

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



**Atzinums 14/2021 par Eiropas Komisijas Īstenošanas lēmuma projektu saskaņā ar Regulu (ES) 2016/679 par personas datu pienācīgu aizsardzību Apvienotajā Karalistē**

**Pieņemts 2021. gada 13. aprīlī**

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

## SATURS

1.	KOPSAVILKUMS .....	4
1.1.	Konverģences jomas.....	5
1.2.	Problēmas.....	5
1.2.1.	Vispārīgie jautājumi .....	5
1.2.2.	Vispārīgi datu aizsardzības aspekti .....	6
1.2.3.	Par publisko iestāžu piekļuvi datiem, kas nosūtīti uz AK.....	8
1.3.	Secinājums.....	9
2.	IEVADS.....	10
2.1.	AK datu aizsardzības regulējums .....	10
2.2.	EDAK novērtējuma darbības joma .....	11
2.3.	Vispārīgas piezīmes un apsvērumi .....	12
2.3.1.	Starptautiskās saistības, ko uzņēmusies AK.....	12
2.3.2.	Iespējama novirzīšanās Apvienotās Karalistes datu aizsardzības regulējumā nākotnē .....	12
3.	VISPĀRĪGI DATU AIZSARDZĪBAS ASPEKTI .....	14
3.1.	Satura principi .....	14
3.1.1.	Tiesības piekļūt datiem, labot, dzēst tos un celt iebildumus .....	15
3.1.2.	Tālākas nosūtīšanas ierobežojumi .....	19
3.2.	Procesuālie un izpildes panākšanas mehānismi .....	26
3.2.1.	Kompetentā neatkarīgā uzraudzības iestāde .....	26
3.2.2.	Datu aizsardzības sistēma, kas nodrošina labu atbilstības līmeni.....	26
3.2.3.	Datu aizsardzības sistēmai jānodrošina atbalsts un palīdzība datu subjektiem, īstenojot viņu tiesības, kā arī atbilstoši tiesiskās aizsardzības mehānismi.....	27
4.	APVIENOTĀS KARALISTES PUBLISKO IESTĀŽU PIEKĻUVE PERSONAS DATIEM, KO NOSŪTA NO ES, UN TO IZMANTOŠANA .....	27
4.1.	Apvienotās Karalistes publisko iestāžu piekļuve datiem un to izmantošana krimināltiesību aizsardzības nolūkos .....	27
4.1.1.	Juridiskais pamats un piemērojamie ierobežojumi / aizsardzības pasākumi.....	27
4.1.2.	Savāktās informācijas turpmāka izmantošana tiesībaizsardzības nolūkos (140.–154. apsvērumi).....	30
4.1.3.	Uzraudzība.....	31
4.2.	Datu aizsardzības vispārējais tiesiskais regulējums nacionālās drošības jomā .....	31
4.2.1.	Nacionālās drošības sertifikāti .....	31
4.2.2.	Tiesības uz labošanu un dzēšanu.....	32

4.2.3. Ar nacionālo drošību saistīti atbrīvojumi .....	32
4.3. Apvienotās Karalistes publisko iestāžu piekļuve datiem un to izmantošana nacionālās drošības nolūkos.....	33
4.3.1. Juridiskais pamats, ierobežojumi un aizsardzības pasākumi — izmeklēšanas pilnvaras, ko izmanto nacionālās drošības kontekstā.....	33
4.3.2. Savāktās informācijas turpmāka izmantošana nacionālās drošības nolūkos un atklāšana ārvalstīs .....	42
4.3.3. Uzraudzība.....	45
4.3.4. Tiesiskā aizsardzība.....	47

## Eiropas Datu aizsardzības kolēģija,

ņemot vērā 70. panta 1. punkta s) apakšpunktu Eiropas Parlamenta un Padomes Regulā (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (turpmāk tekstā — VDAR),

ņemot vērā Eiropas Ekonomikas zonas (turpmāk tekstā — EEZ) līgumu un jo īpaši tā XI pielikumu un 37. protokolu, kas grozīts ar EEZ Apvienotās komitejas 2018. gada 6. jūlija Lēmumu Nr. 154/2018<sup>1</sup>,

ņemot vērā Reglamenta 12. un 22. punktu,

## IR PIEŅĒMUSI ŠO ATZINUMU.

### 1. KOPSAVILKUMS

1. Eiropas Komisija 2021. gada 19. februārī saskaņā ar VDAR apstiprināja īstenošanas lēmuma projektu (turpmāk tekstā — lēmuma projekts) par Apvienotās Karalistes (turpmāk tekstā — AK) nodrošinātu pienācīgu personas datu aizsardzību<sup>2</sup>. Pēc tam Eiropas Komisija uzsāka tā oficiālas pieņemšanas procedūru.
2. Tajā pašā dienā Eiropas Komisija lūdza Eiropas Datu aizsardzības kolēģijas (turpmāk tekstā — EDAK) atzinumu<sup>3</sup>. EDAK novērtējums par Apvienotajā Karalistē nodrošinātā aizsardzības līmeņa pietiekamību ir veikts, pamatojoties uz paša lēmuma projekta izskatīšanu, kā arī uz tās dokumentācijas analīzi, ko darījusi pieejamu Eiropas Komisija.
3. EDAK koncentrēja uzmanību uz lēmuma projekta vispārējo VDAR aspektu novērtēšanu un uz publisko iestāžu piekļuvi personas datiem, kas no EEZ nosūtīti tiesībaizsardzības un nacionālās drošības nolūkos, tostarp tiesiskās aizsardzības līdzekļiem, kas personām pieejami EEZ. EDAK arī novērtēja, vai AK tiesiskajā regulējumā paredzētie aizsardzības pasākumi ir ieviesti un vai tie ir efektīvi.
4. EDAK šim darbam kā galvenos atsauces dokumentus ir izmantojusi 2018. gada februārī pieņemto VDAR pietiekamības atsauci<sup>4</sup> un EDAK leteikumus 02/2020 attiecībā uz Eiropas būtiskajām garantijām uzraudzības pasākumiem<sup>5</sup>.

---

<sup>1</sup> Atsauces uz “dalībvalstīm” šajā atzinumā būtu jāsaprot kā atsauces uz “EEZ dalībvalstīm”.

<sup>2</sup> Sk. Eiropas Komisijas paziņojumu presei “Datu aizsardzība: Eiropas Komisija sāk procesu par personas datu plūsmām uz Apvienoto Karalisti”, 2021. gada 19. februāris, [https://ec.europa.eu/commission/presscorner/detail/lv/ip\\_21\\_661](https://ec.europa.eu/commission/presscorner/detail/lv/ip_21_661).

<sup>3</sup> Sk. iepriekšējo zemsvītras piezīmi.

<sup>4</sup> Sk. 29. panta darba grupas (WP) “Pietiekamības atsauci” (*Adequacy Referential*), kas pieņemta 2017. gada 28. novembrī, pēdējo reizi pārskatīta un pieņemta 2018. gada 6. februārī, WP254 rev.01 (ko apstiprinājusi EDAK, sk. <https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines>); (turpmāk tekstā — VDAR pietiekamības atsauce).

<sup>5</sup> Sk. EDAK 2020. gada 10. novembra leteikumus 02/2020 attiecībā uz Eiropas būtiskajām garantijām uzraudzības pasākumiem, [https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees\\_lv](https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_lv).

## 1.1. Konverģences jomas

5. Svarīgākais EDAK mērķis ir sniegt atzinumu Eiropas Komisijai par personām piedāvātā aizsardzības līmeņa pietiekamību AK. Ir svarīgi saprast, ka EDAK neuzskata, ka AK tiesiskajam regulējumam būtu jādublē Eiropas tiesību akti datu aizsardzības jomā.
6. Tomēr EDAK atgādina, ka, lai uzskatītu, ka aizsardzība nodrošināta pietiekamā līmenī, VDAR 45. pants un Eiropas Savienības Tiesas (turpmāk tekstā — EST) judikatūra paredz, ka trešās valsts tiesību aktiem jābūt saskaņā ar VDAR nostiprināto pamatprincipu būtību. Apvienotās Karalistes datu aizsardzības regulējums lielā mērā balstās uz ES datu aizsardzības regulējumu (konkrēti, VDAR un Eiropas Parlamenta un Padomes Direktīvu (ES) 2016/680, turpmāk tekstā — ES Tiesībaizsardzības direktīva jeb *LED*); tas izriet no fakta, ka AK ir bijusi ES dalībvalsts līdz 2020. gada 31. janvārim. Turklāt Apvienotās Karalistes 2018. gada Datu aizsardzības likums (*DPA 2018*), kas stājās spēkā 2018. gada 23. maijā un ar ko tika atcelts Apvienotās Karalistes 1998. gada Datu aizsardzības likums, precizē VDAR piemērošanu Apvienotās Karalistes tiesību aktos papildus ES Tiesībaizsardzības direktīvas transponēšanai, kā arī pilnvaru piešķiršanai un pienākumu uzlikšanai valsts datu aizsardzības uzraudzības iestādei, t. i., AK Informācijas komisāra birojam (turpmāk tekstā — *ICO*). Tāpēc EDAK atzīst, ka AK datu aizsardzības regulējumā lielākoties ir atspoguļojusi VDAR.
7. **Analizējot tādas trešās valsts tiesību aktus un praksi, kas vēl nesen ir bijusi ES dalībvalsts, ir acīmredzams, ka EDAK ir identificējusi daudzus aspektus, kas ir līdzvērtīgi pēc būtības.**
8. Datu aizsardzības jomā EDAK norāda, ka starp VDAR regulējumu un Apvienotās Karalistes tiesisko regulējumu ir cieši saskaņoti daži pamatnoteikumi, piemēram, jēdzieni (piemēram, “personas dati”; “personas datu apstrāde”; “datu pārzinis”); iemesli likumīgai un godprātīgai apstrādei likumīgos nolūkos; mērķa ierobežojums; datu kvalitāte un proporcionalitāte; datu saglabāšana, drošība un konfidencialitāte; pārredzamība; īpašās datu kategorijas; tieša tirdzniecība; automatizēta lēmumu pieņemšana un profilēšana.

## 1.2. Problēmas

9. Apvienotā Karaliste vēl nesen bija ES dalībvalsts; tāpēc, analizējot tās tiesību aktus un praksi, EDAK ir noteikusi daudzus aspektus, kas pēc būtības ir līdzvērtīgi. Tajā pašā laikā, ņemot vērā ne tikai tās lomu pietiekamības konstatējuma pieņemšanas procesā, bet arī laika ierobežojumus, EDAK ir nolēmusi koncentrēt uzmanību uz tiem aspektiem, kuriem, pēc tās domām, ir vajadzīga rūpīgāka un detalizētāka pārbaude.
10. Neskatoties uz to, problēmas joprojām pastāv, un EDAK uzskata, ka būtu plašāk jāvērtē turpmāk minētie jautājumi, lai nodrošinātu, ka tiek sasniegts pēc būtības līdzvērtīgs aizsardzības līmenis, un Eiropas Komisijai Apvienotajā Karalistē tie būtu rūpīgi jāuzrauga.

### 1.2.1. Vispārīgie jautājumi

11. Pirmā problēma, kas ir vispārīga rakstura, saistās ar AK tiesību sistēmas attīstības uzraudzību attiecībā uz datu aizsardzību kopumā. Patiešām, AK valdība ir norādījusi uz savu nodomu izstrādāt atsevišķu un neatkarīgu datu aizsardzības politiku ar iespējamu nodomu atkāpties no ES datu aizsardzības tiesību aktiem. Šādas politikas nostādnes AK tiesiskajā regulējumā vēl nav īstenojušās. Tomēr šī iespējamā **novirzīšanās** nākotnē **varētu radīt risku saglabāt no ES nosūtīto personas datu aizsardzības līmeni**. Tāpēc Eiropas Komisija tiek aicināta cieši uzraudzīt šādas izmaiņas, sākot no lēmuma par pietiekamību stāšanās spēkā, un veikt nepieciešamās darbības, tostarp vajadzības gadījumā grozīt un/vai apturēt šo lēmumu.

### 1.2.2. Vispārīgi datu aizsardzības aspekti

12. Pirmkārt, tā sauktais **“imigrācijas atbrīvojums”**, kas noteikts **2018. gada Datu aizsardzības likuma 2. pielikuma 1. daļas 4. punktā, ir “plaši” formulēts**. Tas jo īpaši attiecas arī uz gadījumiem, kad personas datus pārzinis nav ievācis imigrācijas kontroles nolūkā, bet tos darījis pieejamus citam pārzinim, kurš apstrādā šādus personas datus imigrācijas kontroles nolūkā.
13. EDAK aicina Eiropas Komisiju pārbaudīt pašreizējo stāvokli tiesvedībā *Open Rights Group & Anor, R (On the Application Of) pret Iekšlietu ministrijas valsts sekretāru un Anor [2019] EWHC 2562 (Admin)* un, tā kā šis spriedums nav galīgs (*res judicata*), pārbaudīt, vai pārsūdzētais spriedums to apstiprina vai tas tiek pārskatīts, ņemot vērā visus jaunākos lietas apstākļus šajā sakarā, un precizēt to lēmumā. **EDAK arī aicina Eiropas Komisiju lēmumā par pietiekamību sniegt papildu informāciju par imigrācijas atbrīvojumu<sup>6</sup>, konkrēti, attiecībā uz šāda plaša atbrīvojuma nepieciešamību un proporcionalitāti Apvienotās Karalistes tiesību aktos, jo īpaši ņemot vērā plašo *ratione personae* piemērošanas tvērumu**. Vienlaikus EDAK aicina Eiropas Komisiju sīkāk izpētīt, vai AK tiesiskajā regulējumā pastāv papildu aizsardzības pasākumi, vai arī tādi ir paredzami, piemēram, izmantojot juridiski saistošus instrumentus, kas papildinātu imigrācijas atbrīvojumu, uzlabojot tā paredzamību un datu aizsardzības pasākumus attiecībā uz datu subjektiem, ļaujot arī labāk un ātrāk novērtēt un uzraudzīt šādu nepieciešamību un proporcionalitātes prasības.
14. Otrkārt, lai arī EDAK atzīst, ka AK savā datu aizsardzības regulējumā lielākoties ir atspoguļojusi VDAR V nodaļu, EDAK ir identificējusi dažus AK tiesiskā regulējuma aspektus **attiecībā uz tālāku nosūtīšanu**, kas varētu mazināt to personas datu aizsardzības līmeni, kas nosūtīti no EEZ.
15. Patiešām, VDAR 44. pantā<sup>7</sup> noteikts, ka personas datu nosūtīšana un tālāka nosūtīšana notiek tikai tad, ja nemazinās VDAR garantētais fizisko personu aizsardzības līmenis. **Tas nozīmē, ka ne tikai AK tiesību aktiem jābūt “pēc būtības līdzvērtīgiem” ES tiesību aktiem attiecībā uz tādu personas datu apstrādi, kas saskaņā ar turpmāko lēmumu par pietiekamību tiek nosūtīti uz AK, bet arī to, ka Apvienotajā Karalistē piemērojami noteikumi attiecībā uz tālāku šo datu nosūtīšanu uz trešām valstīm nodrošina, ka joprojām tiks garantēts pēc būtības līdzvērtīgs aizsardzības līmenis.**
16. Lai gan EDAK atzīmē AK spēju saskaņā ar tās tiesisko regulējumu konstatēt teritorijas ar pietiekamu datu aizsardzības līmeni, ņemot vērā Apvienotās Karalistes datu aizsardzības regulējumu, EDAK vēlas uzsvērt, ka līdz šim šīs teritorijas varētu negūt labumu no lēmuma par pietiekamību, ko izdevusi Eiropas Komisija, un nenodrošināt aizsardzības līmeni, kas “pēc būtības ir līdzvērtīgs” garantētajam EEZ. Tas varētu radīt iespējamus riskus to personas datu aizsardzībā, kas nosūtīti no EEZ, īpaši tad, ja nākotnē Apvienotās Karalistes datu aizsardzības regulējums atšķirtos no ES *acquis*. Turklāt AK aizsardzības līmeni par pietiekamu jau ir atzinusi trešās valstīs, kurās saskaņā ar Direktīvu 95/46/EK<sup>8</sup>

---

<sup>6</sup> Arī kā iznākumu notiekošajā pārskatīšanā par imigrācijas atbrīvojuma izmantošanu, kā minēts AK valdības pietiekamības apspriešanas skaidrojumu 5. lpp., E3 iedaļa: 2. pielikums “Ierobežojumi”, 2020. gada 13. marts, [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> “Personas datus, kas tiek apstrādāti vai kurus ir paredzēts apstrādāt pēc nosūtīšanas uz trešo valsti vai starptautisku organizāciju, nosūta tikai tad, ja, ņemot vērā citus šīs regulas noteikumus, pārzinis un apstrādātājs ir ievērojuši šajā nodaļā paredzētos nosacījumus, ietverot arī personas datu tālāku nosūtīšanu no trešās valsts vai starptautiskās organizācijas uz citu trešo valsti vai citu starptautisku organizāciju. Piemēro visus šīs nodaļas noteikumus, lai nodrošinātu, ka nemazinās ar šo regulu garantētais fizisku personu aizsardzības līmenis.”

<sup>8</sup> Eiropas Parlamenta un Padomes Direktīva 95/46/EK (1995. gada 24. oktobris) par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (OV L 281, 23.11.1995., 31. lpp.).

aizsardzības līmeni par pietiekamu atzinusi Eiropas Komisija, savukārt Eiropas Komisija drīz pārskatīs šos konstatējumus, un šīs pārskatīšanas secinājumi vēl nav zināmi.

17. **Iepriekš minētajās situācijās Eiropas Komisijai būtu jāpilda uzraudzības funkcija, un, ja netiek saglabāts pēc būtības līdzvērtīgs no EEZ nosūtīto personas datu aizsardzības līmenis, Eiropas Komisijai būtu jāapsver lēmuma par pietiekamību grozīšana ar mērķi ieviest īpašus aizsardzības pasākumus no EEZ nosūtītajiem datiem un/vai lēmuma par pietiekamību apturēšana.**
18. **Attiecībā uz starptautiskajiem nolīgumiem, kas noslēgti starp AK un trešām valstīm,** Eiropas Komisija tiek aicināta izskatīt Apvienotās Karalistes datu aizsardzības regulējuma un tās starptautisko saistību mijiedarbību, kas pārsniedz Nolīgumu par piekļuvi elektroniskajiem datiem ar mērķi apkarot smagus noziegumus, kurš noslēgts starp AK un Amerikas Savienotajām Valstīm (turpmāk tekstā — ASV)<sup>9</sup> (turpmāk tekstā — AK un ASV *CLOUD* akta nolīgums), jo īpaši tādēļ, lai nodrošinātu aizsardzības līmeņa nepārtrauktību, ja personas dati tiek nosūtīti no ES uz AK, pamatojoties uz AK izdoto lēmumu par pietiekamību, un pēc tam nosūtīti uz citām trešām valstīm, kā arī nepārtraukti uzraudzīt un vajadzības gadījumā rīkoties, ja starptautisku nolīgumu noslēgšana starp Apvienoto Karalisti un trešām valstīm var apdraudēt personas datu aizsardzības līmeni ES.
19. Turklāt Eiropas Komisija tiek aicināta uzraudzīt, vai AK un ASV *CLOUD* akta nolīgums nodrošina atbilstošus papildu aizsardzības pasākumus, ņemot vērā attiecīgo datu kategoriju sensitivitātes līmeni un vienīgās prasības, lai pakalpojumu sniedzēji nosūtītu elektroniskos pierādījumus tiešā veidā, nevis tas notiktu starp iestādēm, kā arī izvērtēt, kādos apstākļos aizsardzības pasākumus var nodrošināt, pienācīgi pielāgojot ES un ASV jumta nolīgumu<sup>10</sup>.
20. Turklāt EDAK atzīmē, ka tālāka nosūtīšana var notikt arī no AK uz citu trešo valsti, pamatojoties uz **nosūtīšanas rīkiem saskaņā ar Apvienotajā Karalistē piemērojamajiem datu aizsardzības tiesību aktiem**<sup>11</sup>. Pēc *Schrems II*<sup>12</sup> EDAK aicina Eiropas Komisiju lēmumā par pietiekamību nodrošināt garantijas, ka nepieciešamie aizsardzības pasākumi tiks efektīvi ieviesti, ņemot vērā arī saņēmējas trešās valsts tiesību aktus.
21. Attiecībā uz to, ka Apvienotās Karalistes tiesību aktos nav nodrošināta **aizsardzība, kas paredzēta VDAR 48. pantā**, EDAK aicina Eiropas Komisiju sniegt papildu garantijas un īpašas atsauces uz Apvienotās Karalistes tiesību aktiem, kas nodrošina, ka aizsardzības līmenis saskaņā ar AK tiesisko regulējumu ir pēc būtības līdzvērtīgs aizsardzības līmenim, kas garantēts EEZ.
22. Attiecībā uz **procesuālajiem un izpildes panākšanas mehānismiem** EDAK norāda, ka neatkarīga uzraudzības iestāde un tās efektīva darbība, sistēma, kas nodrošina labu atbilstības līmeni, un piekļuves sistēma atbilstošiem tiesiskās aizsardzības mehānismiem, kas EEZ personām nodrošina līdzekļus, lai tās varētu izmantot savas tiesības un pārsūdzēt lēmumus, nesaskaroties ar

---

<sup>9</sup> Sk. Nolīgumu starp Lielbritānijas un Ziemeļīrijas Apvienotās Karalistes valdību un Amerikas Savienoto Valstu valdību par piekļuvi elektroniskajiem datiem ar mērķi apkarot smagus noziegumus, Vašingtona, ASV, 2019. gada 3. oktobris, <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> Sk. ES un ASV nolīgumu par personas informācijas aizsardzību saistībā ar noziedzīgu nodarījumu novēršanu, izmeklēšanu un atklāšanu, kā arī saukšanu pie kriminālatbildības par tiem, 2016. gada decembris (turpmāk tekstā — ES un ASV jumta nolīgums), [https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=LEGISSUM%3A3104\\_8](https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=LEGISSUM%3A3104_8).

<sup>11</sup> Sk. AK VDAR 46. un 47. pantu.

<sup>12</sup> Sk. *Schrems II*.

apgrūtināšiem šķēršļiem administratīvai un tiesiskajai aizsardzībai, ir būtiski elementi, kuriem jāraksturo Eiropas datu aizsardzības regulējumam atbilstošs datu aizsardzības regulējums.

23. EDAK atzīst, ka Apvienotā Karaliste lielākoties ir atspoguļojusi attiecīgos VDAR noteikumus Apvienotās Karalistes VDAR un 2018. gada Datu aizsardzības likumā; neskatoties uz to, Eiropas Komisija tiek aicināta pastāvīgi uzraudzīt visas tādas izmaiņas Apvienotās Karalistes tiesiskajā regulējumā un praksē, kas varētu izraisīt negatīvu ietekmi uz šīm jomām.

### 1.2.3. Par publisko iestāžu piekļuvi datiem, kas nosūtīti uz AK

24. EDAK atzīmē būtiskās izmaiņas AK tiesiskajā regulējumā, kas piemērojams drošības un izlūkošanas iestādēm, īpaši attiecībā uz sakaru datu pārtveršanu un iegūšanu. EDAK saprot, ka šīs izmaiņas cita starpā ir atbilde uz procesu, kas uzsākts EST un Eiropas Cilvēktiesību tiesā (turpmāk tekstā — ECT), un to nesējaiem spriedumiem šajā saistībā.
25. Konkrēti, EDAK atzinīgi vērtē faktu, ka Apvienotā Karaliste ir izveidojusi izmeklēšanas pilnvaru tiesu (turpmāk tekstā — IPT). IPT ir kompetenta izskatīt ne tikai lietas par izmeklēšanas pilnvaru izmantošanu tiesībaizsardzības iestādēs, bet arī izlūkdienestos. Tāpēc EDAK izpratnē IPT darbojas kā atbilstīga tiesa Eiropas Savienības Pamattiesību hartas (turpmāk tekstā — ES harta) 47. panta nozīmē.
26. Turklāt EDAK pozitīvi novērtē “tiesu komisāru” ieviešanu 2016. gada Izmeklēšanas pilnvaru likumā (turpmāk tekstā — *IPA 2016*) kā būtisku uzlabojumu. Tā saprot, ka svarīga tiesu komisāru funkcija ir atsevišķos gadījumos *ex ante* apstiprināt dažādus uzraudzības pasākumus, tostarp sakaru datu mērķorientētu pārtveršanu un lielapjoma iegūšanu (tā sauktā “dubultās bloķēšanas” procedūra).
27. Tomēr, lai novērtētu šā papildu uzraudzības līmeņa efektivitāti, EDAK uzskata, ka ir nepieciešams sīkāk precizēt scenārijus, saskaņā ar kuriem ir iespējama likumīga pārtveršana bez izmeklēšanas pilnvaru komisāra (turpmāk tekstā — *IPC*) vai tiesas komisāru apstiprinājuma, un aicina Eiropas Komisiju turpināt novērtēt un pierādīt, ka pat gadījumos, kad nepiemēro divkāršās bloķēšanas procedūru, AK tiesiskais regulējums paredz piemērotus aizsardzības pasākumus, tostarp izmantojot efektīvas *ex post* uzraudzības un pārsūdzības iespējas, kas ir piedāvātas personām, tādējādi nodrošinot aizsardzības līmeni, kas pēc būtības ir līdzvērtīgs ES nodrošinātajam.
28. Turklāt EDAK aicina Eiropas Komisiju sīkāk izvērtēt nosacījumus, ar kādiem var atsaukties uz steidzamību, un sniegt skaidrojumus par iespējām izmantot attiecīgo datu subjektu tiesības un iespējamās tiesiskās aizsardzības veidus, kas tiek piedāvāti saistībā ar ieviešanas operācijām iekārtās, īpaši attiecībā uz atkāpi saistībā ar divkāršās bloķēšanas procedūru.
29. Turklāt EDAK uzskata, ka ir nepieciešams sīkāk precizēt un novērtēt lielapjoma pārtveršanu, jo īpaši attiecībā uz atlasītāju atlasīšanu un piemērošanu, lai precizētu, cik lielā mērā piekļuve personas datiem atbilst EST noteiktajam sliekšnim un kādi aizsardzības pasākumi ir piemērojami, lai aizsargātu to personu pamattiesības, kuru dati tiek pārtverti šajā kontekstā, tostarp attiecībā uz datu glabāšanas periodiem. Īpaši noderīgs būtu kompetentu AK uzraudzības iestāžu neatkarīgs novērtējums. EDAK arī uzsver, ka vēl jo svarīgāks var būt fakts, ka “ar ārvalstīm saistīta saziņa”, kas ietilpst lielapjoma pārtveršanas prakses darbības jomā, nozīmē, ka AK datus varētu tieši pārtvert un ES apkopot lielā apjomā, tostarp attiecībā uz datiem, kas nosūtīti tranzītā starp ES un AK, tādējādi tas ietilpst lēmuma projekta darbības jomā. Ņemot vērā šā aspekta nozīmi, EDAK aicina Eiropas Komisiju cieši uzraudzīt notikumus šajā sakarā.
30. Joprojām attiecībā uz lielapjoma pārtveršanu EDAK uzsver ECT un EST konsekventu novērtējumu un atgādina par bažām, kas paustas saistībā ar sekundārajiem datiem, kuriem to sensitivitātes dēļ būtu



jāpiešķir īpaši aizsardzības pasākumi. Tāpēc EDAK aicina Eiropas Komisiju rūpīgi izvērtēt, vai AK tiesību aktos paredzētie aizsardzības pasākumi attiecībā uz šādu personas datu kategoriju nodrošina pēc būtības līdzvērtīgu aizsardzības līmeni tam, kāds garantēts EEZ.

31. Šajā kontekstā EDAK apzinās faktu, ka 2016. gada Izlūkošanas un drošības komitejas publiskais ziņojums par lielapjoma pilnvaru izmantošanu<sup>13</sup> attiecas uz praksi, kas izveidojusies saskaņā ar iepriekšējo tiesisko regulējumu, kurš vēlāk aizstāts ar *IPA 2016*. Neskatoties uz to, tā uzskata, ka kompetentajām AK uzraudzības iestādēm ir jāveic papildu neatkarīgs novērtējums un automatizēto apstrādes rīku izmantošanas uzraudzība, un aicina Eiropas Komisiju sīkāk novērtēt šo jautājumu un aizsardzības pasākumus, kas tiktu un/vai varētu tikt piešķirti EEZ datu subjektiem šajā saistībā.
32. EDAK piekrīt *IPC* paustajam viedoklim, ka ir nepieciešama turpmāka pārskatīšana un uzraudzība, lai nodrošinātu, ka tiek saglabāti un turpmāk uzlaboti aizsardzības pasākumi, ko kompetentās iestādes nacionālās drošības un izlūkošanas jomā piemēro praksē, lai novērstu neatbilstības attiecīgo tiesību aktu piemērošanā. EDAK atzinīgi vērtē arī faktu, ka līdz ar to *IPC* pārskatījis savu pieeju lielapjoma pārtveršanas pārbaudei 2019. gadā, *kas ietvēra rūpīgu pārskatīšanu attiecībā uz tehniski sarežģītajiem veidiem, kā faktiski notiek lielapjoma pārtveršana*, un apņēmas lielapjoma pārtveršanas pārbaudēs no 2020. gada un turpmāk iekļaut *atlasītāju un meklēšanas kritēriju detalizētu pārbaudi, uz ko iepriekš atsaucās ECT*. Ņemot vērā šā aspekta nozīmi, EDAK pauž bažas, ka *IPC* vēl nav veicis atlasītāju un meklēšanas kritēriju detalizētu pārbaudi, un aicina Eiropas Komisiju cieši uzraudzīt norises šajā saistībā, jo īpaši tāpēc, ka konkrētais šādas uzraudzības formāts vēl jāprecizē.
33. EDAK uzsver, ka attiecībā uz informācijas atklāšanu ārvalstīs AK tiesību aktos paredzētā nacionālās drošības atbrīvojuma piemērošana var novest pie tā, ka nav aizsardzības pasākumu, kuri nodrošina, ka tiek ievēroti arī mērķa ierobežošanas, nepieciešamības un proporcionalitātes principi, vai paredz, ka pietiekamas personas tiesības, uzraudzības un pārsūdzības tiesības tiktu nodrošinātas vai ievērotas arī galamērķa trešā valstī. Tāpēc EDAK iesaka Eiropas Komisijai sīkāk izskatīt Apvienotās Karalistes tiesību aktos paredzētos vispārējos aizsardzības pasākumus, kad runa ir par informācijas atklāšanu ārvalstīs, jo īpaši ņemot vērā nacionālās drošības atbrīvojumu piemērošanu.
34. Visbeidzot, EDAK pauž bažas par citiem informācijas apmaiņas un atklāšanas veidiem, pamatojoties uz citiem instrumentiem, jo īpaši uz dažādiem starptautiskajiem nolīgumiem, kurus Apvienotā Karaliste ir noslēgusi ar citām trešām valstīm, jo īpaši gadījumos, ja šie instrumenti joprojām nav pieejami sabiedrībai, piemēram, AK un ASV nolīgums par izlūkošanu sakaru jomā. Šāda nolīguma sekas varētu būt to aizsardzības pasākumu apiešana, kas noteikti attiecībā uz piekļuvi personas datiem un to izmantošanu nacionālās drošības nolūkos. EDAK uzskata, ka divpusēju vai daudzpusēju nolīgumu noslēgšana ar trešām valstīm izlūkošanas sadarbības nolūkā, nodrošinot juridisku pamatu personas datu tiešai pārtveršanai un iegūšanai vai personas datu nosūtīšanai uz šīm valstīm, var arī būtiski ietekmēt nosacījumus turpmākai apkopotās informācijas izmantošanai, jo šādi nolīgumi var ietekmēt novērtēto AK datu aizsardzības tiesisko regulējumu.

### 1.3. Secinājums

---

<sup>13</sup> Sk. Ziņojumu par lielapjoma pilnvaru pārskatīšanu, ko sagatavojis terorisma novēršanas tiesību aktu neatkarīgais pārskatītājs, 2016. gada augusts, <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf>.

35. EDAK uzskata, ka AK pietiekamības novērtējums ir unikāls, jo AK ir bijušās ES dalībvalsts statuss. Turklāt tas būtu arī pirmais lēmums par pietiekamību, kurā iekļauta turpināmības klauzula.
36. Attiecīgi EDAK atzīst daudzas AK un ES datu aizsardzības regulējumu konverģences jomas. Tomēr vienlaikus un pēc rūpīgas Eiropas Komisijas lēmuma projekta un Apvienotās Karalistes datu aizsardzības tiesību aktu analīzes EDAK ir identificējusi vairākas problēmas, kuras šajā atzinumā tiek plaši izskatītas. Šajā kontekstā EDAK vēlas uzsvērt Eiropas Komisijas svarīgo lomu visu attiecīgo norišu uzraudzībā AK.
37. Ņemot vērā iepriekš minēto, EDAK iesaka Eiropas Komisijai risināt šajā atzinumā uzskaitītās problēmas. EDAK arī aicina Eiropas Komisiju cieši uzraudzīt visas attiecīgās norises Apvienotajā Karalistē, kas var ietekmēt personas datu aizsardzības līmeņa būtisku līdzvērtīgumu, un nepieciešamības gadījumā ātri veikt atbilstošas darbības.

## 2. IEVADS

### 2.1. AK datu aizsardzības regulējums

38. Apvienotās Karalistes datu aizsardzības regulējums lielā mērā balstās uz ES datu aizsardzības regulējumu (jo īpaši VDAR un *LED*); tas izriet no fakta, ka AK līdz 2020. gada 31. janvārim bija ES dalībvalsts. Turklāt Apvienotās Karalistes 2018. gada Datu aizsardzības likumā, kas stājās spēkā 2018. gada 23. maijā un atcēla Apvienotās Karalistes 1998. gada Datu aizsardzības likumu, precizē VDAR piemērošanu AK tiesību aktos papildus ES Tiesībaizsardzības direktīvas transponēšanai, kā arī pilnvaru piešķiršanai un pienākumu uzlikšanai valsts datu aizsardzības uzraudzības iestādei — AK ICO.
39. Kā minēts Eiropas Komisijas lēmuma projekta 12. apsvērumā, AK valdība pieņēma 2018. gada Eiropas Savienības (Izstāšanās) likumu, kas tieši piemērojamos ES tiesību aktus iekļauj Apvienotās Karalistes tiesību aktos. Saskaņā ar šo likumu AK ministriem ir pilnvaras ar likumīgiem instrumentiem ieviest sekundāros tiesību aktus, lai pēc AK izstāšanās no ES veiktu nepieciešamās izmaiņas spēkā saglabātajos ES tiesību aktos un tie atbilstu vietējam kontekstam.
40. Līdz ar to attiecīgo tiesisko regulējumu, kas AK piemērojams pēc pārejas perioda<sup>14</sup> beigām, veido šādi dokumenti:
  - Apvienotās Karalistes Vispārīgā datu aizsardzības regula (turpmāk tekstā — AK VDAR), kas iekļauta Apvienotās Karalistes tiesību aktos saskaņā ar 2018. gada Eiropas Savienības (Izstāšanās) likumu, kurā grozījumi izdarīti ar 2019. gada *DPPEC* noteikumiem (datu aizsardzība, privātums un elektroniskie sakari (grozījumi utt.) (izstāšanās no ES)),
  - 2018. gada Datu aizsardzības likums (turpmāk tekstā — *DPA 2018*), kurā grozījumi izdarīti ar 2019. gada *DPPEC* noteikumiem un 2020. gada Datu aizsardzības, privātuma un elektronisko sakaru (grozījumi utt.) (izstāšanās no ES) noteikumiem,
  - *IPA 2016*.

(Kopā — AK datu aizsardzības regulējums)

---

<sup>14</sup> Pārejas periods ir noteikts 2020. gada 31. decembrī, pēc kura ES tiesību akti AK vairs netiek piemēroti. "Pārejas periods" termiņš ir noteikts vēlākais 2021. gada 30. jūnijā, un tas attiecas uz papildu periodu, kurā personas datu nosūtīšana no EEZ uz AK netiek uzskatīta par nosūtīšanu.

## 2.2. EDAK novērtējuma darbības joma

41. Eiropas Komisijas lēmuma projekts ir rezultāts, kas sasniegts Apvienotās Karalistes datu aizsardzības regulējuma novērtējumā, pēc kura notika apspriešanās ar Apvienotās Karalistes valdību. Paredzams, ka saskaņā ar VDAR 70. panta 1. punkta s) apakšpunktu EDAK sniegs neatkarīgu atzinumu par Eiropas Komisijas konstatējumiem, identificēs trūkumus pietiekamības regulējumā, ja tādi ir, un centīsies iesniegt priekšlikumus to novēršanai.
42. Kā minēts VDAR pietiekamības atsaucē: *Eiropas Komisijas sniegtajai informācijai vajadzētu būt izsmelšai, un EDAK jāspēj veikt savu novērtējumu attiecībā uz datu aizsardzības līmeni trešā valstī<sup>15</sup>.*
43. Šajā saistībā jāatzīmē, ka EDAK tikai daļēji savlaicīgi saņēma dokumentus, kas attiecas uz AK tiesiskā regulējuma pārbaudi. EDAK lielāko daļu AK tiesību aktu, kas minēti lēmuma projektā, saņēma, izmantojot saites, uz kurām tā atsaukusies minētajā dokumentā. Eiropas Komisija nevarēja sniegt EDAK rakstiskus paskaidrojumus un informāciju no Apvienotās Karalistes par tādu apmaiņu starp Apvienotās Karalistes iestādēm un Eiropas Komisiju, kas attiecas uz šo uzdevumu<sup>16</sup>.
44. Ņemot vērā iepriekš minēto un ierobežoto laika periodu (divi mēneši), kurā EDAK ir atļauts pieņemt šo atzinumu, EDAK ir izvēlējusies koncentrēt uzmanību uz dažiem konkrētiem lēmuma projektā izklāstītajiem jautājumiem un sniegt par tiem savu analīzi un atzinumu.
45. Analizējot tādas trešās valsts tiesību aktus un praksi, kas vēl nesen ir bijusi ES dalībvalsts, ir acīmredzams, ka EDAK ir identificējusi daudzus aspektus, kas ir līdzvērtīgi pēc būtības. Ņemot vērā savu lomu pietiekamības konstatējuma pieņemšanas procesā un analizējamo tiesību aktu un prakses apjomu, EDAK ir nolēmusi koncentrēt savu uzmanību uz tiem aspektiem, kurus visvairāk nepieciešams aplūkot tuvāk. Turklāt saskaņā ar EST judikatūru ļoti svarīga analīzes daļa attiecas uz nacionālās drošības piekļuves tiesisko režīmu attiecībā uz personas datiem, kas nosūtīti uz AK, un nacionālās drošības sistēmas īstenoto praksi AK. Tomēr jāpatur prātā, ka nacionālā drošība acīmredzami ir tā tiesību aktu un prakses joma, kurā dalībvalstu tiesību akti nav saskaņoti ES līmenī un tāpēc var atšķirties.
46. EDAK ņēma vērā piemērojamo Eiropas datu aizsardzības regulējumu, tostarp ES hartas 7., 8. un 47. pantu, ar kuriem attiecīgi tiek aizsargātas tiesības uz privāto un ģimenes dzīvi, tiesības uz personas datu aizsardzību un tiesības uz efektīvu tiesību aizsardzību un taisnīgu tiesu; un 8. pantu Eiropas Cilvēktiesību konvencijā (turpmāk tekstā — ECTK), ar kuru tiek aizsargātas tiesības uz privāto

---

<sup>15</sup> Sk. WP254 rev.01, 3. lpp.

<sup>16</sup> Attiecībā uz: VDAR 48. pantu (lēmuma projekta 78. zemsvītras piezīme); pastiprinātiem aizsardzības pasākumiem un drošības pasākumiem, ko pārziņi piemēro, apstrādājot datus nacionālās drošības kontekstā (lēmuma projekta 64. zemsvītras piezīme); prasību pārziņim apsvērt, vai ir nepieciešams paļauties uz atbrīvojumu katrā gadījumā atsevišķi, pat ja ir izsniegts nacionālās drošības sertifikāts (lēmuma projekta 126. apsvērums un 172. zemsvītras piezīme); faktu, ka ES un ASV jumta nolīguma aizsardzības pasākumi tiks piemēroti visiem personas datiem kas sagatavoti vai saglabāti saskaņā ar AK un ASV CLOUD akta nolīgumu, neatkarīgi no pieteikuma iesniedzējas iestādes veida vai būtības, ņemot vērā tādas sīkākas detaļas datu aizsardzības pasākumu īstenošanā, par kurām joprojām notiek apspriešanās starp AK un ASV, apstiprinājumu, ka AK iestādes ļaus šim nolīgumam stāties spēkā tikai pēc tam, kad tās būs pārliecinātas, ka tā īstenošana atbilst tajā paredzētajām juridiskajām saistībām, tostarp skaidrībai par datu aizsardzības standartu ieviešanu attiecībā uz visiem datiem, kas pieprasīti saskaņā ar šo nolīgumu (lēmuma projekta 153. apsvērums); situācijām, kad dati tiek nosūtīti no ES uz AK šā lēmuma projekta tvērumā, un faktu, ka vienmēr pastāvēs "Britu salu savienojums", un uz jebkādiem iekārtu traucējumiem, kas skar šādus datus, tādējādi attiektos prasība par obligātajām garantijām saskaņā ar IPA 2016 13. panta 1. punktu (lēmuma projekta 206. apsvērums); un sniegtajiem darbības nolūku piemēriem (lēmuma projekta 216. apsvērums un 369. zemsvītras piezīme).

un ģimenes dzīvi. Papildus iepriekš minētajam EDAK ņēma vērā VDAR prasības, kā arī attiecīgo judikatūru.

47. Šā uzdevuma mērķis ir sniegt Eiropas Komisijai atzinumu par aizsardzības līmeņa pietiekamības novērtējumu Apvienotajā Karalistē. Jēdzienu “pietiekams aizsardzības līmenis”, kas bija ietverts jau Direktīvā 95/46/EK, turpināja attīstīt EST. Ir svarīgi atgādināt standartu, kādu EST ir noteikusi lietā *Schrems I*, proti — lai gan aizsardzības līmenim trešā valstī jābūt pēc būtības līdzvērtīgam ES garantētajam līmenim, — “*līdzekļi, pie kuriem šī trešā valsts ņemas šādas aizsardzības nodrošināšanai, var atšķirties no tiem, kas tikuši likti lietā [ES]*”<sup>17</sup>. Tāpēc mērķis nav Eiropas tiesību aktu precīzs atspoguļojums, bet gan šo izskatāmo tiesību aktu būtisko prasību un pamatprasību noteikšana. Pietiekamību var panākt, apvienojot datu subjektu tiesības un to personu pienākumus, kuras datus apstrādā vai arī kuras īsteno kontroli pār šādu apstrādi un neatkarīgu struktūru veiktu uzraudzību. Tomēr datu aizsardzības noteikumi ir efektīvi tikai tad, ja tie ir izpildāmi un tiek ievēroti praksē. Tāpēc ir jāņem vērā ne tikai to noteikumu saturs, kuri attiecas uz personas datiem, kas nosūtīti uz trešo valsti vai starptautisku organizāciju, bet arī ieviestā sistēma, kas nodrošina šādu noteikumu efektivitāti. Efektīvi izpildes panākšanas mehānismi ir ārkārtīgi svarīgi, lai nodrošinātu datu aizsardzības noteikumu efektivitāti<sup>18</sup>.

## 2.3. Vispārīgas piezīmes un apsvērumi

### 2.3.1. Starptautiskās saistības, ko uzņēmusies AK

48. Saskaņā ar VDAR 45. panta 2. punkta c) apakšpunktu un VDAR pietiekamības atsauci<sup>19</sup>, izvērtējot trešās valsts aizsardzības līmeņa pietiekamību, Eiropas Komisija cita starpā ņem vērā arī starptautiskās saistības, kuras trešā valsts ir uzņēmusies, vai citus pienākumus, kas izriet no trešās valsts dalības daudzpusējās vai reģionālās sistēmās, jo īpaši attiecībā uz personas datu aizsardzību, kā arī šādu pienākumu īstenošanu. Turklāt būtu jāņem vērā trešās valsts pievienošanās Eiropas Padomes 1981. gada 28. janvāra Konvencijai par personu aizsardzību attiecībā uz personas datu automātisko apstrādi (turpmāk tekstā — 108. konvencija)<sup>20</sup> un tās Papildu protokolam<sup>21</sup>.
49. **Šajā saistībā EDAK atzinīgi vērtē to, ka AK ir pievienojusies ECTK un ir ECT jurisdikcijā. Turklāt Apvienotā Karaliste ir arī pievienojusies 108. konvencijai un tās Papildu protokolam, 2018. gadā ir parakstījusi 108+ konvenciju<sup>22</sup>, un pašlaik strādā pie tās ratifikācijas.**

### 2.3.2. Iespējama novirzīšanās Apvienotās Karalistes datu aizsardzības regulējumā nākotnē

50. Kā minēts lēmuma projekta 281. apsvērumā, Eiropas Komisijai ir jāņem vērā, ka, beidzoties Izstāšanās līgumā<sup>23</sup> paredzētajam pārejas periodam, Apvienotā Karaliste administrēs, piemēros un īstenos savu datu aizsardzības režīmu, un tiklīdz ES un Apvienotās Karalistes tirdzniecības un

<sup>17</sup> Sk. EST, C-362/14, *Maximilian Schrems / Data Protection Commissioner*, 2015. gada 6. oktobris, ECLI:EU:C:2015:650 (turpmāk tekstā — *Schrems I*), 73.–74. punkts.

<sup>18</sup> Sk. WP254, rev.01, 2. lpp.

<sup>19</sup> Sk. WP254, rev.01, 2. lpp.

<sup>20</sup> Sk. Konvenciju par personu aizsardzību attiecībā uz personas datu apstrādi, 108. konvencija, 1981. gada 28. janvāris.

<sup>21</sup> Sk. Konvencijas par personu aizsardzību attiecībā uz personas datu automātisku apstrādi Papildu protokolu par uzraudzības institūcijām un pārrobežu datu plūsmām, kas atvērts parakstīšanai 2001. gada 8. novembrī.

<sup>22</sup> Sk. Protokolu, ar ko groza Konvenciju par personu aizsardzību attiecībā uz personas datu automātisku apstrādi (108+ konvencija), 2018. gada 18. maijs.

<sup>23</sup> Sk. Līgumu par Lielbritānijas un Ziemeļīrijas Apvienotās Karalistes izstāšanos no Eiropas Savienības un Eiropas Atomenerģijas kopienas (OV L 029, 31.1.2020., 7. lpp.).

sadarbības nolīguma<sup>24</sup> FINPROV.10.A pantā paredzētais pārejas noteikums vairs netiks piemērots, tas jo īpaši var ietvert grozījumus vai izmaiņas lēmuma projektā novērtētajā datu aizsardzības regulējumā, kā arī citas būtiskas izmaiņas.

51. Tāpēc Eiropas Komisija ir nolēmusi lēmuma projektā iekļaut turpināmības klauzulu<sup>25</sup>, nosakot tā beigu termiņu četrus gadus pēc tā stāšanās spēkā.
52. Ir svarīgi atzīmēt, ka AK ministru un AK valsts sekretāra iespēja ieviest sekundāros tiesību aktus pēc pārejas perioda beigām nākotnē var novest pie būtiskas AK un ES datu aizsardzības regulējumu atšķirības.
53. Patiešām, Apvienotās Karalistes valdība ir norādījusi uz savu nodomu izstrādāt atsevišķu un neatkarīgu datu aizsardzības politiku, kas savā kursā pēc tam var novirzīties no ES datu aizsardzības tiesību aktiem<sup>26</sup>. Šis nodoms ietver personas datu aspektu iekļaušanu tirdzniecības nolīgumos<sup>27</sup>, praksi, kas rada risku pazemināt Apvienotās Karalistes paredzēto personas datu aizsardzības līmeni<sup>28</sup>.
54. Visbeidzot, kopš pārejas perioda beigām AK vairs nav saistoša EST judikatūra, turklāt jau pieņemtie EST spriedumi, kas AK tiesiskajā regulējumā tiek uzskatīti par saglabātu judikatūru, varētu nebūt saistoši AK, jo īpaši tāpēc, ka Apvienotajai Karalistei ir iespēja mainīt saglabāto ES tiesību aktu pēc pārejas perioda beigām un tās Augstajai tiesai nav saistoša nekāda saglabātā ES judikatūra<sup>29</sup>.
55. **Nemot vērā riskus, kas saistīti ar iespējamo AK datu aizsardzības regulējuma novirzīšanos no ES *acquis* pēc pārejas perioda beigām, EDAK atzinīgi vērtē Eiropas Komisijas lēmumu ieviest četru**

---

<sup>24</sup> Sk. Tirdzniecības un sadarbības nolīgumu starp Eiropas Savienību un Eiropas Atomenerģijas kopienu, no vienas puses, un Lielbritānijas un Ziemeļīrijas Apvienoto Karalisti, no otras puses (OV L 444, 31.12.2020., 14. lpp.).

<sup>25</sup> Sk. galīgā lēmuma 4. pantu. Sk. arī lēmuma projekta 282. apsvērumu.

<sup>26</sup> Apvienotās Karalistes Nacionālajā datu stratēģijā (pēdējo reizi atjaunināta 2020. gada 9. decembrī, <https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy>) kā viens no tās uzdevumiem ir iekļautas šādas darbības: “*Starptautiskās datu plūsmas pastiprināšana. Pārrobežu informācijas plūsma veicina pasaules darījumdarbību, piegādes ķēdes un tirdzniecību, stimulējot izaugsmi visā pasaulē. Tai ir arī plašāka loma sabiedrībā. Personas datu nosūtīšana nodrošina cilvēku algu izmaksāšanu un palīdz cilvēkiem sazināties ar tuviniekiem no tālienes. Un, kā to ir pierādījusi koronavīrusa pandēmija, veselības datu kopīgošana var palīdzēt svarīgiem zinātniskiem pētījumiem par slimībām, vienlaikus apvienojot valstis reaģēšanā uz ārkārtas veselības problēmām pasaulē. Pēc izstāšanās no Eiropas Savienības AK atbalstīs ieguvumus, ko var sniegt dati. Mēs veicināsim vietējo paraugpraksi un sadarbosimies ar starptautiskajiem partneriem, lai novērstu, ka datus nepietiekami ierobežo valstu robežas un sadrumstaloti regulēšanas režīmi, un lai tos varētu izmantot pilnībā.*” (izcēlums pievienots).

<sup>27</sup> Sk. iepriekšējo zemsvītras piezīmi: “*Pārrobežu datu plūsmu veicināšana. Mēs strādāsim globālā līmenī, lai novērstu nevajadzīgus šķēršļus starptautiskām datu plūsmām. Savās tirdzniecības sarunās vienosimies par vērienīgiem datu noteikumiem un izmantosim savu tikko iegūto neatkarīgo vietu Pasaules Tirdzniecības organizācijā, lai ietekmētu labāku datu tirdzniecības noteikumu pieņemšanu. Novērsīsim šķēršļus starptautiskai datu nosūtīšanai, kas atbalsta izaugsmi un inovāciju, tostarp attīstot jaunu AK spēju, kas nodrošina jaunus un inovatīvus mehānismus starptautiskai datu nosūtīšanai. Turklāt strādāsim arī ar partneriem G20, lai izveidotu sadarbību starp valstu datu režīmiem un samazinātu traucējumus, kas var rasties, nosūtot datus starp dažādām valstīm.*” (izcēlums pievienots).

<sup>28</sup> Sk. Eiropas Parlamenta 2017. gada 12. decembra rezolūcijas par virzību uz digitālās tirdzniecības stratēģiju (2017/2065(INI)) V iedaļu, kurā uzsvērts, ka “*personas datu aizsardzība nav apspriežama [ES] tirdzniecības nolīgumos*”, pieejama vietnē: [https://www.europarl.europa.eu/doceo/document/TA-8-2017-0488\\_LV.pdf](https://www.europarl.europa.eu/doceo/document/TA-8-2017-0488_LV.pdf). Sk. arī Eiropas Parlamenta 2021. gada 25. marta rezolūcijas par Komisijas novērtējuma ziņojumu attiecībā uz Vispārīgās datu aizsardzības regulas īstenošanu divus gadus pēc tās piemērošanas 28. punktu, kurā minēts: “*atbalsta Komisijas praksi datu aizsardzību un personas datu plūsmas skatīt atsevišķi no tirdzniecības nolīgumiem*”, [https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111\\_LV.html](https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_LV.html).

<sup>29</sup> Sk. 2018. gada ES (Izstāšanās) likuma 6. panta 3.–6. punktu.

gadu turpināmības klauzulu lēmuma projektā. Tomēr EDAK šajā saistībā vēlas uzsvērt Eiropas Komisijas uzraudzības lomas nozīmi<sup>30</sup>. Patiešām, Eiropas Komisijai būtu nepārtraukti un pastāvīgi jāuzrauga visi attiecīgie notikumi Apvienotajā Karalistē, kas var ietekmēt to personas datu aizsardzības līmeņa būtisko līdzvērtīgumu, kuri tiek nosūtīti saskaņā ar AK izdoto lēmumu par pietiekamību kopš tā stāšanās spēkā. Turklāt Eiropas Komisijai būtu jāveic atbilstoša rīcība, lai apturētu, grozītu vai atceltu šo lēmumu par pietiekamību, pamatojoties uz konkrētiem apstākļiem, ja pēc lēmuma par pietiekamību pieņemšanas Eiropas Komisija saņemtu norādes, ka vairs netiek nodrošināts pietiekams aizsardzības līmenis AK.

56. No otras puses, EDAK pieliks visas pūles, lai informētu Eiropas Komisiju par visām attiecīgajām darbībām, ko komerciālā vai publiskā sektorā veikušas jebkuras dalībvalsts datu aizsardzības uzraudzības iestādes (turpmāk tekstā — UI), un jo īpaši par sūdzībām, ko iesnieguši datu subjekti EEZ par personas datu nosūtīšanu no EEZ uz AK.

### 3. VISPĀRĪGI DATU AIZSARDZĪBAS ASPEKTI

#### 3.1. Satura principi

57. VDAR pietiekamības atsauces 3. nodaļa ir veltīta “Satura principiem”. Tie ir jāiekļauj trešās valsts sistēmā, lai tās datu aizsardzības līmeni varētu uzskatīt par tādu, kas ir pēc būtības līdzvērtīgs ES garantētajam. EDAK atzīst faktu, ka Apvienotajai Karalistei nav kodificētas konstitūcijas, jo nav viena dokumenta, kurā būtu izklāstīti tās galvenie pamatnoteikumi. Tomēr tiesības uz privātās un ģimenes dzīves neaizskaramību (un tiesības uz datu aizsardzību kā daļu no šīm tiesībām) un tiesības uz lietas taisnīgu izskatīšanu<sup>31</sup> ir iekļautas 1998. gada Cilvēktiesību likumā, un šo likumā noteikto tiesību konstitucionālo vērtību ir atzinušas AK tiesas. 1998. gada Cilvēktiesību likumā ir iekļautas ECTK ietvertās tiesības<sup>32</sup>. Turklāt 1998. gada Cilvēktiesību likumā ir ietverts ļoti svarīgs noteikums, ka jebkurai publisko iestāžu darbībai jābūt saderīgai ar ECTK<sup>33</sup>.
58. Papildus strukturālajām un formālajām atšķirībām starp AK un ES tiesību aktiem EDAK atzīmē, kā bija sagaidāms, ka AK pieeja datu aizsardzībai ir līdzīga pieejai ES, kas izriet no fakta, ka Apvienotā Karaliste bija ES dalībvalsts līdz 2020. gada 31. janvārim. Tā rezultātā daudzi satura principi ir saskaņoti ar VDAR; tāpēc ir nodrošināts tāds aizsardzības līmenis, kas pēc būtības ir līdzvērtīgs ES nodrošinātajam. EDAK ir nolēmusi neturpināt veikt analīzi par tiem satura principiem, kas ir saskaņā ar ES tiesību aktiem, un ir gandarīta par analīzi, ko Eiropas Komisija sniedza savā lēmuma projektā. Šādi satura principi ir, piemēram, šādi: jēdzieni (piemēram, “personas dati”; “personas datu apstrāde”; “datu pārzinis”); iemesli likumīgai un godprātīgai apstrādei likumīgos nolūkos; mērķa ierobežojums; datu kvalitāte un proporcionalitāte; datu saglabāšana, drošība un konfidencialitāte; pārredzamība; īpašās datu kategorijas; tieša tirdzniecība; automatizēta lēmumu pieņemšana un profilēšana. EDAK turklāt norāda, ka Apvienotās Karalistes VDAR un *DPA 2018* ietver tādus satura principus, kas pārsniedz to, ko prasa VDAR pietiekamības atsauce, un atspoguļo VDAR iekļautos principus, tādējādi paaugstinot AK paredzēto aizsardzības līmeni. Šādi satura principi, piemēram, attiecas uz paziņojumiem par personas datu pārkāpumiem, datu aizsardzības speciālistu, datu aizsardzības ietekmes novērtējumu, integrētu datu aizsardzību un datu aizsardzību pēc noklusējuma.

<sup>30</sup> Sk. VDAR 45. panta 4. punktu.

<sup>31</sup> Sk. ECTK 6. un 8. pantu (1998. gada Cilvēktiesību likuma 1. pielikums).

<sup>32</sup> Plašāku informāciju sk. lēmuma projekta 8.–10. apsvērumā.

<sup>33</sup> Sk. 1998. gada Cilvēktiesību likuma 6. pantu.

59. Tomēr, kā minēts ievadā, EDAK šajā atzinumā vēlas īpaši pievērsties dažiem jautājumiem, par kuriem EDAK ir bažas, un vēlas lūgt Eiropas Komisijai skaidrojumus.

### 3.1.1. Tiesības piekļūt datiem, labot, dzēst tos un celt iebildumus

60. Tā dēvētais “imigrācijas atbrīvojums”, kas noteikts **DPA 2018 2. pielikuma 1. daļas 4. punktā**, ļauj pārziņiem, kas iesaistīti “imigrācijas kontrolē”, nepiemērot noteiktas datu subjektu tiesības, ko nodrošina *DPA 2018*, ja tas varētu *aizskart efektīvas imigrācijas kontroles uzturēšanu vai tādu darbību izmeklēšanu vai atklāšanu, kas grauj efektīvas imigrācijas kontroles uzturēšanu*.
61. Kā to atzinusi Eiropas Komisija lēmuma projektā<sup>34</sup> un kā minēts atzinumā, ko sniedz Eiropas Parlamenta *LIBE* komiteja par to, lai ES vārdā noslēgtu Tirdzniecības un sadarbības nolīgumu starp ES un AK<sup>35</sup>, šis atbrīvojums ir “**plaši**” formulēts. Tas attiecas uz šādām tiesībām: tiesības tikt informētam; piekļuves tiesības; tiesības uz datu dzēšanu; tiesības ierobežot apstrādi un tiesības iebilst.
62. Turklāt ir svarīgi atzīmēt, ka šis atbrīvojums attiecas arī uz gadījumiem, kad personas datus pārzinis nav ievācis imigrācijas kontroles nolūkā (“1. pārzinis”), bet viņš tos dara pieejamus citam pārzinim (“2. pārzinis”), kurš apstrādā šādus personas datus imigrācijas kontroles nolūkā (piemēram, AK Iekšlietu ministrija)<sup>36</sup>.
63. Lietā *Open Rights Group & Anor, R (On the Application Of) / Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin)* (2019. gada 3. oktobris) iesniedzēji apstrīdēja imigrācijas atbrīvojuma likumību, pamatojoties uz to, ka tas ir pretrunā VDAR 23. pantam un nav saderīgs ar tiesībām, kuras garantē ES hartas 7. un 8. pants par privātumu un personas datu

<sup>34</sup> Sk. lēmuma projekta 62.–65. apsvērumu.

<sup>35</sup> Šajā saistībā par **plašo** imigrācijas atbrīvojuma **formulējumu** sk. 10. punktu atzinumā, ko sniedz Pilsoņu brīvību, tieslietu un iekšlietu komiteja par to, lai Savienības vārdā noslēgtu Tirdzniecības un sadarbības nolīgumu starp Eiropas Savienību un Eiropas Atomenerģijas kopienu, no vienas puses, un Lielbritānijas un Ziemeļīrijas Apvienoto Karalisti, no otras puses, un Nolīgumu starp Eiropas Savienību un Lielbritānijas un Ziemeļīrijas Apvienoto Karalisti par drošības procedūrām klasificētas informācijas apmaiņai un aizsardzībai (2020/0382(NLE)), 2021. gada 5. februāris, [https://www.europarl.europa.eu/doceo/document/LIBE-AL-680848\\_LV.pdf](https://www.europarl.europa.eu/doceo/document/LIBE-AL-680848_LV.pdf), “šajā saistībā atgādina par Parlamenta 2020. gada februāra un jūnija rezolūcijām, kas norāda uz **vispārīgu un plašu atbrīvojumu** attiecībā uz personas datu apstrādi imigrācijas vajadzībām, kāds paredzēts Apvienotās Karalistes Datu aizsardzības likumā”, un 11. punktu: “uzskata, ka pirms spēkā esoša lēmuma par pietiekamību pieņemšanas ir jāgroza **vispārīgais un plašais atbrīvojums attiecībā uz personas datu apstrādi imigrācijas vajadzībām, kas noteikts Apvienotās Karalistes Datu aizsardzības likumā** (...)” (izcēlums pievienots).

<sup>36</sup> Sk. piemēru, kas sniegts *ICO Guide to the General Data Protection Regulation (GDPR)*, 2021. gada 1. janvāris, 307. lpp. (izcēlums pievienots): “Privāta organizācija (1. pārzinis) brīdina Iekšlietu ministriju (2. pārzinis) par darbinieku, kurš, domājams, ir iesniedzis nepatiesus dokumentus par savu identitāti un kvalifikāciju, lai iegūtu darbu. Darba devējs sniedz Iekšlietu ministrijai attiecīgo informāciju. Personas tiesības tikt informētai, ka tās personas dati ir nodoti Iekšlietu ministrijai, ir ierobežotas, ciktāl to īstenošana varētu kaitēt izmeklēšanai.

**Tāpēc darba devējam nav pienākuma informēt personu par to, ka tās personas dati nodoti Iekšlietu ministrijai, un savukārt Iekšlietu ministrijai nav pienākuma sniegt šai personai privātuma paziņojumu, ar ko šo personu informē, ka ministrija apstrādā viņas personas datus. Atbrīvojums vienādā mērā attiecas uz abiem pārziņiem.**

Tomēr darbinieks pieprasa savu personas datu kopiju Iekšlietu ministrijai, kas tagad par viņu veic izmeklēšanu. **Iekšlietu ministrija var pajauties uz atbrīvojumu, lai neatklātu daļu no savā rīcībā esošajiem datiem, ja to atklāšana varētu kaitēt izmeklēšanai. Ja darbinieks iesniegtu līdzīgu lūgumu savam darba devējam, arī tas tāpat varētu piemērot šo atbrīvojumu.**”

Citiem vārdiem sakot, kā precizēts 300. lpp., vairumā gadījumu Iekšlietu ministrija vai kāda no tās aģentūrām un darbuuzņēmējiem būs pārzinis, kurš piemēros šo atbrīvojumu. Tomēr ir svarīgi atzīmēt, ka šā atbrīvojuma piemērošana attiecas ne tikai uz Iekšlietu ministriju. Tas var būt aktuāls arī citiem pārziņiem, piemēram, darba devējiem, universitātēm un policijai, kas imigrācijas jautājumus uztur sakarus ar Iekšlietu ministriju.

aizsardzību. Anglijas un Velsas Augstā tiesa (turpmāk tekstā — Augstā tiesa) izskatīja, vai DPA 2018 2. pielikuma 1. daļas 4. punktā minētais imigrācijas atbrīvojums ir likumīgs, un lēma par labu tā likumībai.

64. Augstā tiesa jo īpaši uzskatīja, ka:

- “(..) imigrācijas atbrīvojums acīmredzami ir “svarīgu sabiedrības interešu” jautājums, un tam ir likumīgs mērķis (..)”, 30. punkts;
- “imigrācijas atbrīvojums atbilst prasībām, lai pasākums būtu saskaņā ar likumu. (..)”, 38. punkts;
- “uz imigrācijas atbrīvojumu var paļauties tikai tad un tiktāl, ciktāl “uzskaitīto VDAR noteikumu” ievērošana **varētu kaitēt** efektīvas imigrācijas kontroles uzturēšanai vai tādu darbību izmeklēšanai vai atklāšanai, kas grauj efektīvas imigrācijas kontroles uzturēšanu. Vārdi “varētu kaitēt” saistībā ar 1998. gada Datu aizsardzības likumu (kas bija spēkā pirms DPA 2018) tika interpretēti kā “ļoti nozīmīga un svarīga iespēja aizskart konkrētās sabiedrības intereses. Riska pakāpei jābūt tādai, lai šīm interesēm varētu kaitēt pat tad, ja risks nav ticamāks (..)”, 39. punkts (izcēlums pievienots).

65. Būtu jāatzīmē, ka šis spriedums saskaņā ar EDAK rīcībā esošajām ziņām nav galīgs un ir pārsūdzēts.

66. Kā norādīts EDAK pamatnostādņēs par ierobežojumiem saskaņā ar VDAR 23. pantu (“VDAR 23. panta pamatnostādnes”)<sup>37</sup>, “(..) VDAR kontekstā ierobežojumus **paredz atsevišķā leģislatīvajā pasākumā**, tie attiecas **uz ierobežotu skaitu datu tiesību subjektu un/vai pārziņa pienākumiem**, kas uzskaitīti VDAR 23. pantā, tajos **ievēro** attiecīgo pamattiesību un pamatbrīvību **būtību**, tie ir **nepieciešams un proporcionāls pasākums** demokrātiskā sabiedrībā un aizsargā kādu no VDAR 23. panta 1. punktā izklāstītajiem pamatiem (..)”<sup>38</sup>.

67. EDAK arī atgādina, ka VDAR 41. apsvērumā teikts, ka “[ja] šajā regulā atsaucas uz **juridisku pamatu vai leģislatīvu pasākumu**, tas obligāti nenozīmē, ka vajadzīgs parlamenta pieņemts leģislatīvs akts, neskarot prasības, kas izriet no attiecīgās dalībvalsts konstitucionālās kārtības. Tomēr šādam juridiskam pamatam vai leģislatīvam pasākumam vajadzētu būt **skaidram un precīzam un personām, uz kurām tas attiecas**, vajadzētu spēt paredzēt tā piemērošanu saskaņā ar Eiropas Savienības Tiesas (..) un Eiropas Cilvēktiesību tiesas judikatūru” (izcēlums pievienots).

68. Lai gan ECT precizējusi, ka attiecībā uz vārdiem “saskaņā ar likumu” un “ar likumu noteikts”, kas ir minēti ECTK 8.–11. pantā, ECTK norādīts, ka termins “likums” vienmēr ticis saprasts tā “saturiskajā”, nevis “formālajā” nozīmē; tas ietver gan “rakstiskos likumus”, kas aptver zemāka līmeņa noteikumu pieņemšanu, gan regulatīvos pasākumus, ko profesionālās regulatīvās iestādes veic saskaņā ar neatkarīgām noteikumu pieņemšanas pilnvarām, kuras tām deleģējis parlaments, kā arī nerakstītus likumus. “Likums” ir jāsaprot gan kā likums, gan kā **tiesnešu pieņemts “likums”**,<sup>39</sup> VDAR pamatnostādņu 23. pantā ir atgādināts, ka saskaņā ar EST judikatūru jebkuram **leģislatīvajam pasākumam**, kas pieņemts, pamatojoties uz VDAR 23. panta 1. punktu, jo īpaši **jāatbilst VDAR 23. panta 2. punktā noteiktajām īpašajām prasībām**. VDAR 23. panta 2. punktā ir noteikts, ka

<sup>37</sup> Sk. EDAK pamatnostādnes Nr. 10/2020 par ierobežojumiem saskaņā ar VDAR 23. pantu, 1.0. versija, pieņemtas 2020. gada 15. decembrī un pašlaik pēc sabiedriskās apspriešanas ir izstrādes nobeiguma posmā, [https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-102020-restrictions-under-article-23\\_en](https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-102020-restrictions-under-article-23_en).

<sup>38</sup> Sk. VDAR pamatnostādņu 23. panta 9. punktu, 5. lpp.

<sup>39</sup> Sk. ECT 2010. gada 14. septembra sprieduma 83. punktu lietā *Sanoma Uitgevers B.V. / Nīderlande*, EC:ECHR:2010:0914JUD003822403 (izcēlums pievienots).



leģislatīvie pasākumi, kas nosaka datu subjektu tiesību un pārziņu pienākumu ierobežojumus, attiecīgā gadījumā ietver **īpašus noteikumus par vairākiem turpmāk izklāstītajiem kritērijiem**. Parasti visas turpmāk sīki izklāstītās prasības **būtu jāiekļauj leģislatīvajā pasākumā, ar kuru nosaka ierobežojumus saskaņā ar VDAR 23. pantu**<sup>40</sup>.

69. Šajā saistībā var novērot, ka pats **imigrācijas atbrīvojums neietver šādus elementus, kas minēti VDAR 23. panta 2. punktā:**
- d) garantijas, kas novērš ļaunprātīgu izmantošanu vai nelikumīgu piekļuvi vai nosūtīšanu,
  - e) pārzinis vai pārzīņu kategorijas<sup>41</sup>,
  - g) riski attiecībā uz datu subjektu tiesībām un brīvībām,
  - h) datu subjektu tiesības saņemt informāciju par ierobežojumu, izņemot tad, ja tas var kaitēt ierobežojuma mērķim.
70. ICO izstrādātā *Guide to the General Data Protection Regulation (GDPR)*<sup>42</sup> ("Vispārīgās datu aizsardzības regulas (VDAR) rokasgrāmata"), tostarp nodaļa par imigrācijas atbrīvojumu, sniedz skaidrojumus par imigrācijas atbrīvojumu, taču pati par sevi **nevar** sniegt saistošus noteikumus, kas to papildina. Turklāt jautājums par likuma kvalitāti ir īpaši aktuāls, ņemot vērā ierobežoto tiesību un atbrīvojuma paplašināšanas nozīmi<sup>43</sup>.

---

<sup>40</sup> Sk. 23. pantu VDAR pamatnostādņēs, 45. un 46. punkts, 11. lpp. Atbilstīgi ES hartas 52. panta 3. punktam, "ciktāl Hartā ir ietvertas tiesības, kuras atbilst Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencijā garantētajām tiesībām, šo tiesību nozīme un apjoms ir tāds pats kā minētajā Konvencijā noteiktajām tiesībām. Šis noteikums neliedz Savienības tiesībās paredzēt plašāku aizsardzību". Attiecībā uz jēdzienu "**paredzēts likumā**" saskaņā ar ES hartas 52. panta 1. punktu būtu jāizmanto ECT izstrādātie kritēriji, kā ierosināts vairākos EST ģenerālvokāta atzinumos, piemēram, sk. atzinumus apvienotajās lietās C-203/15 un C-698/15, *Tele2 Sverige AB*, ECLI:EU:C:2016:572, 137.–154. punkts, un lietā C-70/10, *Scarlet Extended*, ECLI:EU:C:2011:255, 88.–114. punkts. Tādējādi cita starpā var atsaukties uz ECT spriedumu lietā *Weber and Saravia / Vācija*, 84. punkts: "Tiesa atkārtoti, ka izteiciens "**saskaņā ar likumu**" [ECTK] 8. panta 2. punkta nozīmē, pirmkārt, paredz, ka apstrīdētajam pasākumam vajadzētu būt kādam pamatam **valsts tiesību aktos**; tas attiecas arī uz attiecīgā **likuma kvalitāti**, paredzot, ka tam vajadzētu būt pieejamam attiecīgajai personai, kurai turklāt jāspēj paredzēt tā sekas attiecībā uz sevi, un saderīgam ar tiesiskumu" (izcēlums pievienots).

Sk. arī VDAR 41. apsvērumu: "šādam juridiskam pamatam vai leģislatīvam pasākumam vajadzētu būt **skaidram un precīzam un personām, uz kurām tas attiecas, vajadzētu spēt paredzēt tā piemērošanu saskaņā ar Eiropas Savienības Tiesas (...) un Eiropas Cilvēktiesību tiesas judikatūru**" (izcēlums pievienots).

<sup>41</sup> Sk. iepriekš minēto Augstās tiesas lietu, 54. punkts: "Manuprāt, nav nekā nelikumīga saistībā ar to, ka imigrācijas atbrīvojums ir pieejams **visiem datu pārziņiem**, kuri apstrādā datus norādītajiem mērķiem. Kā norāda atbildētāji, bez 4. punkta 3.–4. apakšpunkta imigrācijas atbrīvojums būtu spēkā neesošs gadījumos, kad dati tiek iegūti no trešām personām (piemēram, tādām kā vietējās pašvaldības vai VM leņēmumu un muitas dienests), lai uzturētu efektīvu imigrācijas kontroli." (izcēlums pievienots), tādējādi apstiprinot ierobežojumu **vispārēju** piemērošanu.

<sup>42</sup> *ICO Guide to the General Data Protection Regulation (GDPR)*, 2021. gada 1. janvāris, 299.–307. lpp.

<sup>43</sup> Sk. 57. punktu iepriekš minētajā Augstās tiesas lietā: "*Knights kungs man paziņo, ka komisārs beidz darbu norādījumu izstrādē par atbrīvojumu, taču tam būs "tiesību aktos noteikts" statuss tikai tādā nozīmē, ka to izdod, pamatojoties uz komisāra pilnvarām saskaņā ar VDAR 57. panta 1. punktu. Tam nebūs juridiska statusa saskaņā ar [DPA 2018](#)."*

ICO atbalstīto juridiski saistošo pamatnostādņu ieviešanas pamatojums ir konkrēti norādīts sprieduma 56.–60. punktā:

"56. Visbeidzot, es pievērsīšos komisāra apgalvojumam, ka, ja nav pievienotas tiesību aktos izklāstītās norādes, lai nodrošinātu aizsardzības pasākumus attiecībā uz imigrācijas atbrīvojuma nozīmi un piemērošanu,

71. Vēl jo vairāk, **“aizspriedumu pārbaudē”** nav noteikti aizsardzības pasākumi ļaunprātīgas izmantošanas vai nelikumīgas piekļuves vai nosūtīšanas novēršanai, un tie jāievieš, piemēram, Iekšlietu ministrijai.
72. Ņemot vērā visu iepriekš minēto, EDAK atzīmē, ka ir nepieciešami papildu paskaidrojumi par imigrācijas atbrīvojuma piemērošanu.
73. Turklāt EDAK norāda, ka trūkst juridiski saistoša instrumenta, kas paskaidro imigrācijas atbrīvojumu, lai apsvērtu, vai tas pēc būtības ir līdzvērtīgs VDAR 23. pantam un ES hartas 7. un 8. pantam. Tajā pašā laikā EDAK uzskata, ka Eiropas Komisijai ir jāpierāda plaša imigrācijas atbrīvojuma *ratione personae* nepieciešamība un proporcionalitāte, to pamatojot ar pierādījumiem.
74. **Noslēgumā EDAK aicina Eiropas Komisiju pārbaudīt pašreizējo stāvokli tiesvedībā *Open Rights Group & Anor, R (On the Application Of) / Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin)*, kā minēts iepriekš, un, tā kā šis spriedums nav galīgs (*res judicata*), pārbaudīt, vai tas ir apstiprināts vai pārskatīts ar pārsūdzēto spriedumu, ņemot vērā visus jaunākos lietas apstākļus šajā sakarā, un precizēt tos lēmumā par pietiekamību. EDAK arī aicina Eiropas**

---

*atbrīvojums nebūtu jāuzskata par VDAR 23. panta 1. punkta proporcionālu īstenošanu. Knight kungs uzskata, ka papildināts ar šādām norādēm šis noteikums ir proporcionāls.*

*57. Knight kungs man paziņo, ka komisārs beidz darbu norādījumu izstrādē par atbrīvojumu, taču tam būs “tiesību aktos noteikts” statuss tikai tādā nozīmē, ka to izdod, pamatojoties uz komisāra pilnvarām saskaņā ar VDAR 57. panta 1. punktu. Tam nebūs juridiska statusa saskaņā ar [DPA 2018](#). Es arī saprotu, ka Iekšlietu ministrija ir izstrādājusi personāla iekšējo norāžu projektu par imigrācijas atbrīvojumu (sk. iepriekš 22. punktu). Praksē komisāra izdotie norādījumi ir ietekmīgi neatkarīgi no to juridiskā pamata. Tomēr komisāram nav pilnvaru izdot tāda veida “saistošas” norādes, kādas Augstā tiesa paredzēja [Christian Institute](#) lietā (101. un 107. punkts). Šķiet, ka primārie tiesību akti būtu vajadzīgi, ja par nepieciešamiem uzskatītu norādījumus par imigrācijas atbrīvojumu ar tādu pašu statusu kā prakses kodeksi, kas pašlaik paredzēti [DPA 2018 121.–124. pantā](#).*

*58. Argumentā par likumā noteiktām norādēm Knight kungs apgalvo, ka konteksts, kurā radies nepieciešamība izmantot imigrācijas atbrīvojumu, noteikti rada bažas par tā pastāvēšanas un izmantošanas nepieciešamību un proporcionalitāti. Viņš vērš uzmanību uz diviem jautājumiem, jo īpaši juridiskajā kontekstā. Pirmkārt, personas dati, kuriem piemēro imigrācijas atbrīvojumu, pēc būtības, visticamāk, ietver datus par īpašām kategorijām VDAR 9. panta 1. punkta nozīmē (t. i., datus, kas “atklāj rases vai etnisko piederību”). Šādi dati ir noteikti VDAR, jo tiem ir nepieciešams augstāks aizsardzības līmenis ([Atzinums 1/15 \[2019\] 3 C.M.L.R. 25](#), 141. punkts). Otrkārt, Datu aizsardzības likuma pamat nodoms ir šāds: jo īpaši subjektu piekļuves tiesībām ir liela nozīme kā vārtejai, kas vajadzīga, lai varētu izmantot citas datu subjektiem piešķirtās tiesības (sk. [YS/Minister voor Immigratie, Integratie en Asiel \(C-141/12\) EU:C:2014:2081; \[2015\] 1 C.M.L.R. 18](#), 44. punkts).*

*59. Knight kungs identificē četrus praktiska rakstura jautājumus. Pirmkārt, ja pārzīņi nepaskaidro datu subjektiem, ka viņi ir paļāvušies uz likumā noteikto atbrīvojumu, un nesniedz plašu iemeslu kopsavilkumu, datu subjekts nezinās, ka ir piemērots atbrīvojums, un tā rezultātā nespēs to efektīvi apstrīdēt. Otrkārt, datu subjekti īpaši paļausies uz pārzīņiem, lai atbrīvojumu piemērotu uzmanīgi un tikai tik daudz, cik tas ir nepieciešams. Lai gan jebkuram datu subjektam ir tiesības sūdzēties komisāram par atbrīvojuma piemērošanu vai ierosināt tiesvedību tiesā, iespējams, ka datu subjekts nemaz nezinās par savām tiesībām un viņam trūks līdzekļu juridisku darbību veikšanai apstākļos, kad nepieciešama tūlītēja un precīza datu aizsardzības tiesību ievērošana. Treškārt, datu subjekts kā imigrants, iespējams, atrodas neaizsargātā stāvoklī. Ceturtkārt, tas nav abstrakts jautājums, ņemot vērā atbildētāju pierādījumus par imigrācijas atbrīvojuma izmantošanu (sk. 4. punktu iepriekš).*

*60. Knight kungs norāda, ka pastāv cieša saikne starp pašreizējo imigrācijas atbrīvojuma apstrīdēšanu un Tiesas pamatojumu lietā [Christian Institute \[2016\] UKSC 51](#). Tāpat kā [Christian Institute](#) lietā, viņš apgalvo, ka imigrācijas atbrīvojums ir plašs, tajā lietoti nedefinēti termini, piemērots zems sliekšnis, uz to attiecas kontrole, kas nav nešaubīgi attiecināma uz šo noteikumu, un tas attiecas uz ļoti plašu kontekstu un tiesību klāstu. Atšķirībā no [Christian Institute](#) lietas attiecībā uz imigrācijas atbrīvojumu nav publiski pieejamu norāžu, vēl jo mazāk — tiesību aktos noteikta statusa.”*

Komisiju sniegt papildu informāciju par imigrācijas atbrīvojuma nepieciešamību un proporcionalitāti, jo īpaši ņemot vērā plašo *ratione personae* piemērošanas tvērumu.

75. Vienlaikus EDAK aicina Eiropas Komisiju sīkāk izpētīt, vai AK tiesiskajā regulējumā pastāv papildu aizsardzības pasākumi, vai arī tādi ir paredzami, piemēram, izmantojot juridiski saistošus instrumentus, kas papildinātu imigrācijas atbrīvojumu, uzlabojot tā paredzamību, un aizsardzības pasākumus attiecībā uz datu subjektiem, ļaujot arī labāk un ātrāk novērtēt un uzraudzīt šādu nepieciešamību un proporcionalitātes prasības.

### 3.1.2. Tālākas nosūtīšanas ierobežojumi

76. VDAR 44. pantā noteikts, ka personas datu nosūtīšana un tālāka nosūtīšana notiek tikai tad, ja nemazinās VDAR garantētais fizisko personu aizsardzības līmenis. Tāpēc personas datiem, kas no EEZ nosūtīti uz Apvienoto Karalisti, pamatojoties uz lēmumu par pietiekamību, tiek piešķirts pēc būtības līdzvērtīgs aizsardzības līmenis tam, kāds paredzēts ES datu aizsardzības regulējumā. **Tas nozīmē, ka ne tikai AK tiesību aktiem jābūt “pēc būtības līdzvērtīgiem” ES tiesību aktiem attiecībā uz tādu personas datu apstrādi, kas saskaņā ar lēmuma projektu tiek nosūtīti uz AK, bet arī to, ka Apvienotajā Karalistē piemērojami noteikumi attiecībā uz tālāku šo datu nosūtīšanu uz trešām valstīm nodrošina, ka joprojām tiks garantēts pēc būtības līdzvērtīgs aizsardzības līmenis.**
77. Tādējādi ir svarīgi, lai personas datu no EEZ tālāka nosūtīšana no AK uz citu trešo valsti būtu pienācīgi aizsargāta ar aizsardzības pasākumiem vai tiktu veikta saskaņā ar noteikumiem par atkāpēm<sup>44</sup>, lai nodrošinātu ES tiesību aktos paredzētās aizsardzības nepārtrauktību. **Patiešām, ja šādu aizsardzību nevar nodrošināt, EEZ personas datu tālākai nosūtīšanai nevajadzētu notikt.**
78. EDAK atzīst, ka AK lielākoties VDAR V nodaļu ir atspoguļojusi Apvienotās Karalistes VDAR (44.–49. pants) un *DPA 2018*<sup>45</sup>. **Tomēr EDAK ir identificējusi dažus Apvienotās Karalistes tiesiskā regulējuma aspektus attiecībā uz tālāku nosūtīšanu, kas varētu mazināt no EEZ nosūtīto personas datu aizsardzības līmeni.**
79. **Pirmā problēma**, ko EDAK ir identificējusi, attiecas uz to, ka Apvienotā Karaliste saskaņā ar *DPA 2018* izstrādāto procedūru atzīst trešās valstis, starptautiskās organizācijas vai teritorijas<sup>46</sup> kā atbilstīgus saņēmējus. Patiešām, EEZ personas datu tālāka nosūtīšana var notikt no AK uz citām trešām valstīm, pamatojoties uz iespējamo turpmāko AK pietiekamības regulējumu<sup>47</sup>.
80. Konkrētāk, kā paskaidrots lēmuma projekta 77. apsvērumā, AK valsts sekretāram pēc apspriešanās ar ICO ir tiesības atzīt trešo valsti (vai teritoriju vai sektoru trešā valstī), starptautisku organizāciju vai šādas valsts, teritorijas, sektora vai organizācijas aprakstu par tādu, kas nodrošina pietiekamu personas datu aizsardzības līmeni<sup>48</sup>. Novērtējot aizsardzības līmeņa pietiekamību, AK valsts sekretāram jāņem vērā tie paši elementi, kas Eiropas Komisijai jāizvērtē saskaņā ar VDAR 45. panta 2. punkta a)–c) apakšpunktu un kas interpretējami kopā ar VDAR 104. apsvērumu un saglabāto ES judikatūru. Tas nozīmē, ka, novērtējot trešās valsts aizsardzības līmeņa pietiekamību, attiecīgais standarts būs tas, vai šī trešā valsts nodrošina aizsardzības līmeni, kas “pēc būtības ir līdzvērtīgs”

<sup>44</sup> Sk. AK VDAR 49. pantu.

<sup>45</sup> Sk. *DPA 2018* 17.A, 17.B, 17.C un 18. pantu.

<sup>46</sup> Sk. *DPA 2018* 17.A pantu.

<sup>47</sup> AK ekvivalents lēmumam par pietiekamību saskaņā ar VDAR.

<sup>48</sup> Sk. *DPA 2018* 182. panta 2. punktu. Sk. arī Saprāšanās memorandu par ICO lomu saistībā ar jauniem AK pietiekamības novērtējumiem, <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/>.

līmenim, kurš garantēts AK. Lai gan EDAK atzīmē AK spēju saskaņā ar AK VDAR konstatēt teritorijas ar pietiekamu datu aizsardzības līmeni, ņemot vērā Apvienotās Karalistes datu aizsardzības regulējumu, EDAK vēlas uzsvērt, ka līdz šim šīs minētās teritorijas varētu negūt labumu no lēmuma par pietiekamību, kuru izdevusi Eiropas Komisija un kurā atzīts aizsardzības līmenis, kas “pēc būtības ir līdzvērtīgs” ES garantētajam līmenim. Tas varētu radīt iespējamus riskus tādu personas datu aizsardzībā, kas nosūtīti no EEZ, īpaši tad, ja Apvienotās Karalistes datu aizsardzības regulējums nākotnē atšķirtos no ES *acquis*. Jāatzīmē, ka 2020. gada jūlijā *Schrems II* EST nozīmīgā lieta<sup>49</sup> izraisīja ASV Privātuma aizsardzības lēmuma atzīšanu par spēkā neesošu, jo saskaņā ar EST nevar uzskatīt, ka ASV tiesiskais regulējums nodrošina pēc būtības līdzvērtīgu aizsardzības līmeni salīdzinājumā ar ES. Tomēr jau pieņemtie EST spriedumi, kas AK tiesiskajā regulējumā tiek uzskatīti par saglabātu judikatūru, varētu vairs nebūt saistoši AK, jo īpaši tāpēc, ka Apvienotajai Karalistei ir iespēja mainīt saglabāto ES tiesību aktu pēc pārejas perioda beigām un tās Augstajai tiesai nav saistoša nekāda saglabātā ES judikatūra<sup>50</sup>.

81. **EDAK aicina Eiropas Komisiju cieši uzraudzīt AK iestāžu veikto pietiekamības novērtēšanas procesu un kritērijus attiecībā uz citām trešām valstīm, jo īpaši attiecībā tām uz trešām valstīm, kuru aizsardzības līmeni ES nav atzinusi par pietiekamu saskaņā ar VDAR. Ja Eiropas Komisija konstatē, ka trešā valsts, kuras aizsardzības līmeni Apvienotā Karaliste atzīst par pietiekamu, nenodrošina pēc būtības līdzvērtīgu aizsardzības līmeni tam, kāds garantēts ES, EDAK aicina Eiropas Komisiju veikt visus nepieciešamos pasākumus, piemēram, grozīt AK izdoto lēmumu par pietiekamību, lai ieviestu īpašus aizsardzības pasākumus attiecībā uz personas datiem, kuru izcelsme ir EEZ, un/vai apsvērt AK lēmuma par pietiekamību apturēšanu, ja personas dati, kas no EEZ nosūtīti uz AK, tiek nosūtīti tālāk uz attiecīgo trešo valsti, pamatojoties uz AK pietiekamības regulējumu.**
82. **Otra problēma** ir saistīta ar gaidāmo pārskatīšanu attiecībā uz jau esošo lēmumu par pietiekamību, ko Eiropas Komisija ir pieņēmusi saskaņā ar Direktīvu 95/46/EK. Pēc šīs pārskatīšanas Eiropas Komisija varētu nolemt, ka dažas valstis, kuras līdz šim guva labumu no lēmuma par pietiekamību, vairs nenodrošina pēc būtības līdzvērtīgu aizsardzības līmeni, ņemot vērā pašreizējos ES tiesību aktus un jaunāko judikatūru. Tomēr, kā paredzēts *DPA 2018* 21. pielikuma 4. punktā, AK jau ir atzinusi šīs valstis par valstīm, kas nodrošina pietiekamu aizsardzības līmeni. Lai arī AK valsts sekretāram četru gadu laikā jāpārskata šie pietiekamības konstatējumi, Eiropas Komisija savā lēmuma projektā atzīmē, ka šie pietiekamības konstatējumi automātiski nepārstās pastāvēt, ja AK valsts sekretārs neveiks prasīto pārskatīšanu noteiktajā četru gadu termiņā<sup>51</sup>.
83. **EDAK aicina Eiropas Komisiju uzraudzīt, vai pēc tam, kad ES būs veikusi jau esošā lēmuma par pietiekamību pārskatīšanu, Apvienotā Karaliste valsti, kurā aizsardzība vairs netiek nodrošināta pietiekamā līmenī, uzskatīs par tādu, kurā aizsardzības līmenis joprojām ir pietiekams. Šādā gadījumā EDAK aicina Eiropas Komisiju, pamatojoties uz lēmuma projekta 277.–280. apsvērumu, veikt visus attiecīgos pasākumus, lai situāciju labotu, piemēram, grozot lēmumu par pietiekamību, lai pievienotu īpašas prasības attiecībā uz personas datiem, kuru izcelsme ir no EEZ, un/vai apturot lēmumu par pietiekamību, ja personas dati, kas no EEZ nosūtīti uz AK, tiek tālāk nosūtīti uz attiecīgo trešo valsti. EDAK aicina Eiropas Komisiju turpināt šo uzraudzību visā AK lēmuma par pietiekamību darbības laikā.**
84. **Trešā problēma** attiecas uz personas datu tālāku nosūtīšanu no EEZ uz valstīm, kuru aizsardzības līmenis nav pietiekams, pamatojoties uz nosūtīšanas rīkiem, kas paredzēti AK VDAR 46. un 47. pantā.

---

<sup>49</sup> Sk. *Schrems II*.

<sup>50</sup> Sk. 2018. gada ES (Izstāšanās) likuma 6. panta 3.–6. punktu.

<sup>51</sup> Sk. lēmuma projekta 82. apsvērumu.

Lai gan AK VDAR paredz tādas pašas nosūtīšanas rīkus kā tos, kas paredzēti VDAR, EDAK uzsver nepieciešamību nodrošināt, lai tajos ietvertie aizsardzības pasākumi garantē efektīvu aizsardzību trešā valstī, īpaši ņemot vērā spriedumu lietā *Schrems II*.

85. Pēc nolēmuma lietā *Schrems II*, kurā EST atgādina, ka personas datu aizsardzībai ES ir jāattiecas uz šiem datiem visā to nosūtīšanas laikā, lai kur tie tiktu sūtīti, EDAK jau ir pieņēmusi sākotnējos ieteikumus par papildu pasākumiem<sup>52</sup>, lai vajadzības gadījumā palīdzētu nosūtītājiem nodrošināt, ka datu subjektiem tiek nodrošināts tāds aizsardzības līmenis, kas pēc būtības ir līdzvērtīgs ES garantētajam līmenim.
86. EST uzskata, ka datu nosūtītājiem katrā atsevišķā gadījumā un, kad nepieciešams, sadarbībā ar datu saņēmēju trešā valstī ir jāpārbauda, vai trešās valsts tiesību akti vai prakse traucē to attiecīgo aizsardzības pasākumu efektivitātei, kas ietverti VDAR 46. panta nosūtīšanas rīkos<sup>53</sup>. Tādā gadījumā datu nosūtītājiem būtu jāīsteno papildu pasākumi, kas novērš šīs aizsardzības nepilnības un paaugstina to līdz līmenim, ko paredz ES tiesību akti.
87. **Lai nodrošinātu aizsardzības nepārtrauktību, EDAK aicina Eiropas Komisiju lēmuma projektā ieviest garantijas, ka tad, kad Apvienotās Karalistes datu nosūtītāji AK VDAR 46. un 47. pantā paredzētos nosūtīšanas rīkus izmanto EEZ nosūtīto datu tālākai nosūtīšanai uz citām trešām valstīm, šie datu nosūtītāji katrā gadījumā atsevišķi novērtētu šīs trešās valsts datu aizsardzības regulējumu un, ja nepieciešams, veiktu atbilstošus pasākumus ar mērķi īstenot izvēlētajā nosūtīšanas rīkā ietvertu aizsardzības pasākumu efektīvu ievērošanu nolūkā nodrošināt pēc būtības līdzvērtīgu aizsardzības līmeni tam, kāds garantēts ES. EDAK uzsver, ka bez šīm garantijām arvien pastāv risks, ka, nosūtot tālāk datus no Apvienotās Karalistes, tiks mazināts aizsardzības līmenis, kas pēc būtības līdzvērtīgs līmenim, kāds garantēts ES.**
88. **Ceturtnā problēma** saistībā ar tālāku nosūtīšanu attiecas uz starptautiskiem nolīgumiem, kurus AK ir noslēgusi vai nākotnē plāno noslēgt, un šādu nolīgumu puses(-šu) trešās(-o) valsts(-u) iestāžu iespējamu tiešu piekļuvi šādiem personas datiem no EEZ. Patiešām, EDAK ir lielas bažas par jau noslēgto AK un ASV *CLOUD* akta nolīgumu, un Eiropas Komisija atzīst šo problēmu, uzsverot, ka *šā nolīguma iespējamā stāšanās spēkā var ietekmēt šajā lēmumā novērtēto aizsardzības līmeni*<sup>54</sup>. Pamatojoties uz šo nolīgumu, tiklīdz tas stājas spēkā, uz personas datiem, kas saskaņā ar lēmuma projektu tiek nosūtīti no EEZ uz AK, attiektos šā nolīguma noteikumi, ar kuriem paredz nosacījumus ASV iestāžu tiešai piekļuvei, kas ietekmēs AK datu aizsardzības regulējumu, tostarp noteikumus par tālāku nosūtīšanu. Tā rezultātā no EEZ nosūtīto datu aizsardzības līmeni var būtiski ietekmēt ar ASV noslēgtā nolīguma noteikumi un iespāids uz šādu datu aizsardzības līmeni. EDAK šajā kontekstā atzīmē, ka Eiropas Komisija lēmuma projekta 153. apsvērumā atsaucas uz AK iestāžu skaidrojumiem, nepiedāvājot vai nesniedzot nekādu konkrētu rakstisku apliecinājumu vai apņemšanos, kā arī nenorādot uz AK tiesību aktos ietvertajām īpašām tiesību normām, ar ko īstenotu šādus skaidrojumus.

---

<sup>52</sup> Sk. EDAK ieteikumus 01/2020 pasākumiem, kas papildina nosūtīšanas rīkus nolūkā nodrošināt atbilstību ES persondatu aizsardzības līmenim, kas pieņemti 2020. gada 10. novembrī un pašlaik pēc sabiedriskās apspriešanas tiek sagatavoti galīgajā redakcijā, [https://edpb.europa.eu/sites/default/files/consultation/edpb\\_recommendations\\_202001\\_supplementarymeasures\\_transfer\\_tools\\_lv.pdf](https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasures_transfer_tools_lv.pdf).

<sup>53</sup> Sk. *Schrems II*, 134. punkts.

<sup>54</sup> Sk. lēmuma projekta 153. apsvērumu.

89. EDAK jau iepriekš ir paudusi šīs bažas savā 2020. gada 15. jūnija vēstulē, kas adresēta Eiropas Parlamentam<sup>55</sup>. EDAK ir uzsvērusi, ka, pamatojoties uz *ES acquis datu aizsardzības jomā un jo īpaši uz VDAR un Tiesībaizsardzības direktīvu*, EDAK ir iebildumi attiecībā uz to, vai aizsardzības pasākumi, kas paredzēti nolīgumā par piekļuvi personas datiem AK, tiktu piemēroti noteiktos apstākļos, kad nepieciešams pildīt informācijas atklāšanas pienākumu attiecībā pret ASV, kā arī vai šie aizsardzības pasākumi saskaņā ar ES standartiem ir pietiekami, lai nemazinātu ES nodrošināto aizsardzības līmeni.
90. Turklāt AK un ASV *CLOUD* akta nolīguma noteikumi var būtiski ietekmēt materiālos un procesuālos nosacījumus, saskaņā ar kuriem personas datiem, kas atrodas pārzīņu vai apstrādātāju rīcībā AK, var tieši piekļūt ASV iestādes, tādējādi ietekmējot AK tiesību aktos garantēto aizsardzības līmeni. Lai nodrošinātu aizsardzības līmeni, kas pēc būtības ir līdzvērtīgs ES tiesību aktos garantētajam, piemēram, ir *svarīgi, lai aizsardzības pasākumi, kas paredzēti šādā nolīgumā, ietvertu obligātu iepriekšēju tiesas atļauju kā būtisku garantiju piekļuvei metadatiem un satura datiem. Pamatojoties uz sākotnējo novērtējumu, EDAK, lai arī atzīmējot, ka nolīgums attiecas uz vietējo tiesību aktu piemērošanu, nav varējusi identificēt tik skaidru noteikumu starp AK un ASV noslēgtajā nolīgumā*<sup>56</sup>.
91. Lai gan Eiropas Komisija uzsver, ka datiem, kas iegūti saskaņā ar šo nolīgumu, tiktu piemērota aizsardzība, kura ir līdzvērtīga īpašajiem aizsardzības pasākumiem, ko nodrošina tā dēvētais “ES un ASV jumta nolīgums”, EDAK ir bažas par to, vai šo aizsardzības pasākumu iekļaušana AK un ASV *CLOUD* akta nolīgumā, izmantojot tikai atsauci, ko piemēro *mutatis mutandis*, atbilstu skaidru, precīzu un pieejamu noteikumu kritērijiem attiecībā uz piekļuvi personas datiem vai arī pietiekami nostiprinātu šādus aizsardzības pasākumus, lai tie būtu efektīvi un piemērojami saskaņā ar AK tiesību aktiem.
92. **Tāpēc EDAK iesaka Eiropas Komisijai izskaidrot, kādā veidā un pamatojoties uz kuru juridisko instrumentu līdzvērtīga aizsardzība ES un ASV jumta nolīgumā paredzētajiem īpašajiem aizsardzības pasākumiem tiktu piemērota un vai tai būtu saistošs raksturs saskaņā ar AK tiesību aktiem.**
93. EDAK arī atzīmē, ka AK un ASV *CLOUD* akta nolīguma noteikumi, lasot to kopā ar ASV *CLOUD* akta 3. iedaļu<sup>57</sup>, rada jautājumus par to, kā reāli piemērojami ASV tiesībaizsardzības iestāžu piekļuves līgumā piedāvātie aizsardzības pasākumi tiem personas datiem AK, kurus apstrādā elektronisko sakaru pakalpojumu vai attālās datošanas pakalpojumu sniedzēji (turpmāk tekstā — *CSP*) un kuri atrodas ASV jurisdikcijā. Patiešām, ja *CSP*, kas atrodas AK, būtu jāpiemēro ASV tiesību akti (piemēram, tāpēc, ka tas ir ASV uzņēmuma meitasuzņēmums), vēl ir jānoskaidro, vai ASV iestādēm būtu pienākums pajauties uz AK un ASV *CLOUD* akta nolīgumu, lai iegūtu šos datus. Tā kā Eiropas Komisija norāda, ka *īpaša uzmanība tiks pievērsta jumta nolīguma aizsardzības pasākumu piemērošanai un pielāgošanai attiecībā uz īpašu datu nosūtīšanas veidu, uz kuru attiecas šis AK un ASV nolīgums*, EDAK uzsver, ka, pamatojoties uz provizorisku novērtējumu, nav skaidrs, vai AK un ASV *CLOUD* akta nolīgumā un līdz ar to ES un ASV jumta nolīgumā paredzētie aizsardzības pasākumi būtu piemērojami visiem ASV iestāžu pieprasījumiem, ja tādi ir, par piekļuvi datiem AK saskaņā ar ASV *CLOUD* aktu.
94. Iespējams, ka nākotnē būs citi starptautiski nolīgumi vai saistības ar trešām valstīm, kuras AK varētu noslēgt nākotnē, un tas attiektos uz personas datiem, kas tiek nosūtīti no EEZ uz AK saskaņā ar

---

<sup>55</sup>Sk. EDAK 2020. gada 15. jūnija atbildi EP deputātiem *Sophie in't Veld* un *Moritz Körner* par ASV un AK nolīgumu saskaņā ar ASV *CLOUD* aktu, [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> Sk. iepriekš minēto EDAK vēstuli.

<sup>57</sup> Sk. ASV *CLOUD* aktu, <https://www.congress.gov/bill/115th-congress/senate-bill/2383/text>.

lēmuma projektu<sup>58</sup>. Atkarībā no šo nolīgumu noteikumiem un īpašu drošības klauzulu piemērošanas šie starptautiskie nolīgumi, ietekmējot AK datu aizsardzības regulējumu, var arī būtiski ietekmēt materiālos un procesuālos nosacījumus trešo valstu iestāžu piekļuvei personas datiem AK. Tas jo īpaši attiecas uz otrā Papildu protokola projektu Eiropas Padomes Konvencijai par kibernetizāciju (turpmāk tekstā — Budapeštas konvencija), par kuru pašlaik notiek sarunas starp šīs konvencijas pusēm, kuru vidū ir vairākas valstis, kas nav ES dalībvalstis. Patiešām, protokola projektā ir klauzulas, kuras puses var brīvi aktivizēt, piemēram, attiecībā uz atļauju piešķirt piekļuvi satura datiem vai to nepiešķirt. Lai arī visas ES dalībvalstis aktivizētu klauzulas saskaņā ar ES datu aizsardzības noteikumiem, AK nav sniegta nekāda garantija, kas ļautu būtiski novirzīties no aizsardzības līmeņa, kādu pēc tam piedāvātu ES. Vēl viens iepriekš izklāstīto jautājumu piemērs ir AK un Japānas Visaptverošas ekonomiskās partnerības nolīgums<sup>59</sup> (CEPA), AK pirmais tirdzniecības darījums pēc *Brexit*, kurš stājās spēkā 2021. gada 1. janvārī<sup>60</sup> un kurā iekļauti noteikumi par personas datiem<sup>61</sup>. Turklāt EDAK atzīmē, ka AK arī 2021. gada 1. februārī ir oficiāli paziņojusi par savu lūgumu pievienoties Visaptverošai un progresīvai Klusā okeāna valstu partnerībai (CPTPP), kas ietver Klusā okeāna valstu partnerības nolīgumu (TPP)<sup>62</sup>.

95. EDAK norāda, ka, izņemot AK un ASV *CLOUD* akta nolīgumu, iepriekš minētie starptautiskie nolīgumi lēmuma projektā nav apskatīti.

96. **EDAK aicina Eiropas Komisiju:**

- izskatīt mijiedarbību starp AK datu aizsardzības regulējumu un tās starptautiskajām saistībām, kas pārsniedz AK un ASV *CLOUD* akta nolīguma darbības jomu, jo īpaši tādēļ, lai nodrošinātu aizsardzības līmeņa nepārtrauktību gadījumā, kad no EEZ uz AK nosūtītie personas dati tiek tālāk nosūtīti uz citām trešām valstīm, pamatojoties uz AK izdoto lēmumu par pietiekamību, un nepārtraukti uzraudzīt un vajadzības gadījumā rīkoties attiecībā uz citu starptautisku nolīgumu noslēgšanu starp AK un trešām valstīm, kas varētu mazināt ES nodrošināto personas datu aizsardzības līmeni,
- sniegt EDAK rakstisku informāciju par AK iestāžu saistībām un norādīt īpašus noteikumus saskaņā ar AK tiesību aktiem attiecībā uz skaidrojumu, kas saistīts ar iespējamo AK un ASV *CLOUD* akta nolīguma piemērošanu un īstenošanu, kā minēts lēmuma projekta 153. apsvērumā,
- šajā saistībā uzraudzīt, vai papildus aizsardzības pasākumiem, ko varētu nodrošināt, pienācīgi pielāgojot ES un ASV jumta nolīgumu, AK un ASV *CLOUD* akta nolīgums nodrošina atbilstošus

---

<sup>58</sup> Sk. iepriekš minēto 2.3.3. iedaļu.

<sup>59</sup> Sk. AK un Japānas Visaptverošas ekonomiskās partnerības nolīgumu [CS Japan Nr.1/2020], <https://www.gov.uk/government/publications/ukjapan-agreement-for-a-comprehensive-economic-partnership-cs-japan-no12020>.

<sup>60</sup> Sk. AK valdības norādījumus par AK tirdzniecības nolīgumiem ar valstīm, kas nav ES dalībvalstis, <https://www.gov.uk/guidance/uk-trade-agreements-with-non-eu-countries>.

<sup>61</sup>Saskaņā ar CEPA 8.80. panta 5. punktu puses apņemas sekmēt tādu mehānismu izstrādi, kas veicinātu savietojamību starp dažādām to juridiskajām pieejām (personas) datu aizsardzībai. Saskaņā ar 8.84. pantu puses apņemas neaizliegt un neierobežot informācijas, tostarp personas datu, pārrobežu nosūtīšanu, izmantojot elektroniskos līdzekļus, ja šī darbība ir paredzēta tādas personas darījumdarbībai, uz kuru attiecas CEPA darbības joma.

<sup>62</sup> Saskaņā ar TPP 14.11. panta 2. punktu katra puse atļauj informācijas, tostarp personas datu, pārrobežu nosūtīšanu, izmantojot elektroniskos līdzekļus, ja šī darbība ir paredzēta attiecīgās personas darījumdarbībai.

**papildu aizsardzības pasākumus, lai tiktu ņemta vērā attiecīgo datu kategoriju sensitivitāte un unikālās prasības elektronisko pierādījumu nosūtīšanai tieši no CSP, nevis starp iestādēm,**

- **novērtēt to noteikumu ietekmi uz personas datiem, kuri iekļauti nesen AK parakstītajos starptautiskajos nolīgumos, piemēram, CEPA, kā arī šo noteikumu radītu potenciālu apdraudējumu šādiem personas datiem.**

97. **Piektā** identificētā **problēma** attiecas uz atkāpju piemērošanu personas datu nosūtīšanai uz trešo valsti. Lai arī pieejamās atkāpes saskaņā ar AK VDAR ir tādas pašas kā tās, kas paredzētas VDAR, ir svarīgi, lai ICO piemērotu un turpinātu piemērot tādu interpretāciju saistībā ar šo atkāpju izmantošanu, kas saskaņota ar EDAK. Ja tas tā nav vai ja AK nākotnē novirzīsies no šīs interpretācijas, pastāv risks, ka varētu tikt mazināts to datu aizsardzības līmenis, kuri ar AK starpniecību tiek nosūtīti no EEZ uz trešām valstīm.
98. EDAK aicina Eiropas Komisiju kā daļu no sava uzraudzības uzdevuma īpaši pārbaudīt, vai AK interpretācija par atkāpju izmantošanu joprojām ir saskaņīga ar ES interpretāciju. Ja tomēr AK izmantojusi atšķirīgu atkāpju izmantošanas interpretāciju, kas mazina aizsardzības līmeni, ir svarīgi, lai Eiropas Komisija veiktu nepieciešamos pasākumus, grozot lēmumu par pietiekamību, lai pārliecinātos, ka EEZ personas datu aizsardzības līmenis datu nosūtīšanā uz AK, pamatojoties uz atšķirīgu atkāpju interpretāciju, netiks mazināts, kad šie dati tiks tālāk nosūtīti no AK uz trešām valstīm.
99. **Sestā problēma**, kas ir pēdējais šīs iedaļas risināmais jautājums, attiecas uz to, ka Apvienotās Karalistes datu aizsardzības regulējumā nav ietverta aizsardzība, kas paredzēta VDAR 48. pantā.
100. Eiropas Komisija savā lēmuma projektā paskaidro, ka, ja nav pietiekamības noteikumu vai atbilstošu aizsardzības pasākumu, nosūtīšana var notikt, tikai pamatojoties uz atkāpēm, kas noteiktas AK VDAR 49. pantā, *izņemot Regulas (ES) 2016/679 48. pantu, ko Apvienotā Karaliste ir izvēlējusies neiekļaut AK VDAR*<sup>63</sup>. Tas, ka trūkst VDAR 48. pantā paredzētā noteikuma par līdzvērtīgumu pēc būtības, kas nostiprināts AK datu aizsardzības regulējumā attiecībā uz nosūtīšanu vai atklāšanu pēc tiesas vai tribunāla sprieduma vai citas trešās valsts administratīvās iestādes lēmuma, var izraisīt juridisku nenoteiktību attiecībā uz to, vai tiks būtiski ietekmēts to personas datu aizsardzības līmenis, kas saskaņā ar lēmuma projektu tiks nosūtīti no EEZ uz AK.
101. VDAR pietiekamības atsaucē EDAK norāda, ka attiecībā uz tālāku nosūtīšanu *sākotnējā datu saņēmēja veikta personas datu tālāka nosūtīšana būtu atļauta tikai tad, ja arī uz nākamo saņēmēju attiektos noteikumi, kas nodrošina pietiekamu aizsardzības līmeni, un tiktu ievēroti atbilstoši norādījumi, kas datu pārzinim jāievēro datu apstrādē*<sup>64</sup>. Turklāt EDAK uzsver, ka *no ES nosūtīto datu sākotnējais saņēmējs ir atbildīgs par to, lai tiktu nodrošināti atbilstoši aizsardzības pasākumi datu tālākai nosūtīšanai, ja nav izdots lēmums par pietiekamību. Šādai datu tālākai nosūtīšanai vajadzētu notikt tikai ierobežotiem un noteiktiem mērķiem, ciktāl šai apstrādei ir juridisks pamats*<sup>65</sup>. Lai novērtētu, vai AK tiesiskais regulējums šajā ziņā nodrošina pēc būtības līdzvērtīgu aizsardzības līmeni, VDAR V nodaļas saistībā ir pilnībā jāņem vērā 48. pants<sup>66</sup>.
102. EDAK šajā saistībā uzsver EST judikatūras izmantošanu attiecībā uz datu ļaunprātīgu izmantošanu vai nelikumīgu piekļuvi tiem, jo īpaši norādot, ka *“attiecībā uz Savienībā garantēto pamatbrīvību un*

<sup>63</sup> Sk. lēmuma projekta 78. zemsvītras piezīmi.

<sup>64</sup>Sk. WP254 rev.01, 6. lpp.

<sup>65</sup>Sk. WP254 rev.01, 6. lpp.

<sup>66</sup> Sk. VDAR 44. panta pēdējo teikumu, konkrēti: *“Piemēro visus šīs nodaļas noteikumus, lai nodrošinātu, ka nemazinās ar šo regulu garantētais fizisku personu aizsardzības līmenis.”*



*pamattiesību aizsardzības līmeni tās tiesiskajā regulējumā, kurā ir ietverta iejaukšanās Hartas 7. un 8. pantā garantētajās pamattiesībās, saskaņā ar Tiesas pastāvīgo judikatūru ir jāparedz skaidri un precīzi noteikumi, kas reglamentētu attiecīgā pasākuma apjomu un piemērošanu un noteiktu minimālās prasības tādējādi, lai personām, kuru personas dati ir tikuši skarti, būtu pietiekamas garantijas, kas ļautu to personas datus efektīvi aizsargāt pret ļaunprātīgas izmantošanas risku, kā arī pret jebkādu nelikumīgu piekļuvi šiem datiem un to nelikumīgu izmantošanu. Šādu garantiju nepieciešamība ir vēl jo svarīgāka tādēļ, ka personas dati tiek apstrādāti automātiski un pastāv ievērojams nelikumīgas piekļuves šiem datiem risks*<sup>67</sup>.

103. EDAK šajā saistībā atzīmē, ka, pamatojoties uz lēmuma projektā pieejamo informāciju, AK datu aizsardzības regulējums skaidri neparedz, ka jebkurš tiesas vai tribunāla spriedums un jebkurš trešās valsts administratīvās iestādes lēmums, kurā prasīts, lai pārzinis vai apstrādātājs nosūtītu vai atklātu personas datus, jebkādā veidā var tikt atzīts vai noteikts kā izpildāms tikai tad, ja tas ir balstīts uz spēkā esošu starptautisku nolīgumu starp pieprasītāju trešo valsti un AK. VDAR 48. pants ir būtisks noteikums saskaņā ar VDAR V nodaļu, jo tas paredz, ka personas datu nosūtīšana vai atklāšana pēc trešās valsts tiesas/tribunāla vai administratīvās iestādes sprieduma vai lēmuma var tikt atzīta vai būt izpildāma tikai tad, ja tā balstīta uz starptautisku nolīgumu starp pieprasītāju trešo valsti un Savienību vai tās dalībvalsti, neskarot citu nosūtīšanas pamatojumu saskaņā ar VDAR V nodaļu. Patiešām, EDAK atgādina, ka *ārvalsts iestādes pieprasījums pats par sevi nav juridisks pamats nosūtīšanai. Rīkojumu var atzīt tikai tad, ja tas pamatots ar starptautisku nolīgumu, piemēram, savstarpējas juridiskās palīdzības līgumu, kas ir spēkā starp pieprasītāju trešo valsti un Savienību vai dalībvalsti*<sup>68</sup>. Tāpēc ir svarīgi, lai AK tiesību aktos varētu identificēt pēc būtības līdzvērtīgus noteikumus.
104. Lēmuma projektā Eiropas Komisija ziņo par AK iestāžu skaidrojumiem, saskaņā ar kuriem, balstoties uz anglosakšu tiesībām vai likumiem, ārvalsts spriedums par datu pieprasīšanu nav izpildāms AK, ja tas nav balstīts uz starptautisku nolīgumu, un jebkādai datu nosūtīšanai pēc ārvalstu tiesas vai administratīvās iestādes pieprasījuma paredz izmantot tādu nosūtīšanas rīku kā pietiekamības regulējums vai atbilstoši aizsardzības pasākumi, ja vien nav piemērojama atkāpe saskaņā ar AK VDAR 49. pantu. Tomēr EDAK šajā saistībā nav nodrošināta informācijas apmaiņa starp Eiropas Komisiju un AK iestādēm<sup>69</sup>, un tāpēc tā nespēj analizēt un neatkarīgi novērtēt, vai AK iestāžu sniegtās garantijas ir pietiekamas, lai nodrošinātu pēc būtības līdzvērtīgu aizsardzības līmeni saistībā ar VDAR 48. pantā ietvertajiem aizsardzības pasākumiem.
105. **EDAK aicina Eiropas Komisiju sniegt papildu garantijas un īpašas atsauces uz AK tiesību aktiem, kas nodrošina, ka aizsardzības līmenis saskaņā ar AK tiesisko regulējumu ir pēc būtības līdzvērtīgs tam, kas garantēts EEZ. Tāpēc EDAK aicina Eiropas Komisiju sniegt rakstiskus skaidrojumus un apņemšanos no AK iestādēm attiecībā uz tādas aizsardzības īstenošanu, kas ir pēc būtības līdzvērtīga tai, kura paredzēta VDAR 48. pantā.**
106. **EDAK uzskata, ka to noteikumu identificēšana saskaņā ar AK tiesību aktiem, kas nodrošina pēc būtības līdzvērtīgu aizsardzības līmeni attiecībā uz VDAR 48. pantā ietvertajiem aizsardzības pasākumiem, ir jo svarīgāka, ņemot vērā iepriekš izteiktās bažas par pieprasījumiem piekļūt datiem AK, ko iesniedza ASV vai citu trešo valstu iestādes, un uzskatot, ka saskaņā ar lēmumu par pietiekamību personas datus no EEZ varētu nosūtīt uz AK bez to saņēmēja papildu garantijām vai**

<sup>67</sup> Sk. *Schrems I*, 91. punkts.

<sup>68</sup> Sk. pielikumu EDAK un EDAU 2019. gada 10. jūlija kopīgajai atbildei *LIBE* komitejai par ASV *CLOUD* akta ietekmi uz Eiropas tiesisko regulējumu personas datu aizsardzības jomā, [https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act\\_en](https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en).

<sup>69</sup> Sk. lēmuma projekta 78. zemsvītras piezīmi.

**juridiski saistošamsaistībām attiecībā uz citu trešo valstu iestāžu pieprasījumiem piekļūt šiem datiem.**

### 3.2. Procesuālie un izpildes panākšanas mehānismi

107. Pamatojoties uz VDAR pietiekamības atsaucē noteiktajiem kritērijiem, EDAK ir analizējusi šādus AK datu aizsardzības regulējuma aspektus, uz kuriem attiecas lēmuma projekts: neatkarīgas uzraudzības iestādes esība un tās efektīva darbība, sistēma, kas nodrošina labu atbilstības līmeni, un piekļuves sistēma atbilstošiem tiesiskās aizsardzības mehānismiem, kas ES personām nodrošina līdzekļus, lai tās varētu izmantot savas tiesības un pārsūdzēt lēmumus, neradot apgrūtinājošus šķēršļus administratīvai un tiesiskajai aizsardzībai.

#### 3.2.1 Kompetentā neatkarīgā uzraudzības iestāde

108. EDAK atzinīgi vērtē Eiropas Komisijas centienus lēmuma projekta 2.6. nodaļā vispusīgi izskatīt AK uzraudzības iestādes izveidi, darbību un pilnvaras. AK informācijas komisāram (turpmāk tekstā — *IC*) ir uzdots uzraudzīt atbilstību AK VDAR un *DPA 2018* un panākt šādu atbilstību. Saskaņā ar *DPA 2018* 12. pielikumu *IC* ir *corporation sole*, t. i., atsevišķa juridiska persona, kura izveidota vienā personā un kuru atbalsta birojs, t. i., *ICO*.
109. Attiecībā uz *IC* neatkarību EDAK uzsver, ka AK VDAR 51. pants neietver precīzu skaidrojumu par to, ka *IC* ir neatkarīga publiska iestāde, kā tas ir noteikts VDAR 51. pantā attiecībā uz uzraudzības iestādēm. EDAK tomēr atzīst, ka AK VDAR savā 52. pantā līdzīgā veidā atspoguļo atbilstošos noteikumus attiecībā uz neatkarību, kā noteikts VDAR 52. panta 1.–3. punktā.
110. Turklāt EDAK norāda, ka AK VDAR 52. pants neietver pienākumus, kas atbilstu VDAR 52. panta 4.–6. punktam, kuros skaidri paredzēts, ka attiecīgajai uzraudzības iestādei tiek nodrošināti resursi, kas nepieciešami efektīvai uzdevumu veikšanai un savu pilnvaru īstenošanai. EDAK tomēr atzīst, ka *DPA 2018* ietver noteikumus, kuru mērķis ir nodrošināt atbilstošu *ICO* finansējumu<sup>70</sup>, kā arī apstākli, ka *ICO* pašlaik ir viena no lielākajām uzraudzības iestādēm salīdzinājumā ar uzraudzības iestādēm ES/EEZ. Tā kā pastāvīga atbilstošu resursu piešķiršana, īpaši attiecībā uz personālu un budžetu<sup>71</sup>, ir obligāta, lai nodrošinātu pienācīgu uzraudzības iestādes darbību un tā izpildītu visus uzticētos uzdevumus, un arī Eiropas Parlaments to nesen atzīmējis kā būtisku<sup>72</sup>, EDAK uzskata, ka ir svarīgi pievērst īpašu uzmanību turpmākajām norisēm šajā jomā.
111. **Tāpēc EDAK aicina Eiropas Komisiju novērot jebkādas izmaiņas saistībā ar resursu piešķiršanu *ICO*, kas kaitētu *ICO* uzdevumu pienācīgai izpildei.**

#### 3.2.2. Datu aizsardzības sistēma, kas nodrošina labu atbilstības līmeni

112. Lai nodrošinātu tiesību aktu uzraudzību un izpildes panākšanu, lēmuma projektā tiek veikta visaptveroša to pilnvaru pārbaude, kuras *ICO* piešķirtas ar AK VDAR 58. pantu un *DPA 2018*. EDAK atzīst, ka Apvienotās Karalistes VDAR 58. pants pienācīgi atspoguļo attiecīgos noteikumus saistībā ar uzraudzības iestāžu pilnvarām, kā noteikts VDAR 58. pantā. Attiecībā uz tiesībām uzlikt administratīvos naudas sodus atkarībā no katra atsevišķa gadījuma apstākļiem AK VDAR 83. pantā ir ietverti līdzīgi noteikumi un maksimālās summas, kā noteikts VDAR 83. pantā. Tādējādi EDAK uzskata, ka AK tiesiskais regulējums šajā jomā pašlaik atbilst standartiem, kas noteikti attiecīgajos ES tiesību

<sup>70</sup> Sk. *DPA 2018* 137., 138., 182. pantu un 12. pielikuma 9. punktu.

<sup>71</sup> Sk. WP 254 rev.01, 7. lpp.

<sup>72</sup> Eiropas Parlamenta 2021. gada 25. marta rezolūcija par Komisijas novērtējuma ziņojumu attiecībā uz Vispārīgās datu aizsardzības regulas īstenošanu divus gadus pēc tās piemērošanas, 15. punkts, [https://www.europarl.europa.eu/doceo/document/B-9-2021-0211\\_LV.html](https://www.europarl.europa.eu/doceo/document/B-9-2021-0211_LV.html).

aktos. Šajā saistībā EDAK tomēr uzsver, ka *efektīvu* sankciju esībai ir svarīga loma noteikumu ievērošanas nodrošināšanā<sup>73</sup>.

113. **Nemot vērā iepriekš minēto, EDAK aicina Eiropas Komisiju uzraudzīt sankciju un attiecīgo aizsardzības līdzekļu efektivitāti Apvienotās Karalistes datu aizsardzības regulējumā.**

3.2.3. Datu aizsardzības sistēmai jānodrošina atbalsts un palīdzība datu subjektiem, īstenojot viņu tiesības, kā arī atbilstoši tiesiskās aizsardzības mehānismi

114. Efektīvs uzraudzības mehānisms, kas ļauj neatkarīgi izmeklēt sūdzības, lai praksē identificētu datu subjektu tiesību pārkāpumus un sodītu par tiem, kā arī efektīva administratīvā un tiesiskā aizsardzība (tostarp tādu zaudējumu atlīdzināšana, kas radušies datu subjekta personas datu nelikumīgas apstrādes rezultātā) ir būtiski elementi, kuri palīdz novērtēt, vai datu aizsardzības sistēma nodrošina pietiekamu aizsardzības līmeni.
115. EDAK atzinīgi vērtē to, ka ICO savā tīmekļa vietnē sniedz visaptverošu informāciju un pamatnostādnes, kuru mērķis ir palielināt pārziņu un apstrādātāju izpratni par viņu pienākumiem un uzdevumiem, kā arī atbalstīt datu subjektus, lai viņi tiktu informēti par savu tiesībām personas datu jomā aizstāvētu savas individuālās tiesības saskaņā ar AK VDAR un DPA 2018.
116. **Neskatoties uz pašreizējo stāvokli, EDAK aicina Eiropas Komisiju pastāvīgi vērot atbalsta līmeni, ko ICO sniedz tieši tām personām, kuru personas dati saskaņā ar lēmumu par pietiekamību tiek nosūtīti uz AK, lai palīdzētu viņām īstenot savas tiesības saskaņā ar AK datu aizsardzības režīmu.**

## 4. APVIENOTĀS KARALISTES PUBLISKO IESTĀŽU PIEKĻUVE PERSONAS DATIEM, KO NOSŪTA NO ES, UN TO IZMANTOŠANA

### 4.1. Apvienotās Karalistes publisko iestāžu piekļuve datiem un to izmantošana krimināltiesību aizsardzības nolūkos

#### 4.1.1. Juridiskais pamats un piemērojamie ierobežojumi / aizsardzības pasākumi

117. Attiecībā uz Eiropas Komisijas veikto novērtējumu, kas dokumentēts lēmuma projekta **par piekļuvi tiesībaizsardzības nolūkos** 132. un turpmākajos apsvērumos, Eiropas Komisija sniedz niansētu un sīki izklāstītu informāciju un kopumā nonāk pie saprotamiem secinājumiem. Tāpēc šajā atzinumā EDAK neatkārto lielāko daļu faktu konstatējumu un novērtējumu. Tomēr ir daži gadījumi, kad faktu izklāsts vai secinājumu skaidrojums nav pietiekams, lai EDAK varētu tam piekrist.

##### 4.1.1.1. Piekrišanas izmantošana

118. EDAK ņem vērā to, ka lēmuma projekta 184. zemsvītras piezīmē<sup>74</sup> Eiropas Komisija apgalvo, ka **piekrišanas izmantošana** nav būtiska pietiekamības scenārijā, jo, nosūtot datus, Apvienotās Karalistes tiesībaizsardzības iestāde tos nesavāc tieši no datu subjekta, pamatojoties uz piekrišanu. Attiecīgi Eiropas Komisija nevērtē piekrišanas kā juridiska pamata izmantošanu policijas darbā.
119. Šajā saistībā EDAK atgādina, ka VDAR 45. panta 2. punkta a) apakšpunktā ir noteikts, ka ir jāvērtē plašs elementu klāsts, kas neaprobežojas tikai ar datu nosūtīšanu, tostarp "*tiesiskums, cilvēktiesību*

---

<sup>73</sup> Sk. WP 254 rev.01, 7. lpp.

<sup>74</sup> Sk. lēmuma projekta 37. lpp.

*un pamatbrīvību ievērošana, attiecīgie tiesību akti, gan vispārējie, gan nozaru, tostarp attiecībā uz (...) krimināltiesībām”.*

120. Pamatojoties arī uz informāciju, ko Eiropas Komisija sniegusi 38. apsvērumā sava īstenošanas lēmuma projektā par personas datu pietiekamu aizsardzību Apvienotajā Karalistē saskaņā ar Eiropas Parlamenta un Padomes Direktīvu (ES) 2016/680 (turpmāk tekstā — lēmuma projekts par pietiekamību saskaņā ar *LED*), EDAK norāda, ka piekrišanas izmantošanai, kā tas noteikts Apvienotās Karalistes režīmā tiesībaizsardzības kontekstā, vienmēr vajadzētu būt juridiski pamatotai. Tas nozīmē, ka pat tad, ja policijai ir likumīgas pilnvaras apstrādāt datus izmeklēšanas nolūkā, noteiktos īpašos apstākļos (piemēram, lai savāktu DNS paraugu), policija var uzskatīt par piemērotu lūgt datu subjekta piekrišanu.
121. **EDAK aicina Eiropas Komisiju iekļaut lēmumā par pietiekamību analīzi par iespējamo piekrišanas izmantošanu tiesībaizsardzības kontekstā, kā paredzēts lēmuma projektā par pietiekamību saskaņā ar *LED*.**

#### 4.1.1.2. Kratišanas orderi un elektronisko pierādījumu sniegšanas rīkojumi

122. Kopumā EDAK nav piezīmju par to, ka policija iegūst pierādījumus, izmantojot kratišanas orderus un elektronisko pierādījumu sniegšanas rīkojumus, tomēr no lēmuma projekta 136. apsvēruma var secināt, ka Eiropas Komisija ir koncentrējusi ap policiju savus apsvērumus par tiesībaizsardzības iestāžu piekļuvi un personas datu apstrāde citās tiesībaizsardzības iestādēs tika pārbaudīta mazāk.
123. Piemēram, Apvienotās Karalistes pietiekamības apspriešanas skaidrojumos, F iedaļā “Tiesībaizsardzība”<sup>75</sup>, 11. lpp., ir teikts, ka **Valsts noziedzības apkarošanas aģentūra** (turpmāk tekstā — *NCA*) varētu būt sevišķi svarīga tiesībaizsardzības iestāde, kura cita starpā pilda plašāku kriminālizlūkošanas funkciju. *NCA* raksturo savu misiju kā izlūkdatu apkopošanu no dažādiem avotiem ar mērķi maksimāli palielināt analīzes, novērtēšanas un taktiskās iespējas, tostarp no tehniski pārtvertas saziņas, tiesībaizsardzības partneriem Apvienotajā Karalistē un ārvalstīs, drošības un izlūkošanas iestādēm<sup>76</sup>. *NCA* ir arī viens no galvenajiem starptautisko tiesībaizsardzības partneru sarunu partneriem, un tai ir svarīga loma kriminālizlūkošanas datu apmaiņā<sup>77</sup>.

---

<sup>75</sup> Sk. Apvienotās Karalistes valdības pietiekamības apspriešanas skaidrojumus, F iedaļa “Tiesībaizsardzība”, 2020. gada 13. marts, [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).

<sup>76</sup> Sk. Valsts noziedzības apkarošanas aģentūras tīmekļa vietni, sadaļa “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> Ne visi izlūkdati, ko apstrādā *NCA*, ir personas dati, liela daļa varētu būt personīgā informācija, un šeit aplūkotās darbības atšķiras no parastām policijas darbībām, tāpēc novērtējums par Apvienotās Karalistes tiesībaizsardzības iestāžu piekļuvi personas datiem būtu nepilnīgs bez rūpīga *NCA* veikto darbību izvērtējuma. Šķiet saprātīgi pārliecināties, ka datu aizsardzības principiem tiek piešķirta vienāda nozīme visās attiecīgajās tiesībaizsardzības iestādēs, tādējādi pievēršoties tādām uz datiem jo īpaši orientētām iestādēm kā *NCA*. Turklāt sadaļā “Raugoties nākotnē” (“Looking to the future”) paskaidrojums turpinās: “*Mēs pastāvīgi meklējam jaunas izlūkdatu vākšanas iespējas, kā arī iespējas attīstīt un uzlabot ierastās spējas, lai palielinātu to izlūkdatu daudzumu un kvalitāti, ko iespējams izmantot Apvienotajā Karalistē un ārvalstīs.*” “*Šajā saistībā mēs attīstām jauno valsts datu izmantošanas spēju, izmantojot tās pilnvaras, kas piešķirtas aģentūrai ar Likumu par noziedzību un tiesām, lai savienotu visā valdībā pieejamos datus, tiem piekļūtu un tos izmantotu.*” (...) “*Tas viss palielinās mūsu manevrētspēju un elastību, reaģējot uz jauniem draudiem un darbojoties proaktīvi, lai apkopotu un analizētu informāciju un izlūkdatumus par jauniem draudiem un mēs varētu rīkoties, pirms draudi īstenojas.*”

124. EDAK ņem vērā arī to, ka valdības sakaru štābs (turpmāk tekstā — *GCHQ*), kura darbība parasti ietilpst *DPA 2018* 4. daļas darbības jomā, proti, nacionālā drošība, arī aktīvi darbojas, lai novērstu smagu noziegumu un organizētās noziedzības radītu kaitējumu sabiedrībai un finansēm Apvienotajā Karalistē, cieši sadarbojoties ar Iekšlietu ministriju, *NCA*, VM leņēmumu un muitas dienestu (*HMRC*) un citiem valdības departamentiem<sup>78</sup>. Tā darbības ir saistītas ar seksuālas vardarbības pret bērniem; krāpšanas; citu veidu ekonomisku noziegumu, tostarp nelikumīgi iegūtu līdzekļu legalizācijas; tehnoloģiju izmantošanas noziedzīgiem mērķiem; kibernetizācijas; organizētas imigrācijas noziedzības, tostarp cilvēku tirdzniecības; narkotiku, šaujamieroču un citas nelikumīgas kontrabandas apkarošanu.
125. EDAK aicina Eiropas Komisiju papildināt savu analīzi ar tādu tiesībsardzības jomas iestāžu analīzi, kuras ir izvirzījušas datu, tostarp personas datu, vākšanu un analizēšanu par prioritāti savā ikdienas darbā, jo īpaši *NCA*. Turklāt EDAK aicina Eiropas Komisiju rūpīgāk izpētīt tādas iestādes kā *GCHQ*, kuras darbojas gan tiesībsardzības, gan nacionālās drošības jomā, kā arī tiesisko regulējumu, kas tām piemērojams attiecībā uz personas datu apstrādi.

#### 4.1.1.3. Izmeklēšanas pilnvaras tiesībsardzības nolūkos

126. Atbilstīgi VDAR pietiekamības atsaucē 4. nodaļai “Būtiskas garantijas trešās valstīs tiesībsardzības un nacionālās drošības iestāžu piekļuvei ar mērķi ierobežot iejaukšanos pamattiesībās” EDAK atgādina, ka šajā kontekstā tiesa arī kritiski atzīmēja, ka iepriekšējā lēmumā par “drošības zonu” nebija nekādu secinājumu par to, ka ASV ir valsts pieņemti noteikumi, kas paredzēti, lai ierobežotu jebkādu iejaukšanos tādu personu pamattiesībās, kuru dati ir nosūtīti no Eiropas Savienības uz Amerikas Savienotajām Valstīm, taču šāda **iejaukšanās varētu tikt atļauta minētās valsts iestādēm, ja tām būtu likumīgi mērķi, piemēram, nacionālā drošība**<sup>79</sup>. Šajā atsaucē EDAK norāda, ka, **piekļūstot datiem** vai nu nacionālās drošības, vai **tiesībsardzības nolūkos, visām trešām valstīm ir jāievēro četras Eiropas būtiskās garantijas**<sup>80</sup>, lai tās uzskatītu par pietiekamām, jo īpaši jāpierāda nepieciešamība un proporcionalitāte attiecībā uz izvirzītajiem likumīgajiem mērķiem.
127. Saskaņā ar šo lēmuma projekta iedaļu Eiropas Komisija secina (139. apsvēruma), ka, *tā kā IPA 2016 paredzētās izmeklēšanas pilnvaras ir tādas pašas kā nacionālās drošības iestāžu pilnvaras, tām piemērojamie nosacījumi, ierobežojumi un aizsardzības pasākumi ir sīki aplūkoti iedaļā par Apvienotās Karalistes publisko iestāžu piekļuvi personas datiem un to izmantošanu nacionālās drošības nolūkos*. Tomēr no EST judikatūras var secināt, ka, piemērojot nepieciešamības un proporcionalitātes pārbaudi dalībvalstu tiesību aktiem, kas ļauj publiskām iestādēm saglabāt personas datus un tiem piekļūt, likumīgie mērķi, piemēram, nacionālā drošība vai smagu noziegumu apkarošana, ir atšķirīgi, un tāpēc kāds varētu attaisnot noteiktu iejaukšanās veidu, bet cits nevarētu<sup>81</sup>.
128. Tāpēc EDAK atzinīgi novērtētu, ja lēmumā būtu īpašs novērtējums par 174. un turpmākajos apsvērumos — iedaļā, kas veltīta nacionālās drošības mērķu sasniegšanai paredzētiem pasākumiem, — izklāstīto nosacījumu, ierobežojumu un aizsardzības pasākumu nepieciešamību un proporcionalitāti, kad runa ir par šo nosacījumu, ierobežojumu un aizsardzības pasākumu piemērošanu tiesībsardzības mērķa sasniegšanai paredzēta pasākuma kontekstā. Tādējādi tā

<sup>78</sup> Sk. *GCHQ* tīmekļa vietni, sadaļu “Mission, Serious and Organised Crime”, <https://www.gchq.gov.uk/section/mission/serious-crime>.

<sup>79</sup> Sk. WP254, rev.01, 9. lpp.

<sup>80</sup> Sk. EDAK Ieteikumus 02/2020 attiecībā uz Eiropas būtiskajām garantijām uzraudzības pasākumiem.

<sup>81</sup> Sk. EST, apvienotās lietas C-511/18, C-512/18 un C-520/18, *La Quadrature du Net* un citi, 2020. gada 6. oktobris, ECLI:EU:C:2020:791.

aicina Eiropas Komisiju sīkāk paskaidrot, vai aprakstītā personas datu saglabāšana un piekļuve tiem tiesībaizsardzības nolūkos ir pietiekami ierobežota, lai nodrošinātu pēc būtības līdzvērtīgu aizsardzības līmeni tam, kāds tiek garantēts ES.

#### 4.1.2. Savāktās informācijas turpmāka izmantošana tiesībaizsardzības nolūkos (140.–154. apsvērumi)

129. EDAK norāda, ka Apvienotās Karalistes datu aizsardzības regulējums attiecībā uz turpmāku savāktās informācijas izmantošanu tiesībaizsardzības nolūkos paredz līdzīgus aizsardzības pasākumus un ierobežojumus tiem, kas paredzēti ES tiesību aktos.

##### 4.1.2.1. Turpmāka izmantošana citos tiesībaizsardzības nolūkos

130. *DPA 2018* patiešām ir noteikts, ka personas datus, ko kompetentā iestāde savākusi tiesībaizsardzības nolūkos, var tālāk apstrādāt (vai nu sākotnējais pārzinis, vai cits pārzinis) jebkādos citos tiesībaizsardzības nolūkos ar nosacījumu, ka pārzinis ir pilnvarots saskaņā ar likumu apstrādāt datus citos nolūkos un apstrāde ir nepieciešama un proporcionāla šim mērķim. Eiropas Komisija norāda, ka visi *DPA 2018* 3. daļā paredzētie aizsardzības pasākumi attiecas uz apstrādi, ko veic saņēmēja iestāde. Tomēr EDAK uzsver, ka *DPA 2018* 3. daļas 44. panta 4. punktā, 45. panta 4. punktā, 48. panta 3. punktā un 68. panta 7. punktā ir paredzēta iespēja ierobežot datu subjekta tiesības, un 79. pantā ir paredzēta iespēja izsniegt sertifikātus, kas apliecina, ka ierobežojums ir nepieciešams un proporcionāls nacionālās drošības aizsardzības pasākums. **Tāpēc EDAK iesaka Eiropas Komisijai sīkāk izvērtēt šādu ierobežojumu iespējamo ietekmi uz personas datu aizsardzības līmeni saistībā ar savāktās informācijas turpmāku izmantošanu. Tāpat būtu jāsniedz sīkāks skaidrojums saistībā ar Apvienotās Karalistes tiesisko regulējumu, kas pieļauj šādu turpmāku koplietošanu, jo īpaši 2017. gada Digitālās ekonomikas likumu, kā arī 2013. gada Likumu par noziegumiem un tiesām, kas ļauj koplietot informāciju ar *NCA*.**

##### 4.1.2.2. Turpmāka izmantošana Apvienotajā Karalistē citos nolūkos, kas nav saistīti ar tiesībaizsardzību

131. *DPA 2018* arī paredz, ka personas datus, kas savākti kādā tiesībaizsardzības nolūkā, var apstrādāt nolūkā, kas nav tiesībaizsardzība, ja apstrādi atļauj likums. Šajā gadījumā juridiskais pamats, kas atļauj šādu koplietošanu, ir 2008. gada Terorisma apkarošanas likuma 19. pants. Šajā saistībā EDAK norāda, ka Terorisma apkarošanas likuma 19. panta darbības joma un noteikumi nav pilnībā aplūkoti Eiropas Komisijas novērtējumā, un tas var nozīmēt plašāku izmantošanu, turpmāk jo īpaši attiecībā uz 19. panta 2. punktu, kas paredz, ka *informāciju, ko kāds no izlūkdienestiem ieguvis, veicot kādu no savām funkcijām, minētais dienests var izmantot, pildot jebkuru citu savu funkciju*.
132. EDAK arī norāda, ka Eiropas Komisijas atsauci uz to, ka kompetentās iestādes ir publiskas iestādes, kurām jārikojas saskaņā ar ECTK, tostarp tās 8. pantu, tādējādi nodrošinot, ka visa datu koplietošana starp tiesībaizsardzības iestādēm un izlūkdienestiem atbilst tiesību aktiem datu aizsardzības jomā un ECTK, varētu vēl vairāk pamatot, nosakot attiecīgos aktus un likumus saskaņā ar Apvienotās Karalistes tiesisko kārtību, kuros skaidri un precīzi noteikti šādi ierobežojumi.

##### 4.1.2.3. Turpmāka izmantošana saistībā ar tālāku nosūtīšanu ārpus Apvienotās Karalistes

133. Lai gan Eiropas Komisija ir atsaukusies uz to, ka Apvienotās Karalistes un ASV *CLOUD* akta nolīgums var ietekmēt tālāku nosūtīšanu uz ASV no *CSP* Apvienotajā Karalistē, EDAK arī uzsver, ka šā nolīguma stāšanās spēkā var ietekmēt arī tādas informācijas turpmāko izmantošanu, kas savākta, veicot tālāku nosūtīšanu no tiesībaizsardzības iestādēm Apvienotajā Karalistē, jo īpaši saistībā ar rīkojumu izdošanu un nosūtīšanu saskaņā ar Apvienotās Karalistes un ASV *CLOUD* akta nolīguma 5. pantu.

134. Plašākā mērogā EDAK uzskata, ka turpmāku divpusēju nolīgumu noslēgšana ar trešām valstīm nolūkā sadarboties tiesībaizsardzības jomā, nodrošinot juridisku pamatu personas datu nosūtīšanai uz šīm valstīm, var arī būtiski ietekmēt savāktās informācijas turpmākas izmantošanas nosacījumus, jo šādi nolīgumi var ietekmēt novērtēto Apvienotās Karalistes datu aizsardzības regulējumu. Tāpēc EDAK iesaka Eiropas Komisijai sīkāk izvērtēt arī šo punktu, nosakot starptautisko nolīgumu esību un precizējot, vai šo nolīgumu noteikumi var ietekmēt Apvienotās Karalistes datu aizsardzības likumu piemērošanu un paredzēt papildu ierobežojumus vai atbrīvojumus attiecībā uz tiesībaizsardzības nolūkos savāktas informācijas turpmāku izmantošanu un atklāšanu ārvalstīs. EDAK uzskata, ka šāda informācija un novērtējums ir būtiski, lai varētu visaptveroši novērtēt aizsardzības līmeni, ko nodrošina Apvienotās Karalistes tiesiskais regulējums un prakse attiecībā uz informācijas atklāšanu un turpmāku izmantošanu ārvalstīs.

#### 4.1.3. Uzraudzība

135. EDAK norāda, ka papildus *ICO* krimināltiesību aizsardzības iestāžu uzraudzību nodrošina dažādi komisāri. Pietiekamības konstatējumu projektā ir minēts *IPC*, biometrisku materiālu saglabāšanas un izmantošanas komisārs, kā arī Uzraudzības kameras komisārs. Šajā saistībā jānorāda, ka EST ir atkārtoti uzsvērusi neatkarīgas uzraudzības nepieciešamību. Jautājumos par piekļuvi personas datiem, kas nosūtīti uz Apvienoto Karalisti, īpaša nozīme ir *IPC*. EDAK saprot, ka *IPC* ir tā sauktais “tieslietu komisārs”, tāpat kā citi tieslietu komisāri, uz kuriem jāatsaucas nacionālās drošības nodaļas kontekstā, un ka šiem tieslietu komisāriem ir tiesnešu neatkarība arī tad, ja tie darbojas kā komisāri. Attiecībā uz *IPC* biroju Eiropas Komisija lēmuma projekta 245. apsvērumā paskaidro, ka tas darbojas neatkarīgi kā “godīgas konkurences struktūra”, bet to finansē Iekšlietu ministrija.
136. EDAK lēmuma projektā nav konstatējusi papildu norādes, lai novērtētu biometrisku materiālu saglabāšanas un izmantošanas komisāra, kā arī Uzraudzības kameras komisāra neatkarību.
137. **Eiropas Komisija tiek aicināta sīkāk izvērtēt tieslietu komisāru neatkarību arī gadījumos, kad komisārs (vairs) nedarbojas kā tiesnesis, kā arī novērtēt biometrisku materiālu saglabāšanas un izmantošanas komisāra un Uzraudzības kameras komisāra neatkarību.**

## 4.2. Datu aizsardzības vispārējais tiesiskais regulējums nacionālās drošības jomā

### 4.2.1. Nacionālās drošības sertifikāti

138. Saskaņā ar *DPA 2018* 111. pantu pārziņi var pieteikties nacionālās drošības sertifikātiem, ko izsniedzis ministrs, Ministru kabineta loceklis, ģenerālprokurors vai Skotijas ģenerāladvokāts un kas apliecina, ka atbrīvojumi no pienākumiem un tiesībām, kuri noteikti *DPA 2018* 4.– 6. daļā, ir nacionālās drošības aizsardzībai nepieciešams un proporcionāls pasākums. Šie sertifikāti ir paredzēti, lai nodrošinātu pārziņiem lielāku juridisko noteiktību, un tie būs pārlicinoši pierādījumi tam, ka personas datu apstrādē ir jāņem vērā nacionālā drošība. Tomēr būtu jāpiemin, ka šie sertifikāti nav nepieciešami, lai izmantotu nacionālās drošības atbrīvojumus, bet gan ir pārredzamības nodrošināšanas pasākums<sup>82</sup>.
139. Saskaņā ar *DPA 2018* 20. pielikuma 17. un 18. punktu EDAK saprot, ka nacionālās drošības sertifikātam, kas izsniegts saskaņā ar 1998. gada Datu aizsardzības likumu (turpmāk tekstā — vecais

---

<sup>82</sup> Sk. Iekšlietu ministrijas 2018. gada Datu aizsardzības likumu, Norādījumus par nacionālās drošības sertifikātiem, 2020. gada augusts, 4. punkts, 3. lpp., [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).

sertifikāts), bija pagarināta iedarbība uz personas datu apstrādi saskaņā ar *DPA 2018* līdz 2019. gada 25. maijam. Ja vien vecie sertifikāti netika aizstāti vai atsaukti, līdz minētajam datumam tos uzskatīja par tādiem, kas izsniegti saskaņā ar *DPA 2018*.

140. Tomēr, ja saskaņā ar 1998. gada Datu aizsardzības likumu izdotā nacionālās drošības sertifikātā nav skaidri norādīts derīguma termiņš, EDAK saprot, ka šāds sertifikāts aizvien ir spēkā attiecībā uz apstrādi saskaņā ar 1998. gada Datu aizsardzības likumu, izņemot gadījumus, kad sertifikāts ir atsaukts vai atcelts<sup>83</sup>. Šo veco sertifikātu sniegtā aizsardzība aprobežojas ar personas datu apstrādi saskaņā ar 1998. gada Datu aizsardzības likumu, tomēr EDAK ņem vērā to, ka jaunus nacionālās drošības sertifikātus var izdot saskaņā ar 1998. gada Datu aizsardzības likumu attiecībā uz personas datiem, kas tika apstrādāti saskaņā ar 1998. gada Datu aizsardzības likumu<sup>84</sup>.
141. **Vispusības labad EDAK aicina Eiropas Komisiju savā lēmuma projektā precizēt, ka nacionālās drošības sertifikātus aizvien var izsniegt saskaņā ar 1998. gada Datu aizsardzības likumu. Turklāt EDAK aicina Eiropas Komisiju savā lēmuma projektā aprakstīt tiesiskās aizsardzības un uzraudzības mehānismus attiecībā uz sertifikātiem, kas izdoti saskaņā ar 1998. gada Datu aizsardzības likumu. Visbeidzot, EDAK aicina Eiropas Komisiju savā lēmuma projektā norādīt saskaņā ar 1998. gada Datu aizsardzības likumu izsniegto spēkā esošo sertifikātu skaitu un uzmanīgi uzraudzīt šo aspektu.**

#### 4.2.2. Tiesības uz labošanu un dzēšanu

142. Attiecībā uz datu labošanas un dzēšanas tiesībām EDAK ņem vērā to, ka saskaņā ar *DPA 2018* 100. un 149. pantu datu subjektiem ir iespēja paļauties uz to, ka Augstā tiesa (Skotijā — Sesijas tiesa) izdos rīkojumu pārzinim labot vai dzēst datus bez liekas kavēšanās.
143. **EDAK uzsver, ka ir efektīvi jānodrošina datu subjektu tiesību izmantošana, un tāpēc aicina Eiropas Komisiju savā lēmuma projektā izklāstīt, kā *DPA 2018* 100. pants darbojas praksē, un cieši uzraudzīt šā panta piemērošanu.**

#### 4.2.3. Ar nacionālo drošību saistīti atbrīvojumi

144. EDAK vēlas pievērst uzmanību *DPA 2018* 110. pantam un jo īpaši 11. pielikumam, kurā izklāstīti konkrēti nolūki, kuros izlūkdienesti var novirzīties no konkrētiem datu aizsardzības principiem, tostarp attiecībā uz datu subjektu tiesībām, un nepaziņot *ICO* personas datu pārkāpumus<sup>85</sup>.
145. **EDAK aicina Eiropas Komisiju sīkāk precizēt atbrīvojumu darbības jomu, jo rodas jautājums, vai visi *DPA 2018* 11. pielikumā paredzētie atbrīvojumi ir saistīti ar izlūkdienestu darbu un vai tie atbilst nepieciešamības un proporcionālītātes principam. Jo īpaši EDAK aicina Eiropas Komisiju sniegt sīkāku skaidrojumu par to, kādos apstākļos izlūkdienests varētu paļauties uz *DPA 2018* 11. pielikuma 10. punktu, kurā teikts, ka *uzskaitītie noteikumi neattiecas uz personas datiem, kas sastāv no pārziņa nodomu ierakstiem saistībā ar jebkādam sarunām ar datu subjektu, ciktāl uzskaitīto noteikumu piemērošana varētu kaitēt sarunām.***

---

<sup>83</sup> Sk. Iekšlietu ministrijas 2018. gada Datu aizsardzības likumu, Norādījumus par nacionālās drošības sertifikātiem, 2020. gada augusts, 5. lpp.

<sup>84</sup> Sk. Iekšlietu ministrijas 2018. gada Datu aizsardzības likumu, Norādījumus par nacionālās drošības sertifikātiem, 2020. gada augusts, 8. punkts, 5. lpp.

<sup>85</sup> Šie nolūki ir "nozieguma" novēršana un atklāšana, "informācija, kas jāatklāj saskaņā ar likumu utt. vai saistībā ar tiesvedību", "parlamentārā privilēģija", "tiesvedība", "kroņa cieņa un gods", "bruņotie spēki", "ekonomiskā labklājība", "advokāta un klienta saziņas konfidencialitāte", "sarunas", "pārziņa sniegtas konfidencialas atsaucēs", "eksāmenu pieraksti un atzīmes", "pētījumi un statistika" un "arhivēšana sabiedrības interesēs".



### 4.3. Apvienotās Karalistes publisko iestāžu piekļuve datiem un to izmantošana nacionālās drošības nolūkos

146. Kopumā EDAK atzīst, ka valstīm ir piešķirta plaša rīcības brīvība nacionālās drošības jautājumos, ko atzinusi arī ECT. EDAK arī atgādina, ka atbilstīgi tam, kā uzsvērts tās atjauninātajos ieteikumos attiecībā uz Eiropas būtiskajām garantijām uzraudzības pasākumiem<sup>86</sup>, Līguma par Eiropas Savienību 6. panta 3. punktā ir noteikts, ka ECTK nostiprinātās pamattiesības ir ES tiesību vispārīgo principu pamats. Tomēr, kā EST atgādina savā judikatūrā, tas nav ES tiesību sistēmā formāli integrēts juridisks instruments, kamēr ES tam nav pievienojusies<sup>87</sup>. Tādējādi VDAR 45. pantā prasītais pamattiesību aizsardzības līmenis jānosaka, pamatojoties uz minētās regulas noteikumiem, lasot tos, ņemot vērā ES hartā nostiprinātās pamattiesības. Tas nozīmē, ka saskaņā ar ES hartas 52. panta 3. punktu tajā ietvertajām tiesībām, kas atbilst ECTK garantētajām tiesībām, ir tāda pati nozīme un darbības joma kā tām, kas noteiktas ECTK. Attiecīgi, kā atgādināja EST, ir jāņem vērā ECT judikatūra par tiesībām, kas paredzētas arī ES hartā, kā minimālais aizsardzības sliekšnis, interpretējot atbilstošās tiesības ES hartā<sup>88</sup>. Tomēr saskaņā ar ES hartas 52. panta 3. punkta pēdējo teikumu “*šis noteikums neliedz Savienības tiesībās paredzēt plašāku aizsardzību*”.
147. Tāpēc turpmākajā novērtējumā EDAK ir ņēmusi vērā ECT judikatūru, ciktāl ES harta, kā to interpretē EST, neparedz augstāku aizsardzības līmeni, kas paredz citas prasības, kuras atšķiras no ECT judikatūrā paredzētajām.

#### 4.3.1. Juridiskais pamats, ierobežojumi un aizsardzības pasākumi — izmeklēšanas pilnvaras, ko izmanto nacionālās drošības kontekstā

##### 4.3.1.1. Vispārīgas piezīmes

148. EDAK atgādina, ka *IPA 2016* ir jauns likums, ar kuru tika grozīti vairāki 1994. gada Izlūkdienestu likuma noteikumi. Tajā noteikts, kādā mērā dažas izmeklēšanas pilnvaras var izmantot, lai iejauktos privātumā<sup>89</sup>. Neraugoties uz diviem *IPC* ziņojumiem, kuros sniegta lietderīga informācija par šā jaunā tiesiskā regulējuma piemērošanu, joprojām nav pārskatīti daži aspekti, jo īpaši attiecībā uz izmantotajiem atlasītājiem un meklēšanas kritērijiem.
149. Turklāt EDAK kā vispārīgu piezīmi par *IPA 2016* un tā piemērošanas jomu izceļ turpmākos četrus punktus, kam jāpievērš uzmanība.
150. Saistībā ar **pirmo punktu, kam jāpievērš uzmanība**, ņemot vērā likuma iezīmes, EDAK vēlas uzsvērt divus aspektus.
151. Pirmkārt, EDAK norāda, ka tiesību akti attiecas uz plašiem *IPA 2016* paredzēto procedūru izmantošanas nolūkiem, nevis uz to personu kategorijām, kuras varētu ietekmēt datu vākšana, pamatojoties uz *IPA 2016* 2.–7. daļu. Šajā saistībā EDAK atgādina, ka vajadzētu būt saiknei starp to personu kategorijām, uz kurām var attiekties uzraudzības pasākumi, un tiesību aktos paredzētajiem nolūkiem, nosakot likuma darbības jomu attiecībā uz personu.
152. Turklāt EDAK arī uzsver, ka “telesakaru operatoru”, “telesakaru pakalpojuma” un “telesakaru sistēmas” definīcija, kas nosaka likuma darbības jomu, arī ir ļoti plaša un zināmā mērā neskaidra.

<sup>86</sup> Sk. EDAK ieteikumus 02/2020 attiecībā uz Eiropas būtiskajām garantijām uzraudzības pasākumiem.

<sup>87</sup> Sk. *Schrems II*, 98. punkts.

<sup>88</sup> Sk. EST apvienotās lietas C-511/18, C-512/18 un C-520/18, *La Quadrature du Net* un citi, 2020. gada 6. oktobris, ECLI:EU:C:2020:791, 124. punkts.

<sup>89</sup> Sk. *IPA 2016* 1. pantu.

Patiešām, EDAK uzsver, ka *IPA 2016* jomā šie jēdzieni ir jāsaprot daudz plašāk nekā saistībā ar telesakaru tiesību aktiem, kā tas noteikts, piemēram, Eiropas Elektronisko sakaru kodeksā<sup>90</sup>. EDAK norāda, ka “telesakaru pakalpojuma” un “telesakaru sistēmas” definīcijas likumā ir apzināti noteiktas plašas, lai tās būtu attiecināmas arī uz jaunajām tehnoloģijām. Arī telesakaru operatora definīcija ir ļoti plaša, un tā, piemēram, varētu ietvert tiešsaistes videospēles ar iekļautu tērzēšanas funkciju vai citas tiešsaistes tīmekļa vietnes, kurās vienkārši iekļauti šādi tērzēšanas logi<sup>91</sup>.

153. Turklāt, lai gan procedūras un uzraudzība attiecībā uz datu vākšanas un piekļuves tiem nepieciešamības un proporcionalitātes novērtēšanu parasti ir nodrošinātas, pašā likumā nav noteikti kritēriji šāda novērtējuma veikšanai. Papildu elementi ir atrodami citos dokumentos, piemēram, prakses kodeksos.
154. Tomēr, kā atgādināts EDAK leteikumos 02/2020 attiecībā uz Eiropas būtiskajām garantijām uzraudzības pasākumiem, EST ir norādījusi, ka “*prasība, saskaņā ar kuru jebkuram pamattiesību izmantošanas ierobežojumam ir jābūt noteiktam tiesību aktos, nozīmē, ka pašā juridiskajā pamatā ir jānosaka attiecīgo tiesību īstenošanas ierobežojuma apjoms*”<sup>92</sup>. Precīzāk, EST paskaidroja, ka, “*lai izpildītu samērīguma prasību, tiesiskajā regulējumā ir jāparedz skaidri un precīzi noteikumi, kas reglamentē attiecīgā pasākuma tvērumu un piemērošanu un paredz minimālās prasības, lai tā rezultātā personām, kuru personas dati tikuši pārsūtīti, būtu pietiekamas garantijas, kas ļautu šos datus efektīvi aizsargāt pret ļaunprātīgas izmantošanas risku. Šim tiesiskajam regulējumam ir jābūt juridiski saistošam valsts tiesībās un tajā it īpaši ir jānorāda, kādos apstākļos un saskaņā ar kādiem nosacījumiem var īstenot pasākumu, kas ietver šādu datu apstrādi, tādējādi garantējot, ka šāda iejaukšanās notiek tikai absolūti nepieciešamā robežās*”<sup>93</sup>.
155. ECT arī uzsvēra, ka ir svarīgi, lai likums nepārprotami sniegtu indivīdiem *pietiekamu norādi par to, kādos apstākļos un ar kādiem nosacījumiem publiskās iestādes ir pilnvarotas izmantot šādus pasākumus*<sup>94</sup>.
156. **Tāpēc EDAK aicina Eiropas Komisiju sīkāk izvērtēt šos aspektus, kas attiecas uz attiecīgo tiesību aktu precizitāti, skaidrību un pilnīgumu, un sniegt papildu elementus, lai pierādītu, ka tā nodrošina aizsardzības līmeni, kas pēc būtības ir līdzvērtīgs tam, ko nodrošina ES attiecībā uz tiesību akta iezīmēm. EDAK arī uzsver, ka plašas definīcijas arī būtu jāizvērtē saistībā ar pārtveršanas pasākumu proporcionalitāti.**
157. Turklāt, lai arī vairāki kompetento izlūkošanas kopienas iestāžu iekšējie kodeksi daļēji attīsta dažus no šiem elementiem, piemēram, attiecībā uz datu vākšanas nepieciešamības un proporcionalitātes novērtējumu, EDAK uzsver, ka EST prasības attiecībā uz tiesību akta būtību paredz, ka galvenie elementi, tostarp tas, lai indivīdi varētu uz tiem paļauties tiesiskās aizsardzības ietvaros, ir jāparedz

---

<sup>90</sup> Sk. Eiropas Elektronisko sakaru kodeksa 2. panta 5. punktu, kurā, piemēram, “starppersonu sakaru pakalpojums” ir definēts kā “*pakalpojums, ko parasti sniedz par atlīdzību, kas dod iespēju galīgam personu skaitam elektronisko sakaru tīklos tieši savā starpā interaktīvi dalīties informācijā un kur saziņas sācējas vai dalībnieces personas nosaka saņēmējus, un kurā neietilpst pakalpojumi, kuros interaktīva starppersonu saziņa ir tikai ar citu pakalpojumu saistīta sīka palīgfunckcija*”.

<sup>91</sup> Sk. Iekšlietu ministrijas Saziņas pārtveršanas prakses kodeksu, 2018. gada marts, 2.5. un turpmākie punkti, [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> Sk. *Schrems II*, 175. punkts; minēto judikatūru, kā arī EST lietu C-623/17, *Privacy International / Secretary of State for Foreign and Commonwealth Affairs un citi*, 2020. gada 6. oktobris, ECLI:EU:C:2020:790 (turpmāk tekstā — *Privacy International*), 65. punkts.

<sup>93</sup> Sk. *Privacy International*, 68. punkts.

<sup>94</sup> Sk. ECT, *Zakharov/Russia*, 2015. gada 4. decembris, CE:ECHR:2015:1204JUD004714306, 229. punkts.

tiesību aktos, kas paredz tiesības, kuras var izmantot<sup>95</sup>. Patiešām, *IPA 2016* 7. pielikuma 6. punktā ir minēts tas, ka tiesas (un uzraudzības iestādes) *ņem vērā personas nespēju ņemt vērā kodeksu, nosakot jautājumu jebkurā šādā tiesvedībā*, nepaskaidrojot, vai personas var iesniegt tiesā (vai uzraudzības iestādēs) prasību par kodeksu pārkāpumu. Turklāt lēmuma projektā līdz šim paredzētie elementi vai nu attiecas uz to, ka ECT atzīst šajos kodeksos paredzēto noteikumu paredzamību<sup>96</sup>, nevis to izmantojamību tiesā, kā to pieprasa Eiropas Savienības Tiesa, vai arī to, ka Apvienotās Karalistes tiesas dažās lietās ir atsaukušās uz kodeksiem, taču nevienā no gadījumiem netika minēta iespēja indivīdiem izmantot tiesības, kas izriet no kodeksiem. **Ja tiks secināts, ka Apvienotās Karalistes tiesību aktos ir nepietiekami izklāstīti apstākļi un nosacījumi, saskaņā ar kuriem var pieņemt pasākumu, un ka šos elementus faktiski nodrošina izlūkošanas kopienas iestāžu iekšējie kodeksi, EDAK aicinās Eiropas Komisiju sīkāk izvērtēt, vai indivīdi tiesā var izmantot ierobežojumus un aizsardzības pasākumus, kas paredzēti dažādos izlūkošanas kopienas iestāžu iekšējos kodeksos, un īstenot tos.**

158. **Otrais punkts, kam jāpievērš uzmanība**, ir par to, ka *IPA 2016* vai citu tiesību aktu, piemēram, 1994. gada Izlūkdienestu likuma vai 2000. gada Likuma par izmeklēšanas pilnvaru regulējumu, noteikumi, kas attiecas, no vienas puses, uz saziņas datu mērķorientētu iegūšanu un saglabāšanu un, no otras puses, uz datu vākšanu lielā apjomā, tiks piemēroti arī datiem, kas nosūtīti no ES uz Apvienoto Karalisti. Attiecībā uz datu vākšanu lielā apjomā EDAK uzsver, ka attiecīgie Apvienotās Karalistes tiesību aktu noteikumi ļauj vākt datus ārpus Apvienotās Karalistes, tādējādi varētu ietvert datus, kas atrodas tranzītā un ir nosūtīti no EEZ uz Apvienoto Karalisti, pamatojoties uz lēmumu par pietiekamību<sup>97</sup>. Turklāt EDAK ievēro, ka Eiropas Komisija norāda uz to, ka *saziņas datu saglabāšana un iegūšana parasti neattiecas uz ES datu subjektu personas datiem, kas saskaņā ar šo lēmumu nosūtīti uz Apvienoto Karalisti. Pienākums saglabāt vai atklāt saziņas datus saskaņā ar IPA 2016 3. un 4. daļu attiecas uz datiem, kurus telesakaru operatori Apvienotajā Karalistē vāc tieši no telesakaru pakalpojumu lietotājiem*<sup>98</sup>. Neraugoties uz to, EDAK uzsver, ka nav pietiekamas skaidrības par to, ka tikai šo operatoru uzņēmumi, kas atrodas Apvienotajā Karalistē, var saņemt pieprasījumus no Apvienotās Karalistes kompetentajām iestādēm, jo *IPA 2016* 261. panta 10. punktā sniegtā telesakaru operatora definīcija paredz, ka telesakaru operators ir persona, kas piedāvā vai sniedz telesakaru pakalpojumus personām Apvienotajā Karalistē vai kas kontrolē vai nodrošina telesakaru sistēmu, kura (pilnībā vai daļēji) atrodas Apvienotajā Karalistē vai tiek kontrolēta no tās. Tādējādi faktiski varētu būt skarti EEZ datu subjektu personas dati, piemēram, ja datus savāc vai ģenerē Apvienotās Karalistes telesakaru operatora uzņēmums, kas atrodas EEZ, tos nodod šā paša operatora uzņēmumam, kas atrodas Apvienotajā Karalistē, pamatojoties uz lēmumu par pietiekamību (komerciāliem nolūkiem), un pēc tam Apvienotajā Karalistē tos apkopo kompetentās valsts iestādes.
159. **Tāpēc EDAK uzskata, ka šo noteikumu novērtējums ir svarīgs arī Apvienotās Karalistes tiesiskā regulējuma pietiekamības līmeņa novērtēšanai, un aicina Eiropas Komisiju precizēt šo aspektu un novērtēt arī to, cik svarīgs tas ir. Jo īpaši EDAK aicina Eiropas Komisiju precizēt savu izpratni par šo**

<sup>95</sup> Šajā saistībā EST uzskatīja, ka, piemēram, ASV PPD-28 nebija atbilstoša, lai gan tajā bija paredzēti arī daži ierobežojumi attiecībā uz datu vākšanu lielā apjomā, sk. *Schrems II*, 181. punkts.

<sup>96</sup> Sk. ECT, *Big Brother Watch* un citi / Apvienotā Karaliste, 2018. gada 13. septembris, ECLI:CE:ECHR:2018:0913JUD005817013 (turpmāk tekstā — *Big Brother Watch*), 325. punkts: *tā kā IC kodekss ir publisks dokuments, kas jāapstiprina abām parlamenta palātām un jāņem vērā gan tiem, kas veic pārtveršanas pienākumus, gan tiesām un tribunāliem, Tiesa ir nepārprotami piekritusi, ka tā noteikumus varētu ņemt vērā, novērtējot RIPA režīma paredzamību*.

<sup>97</sup> Sk. *Schrems II* 183. un turpmākos punktus par tādu tiesību aktu novērtējumu, kas nodrošina piekļuvi datiem, kuri atrodas tranzītā starp ES un trešo valsti saistībā ar lēmumu par pietiekamību.

<sup>98</sup> Sk. lēmuma projekta 196. apsvērumu.

tiesību aktu darbības jomu, tostarp par to, ko aptver jēdziens “telesakaru pakalpojumu lietotāji”, un to, vai varētu pieprasīt datus no telesakaru operatoru iestādēm ārpus Apvienotās Karalistes, ciktāl ir skarti EEZ datu subjektu dati, ņemot vērā telesakaru operatoru ļoti plašo definīciju.

160. **Trešais punkts, kam jāpievērš uzmanība**, attiecas uz divkāršās bloķēšanas procedūru. EDAK norāda, ka *IPA 2016* ir ieviesta jauna divkāršās bloķēšanas procedūra. Tomēr EDAK saprot arī to, ka pat tad, ja principā datu vākšana vai piekļuve tiem nacionālās drošības vai izlūkošanas nolūkos var notikt tikai ar tieslietu komisāra apstiprinātu orderi, *IPA 2016* ir paredzēts, ka *īpašos ierobežotos gadījumos ir iespējama likumīga pārtveršana bez ordera, un ir nepieciešama tikai iepriekšēja kompetento IC iestāžu atļauja [skatīt iedaļu par uzraudzību]*, tostarp attiecībā uz pārtveršanu saskaņā ar ārvalstu pieprasījumiem (*IPA 2016 52. pants*). Kā uzsvērts turpmāk, tas atbilst arī EDAK bažām galvenokārt attiecībā uz informācijas atklāšanu ārvalstīs. Turklāt EDAK arī norāda, ka attiecībā uz iejaukšanos ar aprīkojumu neatkarīgi no tā, vai tā notiek mērķorientēti vai lielā apjomā, ir iespējama arī atkāpe no divkāršās bloķēšanas procedūras un tieslietu komisārs pēc maksimālā sākotnējā sešu mēnešu perioda ir tiesīgs apstiprināt tikai tādu orderu atjaunošanu, kas attiecas uz datu lielapjoma pārtveršanu. **EDAK aicina Eiropas Komisiju sīkāk izvērtēt un pierādīt, ka pat gadījumos, kad divkāršās bloķēšanas procedūra nav piemērojama, Apvienotās Karalistes tiesiskais regulējums paredz piemērotus aizsardzības pasākumus, tostarp efektīvas *ex post* uzraudzības un tiesiskās aizsardzības iespējas, kas tiek piedāvātas indivīdiem, nodrošināt, ka sniegtais aizsardzības līmenis pēc būtības ir līdzvērtīgs tam, ko sniedz ES (sk. arī 4.3.3. iedaļu par uzraudzību).**
161. Turklāt, lai gan *IPA 2016* patiešām ir ieviesta divkāršās bloķēšanas procedūra, EDAK joprojām ir noraizējusies par dažām jauno tiesību aktu iezīmēm. Pēc lēmuma projekta attiecīgo iedaļu izklāsta EDAK ir analizējusi turpmāk minētos datu vākšanas un piekļuves tiem veidus tādā pašā secībā, kādā tos iesniedza Eiropas Komisija. Tāpēc turpmāk novērtēto elementu secība neatbilst hierarhiju atbilstīgi EDAK bažu līmenim.
- [4.3.1.2. Mērķorientēta saziņas datu iegūšana un saglabāšana](#)
162. EDAK norāda, ka ir divi ierēdņi, kuri var piešķirt atļaujas tieši saziņas datu iegūšanai: kredītrīkotājs Saziņas datu iegūšanas atļauju biroja (turpmāk tekstā — *IPC*), iecelts vecākais ierēdnis (persona, kurai ir noteikts amats vai dienesta pakāpe attiecīgā publiskajā iestādē) papildus tieslietu komisāra apstiprinājumam noteiktos gadījumos. Tomēr saskaņā ar likumu un attiecīgo kodeksu EDAK aizvien nav skaidrs, kurš ierēdnis atļauj kāda veida saziņas datu mērķorientētu iegūšanu un cik lielā mērā ieceltais ierēdnis būtu pietiekami neatkarīgs<sup>99</sup>.
163. **Tāpēc EDAK aicina Eiropas Komisiju sīkāk izvērtēt arī šo aspektu un sniegt precīzākus skaidrojumus par šiem elementiem.**
164. Attiecībā uz paziņojumu par nepieciešamību saglabāt saziņas datus EDAK arī norāda, ka šādus paziņojumus var attiecināt uz “operatoru aprakstu”. Šķiet, ka šis jēdziens nozīmē, ka vienlaikus vairākiem operatoriem var pieprasīt saglabāt datus. Patiešām, mērķorientēta iegūšana nav saistīta ar operatoru skaitu, bet gan ar personu, organizāciju, atrašanās vietu vai personu grupu, kas veido “mērķi”, nosaukumu vai aprakstu, izmeklēšanas veida aprakstu un to darbību aprakstu, kurām aprīkojums tiek izmantots. Tāpēc EDAK uzsver, ka atkarībā no to operatoru skaita, uz kuriem attiecas šāds “operatoru apraksts”, paziņojums var būt plašāks par to, ko varētu paredzēt mērķorientētas saglabāšanas procedūra. **EDAK aicina Eiropas Komisiju sīkāk izvērtēt arī šo aspektu un sniegt**

---

<sup>99</sup> Sk. arī iedaļu par divkāršās bloķēšanas procedūras novērtējumu un tieslietu komisāra neatkarību.

**papildu garantijas, ka pat tad, ja paziņojumi ir adresēti vairākiem operatoriem, tie joprojām ir ierobežoti līdz tam, kas ir absolūti nepieciešams un proporcionāls.**

#### 4.3.1.3. Iejaukšanās ar aprīkojumu

165. EDAK norāda, ka steidzamības gadījumā, veicot “iejaukšanos ar aprīkojumu”, var atkāpties no divkāršās bloķēšanas procedūras<sup>100</sup>. Tāpēc EDAK ir noraizējusies, ka nolūki, kādos var tikt pieprasīta šāda iejaukšanās ar aprīkojumu, ir plaši un ka steidzamības (šajā gadījumā tieslietu komisāram nav jāpiešķir *ex ante* atļauja pēc tam, kad ir novērtēta iejaukšanās ar aprīkojumu nepieciešamība un proporcionalitāte) kritēriji aizvien ir neskaidri. Tā kā steidzamības gadījumā orderis vairs nav spēkā un to nevar atjaunot, ja tieslietu komisārs neapstiprina *ex post* iejaukšanos ar aprīkojumu, EDAK saprot, ka tikmēr savākie dati joprojām ir likumīgi savākti. Lai šos datus varētu dzēst, tieslietu komisārs var izdot īpašu rīkojumu<sup>101</sup>.
166. **EDAK aicina Eiropas Komisiju sīkāk izvērtēt arī nosacījumus, ar kādiem var atsaukties uz steidzamību, un sniegt skaidrojumus par attiecīgo datu subjektu tiesību iespējamiem izmantošanas gadījumiem, kā arī iespējamiem tiesiskās aizsardzības veidiem, kas tiem ir pieejami saistībā ar iejaukšanās darbībām, izmantojot aprīkojumu, jo īpaši tad, ja tās notiek steidzami, atkāpjoties no divkāršās bloķēšanas procedūras.**

#### 4.3.1.4. Datu lielapjoma pārtveršana no nesējiem

167. Kā aprakstīts ziņojumā par lielapjoma pārtveršanas pilnvaru pārskatu<sup>102</sup>, *lielapjoma pārtveršana parasti ietver saziņas datu vākšanu, kad tie atrodas tranzītā konkrētos nesējos (saziņas saites)*. Oficiālajā faktu lapā par *IPA 2016* lielapjoma pārtveršana ir raksturota kā *lielapjoma saziņas datu vākšanas process, kam seko tādu konkrētu saziņas datu atlase, kas jālasa, jāskatās vai jāklausa, ja tas ir nepieciešami un proporcionāli*. EDAK norāda, ka datu lielapjoma pārtveršana faktiski nozīmē datu vākšanu pat pirms jebkādas atlasītāju veiktas filtrēšanas (vai nu vienkārši, uzraugot personas, par kurām jau zināms, ka tās rada draudus, vai sarežģīti, identificējot jaunus draudus un iepriekš nezināmas personas, kas raisa interesi).
168. Saziņas datu iegūšana lielā apjomā bija arī viens no jautājumiem, ko EST izskatīja *Privacy International* lietā, kurā tika pieņemts virspalātas spriedums, kas tika izdots 2020. gada 6. oktobrī (papildus tam, vai šāda datu vākšana tika veikta saistībā ar ES tiesību aktiem, pat nacionālās drošības nolūkos). *IPA 2016* ir aizstājis tiesību aktus, kas bija šā sprieduma priekšmets.
169. EDAK norāda, ka līdz ar *IPA 2016* ieviešanu Apvienotās Karalistes tiesību aktos tagad ir vajadzīgs orderis arī datu lielapjoma pārtveršanai. Šā ordera izsniegšanas process ir atkarīgs no “darbības nolūku” noteikšanas. Šo darbības nolūku sarakstu izveido izlūkdienestu vadītāji, un pēc tam to apstiprina valsts sekretārs. Pašu lēmumu apstiprina neatkarīgs tieslietu komisārs, kuram jāpārbauda, vai orderis ir nepieciešams un proporcionāls darbības nolūkiem. EDAK saprot, ka tieslietu komisāram nav pilnvaru pašam novērtēt darbības nolūkus, taču viņš var novērtēt, vai orderis ir nepieciešams un proporcionāls orderī minētajiem darbības nolūkiem. Parlamenta Izlūkošanas un drošības komitejai tiek iesniegta saraksta kopija ik pēc trim mēnešiem, un premjerministrs pārskata šo darbības nolūku sarakstu vismaz reizi gadā.

---

<sup>100</sup> Sk. *IPA 2016* 109. pantu.

<sup>101</sup> Sk. *IPA 2016* 110. panta 3. punkta b) apakšpunktu.

<sup>102</sup> Sk. Ziņojumu par lielapjoma pilnvaru pārskatīšanu, ko sagatavojis terorisma novēršanas tiesību aktu neatkarīgais pārskatītājs, 2016. gada augusts.

170. Tomēr, pamatojoties uz Eiropas Komisijas lēmuma projektā norādītajiem elementiem, šķiet grūti novērtēt sarakstā norādīto darbības nolūku apjomu un to, vai atļautā datu vākšana atbilst EST noteiktajam sliekšnim (piemēram, datu vākšanas ierobežošana ģeogrāfiskā apgabalā varētu aptvert gan dažas ielas, gan EEZ kopumā).
171. Turklāt EDAK uzsver, ka lielā apjomā savāktus datus var glabāt ilgu laiku (lai tiem varētu piekļūt turpmāk pārbaudes vajadzībām). Patiešām, EDAK norāda, ka *IPA 2016* 150. panta 5. un 6. punkts paredz tikai savākto datu kopiju iznīcināšanu un tikai tad, ja to saglabāšana nav vajadzīga vai, iespējams, nebūs vajadzīga nacionālās drošības interesēs vai jebkura cita iemesla dēļ saskaņā ar *IPA 2016* 138. panta 2. punktu vai ja saglabāšana nav nepieciešama vairākos citos nolūkos<sup>103</sup>. EDAK uzsver, ka šie iemesli šķiet ļoti plaši, un jebkurā gadījumā tiek minētas tikai iegūto datu kopijas.
172. Turklāt EDAK arī norāda, ka steidzamos gadījumos *IPA 2016* ļauj arī veikt izmaiņas orderos bez iepriekšēja tieslietu komisāra apstiprinājuma un šādā gadījumā, ja tieslietu komisārs *ex post* trīs darbadienu laikā pēc iepazīšanās ar izmaiņām atsakās tās apstiprināt, orderim būtu jāstājas spēkā tā, it kā izmaiņas nebūtu veiktas, bet starplaikā savāktie dati aizvien ir likumīgi savākti<sup>104</sup>. Lai šos datus varētu dzēst, tieslietu komisārs var izdot īpašu rīkojumu<sup>105</sup>.
173. **Tāpēc EDAK aicina Eiropas Komisiju sniegt sīkākus skaidrojumus un novērtēt arī datu lielapjoma pārtveršanu, jo īpaši attiecībā uz atlasītāju atlasī un izmantošanu saistībā ar šīm datu lielapjoma pārtveršanas procedūrām, lai precizētu, cik lielā mērā piekļuve personas datiem atbilst sliekšnim, ko noteikusi EST (sk. arī 4.3.1.7. iedaļu, jo īpaši par atlasītāju uzraudzību), un kādi aizsardzības pasākumi ir ieviesti, lai aizsargātu to personu pamattiesības, kuru dati tiek pārtverti šajā saistībā, tostarp attiecībā uz datu saglabāšanas periodiem. Īpaši lietderīgs būtu Apvienotās Karalistes kompetento uzraudzības iestāžu neatkarīgs novērtējums.**
174. EDAK arī uzsver, ka vēl jo svarīgāk šķiet, ka “ar ārvalstīm saistīta saziņa”, kas ietilpst datu lielapjoma pārtveršanas prakses darbības jomā, nozīmē, ka Apvienotā Karaliste datus varētu tieši pārtvert un vākt lielā apjomā EEZ, ieskaitot datus, kuri atrodas tranzītā starp EEZ un Apvienoto Karalisti un uz kuriem attiecas lēmuma projekts (sk. 4.3.2. iedaļu par savāktās informācijas turpmāku izmantošanu nacionālās drošības nolūkos un informācijas atklāšanu ārvalstīs).

#### 4.3.1.5. Sekundāro datu aizsardzība un aizsardzības pasākumi

175. Turklāt EDAK pauž bažas par to, ka Apvienotās Karalistes attiecīgie tiesību akti, kas saistīti ar datu lielapjoma pārtveršanu, neparedz vienādu aizsardzības līmeni visiem saziņas datiem. “Sekundārie dati”, kurus var iegūt ar orderi datu lielapjoma pārtveršanai, saskaņā ar *IPA 2016* 137. pantu, ir gan “sistēmas dati”, kas veido saziņu, ir iekļauti kā tās daļa, pievienoti tai vai loģiski saistīti ar to (neatkarīgi no tā, vai to paveicis sūtītājs, vai tas izdarīts citādi), gan “identifikācijas dati”, kas veido saziņu, ir iekļauti kā tās daļa, pievienoti tai vai loģiski saistīti ar to (neatkarīgi no tā, vai to paveicis sūtītājs, vai tas izdarīts citādi), ko var loģiski nodalīt no pārējās saziņas un kas, ja tos tā nodalītu, neatklātu neko no tā, ko varētu pamatoti uzskatīt par saziņas nozīmi (ja tāda ir), neņemot vērā nozīmi, kas izriet no saziņas fakta vai jebkādiem datiem, kuri saistīti ar saziņas nosūtīšanu<sup>106</sup>.

<sup>103</sup> Sk. *IPA 2016* 150. panta 3. un 6. punktu.

<sup>104</sup> Sk. *IPA 2016* 147. pantu (6. daļas I nodaļa).

<sup>105</sup> Sk. *IPA 2016* 181. panta 3. punkta b) apakšpunktu.

<sup>106</sup> “Sistēmas dati” un “identifikācijas dati” ir definēti *IPA 2016* 263. pantā.

176. EDAK norāda, ka uz šiem sekundārajiem datiem, kas pazīstami arī kā “metadati”<sup>107</sup> un ir savākti lielā apjomā, neattiecas tādi paši aizsardzības pasākumi kā uz datiem, kas savākti ar mērķorientētu orderi, un satura datiem, kas savākti lielā apjomā. Patiešām, EDAK ievēro, ka jebkura pārtverta satura atlasei ir vairāk aizsardzības pasākumu<sup>108</sup> nekā sekundāro datu atlasei<sup>109</sup>.
177. Turklāt EDAK uzsver, ka gan ECT<sup>110</sup>, gan EST<sup>111</sup> ir apšaubījusi to, ka šādi dati ir mazāk sensitīvi nekā citi un jo īpaši satura dati. Patiešām, pārtveršanas prakses kodeksā ir minēti “sekundāro datu” piemēri (gan “sistēmas dati”, piemēram, maršrutētāja konfigurācijas, e-pasta adreses vai lietotāja ID, gan arī alternatīvi konta identifikatori, kā arī “identifikācijas dati”, piemēram, sanāksmes atrašanās vieta kalendārā, informācija par fotogrāfiju, piemēram, tās uzņemšanas laiks, datums un vieta). **Tādējādi EDAK uzsver ECT un EST konsekvētu novērtējumu un atgādina par paustajām bažām saistībā ar sekundārajiem datiem, kuriem būtu jāpiemēro īpaši aizsardzības pasākumi to sensitivitātes dēļ. Tāpēc EDAK aicina Eiropas Komisiju rūpīgi izvērtēt, vai Apvienotās Karalistes likumos paredzētie aizsardzības pasākumi šādai personas datu kategorijai nodrošina pēc būtības līdzvērtīgu aizsardzības līmeni tam, kāds ir garantēts ES.**

#### 4.3.1.6. Automātiska saziņas datu apstrāde

178. EDAK norāda, ka izlūkošanas kopienas iestādes izmanto ne tikai vienkāršus vai sarežģītus atlasītājus, lai filtrētu lielā apjomā iegūtos datus, bet var izmantot arī citus automātiskas apstrādes rīkus, lai analizētu *lielu informācijas apjomu, kas iestādēm ļauj konstatēt arī saites, modeļus, asociācijas vai uzvedību, kura var liecināt par nopietniem draudiem, kas jāizmeklē*, teikts Izlūkošanas un drošības komitejas 2015. gada ziņojumā<sup>112</sup>. **EDAK apzinās to, ka šis publiskais ziņojums attiecas uz praksi saskaņā ar iepriekšējo tiesisko regulējumu, kuru vēlāk aizstāja ar IPA 2016. Neskatoties uz to, tā uzskata, ka kompetentajām AK uzraudzības iestādēm ir jāveic papildu neatkarīgs novērtējums un automatizēto apstrādes rīku izmantošanas uzraudzība, un aicina Eiropas Komisiju sīkāk novērtēt**

<sup>107</sup> Sk. Ziņojumu par lielapjoma pilnvaru pārskatīšanu, ko sagatavojis terorisma novēršanas tiesību aktu neatkarīgais pārskatītājs, 2016. gada augusts.

<sup>108</sup> Sk. IPA 2016 152. panta 1. punkta c) apakšpunktu, kā arī 3. un turpmākos punktus.

<sup>108</sup> Sk. IPA 2016 152. panta 1. punkta c) apakšpunktu, kā arī 3. un turpmākos punktus.

<sup>109</sup> Skatīt IPA 2016 152. panta 1. punkta a) un b) apakšpunktu.

<sup>110</sup> Sk. ECT, *Big Brother Watch*, 357. punkts, saskaņā ar nodošanu virspalātai: “*attiecīgi, lai arī Tiesa nešaubās, ka saistītie saziņas dati ir izlūkdienestu būtisks rīks cīņā pret terorismu un smagiem noziegumiem, tā neuzskata, ka varas iestādes ir panākušas taisnīgu līdzsvaru starp konkurējošām publiskām un privātām interesēm, pilnībā atbrīvojot to no aizsardzības pasākumiem, kas piemērojami satura meklēšanai un pārbaudei. Lai gan Tiesa neierosina, ka saistītiem saziņas datiem vajadzētu būt pieejamiem tikai nolūkā noteikt, vai indivīds atrodas vai neatrodas Britu salās, jo tāpēc saistītajiem saziņas datiem vajadzētu piemērot stingrākus standartus nekā saturam, tomēr vajadzētu būt pietiekamiem aizsardzības pasākumiem, lai nodrošinātu, ka saistīto saziņas datu atbrīvojums no RIPA 16. panta prasībām ir ierobežots, ciktāl nepieciešams, lai noteiktu, vai indivīds pašlaik atrodas Britu salās*”.

<sup>111</sup> Sk. EST, *Privacy International*, 71. punkts: “*Iejaukšanās Hartas 7. pantā paredzētajās tiesībās, ko rada informācijas par datu plūsmu un atrašanās vietas datu nodošana drošības dienestiem un izlūkdienestiem, ir jāuzskata par īpaši smagu, ņemot vērā tostarp informācijas, kuru var sniegt šie dati, sensitīvo raksturu un it īpaši iespēju, pamatojoties uz tiem, pierādīt datu subjekta profilu, jo šāda informācija ir tikpat sensitīva kā pats komunikācijas saturs. Turklāt šis apstāklis datu subjektu apziņā var radīt sajūtu, ka to privātā dzīve tiek pastāvīgi uzraudzīta (pēc analogijas skat. spriedumus, 2014. gada 8. aprīlis *Digital Rights Ireland* u. c., C-293/12 un C-594/12, EU:C:2014:238, 27. un 37. punkts, kā arī 2016. gada 21. decembris, *Tele2*, C-203/15 un C-698/15, EU:C:2016:970, 99. un 100. punkts).*”

<sup>112</sup> Sk. Parlamenta Izlūkošanas un drošības komitejas ziņojumu “*Privacy and Security: A modern and transparent legal framework*”, 2015. gads, 18. punkts, 13. lpp., [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).

**šo jautājumu un aizsardzības pasākumus, kas tiktu un/vai varētu tikt piešķirti EEZ datu subjektiem šajā saistībā.**

#### 4.3.1.7. Atbilstības riski un kompetento izlūkošanas kopienas iestāžu neatbilstoša prakse

179. EDAK ņem vērā, ka ir pieejami detalizēti uzraudzības ziņojumi. Tajos norādīti vērtīgi elementi attiecībā uz to, kas tiek vērtēta kā pozitīva atbilstības prakse, kā arī attiecībā uz konstatētajiem atbilstības riskiem un neatbilstošu praksi.
180. Šajā ziņā, kā norādīja *IPC* savā ziņojumā par 2019. gadu, vairāki elementi, kas attiecas uz to, kā dažādas kompetentās iestādes piemēro tiesisko regulējumu, ir atklājuši dažas kompetento iestāžu neatbilstības (to riskus).
181. Pirmkārt, EDAK ir ievērojusi, ka kritēriji datu kopas klasificēšanai par lielapjoma personas datu kopu vai mērķorientētiem datiem ne vienmēr ir skaidri pašiem *MI5* un *SIS*, jo īpaši *MI5*; tādējādi datiem var netikt piemēroti atbilstoši aizsardzības pasākumi<sup>113</sup>. *IPC* savā ziņojumā par 2019. gadu ierosināja, ka *šis jautājums būtu jārisina kā prioritārs*<sup>114</sup>. Arī saistībā ar lielapjoma personas datu kopām EDAK norāda, ka attiecībā uz *GCHQ*, lai arī šķiet, ka lielapjoma personas datu kopu klasifikācija ir apmierinoša (bet *IPC* vēl jāveic revīzija par to), 2019. gada martā īpašas komandas veikta orderu iekšējā atbilstības pārbaude raisīja nopietnas bažas — 50 % pamatojumu tādiem orderiem datu iegūšanai lielā apjomā, kurus pārbaudīja *GCHQ* atbilstības komanda, neatbilda noteiktajam standartam. Kā norādīja *IPC*, atbilstības komanda bija sākusi darbu, lai izpētītu problēmu un pārkvalificētu personālu ar mērķi uzlabot šo standartu. Atjauninātā apmācība par *IPA 2016* noteikumiem un papildu apmācība, ko nodrošina politikas un atbilstības tīkli (turpmāk tekstā — *PCN*), ir uzlabojusi *GCHQ* atbilstību šajā jomā. *IPC* negaida, ka turpmākajās pārbaudēs tiks novērots šā standarta kritums, taču turpinās šo jomu rūpīgi pārbaudīt<sup>115</sup>. **Tāpēc EDAK piekrīt viedoklim, ka, veicot aizsardzības līmeņa novērtējumu, Eiropas Komisijai ir jāveic sīkāka minēto elementu pārbaude un uzraudzība, lai nodrošinātu šā standarta uzlabošanu, kā uzsvērts *IPC* ziņojumā, un atgādina, ka, novērtējot trešās valsts līdzvērtīgumu pēc būtības, ņem vērā arī tiesiskā regulējuma īstenošanu un konkrētu piemērošanu, kā paredzēts *VDAR 45. pantā*.**
182. Plašākā mērogā EDAK uzsver punktus, kam jāpievērš uzmanība un ar ko dalījies *IPC* attiecībā uz “uzdevumā balstītu meklēšanu”, ko vada *MI5* darbinieki, kas ļauj izmeklētājam veikt vairāk nekā vienu tam pieejamo lielapjoma personas datu kopu meklēšanu, un *nopietniem atbilstības riskiem, kas saistīti ar noteiktām *MI5* izmantotām tehnoloģiju vidēm* attiecībā uz to, kur dati tika glabāti vidē, kam bija piekļuve tiem, cik lielā mērā tie tika kopēti vai koplietoti, uz tiem attiecināmajiem dzēšanas procesiem, kā arī attiecībā uz saglabāšanas periodiem. Lai gan *IPC* norāda, ka ir veikti pasākumi un ieviesti aizsardzības pasākumi, daži no tiem joprojām ir manuāli un vadāmi individuāli, izmantojot

<sup>113</sup> Sk. izmeklēšanas pilnvaru komisāra 2019. gada ziņojumu, 2020. gada 15. decembris, 8.39. punkts, <https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPC-Annual-Report-2019-Web-Accessible-version-final.pdf>: “mēs esam novērojuši [lielapjoma uzraudzības paneļa (*BOP*)] pozitīvo attīstību un atzīmējuši tā ietekmi uz iekšējās atbilstības pārvaldību. Mēs turpinām viest lielāku skaidrību par procesu, ko *MI5* izmanto, lai veiktu jaunu datu kopu sākotnējās pārbaudes un labāk izprastu lēmumus klasificēt datu kopu kā *BPD* vai, piemēram, kā mērķorientētus datus. Mūs satrauca viena neatrisināta darbība saistībā ar *BOP* protokolliem attiecībā uz neatbilstību novēršanu starp *BPD* sadalījumu starp *MI5* un *SIS*. Datu atšķirīgās izmantošanas un atšķirīgo glabāto datu griezumu dēļ ir iespējams, ka abām iestādēm varētu būt tā pati datu kopa vai tās versijas un ka viena to likumīgi varētu klasificēt kā lielapjoma datu kopu, savukārt otra — kā mērķorientētu datu kopu. Pastāv risks, ka, ja kāda no iestādēm nepareizi klasificē datu glabāšanu kā mērķorientētu, šie dati tiktu glabāti bez atbilstoša ordera un tiem, iespējams, netiktu piemēroti atbilstoši aizsardzības pasākumi”.

<sup>114</sup> Skatīt izmeklēšanas pilnvaru komisāra 2019. gada ziņojumu, 8.39. punkts.

<sup>115</sup> Skatīt izmeklēšanas pilnvaru komisāra 2019. gada ziņojumu, 10.48. punkts.



cilvēkus, tomēr tas uzsver, ka ir ļoti svarīgi, lai *Mi5 turpinātu uzturēt šos jaunus procesus un nodrošinātu pietiekamus līdzekļus, lai tie varētu efektīvi darboties. Ja Mi5 konstatē neatbilstošas uzvedības pieaugumu*<sup>116</sup>. IPC sagaida, ka tiem tiks pievērsta uzmanība pēc iespējas agrāk. **Tāpēc EDAK aicina Eiropas Komisiju turpmāk cieši uzraudzīt šos aspektus.**

183. Attiecībā uz *GCHQ* no IPC ziņojuma EDAK saprot arī to, ka attiecībā uz darbībām, kas veiktas saskaņā ar orderiem datu pārtveršanai lielā apjomā, *iekšējā apstiprinājuma pieteikumu kvalitāte bija mainīga, un mēs novērojam, ka ir iespējams uzlabot izklāstu šajos pieteikumos*<sup>117</sup> un ka, lai veiktu mērķorientētu iejaukšanos ar aprīkojumu, paskaidrojumi par vispārēju deskriptoru izmantošanu dažreiz bija pārāk vispārīgi un neprecīzi<sup>118</sup>. EDAK arī ievēroja, ka saistībā ar iejaukšanos ar aprīkojumu lielā apjomā IPC iesaka *lietojumprogrammās konsekvēnti un skaidri reģistrēt saikni starp mērķi, likumā noteikto nolūku un izlūkošanas prasībām*<sup>119</sup>, ka *visos pieteikumos, novērtējot proporcionalitāti, skaidri jāpievēršas aizskaršanai ar nodrošinājumu un attiecīgiem seku mazināšanas pasākumiem*<sup>120</sup> un ka IPC uzsvēra, ka, neraugoties uz progresu, *vēl ir iespējams veikt uzlabojumus*<sup>121</sup> un nākotnē būs arī jāpievērš papildu uzmanība.
184. Saistībā ar datu lielapjoma pārtveršanas režīmu saskaņā ar 2000. gada Likumu par izmeklēšanas pilnvaru regulējumu (turpmāk tekstā — *RIPA 2000*), kas kopš tā laika ir aizstāts ar *IPA 2016* noteikumiem, EDAK atgādina, ka nepietiekama uzraudzība — gan attiecībā uz interneta nesēju atlasī pārtveršanas vajadzībām, gan attiecībā uz pārtverto paziņojumu filtrēšanu, meklēšanu un atlasī pārbaudes vajadzībām — bija viens no galvenajiem aspektiem, ko ECT uzskatīja par neatbilstošu ECTK 8. pantam attiecībā uz iepriekšējiem tiesību aktiem par Apvienotās Karalistes iestāžu izmeklēšanas pilnvarām nacionālās drošības kontekstā *Big Brother Watch* lietā, kas tagad nodota izskatīšanai virspalātā. **EDAK aicina Eiropas Komisiju pārbaudīt tiesvedības stāvokli, ņemt vērā šos elementus, un precizēt tos lēmumā par pietiekamību, ja Eiropas Komisija tos pieņems.**
185. Šajā gadījumā ECT: *netika pārliecināta, ka aizsardzības pasākumi, kas regulē nesēju atlasī pārtveršanas vajadzībām un pārtverto materiālu atlasī pārbaudes vajadzībām, ir pietiekami stingri, lai sniegtu pietiekamas garantijas pret ļaunprātīgu izmantošanu. Tomēr vislielākās bažas raisa tas, ka nav stingras neatkarīgas tādu atlasītāju un meklēšanas kritēriju uzraudzības, ko izmanto pārtvertās saziņas filtrēšanai*<sup>122</sup>. Kā uzsvēra IPC, *šis konstatējums atkārtoja līdzīgu ieteikumu Izlūkošanas un drošības komitejas 2015. gada marta ziņojumā “Privacy and Security: A modern and transparent legal framework”*<sup>123</sup>. **EDAK atzinīgi vērtē to, ka līdz ar to IPC pārskatīja savu pieeju datu lielapjoma pārtveršanas pārbaudei 2019. gadā, kas ietvēra rūpīgu pārbaudi par to, kā faktiski tiek īstenoti tehniski sarežģīti datu lielapjoma pārtveršanas veidi<sup>124</sup>, un apņēmas iekļaut tādu atlasītāju un meklēšanas kritēriju detalizētu pārbaudi, uz kuriem iepriekš atsaucās ECT<sup>125</sup> datu lielapjoma pārtveršanas pārbaudēs no 2020. gada. Ņemot vērā šā aspekta nozīmi, EDAK pauž bažas par to, ka IPC vēl nav veicis atlasītāju un meklēšanas kritēriju detalizētu pārbaudi, un aicina Eiropas Komisiju**

<sup>116</sup> Skatīt izmeklēšanas pilnvaru komisāra 2019. gada ziņojumu, 8.52. punkts.

<sup>117</sup> Skatīt izmeklēšanas pilnvaru komisāra 2019. gada ziņojumu, 10.2. punkts.

<sup>118</sup> Skatīt izmeklēšanas pilnvaru komisāra 2019. gada ziņojumu, 10.16. un 10.17. punkts.

<sup>119</sup> Skatīt izmeklēšanas pilnvaru komisāra 2019. gada ziņojumu, 10.23. punkts.

<sup>120</sup> Skatīt izmeklēšanas pilnvaru komisāra 2019. gada ziņojumu, 10.23. punkts.

<sup>121</sup> Skatīt izmeklēšanas pilnvaru komisāra 2019. gada ziņojumu, 10.23. punkts.

<sup>122</sup> Sk. ECT, *Big Brother Watch*, 347. punkts.

<sup>123</sup> Sk. izmeklēšanas pilnvaru komisāra 2019. gada ziņojumu, 10.28. punkts.

<sup>124</sup> Sk. izmeklēšanas pilnvaru komisāra 2019. gada ziņojumu, 10.28. punkts.

<sup>125</sup> Sk. izmeklēšanas pilnvaru komisāra 2019. gada ziņojumu, 10.28. punkts.

cieši uzraudzīt norises šajā saistībā, jo īpaši tāpēc, ka konkrētais šādas uzraudzības formāts vēl jāprecizē<sup>126</sup>.

#### 4.3.2. Savāktās informācijas turpmāka izmantošana nacionālās drošības nolūkos un atklāšana ārvalstīs

186. Attiecībā uz savāktās informācijas turpmāku izmantošanu nacionālās drošības nolūkos Eiropas Komisija savā novērtējumā atsaucas uz *DPA 2018* 87. panta 1. punktu, kas patiešām paredz, ka *šādi savāktos personas datus nedrīkst apstrādāt tādā veidā, kas nav savietojams ar nolūku, kādā tie ir savākti*. Tomēr EDAK norāda, ka uz šo noteikumu var attiekties ar nacionālo drošību saistīti atbrīvojumi, kā paredzēts *DPA 2018* 110. pantā. Turklāt EDAK norāda, ka tiesību aktos ir paredzēta iespēja atklāt informāciju ārvalstīs mērķorientētas pārtveršanas un pārbaudes, saziņas datu mērķorientētas iegūšanas un saglabāšanas, mērķtiecīgas iejaukšanās ar aprīkojumu vai datu lielapjoma pārtveršanas un lielapjoma iejaukšanās ar aprīkojumu gadījumā.

##### 4.3.2.1. Turpmāka izmantošana, informācijas atklāšana ārvalstīs un piemērojamais tiesiskais regulējums Apvienotajā Karalistē

187. Eiropas Komisija ir noteikusi *DPA 2018* 4. daļu un jo īpaši tā 109. pantu kā atbilstošus noteikumus, kas paredz īpašas prasības attiecībā uz savāktās informācijas turpmāku izmantošanu un jo īpaši izlūkdienestu veiktu personas datu starptautisku nosūtīšanu uz trešām valstīm vai starptautiskām organizācijām. Tomēr EDAK norāda, ka *DPA 2018* 110. pantā ir paredzēts ar nacionālo drošību saistīts atbrīvojums, precizējot, ka daži *DPA 2018* noteikumi nav piemērojami, ja nacionālās drošības garantēšanai ir nepieciešams atbrīvojums no šiem noteikumiem. Attiecīgie noteikumi, ko var nepiemērot, ietver *DPA 2018* 4. daļas 2. nodaļu saistībā ar datu aizsardzības principiem, tostarp nolūka ierobežojumu, kā arī *DPA 2018* 4. daļas 3. nodaļu attiecībā uz datu subjektu tiesībām. *DPA 2018* 109. pants, lasot kopā ar *DPA 2018* 110. pantu un nosacījumiem, saskaņā ar kuriem tas piemērojams, var radīt situāciju, kurā izlūkdienesti veic personas datu starptautisku nosūtīšanu uz trešām valstīm, nepiemērojot noteikumus, kas saistīti ar datu aizsardzības principiem un datu subjektu tiesībām.
188. Kā noteikusi Eiropas Komisija, šāds atbrīvojums ir jāvērtē katrā gadījumā atsevišķi, un uz to var atsaukties, ciktāl konkrēta noteikuma piemērošana varētu negatīvi ietekmēt nacionālo drošību. Patiešām, valsts sertifikāta izsniegšana Apvienotās Karalistes izlūkdienestiem ir vērsta uz to, lai apliecinātu, ka ir nepieciešams atbrīvojums attiecībā uz konkrētiem personas datiem, kurus apstrādā, lai garantētu nacionālo drošību. Tomēr EDAK norāda, ka Apvienotās Karalistes Iekšlietu ministrija savos norādījumos par nacionālās drošības sertifikātu saskaņā ar *DPA 2018* paskaidro, ka *no paša sākuma ir svarīgi norādīt, ka sertifikāts nav vajadzīgs, lai izmantotu ar nacionālo drošību saistītu atbrīvojumu; faktiski vairumā gadījumu pārziņi paši nosaka, vai ir piemērojams ar nacionālo drošību saistīts atbrīvojums*.<sup>127</sup> Turklāt Apvienotās Karalistes Iekšlietu ministrijas norādījumos ir teikts, ka *nacionālās drošības sertifikātus var attiecināt uz personas datiem, ko var īpaši noteikt vai kas aptver plašāku personas datu kategoriju. Tie var būt gan preventīvi, gan retrospektīvi*.<sup>128</sup> Tāpēc izlūkdienestu

<sup>126</sup> Sk. izmeklēšanas pilnvaru komisāra 2019. gada ziņojumu, 10.28. punkts: "par konkrētu šādas pārbaudes formātu vēl ir jāvienojas".

<sup>127</sup> Sk. Iekšlietu ministrijas 2018. gada Datu aizsardzības likumu, Norādījumus par nacionālās drošības sertifikātiem, 2020. gada augusts, 3. punkts, 3. lpp.

<sup>128</sup> Sk. Iekšlietu ministrijas 2018. gada Datu aizsardzības likumu, Norādījumus par nacionālās drošības sertifikātiem, 2020. gada augusts, 5. punkts, 4. lpp.

veiktai personas datu starptautiskai nosūtīšanai uz trešām valstīm var piemērot ar nacionālo drošību saistītu atbrīvojumu, ja nav nacionālās drošības sertifikāta.

189. EDAK arī norāda, ka, piemēram, nacionālās drošības sertifikāts DPA/S27/Security Service<sup>129</sup> paredz, ka līdz 2024. gada 24. jūlijam personas dati, kas tiek apstrādāti *Drošības dienesta vajadzībām, pēc tā pieprasījuma vai ar tā palīdzību vai atbalstu un ja šāda apstrāde ir nepieciešama, lai sekmētu 1989. gada Drošības dienesta likuma 1. pantā minēto Drošības dienesta funkciju pareizu izpildi*, ir atbrīvoti no Apvienotās Karalistes tiesību aktu noteikumiem, kuri atbilst VDAR V nodaļai attiecībā uz personas datu nosūtīšanu uz trešām valstīm vai starptautiskām organizācijām. Lai arī citi publiski pieejamie nacionālās drošības sertifikāti neparedz atbrīvojumu no *DPA 2018* 109. panta noteikumiem, jāatgādina, ka nacionālās drošības sertifikāta tekstu vai tā daļu var neizpaust, ja tā publicēšana ir pretrunā nacionālās drošības interesēm, pretrunā sabiedrības interesēm vai var apdraudēt jebkuras personas drošību.
190. Kopumā, vērtējot lēmuma projektu saistībā ar šiem noteikumiem, EDAK konstatē, ka šādas informācijas atklāšanas aizsardzības pasākumi ietver tikai prasību, ka datu saņēmējam jāievēro prasības attiecībā uz datu drošību, datu atklāšanas apjomu, kurš ierobežots līdz nepieciešamajam, datu saglabāšanu un ierobežotu piekļuvi datiem ierobežotam personu skaitam. Tādējādi **EDAK uzsver, ka attiecībā uz datu atklāšanu ārvalstīs Apvienotās Karalistes tiesību aktos paredzētā ar nacionālo drošību saistītā atbrīvojuma piemērošana var izraisīt situācijas, kad trešā saņēmējvalstī netiek pilnībā nodrošināti vai ievēroti aizsardzības pasākumi, kas garantē nolūka ierobežošanas, nepieciešamības un proporcionālītātes principa ievērošanu, kā arī personu tiesību, uzraudzības un tiesiskās aizsardzības līdzekļu nodrošināšanu.** Tāpēc EDAK iesaka Eiropas Komisijai sīkāk izskatīt Apvienotās Karalistes tiesību aktos paredzētos vispārējos aizsardzības pasākumus, kad runa ir par informācijas atklāšanu ārvalstīs, jo īpaši ņemot vērā nacionālās drošības atbrīvojumu piemērošanu.

#### 4.3.2.2. Datu atklāšana ārvalstīs un izlūkdatu koplietošana starptautiskās sadarbības kontekstā

191. EDAK arī norāda, ka Eiropas Komisija, veicot pietiekamības novērtējumu, nepievērsās spēkā esošajiem starptautiskajiem nolīgumiem, kas noslēgti starp Apvienoto Karalisti un trešām valstīm vai starptautiskām organizācijām un var paredzēt īpašus noteikumus par izlūkdienestu veiktu personas datu starptautisku nosūtīšanu uz trešām valstīm.
192. EDAK arī uzsver, ka Eiropas Komisijas novērtējuma pamatā galvenokārt ir *DPA 2018* 4. daļas novērtējums, un tā ir īpaši noraizējusies, ka *IPA 2016* lielākā uzmanība ir pievērsta “pieprasījumiem” koplietot izlūkdatus ar ārvalstu partneriem, taču tajā nav apskatīti citi izlūkdatu koplietošanas veidi. Šajā saistībā EDAK norāda, ka Eiropas Komisijas lēmuma projektā neatsaucas uz saikni starp Apvienotās Karalistes tiesisko regulējumu un “Apvienotās Karalistes un ASV Saiziņas izlūkošanas nolīgumu” (“Apvienotās Karalistes un ASV SI nolīgums”) un nenovērtē šo saikni. Savā nesenajā paziņojumā, pieminot šā nolīguma 75. gadadienu, ASV Nacionālās drošības aģentūra (turpmāk tekstā — NSA) minēja, ka šī partnerība ļauj *abām iestādēm koplietot informāciju, cik vien tas ir iespējams, kā arī ar minimāliem ierobežojumiem un ka ar šo revolucionāro dokumentu tika izveidota politika un procedūras, lai Apvienotās Karalistes un ASV izlūkošanas speciālisti varētu koplietot*

---

<sup>129</sup> Sk. DPA/S27/Security Service, *DPA 2018* 27. pants, valsts sekretāra sertifikāts, 2019. gada 24. jūlijs, <https://ico.org.uk/media/about-the-ico/documents/nscs/2615660/nsc-part-2-mi5-201908.pdf>.

saziņu, tulkojumus, analīzi un kodu uzlaušanas informāciju<sup>130</sup>. Šis nolīgums arī kļuva par pamatu citām partnerībām izlūkošanas jomā ar Austrāliju, Kanādu un Jaunzēlandi.

193. Šā nolīguma un tā īpašo noteikumu slepenība rada nopietnu problēmu likuma skaidrības un paredzamības ziņā attiecībā uz turpmāku tādas informācijas izmantošanu un atklāšanu ārvalstīs, ko savākušas Apvienotās Karalistes iestādes nacionālās drošības nolūkos. Šajā saistībā EDAK atgādina, ka attiecībā uz ES garantēto aizsardzības līmeni EST ir uzsvērusi, ka tiesību aktos, kas saistīti ar iejaukšanos pamattiesībās uz personas datu aizsardzību, “*jāparedz skaidri un precīzi noteikumi, kas reglamentētu attiecīgā pasākuma apjomu un piemērošanu un noteiktu minimālās prasības tādējādi, lai personām, kuru personas dati ir tikuši skarti, būtu pietiekamas garantijas, kas ļautu to personas datus efektīvi aizsargāt pret ļaunprātīgas izmantošanas risku, kā arī pret jebkādu nelikumīgu piekļuvi šiem datiem un to nelikumīgu izmantošanu. Šādu garantiju nepieciešamība ir vēl jo svarīgāka tādēļ, ka personas dati tiek apstrādāti automātiski un pastāv ievērojams nelikumīgas piekļuves šiem datiem risks*”<sup>131</sup>. Tāpēc EDAK uzskata, ka Eiropas Komisijai būtu jāapsver Apvienotās Karalistes un ASV SI nolīguma ietekme savā pietiekamības novērtējumā.
194. ECT savā pirmajā 2018. gada 13. septembra sprieduma iedaļā *Big Brother Watch* lietā ir novērtējusi Apvienotās Karalistes izlūkdatu koplietošanas režīmu un jo īpaši Apvienotās Karalistes un ASV SI nolīgumu. ECT norādīja, ka *tiesiskais regulējums, kas ļauj ar Apvienotās Karalistes izlūkdienestiem pieprasīt pārtvertu materiālu no ārvalstu izlūkdienestiem, nav ietverts RIPA. Apvienotās Karalistes un ASV 1946. gada 5. marta Saziņas izlūkošanas nolīgums jo īpaši atļauj veikt materiāla apmaiņu starp Amerikas Savienotajām Valstīm un Apvienoto Karalisti*<sup>132</sup>, un tajā ir noteikts, ka *likumā ir pamats izlūkdatu pieprasīšanai no ārvalstu izlūkošanas iestādēm un šis likums ir pietiekami pieejams*<sup>133</sup>. Lai arī ECT ir secinājusi, ka nav pārkāpts ECTK 8. pants<sup>134</sup> attiecībā uz izlūkdatu koplietošanas režīmu, EDAK norāda, ka šis spriedums tagad ir nodots virspalātai, kur lēmums vēl nav pieņemts. EDAK arī norāda, ka daļēji piekritošajā, daļēji atšķirīgajā atzinumā par šo spriedumu, tiesnesis *Koskelo*, kam pievienojās tiesnesis *Turković*<sup>135</sup>, ir secinājis, ka ir pārkāpts ECTK 8. pants attiecībā uz izlūkdatu koplietošanas režīmu, norādot, ka *ir viegli piekrist principam, ka nevienā kārtībā, saskaņā ar kuru izlūkdati no pārtvertās saziņas tiek iegūti ar ārvalstu izlūkdienestu palīdzību, pamatojoties uz pieprasījumiem veikt šādu pārtveršanu vai nodot tās rezultātus, nevajadzētu pieļaut to, ka tiek apieti aizsardzības pasākumi, kas jāievieš vietējo iestāžu veiktas uzraudzības vajadzībām (sk. 216., 423. un 447. punktu). Jebkura cita pieeja patiešām būtu neiedomājama*.
195. Kā uzsvērts vairākos mediju un nevalstisko organizāciju ziņojumos<sup>136137</sup>, jaunākā Apvienotās Karalistes un ASV SI līguma versija tika publiskota 1956. gadā, un kopš tā laika sakaru tehnoloģijas un sakaru izlūkdatu būtība ir ievērojami mainījies. Mediju ziņojumi, piemēram, ir atklājuši, ka *GCHQ*

---

<sup>130</sup> Sk. NSA paziņojumu presei *GCHQ and NSA Celebrate 75 Years of Partnership*, 2021. gada 5. februāris, <https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2494453/gchq-and-nsa-celebrate-75-years-of-partnership/>.

<sup>131</sup> Sk. *Schrems I*, 91. punkts.

<sup>132</sup> Sk. ECT, *Big Brother Watch*, 425. punkts

<sup>133</sup> Sk. ECT, *Big Brother Watch*, 427. punkts

<sup>134</sup> Sk. ECT, *Big Brother Watch*, 448. punkts

<sup>135</sup> Sk. ECT, *Big Brother Watch*, daļēji piekritis, daļēji atšķirīgs atzinums, ko sniedzis tiesnesis *Koskelo*, kam pievienojās tiesnesis *Turković*.

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

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

pārtver datus, kas tiek nosūtīti pa zemūdens kabeļiem, kuri beidzas Apvienotajā Karalistē, un tos dara pieejamus NSA<sup>138</sup>.

196. EDAK svarīgs jautājums saistībā ar izlūkdatu koplietošanu ir par to, vai *DPA 2018* 109. pants un *IPA 2016* noteikumi aizvien ir piemērojami, ja Apvienotās Karalistes izlūkdienesti rīkojas saskaņā ar Apvienotās Karalistes un ASV SI nolīgumu. Vēl viens svarīgs elements, kas jāvērtē, ir tas, vai šā nolīguma noteikumi vai efektīva piemērošana ietekmē tādu personas datu aizsardzības līmeni, kas atrodas tranzītā no EEZ uz Apvienoto Karalisti, vai arī ļauj citu trešo valstu izlūkdienestiem tieši piekļūt personas datiem un tos iegūt.
197. Attiecīgi papildus atrunām, kas izteiktas attiecībā uz atklāšanu ārvalstīs, pamatojoties uz *DPA 2018* 4. daļu un attiecīgo ar nacionālo drošību saistīto atbrīvojumu, kā arī pieprasījumiem saskaņā ar *IPA 2016*, **EDAK ir noraizējusies par citiem informācijas koplietošanas un atklāšanas veidiem, pamatojoties uz citiem instrumentiem, jo īpaši dažādiem starptautiskiem nolīgumiem, kurus Apvienotā Karaliste ir noslēgusi ar citām trešām valstīm, jo īpaši tad, ja šie instrumenti joprojām nav pieejami sabiedrībai, piemēram, Apvienotās Karalistes un ASV SI nolīgums. Šāda nolīguma sekas varētu būt to aizsardzības pasākumu apiešana, kas noteikti attiecībā uz piekļuvi personas datiem un to izmantošanu nacionālās drošības nolūkos.**
198. EDAK piekrīt viedoklim, ko paudis Apvienoto Nāciju Organizācijas īpašais referents *Joe Cannataci* par to, ka *izlūkdatu koplietošana nedrīkst radīt iespēju citiem iegūt izlūkdatus, kuriem nepiemēro iekšzemes aizsardzības pasākumus, vai veicināt šādu izlūkdatu iegūvi, kā arī tā nedrīkst radīt iespēju ārvalstu valdībām ar zemākiem privātuma (vai citu cilvēktiesību) aizsardzības standartiem iegūt no Apvienotās Karalistes izlūkdatus, kas varētu radīt cilvēktiesību pārkāpumus*<sup>139</sup>.
199. Turklāt **EDAK uzskata, ka divpusēju vai daudzpusēju nolīgumu noslēgšana ar trešām valstīm izlūkošanas sadarbības nolūkā, nodrošinot juridisko pamatu personas datu tiešai pārtveršanai un iegūšanai vai personas datu nosūtīšanai uz šīm valstīm, var arī būtiski ietekmēt savāktās informācijas turpmākas izmantošanas nosacījumus, jo šādi nolīgumi var ietekmēt novērtēto Apvienotās Karalistes datu aizsardzības tiesisko regulējumu.**

#### 4.3.3. Uzraudzība

200. EDAK uzsver neatkarīgu uzraudzības iestāžu veiktas visaptverošas uzraudzības nozīmi, lai nodrošinātu pietiekamu datu aizsardzības līmeni. Uzraudzības iestāžu neatkarības garantija ES hartas 8. panta 3. punkta nozīmē ir paredzēta, lai nodrošinātu, ka efektīvi un uzticami tiek uzraudzīta atbilstība noteikumiem par personu aizsardzību attiecībā uz personas datu apstrādi.
201. Kad personas datiem piekļūst un tos izmanto nacionālās drošības nolūkos, uzraudzības funkciju galvenokārt veic *IPC* un tieslietu komisāri (turpmāk tekstā — tieslietu komisāri).
202. **EDAK kopumā atzīst tieslietu komisāru ieviešanu *IPA 2016* kā būtisku uzlabojumu.** Saskaņā ar iepriekš minēto lūgumu Eiropas Komisija tiek aicināta sīkāk izvērtēt **tieslietu komisāru neatkarību un jo īpaši to, cik lielā mērā ir juridiski nodrošināta *IPC* un *IPC* biroja (turpmāk tekstā — *IPCO*)**

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

<sup>139</sup> Sk. *End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion Of his Mission to the United Kingdom of Great Britain and Northern Ireland*, Londona, 2018. gada 29. jūnijs, <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E#:~:text=Intelligence%20sharing%20must%20not%20result,UK%20intelligence%20that%20could%20give>.

**neatkarība, jo tas nav atrodams IPA 2016.** Tas ir vēl jo svarīgāk, jo *IPC* lemj par valdības pārsūdzības prasībām, ja tieslietu komisārs ir noraidījis pieteikumu par uzraudzības **pasākumu**.

203. *IPC* pilda *ex ante* un arī *ex post* uzraudzības funkcijas. Attiecībā uz *ex ante* uzraudzību EDAK saprot, ka tieslietu komisāru funkcija ir atsevišķos gadījumos apstiprināt dažādus uzraudzības pasākumus, tostarp mērķorientētu pārtveršanu un saziņas datu iegūšanu lielā apjomā. EDAK arī norāda, ka uzraudzības pasākumu iepriekšēju apstiprināšanu nevar pieņemt, pamatojoties uz EST judikatūru, kā absolūtu prasību, lai uzraudzības pasākumi būtu proporcionāli<sup>140</sup>.
204. Lai novērtētu šāda līmeņa uzraudzības efektivitāti, EDAK tomēr uzskata, ka ir sīkāk jāprecizē scenāriji, kuros ir iespējama likumīga pārtveršana bez iepriekšēja tieslietu komisāru apstiprinājuma.
205. Sava lēmuma projekta 201. un 266. zemsvītras piezīmē Eiropas Komisija piemin "īpašus ierobežotus gadījumus", kas minēti *IPA 2016* 44.–52. pantā attiecībā uz mērķorientētu pārtveršanu. EDAK norāda, ka *IPA 2016* 45.–51. pants ir atbrīvojumi, par kuriem tiek apgalvots, ka izlūkdienesti tos neizmanto regulāri. Turklāt **EDAK saprot, ka gadījumos, kad tiek piemēroti atbrīvojumi** (piemēram, telesakaru un pasta pakalpojumu sniedzēji), tieslietu komisāriem jāveic iepriekšēja apstiprināšana gadījumā, ja tiesībsardzības iestādes vai izlūkdienesti **pieprasa** piekļuvi šiem datiem, un **aicina Eiropas Komisiju savā lēmumā apstiprināt, ka tas ir pareizi**.
206. EDAK atzīst, ka *IPA 2016* 44. panta 2. punkts pieļauj saziņas pārtveršanu, ja viena no pusēm (sūtītājs vai saņēmējs) ir piekritusi un ja ir saņemta atļauja saskaņā ar *RIPA 2000* vai 2000. gada Likumu par izmeklēšanas pilnvaru regulējumu (Skotija) (2000. gada 11. *ASP*), kas ir agrākā tiesiskā situācija pirms tieslietu komisāru izveidošanas. EDAK **aicina** Eiropas Komisiju precizēt, vai tas nozīmē, ka gadījumos, kad pastāv vienpusēja piekrišana, iepriekšējās apstiprināšanas procedūra vispār netiktu piemērota.
207. Attiecībā uz *ex post* uzraudzību ir svarīgi arī pārbaudīt, vai efektīva neatkarīga uzraudzība tiek nodrošināta bez trūkumiem, joīpaši gadījumos, kad tas nav paredzēts *ex ante*.
208. EDAK norāda, ka saskaņā ar *IPA 2016* 48.–52. pantu tieslietu komisāri veic *ex post* pārbaudi, un **aicina Eiropas Komisiju precizēt, atbilstīgi kādām prasībām un pēc kādas iniciatīvas šāda ex post pārbaude jāveic**.
209. Saskaņā ar *IPA 2016* 229. panta 4. punktu *IPC* nav jāpārbauda noteiktu funkciju izpilde. Šajā saistībā EDAK aicina Eiropas Komisiju precizēt *IPA 2016* 229. panta 4. punkta d) un e) apakšpunkta noteikumus par praktisko ietekmi uz *IPC* pārbaudes kompetenci. **EDAK izpratnē ICO ir kompetentā uzraudzības iestāde, ja tiek piemēroti IPA 2016 229. panta 4. punktā paredzētie atbrīvojumi, un EDAK aicina Eiropas Komisiju savā lēmumā apstiprināt, ka tas ir pareizi**.
210. **Šķiet, ka, veicot ex post uzraudzību, IPC uzdevums ir ierobežots** līdz ieteikumu sniegšanai neatbilstības gadījumos un datu subjekta informēšanai, ja kļūda ir nopietna un personas informēšana ir sabiedrības interesēs. **EDAK aicina Eiropas Komisiju precizēt, kā IPCO var efektīvi nodrošināt likuma ievērošanu**.
211. **Visbeidzot, EDAK saprot, ka ietekmētās personas nevar tieši vērsties IPCO, bet tām ir jāiesniedz sūdzība ICO, kam tomēr ir ierobežota kompetence nacionālās drošības jomā. Tāpēc EDAK aicina Eiropas Komisiju sīkāk paskaidrot, kā juridiski tiek nodrošināts, ka šajos gadījumos sūdzības izskata IPCO**.

---

<sup>140</sup> Tā arī norāda, ka, atzīstot par nederīgu privātuma vairogu *Schrems II*, EST ņēma vērā to, ka saskaņā ar ASV tiesību aktiem tā sauktā ĀIUL tiesa "neapstiprina individuālus uzraudzības pasākumus, bet gan uzraudzības programmas (piemēram, *PRISM*, *UPSTREAM*), pamatojoties uz ikgadējām sertifikācijām" (179. punkts).

#### 4.3.4. Tiesiskā aizsardzība

212. Ņemot vērā EST spriedumus *Schrems I* un *Schrems II* lietā, ir skaidrs, ka efektīvai tiesiskai aizsardzībai ES hartas 47. panta nozīmē ir būtiska nozīme, pieņemot, ka trešās valsts tiesību aktu nodrošinātais aizsardzības līmenis ir pietiekams. Šie nolēmumi arī apliecināja, ka šajā saistībā īpaša uzmanība jāpievērš efektīvai tiesiskajai aizsardzībai, ja personas datiem piekļūst nacionālās drošības nolūkā.
213. **EDAK atzīst, ka Apvienotā Karaliste ir izveidojusi IPT. IPT ir kompetenta izskatīt ne tikai lietas par izmeklēšanas pilnvaru izmantošanu tiesībaizsardzības iestādēs, bet arī izlūkdienestos. EDAK izpratnē IPT darbojas kā pienācīga tiesa ES hartas 47. panta nozīmē. Attiecībā uz pilnvarām Eiropas Komisija tiek aicināta apstiprināt, ka IPT ir visas tās pilnvaras, kas minētas lēmuma projekta 262. apsvērumā, neatkarīgi no sūdzības juridiskā pamata.**
214. Izlūkošanas iestāžu veiktā diskrētā uzraudzība bieži nozīmē, ka uzraudzības objekts — datu subjekts — par uzraudzību nezina un neuzzinās. Šajā saistībā, kad EDAK bija jāanalizē ASV tiesību akti, tā daudzkārt pauda bažas par ASV tiesību aktos interpretēto “pastāvības” prasību uzraudzības lietās. Ņemot to vērā, EDAK norāda, ka, lai varētu iesniegt sūdzību IPT, ir vajadzīgs vienīgi “ticības” tests, saskaņā ar kuru sūdzības iesniedzējam ir jāpierāda, ka tam varētu tikt piemērots pasākums.
215. Analizējot IPT, EDAK arī pievērš īpašu uzmanību tam, ka vairākkārt ir konstatēts, ka IPT darbība atbilst ECTK, kā to interpretē ECT.