fortfarande inte är tillgängliga för allmänheten, såsom avtalet mellan Förenade kungariket och Förenta staterna. Effekten av ett sådant avtal skulle kunna leda till ett kringgående av de säkerhetsgarantier som fastställts i samband med tillgång till och användning av personuppgifter för ändamål som rör nationell säkerhet.**
198. EDPB delar den åsikt som uttryckts av FN:s särskilde rapportör, Joe Cannatacci, att *utbyte av underrättelser inte får leda till en bakväg för att erhålla eller underlätta för andra att erhålla underrättelser som är fria från inhemska skyddsåtgärder, eller ett kryphål för utländska regeringar med lägre standarder för skydd av privatlivet (eller andra mänskliga rättigheter) att erhålla*

---

<sup>135</sup> Se Europeiska domstolen för de mänskliga rättigheterna, Big Brother Watch, delvis instämmande och delvis avvikande yttrande från domare Koskelo, till vilket domare Turković anslöt sig.

<sup>136</sup> Se BBC, *Diary reveals birth of secret UK-US spy pact that grew into Five Eyes*, 5 mars 2021, <https://www.bbc.com/news/uk-56284453>.

<sup>137</sup> Se Privacy International, *Policy Briefing – UK Intelligence Sharing Arrangements*, april 2018, <https://privacyinternational.org/sites/default/files/2018-04/Privacy%20International%20Briefing%20-%20Intelligence%20Sharing%20%28UK%29%20FINAL.pdf>.

<sup>138</sup> Se The Guardian, *GCHQ taps fibre-optic cables for secret access to world's communications*, 21 juni 2013, <https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>.

*underrättelser från brittiska underrättelser som kan ge upphov till kränkningar av de mänskliga rättigheterna*<sup>139</sup>.

199. **EDPB anser också att man för att i framtiden kunna ingå bilaterala eller multilaterala avtal med tredjeländer för underrättelsesamarbete, där man tillhandahåller en rättslig grund för direkt avlyssning och direkt förvärv av personuppgifter eller överföring av personuppgifter till dessa länder, också kan påverka villkoren för vidare användning av insamlad information i större utsträckning, eftersom sådana avtal sannolikt kommer att påverka Förenade kungarikets rättsliga ram för dataskydd så som den bedömts.**

#### 4.3.3. Tillsyn

200. EDPB betonar vikten av omfattande tillsyn av oberoende tillsynsmyndigheter för en adekvat dataskydds nivå. Syftet med tillsynsmyndigheternas garanti för oberoende i den mening som avses i artikel 8.3 i EU-stadgan är att säkerställa en effektiv och tillförlitlig kontroll av att bestämmelserna om skydd för enskilda personer med avseende på behandling av personuppgifter efterlevs.
201. När man får tillgång till personuppgifter och använder dem för ändamål som rör nationell säkerhet utförs tillsynsfunktionen i huvudsak av ombudsmannen för utredningsbefogenheter och justitieombudsmännen (nedan gemensamt kallade *justitieombudsmän*).
202. **EDPB erkänner generellt att införandet av justitieombudsmän i IPA 2016 är en betydande förbättring.** I linje med en begäran ovan uppmanas kommissionen att göra en mer ingående bedömning av **justitieombudsmännens oberoende, och i synnerhet i vilken utsträckning ombudsmannen för utredningsbefogenheter och dennes avdelningar (nedan kallade IPCO) oberoende är rättsligt säkerställt, eftersom detta inte behandlas i IPA 2016.** Detta är ännu viktigare eftersom ombudsmannen för utredningsbefogenheter beslutar om regeringens överklaganden i de fall då en ansökan om **övervakningsåtgärd** har avslagits av en justitieombudsman.
203. Ombudsmannen för utredningsbefogenheter utför både förhands- och efterhandstillsyn. När det gäller förhandstillsyn inser EDPB att justitieombudsmännens uppgift är att i enskilda fall godkänna olika övervakningsåtgärder, inbegripet riktad avlyssning och massinsamling av kommunikationsdata. EDPB noterar vidare att förhandsgodkännande av övervakningsåtgärder inte kan härledas ur EU-domstolens rättspraxis som ett absolut krav för övervakningsåtgärdernas proportionalitet<sup>140</sup>.
204. För att bedöma hur effektiv denna tillsyns nivå är ser EDPB dock behovet av att ytterligare klargöra de scenarier där laglig avlyssning är möjlig utan justitieombudsmännens förhandsgodkännande.
205. I sitt utkast till beslut nämner kommissionen i fotnoterna 201 och 266 "särskilda begränsade fall" som anges i avsnitten 44–52 i IPA 2016 när det gäller riktade avlyssningar. EDPB noterar att avsnitten 45–51 i IPA 2016 är undantag som enligt underrättelsetjänsterna inte används regelbundet. Dessutom **förstår EDPB att i de fall där undantagen är tillämpliga** (t.ex. telekommunikations- och postleverantörer) ska förhandsgodkännandet av justitieombudsmännen genomföras om

---

<sup>139</sup> Se slutrapporten från den särskilda rapportören om rätten till integritet vid avslutandet av hans uppdrag i Förenade konungariket Storbritannien och Nordirland, London, 29 juni 2018, <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E#:~:text=Intelligence%20sharing%20must%20not%20result,UK%20intelligence%20that%20could%20give>.

<sup>140</sup> EDPB noterar dock också att EU-domstolen, när den ogiltigförklarade skölden för skydd av privatlivet i Schrems II, har noterat att den så kallade FISA-domstolen enligt amerikansk lagstiftning inte godkänner "individuella övervakningsåtgärder, utan snarare övervakningsprogram (såsom Prism och Upstream) på grundval av årliga certifieringar" (punkt 179).

brottsbekämpande myndigheter eller underrättelsetjänster **begär** tillgång till dessa uppgifter, **och uppmanar kommissionen att i sitt beslut bekräfta att detta är korrekt.**

206. EDPB erkänner att avsnitt 44.2 i IPA 2016 tillåter avlyssning av kommunikation om en av parterna (avsändare eller mottagare) har samtyckt och det finns ett tillstånd enligt RIPA 2000 eller *Regulation of Investigatory Powers (Scotland) Act 2000 (2000 asp 11)*, dvs. den tidigare rättsliga situationen innan justitieombudsmännen inrättades. EDPB **uppmanar** kommissionen att klargöra huruvida detta innebär att förfarandet för förhandsgodkännande inte alls skulle tillämpas i fall där ett ensidigt samtycke föreligger.
207. När det gäller efterhandstillsyn är det också viktigt att kontrollera att effektiv oberoende tillsyn säkerställs utan luckor, särskilt om den inte planeras på förhand.
208. EDPB noterar att när det gäller avsnitten 48–52 i IPA 2016 görs en efterhandsöversyn av justitieombudsmännen, och **uppmanar kommissionen att klargöra enligt vilka krav och på vems initiativ en sådan efterhandsöversyn ska genomföras.**
209. Enligt avsnitt 229.4 i IPA 2016 ska ombudsmannen för utredningsbefogenheter inte övervaka utövandet av vissa funktioner. I detta avseende uppmanar EDPB kommissionen att förtydliga bestämmelserna i avsnitt 229.4 d och e i IPA 2016 när det gäller deras praktiska inverkan på granskningsbehörighet hos ombudsmannen för utredningsbefogenheter. **Det är EDPB:s uppfattning att den brittiska dataskyddsmyndigheten är den behöriga tillsynsmyndigheten där undantagen i avsnitt 229.4 i IPA 2016 är tillämpliga, och EDPB uppmanar kommissionen att i sitt beslut bekräfta att detta är korrekt.**
210. **Det förefaller som om ombudsmannen för utredningsbefogenheter roll vid efterhandstillsynen är begränsad** till att lämna rekommendationer vid bristande efterlevnad och att meddela den registrerade om felet är allvarligt och om det är i allmänhetens intresse att personen informeras om detta. **EDPB uppmanar kommissionen att klargöra hur IPCO effektivt kan säkerställa efterlevnad av lagstiftningen.**
211. **Slutligen förstår EDPB att berörda personer inte kan vända sig direkt till IPCO, utan måste lämna in ett klagomål till den brittiska dataskyddsmyndigheten, som dock har begränsade befogenheter på området nationell säkerhet. EDPB uppmanar därför kommissionen att ytterligare klargöra hur det i rättsligt hänseende säkerställs att IPCO behandlar klagomål i dessa fall.**

#### 4.3.4. Prövningsmöjligheter

212. Mot bakgrund av EU-domstolens domar i målen Schrems I och Schrems II står det klart att ett effektivt domstolsskydd i den mening som avses i artikel 47 i EU-stadgan är av grundläggande betydelse för antagandet att lagstiftningen i ett tredjeland är adekvat. Domarna har också visat att särskild uppmärksamhet i detta avseende måste ägnas åt ett effektivt rättsligt skydd när det gäller tillgång till personuppgifter för nationell säkerhet.
213. **EDPB är medveten om att Förenade kungariket har inrättat en domstol med utredningsbefogenheter. Domstolen med utredningsbefogenheter är inte bara behörig att pröva mål som rör brottsbekämpande myndigheters användning av utredningsbefogenheter, utan även av underrättelsetjänsters användning av sådana befogenheter. Det är EDPB:s uppfattning att domstolen med utredningsbefogenheter fungerar som en lämplig domstol i den mening som avses i artikel 47 i EU-stadgan. När det gäller dess befogenheter uppmanas kommissionen att bekräfta att domstolen med utredningsbefogenheter har alla de befogenheter som nämns i skäl 262 i utkastet till beslut, oberoende av den rättsliga grunden för klagomålet.**

214. Underrättelsetjänsternas hemliga övervakning innebär ofta att föremålet för övervakningen, den registrerade, inte är och inte kommer att vara medvetet om övervakningen. I detta sammanhang har EDPB, när den analyserat amerikansk lagstiftning, vid många tillfällen uttryckt sin oro över kravet på "talerätt", såsom det tolkas i amerikansk lagstiftning, i övervakningsfall. Mot denna bakgrund noterar EDPB att klagomålet till domstolen med utredningsbefogenheter endast kräver ett "prov på misstanke", enligt vilket klaganden måste visa att han eller hon potentiellt riskerar att bli föremål för en åtgärd.
215. Vid analysen av domstolen med utredningsbefogenheter fäster EDPB särskild uppmärksamhet vid det faktum att domstolen med utredningsbefogenheter upprepade gånger har befunnits vara förenlig med Europakonventionen, såsom den tolkas av Europadomstolen.