Kolēģijas atzinums (70. panta 1. punkta s) apakšpunkts)

Atzinums 32/2021 par Eiropas Komisijas Īstenošanas lēmuma projektu saskaņā ar Regulu (ES) 2016/679 par personas datu pietiekamu aizsardzību Korejas Republikā

Versija 1.0

Pieņemts 2021. gada 24. septembrī

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

SATURS

Eiropas Datu aizsardzības kolēģija,

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

ņemot vērā Eiropas Ekonomikas zonas ("**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[1],

ņemot vērā Reglamenta 12. un 22. pantu,

IR PIEŅĒMUSI ŠĀDU ATZINUMU.

1. KOPSAVILKUMS

1. Eiropas Komisija 2021. gada 16. jūnijā sāka oficiālu procesu, lai pieņemtu savu īstenošanas lēmuma projektu ("**lēmuma projekts**") par pietiekamu personas datu aizsardzību Korejas Republikā saskaņā ar Personas datu aizsardzības likumu atbilstoši VDAR[2].

2. Tajā pašā datumā Eiropas Komisija lūdza Eiropas Datu aizsardzības kolēģijai ("**EDAK**")[3] sniegt atzinumu. EDAK veica Korejas Republikā nodrošinātā aizsardzības līmeņa pietiekamības novērtējumu, pamatojoties uz paša projekta lēmuma pārbaudi, kā arī uz[4] Eiropas Komisijas iesniegtās dokumentācijas analīzi.

3. EDAK savā novērtējumā pievērsās gan lēmuma projekta vispārējiem VDAR aspektiem, gan valsts iestāžu piekļuvei no EEZ nosūtītajiem personas datiem tiesībaizsardzības un valsts drošības mērķiem, tostarp tiesiskās aizsardzības līdzekļiem, kas pieejami EEZ pilsoņiem. Tāpat EDAK novērtēja, vai saskaņā ar Korejas tiesisko regulējumu paredzētie aizsardzības pasākumi ir ieviesti un ir efektīvi.

4. Kā galveno atsauces materiālu šim darbam EDAK izmantoja 2018. gada februārī pieņemtās VDAR pietiekamības atsauces[5] ("**VDAR pietiekamības atsauces**") un EDAK ieteikumus 02/2020 attiecībā uz Eiropas būtiskajām garantijām uzraudzības pasākumiem[6].

1.1. Konverģences jomas

5. EDAK galvenais mērķis bija sniegt atzinumu Eiropas Komisijai par aizsardzības līmeņa pietiekamību personām, kuru personas dati tiek nosūtīti uz Korejas Republiku. Ir svarīgi atzīmēt, ka EDAK nesagaida Korejas datu aizsardzības regulējuma pilnīgu atbilstību Eiropas tiesību aktiem datu aizsardzības jomā.

6. Taču EDAK norāda, ka, lai varētu uzskatīt, ka ir nodrošināts pietiekams aizsardzības līmenis, VDAR 45. pants un Eiropas Savienības Tiesas (turpmāk "**EST**") judikatūra paredz, ka trešās valsts tiesību aktiem ir jābūt saskaņotiem ar VDAR nostiprināto pamatprincipu būtību. Šajā kontekstā Korejas datu

[1] Šajā atzinumā atsauces uz "**dalībvalstīm**" būtu jāsaprot kā atsauces uz "EEZ dalībvalstīm".
[2] Skatīt paziņojumu presei https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2964.
[3] Turpat.
[4] EDAK savu analīzi pamatoja uz Korejas valdības sagatavotajiem oficiālajiem tulkojumiem.
[5] WP254, VDAR pietiekamības atsauces, 2018. gada 6. februāris, (apstiprinājusi EDAK, skatīt https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines).
[6] Skatīt EDAK ieteikumus 02/2020 attiecībā uz Eiropas būtiskajām garantijām uzraudzības pasākumiem, kas pieņemti 2020. gada 10. novembrī, https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_en.

aizsardzības regulējums ir daudzējādā ziņā līdzīgs Eiropas datu aizsardzības regulējumam, un to veido viens galvenais tiesību akts, kas aptver gan publisko, gan privāto sektoru, un papildina nozarei specifiski tiesību akti.

7. Attiecībā uz saturu EDAK atzīmē galvenās VDAR regulējuma un Korejas datu aizsardzības regulējuma saskaņošanas jomas, kā arī dažus pamatnoteikumus, piemēram, jēdzienus ("personas dati", "personas datu apstrāde", "datu subjekts" u. c.); likumīgas un godprātīgas apstrādes leģitīmiem mērķiem pamatojumus; nolūka ierobežojumu; datu kvalitāti un proporcionalitāti; datu saglabāšanu, drošību un konfidencialitāti; pārredzamību; īpašas datu kategorijas.

8. Papildus iepriekš minētajam EDAK atzinīgi vērtē Eiropas Komisijas un Korejas varas iestāžu centienus nodrošināt Korejas Republikā pietiekamu aizsardzības līmeni, kas atbilst VDAR, pieņemot Korejas uzraudzības iestādes paziņojumus (piemērojams ne tikai personas datiem, kas nosūtīti no EEZ uz Koreju), lai novērstu neatbilstības starp VDAR un Korejas datu aizsardzības regulējumu. Šajā kontekstā EDAK vēlas uzsvērt šo paziņojumu nozīmi Korejas Republikas aizsardzības līmeņa pietiekamības novērtēšanā, atzīmējot, piemēram, ka tie sniedz attiecīgus paskaidrojumus par dažiem svarīgiem aizsardzības pasākumiem, tostarp saistībā ar izņēmumiem no PDAL pseidonimizētu personas datu apstrādei zinātniskos, pētniecības un statistikas nolūkos, tālāku nosūtīšanu un noteikumiem, kas ir piemērojami saistībā ar valsts iestāžu piekļuvi datiem.

1.2. Uzdevumi

9. Lai gan EDAK ir konstatējusi, ka daudzi Korejas datu aizsardzības regulējuma aspekti būtībā ir līdzvērtīgi Eiropas datu aizsardzības regulējumam, tā ir arī secinājusi, ka ir daži aspekti, kuriem var būt nepieciešama rūpīgāka izskatīšana un skaidrojums. EDAK jo īpaši uzskata, ka sīkāk būtu jānovērtē tālāk norādītie aspekti, lai nodrošinātu būtībā līdzvērtīga aizsardzības līmeņa ievērošanu, un Eiropas Komisijai tie būtu rūpīgi jāuzrauga.

1.2.1. Vispārīgi jautājumi

10. EDAK ņem vērā, ka Paziņojumam Nr. 2021-1 *ir administratīva noteikuma statuss ar juridiski saistošu spēku personas datu pārzinim tādā nozīmē, ka jebkurš paziņojuma pārkāpums var tikt uzskatīts par PDAL attiecīgo nosacījumu pārkāpumu*[7]. Tomēr ņemot vērā, ka Paziņojumā nav iekļauti papildu noteikumi kā tādi, bet drīzāk skaidrojumi par to, kā būtu jāsaprot PDAL ar likumu noteiktais teksts, lai to piemērotu, ņemot vērā tā vispārējo nozīmi, jo īpaši attiecībā uz PDAL pseidonimizācijas nosacījumiem, kuri EDAK izpratnē ir pamatā notiekošām tiesvedībām, EDAK aicina Eiropas Komisiju sniegt papildu informāciju par Paziņojuma Nr. 2021-1 saistošo raksturu, izpildāmību un derīgumu un iesaka rūpīgi uzraudzīt tā ievērošanu praksē, jo īpaši attiecībā uz tā piemērošanu ne tikai no Korejas uzraudzības iestādes puses, bet arī no tiesas puses tad, ja līdzvērtīgais aizsardzības līmenis, ko paredz Korejas tiesiskais regulējums, ir balstīts uz tajā sniegtajiem skaidrojumiem.

1.2.2. Vispārīgi datu aizsardzības aspekti

11. Attiecībā uz lēmuma par aizsardzības līmeņa pietiekamību piemērošanas jomu EDAK atzīmē, ka tas attieksies uz nosūtīšanas gadījumiem no EEZ tiesiskā regulējuma gan publiskiem, gan privātiem "personas datu pārziņiem", kas ietilpst PDAL darbības jomā. EDAK saprot, ka šajā terminā ir iekļautas struktūras, kas VDAR izpratnē darbojas kā datu apstrādātāji, tomēr, lai izvairītos no pārpratumiem, tā aicina Eiropas Komisiju paskaidrot, ka lēmums par aizsardzības līmeņa pietiekamību attieksies arī uz nosūtīšanas gadījumiem "datu apstrādātājiem" Korejā.

12. Svarīgs aspekts, kam EDAK vēlas pievērst uzmanību, ir saistīts ar pseidonimizētas informācijas jēdzienu Korejas datu aizsardzības sistēmā. Saskaņā ar Korejas tiesību aktiem uz pseidonimizētu personas datu

[7] Skatīt lēmuma projekta I pielikuma I sadaļu.

apstrādi attiecas izņēmumi no vairākiem attiecīgiem noteikumiem, tostarp par atsevišķām datu subjektu tiesībām un datu glabāšanu. Pēc Eiropas Komisijas domām tas ir tikai gadījumā, kad pseidonimizēti personas dati tiek apstrādāti statistikas, zinātniskās izpētes vai arhivēšanas nolūkos sabiedrības interesēs. Tomēr šo apgalvojumu galvenokārt atbalsta Paziņojums Nr. 2021-1, kas šajā kontekstā ļoti būtisku padara jau minēto nepieciešamību pēc papildu informācijas par šī paziņojuma saistošo raksturu, izpildāmību un derīgumu un šo aspektu uzraudzību. Turklāt EDAK aicina Eiropas Komisiju turpināt izvērtēt pseidonimizācijas ietekmi saskaņā ar Korejas tiesību aktiem un, kas ir vissvarīgāk, kā tā var ietekmēt to datu subjektu pamattiesības un brīvības, kuru personas dati tiek nosūtīti uz Korejas Republiku saskaņā ar lēmumu par aizsardzības līmeņa pietiekamību. EDAK jo īpaši aicina Eiropas Komisiju sīkāk izvērtēt PDAL 28. panta 7. punktā un CIP 40. panta 3. punktā ietvertās atkāpes un rūpīgi uzraudzīt to piemērošanu un attiecīgo judikatūru, lai nodrošinātu, ka datu subjekta tiesības netiek nepamatoti ierobežotas, kad personas dati, kas pārsūtīti saskaņā ar lēmumu par aizsardzības līmeņa pietiekamību, tiek apstrādāti šim nolūkam.

13. Turklāt EDAK atzīmē, ka saskaņā ar Korejas tiesību aktiem tiesības atsaukt piekrišanu pastāv tikai īpašos apstākļos, un tāpēc aicina Eiropas Komisiju turpināt izvērtēt vispārējo tiesību uz piekrišanas atsaukšanu trūkuma ietekmi un sniegt papildu garantijas, lai nodrošinātu, ka vienmēr tiek garantēts būtisks datu aizsardzības līmenis, vajadzības gadījumā noskaidrojot arī tiesības uz apturēšanu saskaņā ar PDAL, ja nav vispārēju tiesību atsaukt piekrišanu.

14. Attiecībā uz tālāku nosūtīšanu EDAK atzīst, ka datu subjekta informēta piekrišana parasti tiks izmantota par pamatu datu nosūtīšanai no personas datu apstrādātāja Korejā saņēmējam trešajā valstī un ka paziņojumā Nr. 2021-1 ir paredzēts, ka personas ir jāinformē par trešo valsti, kurai tiks sniegti viņu dati. Tomēr EDAK aicina Eiropas Komisiju nodrošināt to, ka datu subjektam sniedzamajā informācijā ir iekļauta arī informācija par iespējamiem nosūtīšanas riskiem, kas rodas, ja trešajā valstī nav pietiekamas aizsardzības, kā arī piemērotu aizsardzības pasākumu. Turklāt EDAK lēmumā par aizsardzības līmeņa pietiekamību atzinīgi vērtētu atkārtotus apliecinājumus, ka personas dati netiks nosūtīti no Korejas personas datu pārziņiem uz trešo valsti situācijā, kurā saskaņā ar VDAR nevarētu sniegt derīgu piekrišanu, piemēram, varas nestabilitātes dēļ.

15. Attiecībā uz Korejas uzraudzības iestādes pārstāvju iecelšanu — lai gan oficiālā procedūra būtu saskaņā ar VDAR un tādējādi atbilstu EEZ tiesiskā regulējuma līdzvērtības kritērijam, EDAK atzinīgi vērtētu, ja Eiropas Komisija uzraudzītu visas norises, kas varētu ietekmēt Dienvidkorejas uzraudzības iestādes pārstāvju neatkarību.

16. Attiecībā uz budžetu — atkal, pamatojoties uz Eiropas Komisijas sniegto informāciju, nav atsauces ne uz PDAK piešķirtā personāla specifiku, ne arī uz tā rīcībā esošajiem finanšu resursiem. Tāpēc EDAK atzinīgi vērtētu papildinformāciju lēmuma projektā par šīm divām būtiskajām tēmām.

1.2.3. Par publisko iestāžu piekļuvi datiem, kas nosūtīti uz Korejas Republiku

17. EDAK ir arī analizējusi Korejas tiesisko regulējumu attiecībā uz valdības piekļuvi personas datiem, kas nosūtīti no EEZ uz Koreju, tiesībaizsardzības un valsts drošības nolūkos. Atzīstot Korejas valdības sniegtos apgalvojumus un garantijas, kā izklāstīts lēmuma projekta II pielikumā, EDAK ir identificējusi vairākus aspektus, kas ir jāprecizē vai rada bažas.

18. EDAK atzīmē, ka PDAL noteikumi tiek piemēroti bez ierobežojumiem tiesībaizsardzības jomā. EDAK arī atzīmē, ka uz datu apstrādi valsts drošības jomā attiecas vairāk ierobežots PDAL nosacījumu kopums.

19. Attiecībā uz telekomunikāciju pakalpojumu sniedzēju brīvprātīgu personas datu izpaušanu valsts drošības iestādēm — EDAK pauž bažas, ka lēmuma projekta I pielikuma 3. sadaļas saistība, kas nosaka, ka pakalpojumu sniedzējiem principā ir jāpaziņo attiecīgajai personai, ja viņi brīvprātīgi ievēro kādu pieprasījumu, un PDAL 58. panta 1. punkta 2. apakšpunkts, proti, daļējs izņēmums valsts drošības

nolūkos, nav skaidrs. Tas varētu samazināt informācijas prasību efektivitāti, ievērojami apgrūtinot datu subjektu iespējas aizstāvēt savas tiesības uz datu aizsardzību, jo īpaši attiecībā uz tiesisko aizsardzību.

20. Lai gan lēmuma projektā tas nav skaidri pateikts, EDAK no Eiropas Komisijas sniegtajiem paskaidrojumiem saprot, ka Korejas tiesiskais regulējums neatļauj telesakaru pārtveršanu lielapjomā. Tādējādi Eiropas Cilvēktiesību tiesas ("**ECT**") nesenā prakse attiecībā uz masveida pārtveršanas režīmiem nebūtu tieši saistīta ar datu aizsardzības līmeņa novērtējumu Korejā.

21. Lēmuma projektā nav nekādas informācijas par tiesisko regulējumu turpmākai pārsūtīšanai valsts drošības jomā. Lai gan EDAK ir sapratusi, ka, pēc Eiropas Komisijas domām, tālāku nosūtīšanu valsts drošības nolūkos pietiekami regulē vispārējie drošības pasākumi un principi, kas izriet no konstitucionālās sistēmas un PDAL, EDAK ir nobažījusies, vai to var uzskatīt par atbilstošu tiesību aktu precizitātes un skaidrības prasībām un paredz efektīvus un izpildāmus aizsardzības pasākumus. Aizsardzības pasākumi, uz kuriem atsaucas Eiropas Komisija, ir ļoti vispārīgi un neattiecas (ar juridisku pamatu) uz konkrētiem apstākļiem un nosacījumiem, saskaņā ar kuriem var notikt tālāka nosūtīšana valsts drošības nolūkos. Šajā kontekstā EDAK arī atzīmē, ka Eiropas Komisija nav apsvērusi, ka pastāv starptautiski nolīgumi, kas ir noslēgti starp Korejas Republiku un trešajām valstīm vai starptautiskām organizācijām un kas var paredzēt īpašus noteikumus par personas datu starptautisku nosūtīšanu uz trešajām valstīm, ko veic tiesībaizsardzības dienesti un/vai izlūkdienesti. EDAK uzskata, ka divpusēju vai daudzpusēju nolīgumu noslēgšana ar trešajām valstīm tiesībaizsardzības vai izlūkošanas sadarbības nolūkā, visticamāk, ietekmēs Korejas datu aizsardzības tiesisko regulējumu.

22. EDAK atzīmē, ka krimināltiesību izpildes, kā arī valsts drošības iestāžu uzraudzību nodrošina dažādu iekšējo un ārējo struktūru kombinācija, jo īpaši PDAK, kam ir pietiekama izpildvara.

23. Efektīviem tiesiskās aizsardzības līdzekļiem un tiesiskajai aizsardzībai ir nepieciešams, lai datu subjekti varētu vērsties kompetentā iestādē, kas atbilst Eiropas Savienības Pamattiesību hartas ("**Harta**") 47. panta prasībām, proti, kas ir kompetenta noteikt, vai notiek datu apstrāde, lai pārbaudītu apstrādes likumību, un kurai ir izpildāmas pilnvaras gadījumos, kad datu apstrāde ir nelikumīga. Ņemot to vērā, EDAK lūdz Eiropas Komisiju precizēt, vai uz PDAK sūdzību vai jebkuru prasību tiesā attiecas materiālas un/vai procesuālas prasības, piemēram, pierādījumu pienākums, un vai personas EEZ varētu atbilst šādam priekšnosacījumam.

1.3. Secinājumi

24. EDAK uzskata, ka šis lēmums par aizsardzības līmeņa pietiekamību ir ārkārtīgi svarīgs, ņemot vērā arī to, ka — ar atzinumā uzsvērtajiem izņēmumiem — tas attieksies uz nosūtīšanu gan valsts, gan privātajā sektorā.

25. EDAK atzinīgi vērtē Eiropas Komisijas un Korejas iestāžu īstenotos centienus saskaņot Korejas un Eiropas tiesisko regulējumu. Ļoti svarīgi un atzinīgi vērtēti ir uzlabojumi, kurus paredzēts ieviest Paziņojumā Nr. 2021-1 ar mērķi novērst dažas neatbilstības starp abiem tiesiskajiem regulējumiem. Tomēr EDAK konstatē, ka joprojām pastāv bažas par vairākiem aspektiem, tostarp saistībā ar Paziņojumu Nr. 2021-1, kā arī nepieciešamība pēc papildu skaidrojumiem citos jautājumos, un tā iesaka Eiropas Komisijai pievērsties šīm problēmām, kā arī EDAK izvirzītajiem skaidrojuma pieprasījumiem un sniegt papildu informāciju un skaidrojumus par šajā atzinumā minētajiem jautājumiem.

2. IEVADS

2.1. Korejas datu aizsardzības regulējums

26. Galvenais tiesību akts, kas reglamentē datu aizsardzību Korejas Republikā, ir Personas datu aizsardzības likums (2011. gada 29. marta likums Nr. 10465, kurā jaunākie grozījumi izdarīti ar 2020. gada 4. februāra likumu Nr. 16930, "**PDAL**"). To papildina Izpildes dekrēts (Prezidenta 2011. gada 29. septembra dekrēts Nr. 23169, kurā jaunākie grozījumi izdarīti ar Prezidenta 2020. gada 4. augusta dekrētu Nr. 30892, "PDAL Izpildes dekrēts"), kas ir juridiski saistošs un izpildāms.

27. Papildus PDAL Korejas datu aizsardzības regulējumā ir iekļauti Korejas uzraudzības iestādes — Personas datu aizsardzības komisijas ("**PDAK**") normatīvie "paziņojumi", kas sniedz papildu noteikumus par PDAL interpretāciju un piemērošanu. Nesen PDAK pieņēma 2021. gada 21. janvāra Paziņojumu Nr. 2021-1 (ar kuru tika grozīts iepriekšējais 2020. gada 1. septembra Paziņojums Nr. 2020-10, turpmāk — "**Paziņojums Nr. 2021-1**") par dažu PDAL nosacījumu interpretāciju, piemērošanu un izpildi. Konkrētāk var norādīt, ka šis paziņojums radās diskusijās par aizsardzības līmeņa pietiekamību starp Korejas iestādēm un Eiropas Komisiju. Tas ietver skaidrojumus par konkrētu PDAL nosacījumu piemērošanu, tostarp par personas datu apstrādi, kas nosūtīti uz Koreju, pamatojoties uz paredzēto lēmumu par aizsardzības līmeņa pietiekamību[8], un tam *ir administratīva noteikuma statuss ar juridiski saistošu spēku personas datu pārzinim tādā nozīmē, ka jebkurš paziņojuma pārkāpums var tikt uzskatīts par attiecīgo PDAL nosacījumu pārkāpumu*[9]. Šajā kontekstā EDAK vēlas atzīmēt, ka, neraugoties uz to, ka lēmuma projektā tas ir minēts kā "Papildu noteikumi", Paziņojumā nav iekļauti papildu noteikumi*per se*, bet gan skaidrojumi, kuru mērķis ir precizēt, kā jāsaprot PDAL normatīvais teksts, lai to jo īpaši piemērotu no EEZ nosūtītajiem datiem. Ņemot to vērā, EDAK ieteiktu rūpīgi uzraudzīt Paziņojuma Nr. 2021-1 ievērošanu praksē, jo īpaši attiecībā uz tā piemērošanu ne tikai no PDAK, bet arī no tiesu puses, it sevišķi gadījumos, kad līdzvērtīgs aizsardzības līmenis, ko nodrošina Korejas tiesiskais regulējums, ir balstīts uz paziņojumā Nr. 2021-1 paredzētajiem precizējumiem.

28. Citi Korejas tiesiskā regulējuma attiecīgie datu aizsardzības likumi paredz noteikumus personas datu apstrādei noteiktās rūpniecības nozarēs, piemēram:

- Likums par kredītinformācijas izmantošanu un aizsardzību ("**CIP**"), tostarp tā Izpildes dekrēts ("**CIP Izpildes dekrēts**"), kurš nosaka īpašus noteikumus, kas attiecas uz komerciālajiem operatoriem un specializētām struktūrām (piemēram, kredītreitingu aģentūrām, finanšu iestādēm), kad tās apstrādā personas kredītinformāciju, kas nepieciešama, lai noteiktu finanšu vai komerciālo darījumu pušu kredītspēju;
- Likums par informācijas un sakaru tīklu izmantošanu un datu aizsardzības veicināšanu ("**Tīkla likums**"); un
- Komunikācijas privātuma aizsardzības likums ("**KPAL**")

29. Valdības piekļuves jomā, izņemot attiecīgos PDAL un KPAL nosacījumus, EDAK ir izskatījusi dažus citus tiesību aktus, piemēram, Kriminālprocesa likumu ("**KPL**"), Telekomunikāciju uzņēmējdarbības likumu ("**TUL**"), Noteiktas finanšu darījumu informācijas ziņošanas un izmantošanas likumu ("**NFDIZIL**") un Nacionālā izlūkdienesta likumu ("**NIDL**").

[8] Skatīt lēmuma projekta I pielikuma I sadaļu.
[9] Turpat.

2.2. EDAK novērtējuma darbības joma

30. Eiropas Komisijas lēmuma projekts ir izveidots Korejas datu aizsardzības sistēmas novērtējuma rezultātā, kam sekoja diskusijas ar Korejas valdību. Saskaņā ar VDAR 70. panta 1. punkta s) apakšpunktu ir paredzams, ka EDAK sniegs neatkarīgu atzinumu par Eiropas Komisijas konstatējumiem, identificēs atbilstības regulējuma nepilnības, ja tādas būs, un sniegs ierosinājumus to novēršanai.

31. Lai izvairītos no atkārtošanās un palīdzētu novērtēt Korejas tiesisko regulējumu, EDAK ir izvēlējusies koncentrēties uz dažiem konkrētiem lēmuma projektā izklāstītajiem punktiem un sniegt savu analīzi un atzinumu par tiem, atturoties no vairuma faktu konstatējumu un novērtējumu atspoguļošanas tad, ja EDAK nav nekādu pazīmju, lai pieņemtu, ka Korejas Republikas tiesību akti būtībā nebūtu līdzvērtīgi EEZ tiesību aktiem. Turklāt saskaņā ar EST judikatūru ļoti svarīga analīzes daļa attiecas uz tiesisko režīmu saistībā uz valsts drošības piekļuvi Korejas Republikai nosūtītajiem personas datiem un valsts drošības aparāta praksi.

32. Savā novērtējumā EDAK ņēma vērā piemērojamo Eiropas datu aizsardzības regulējumu, tostarp Hartas 7., 8. un 47. pantu, attiecīgi aizsargājot tiesības uz privāto un ģimenes dzīvi, tiesības uz personas datu aizsardzību un tiesības uz efektīvu tiesiskās aizsardzības līdzekli un taisnīgu tiesu, kā arī ECTK 8. pantu, kas aizsargā tiesības uz privāto un ģimenes dzīvi. Papildus iepriekš minētajam EDAK ņēma vērā VDAR prasības un attiecīgo judikatūru.

33. Šī uzdevuma mērķis ir sniegt Eiropas Komisijai atzinumu par aizsardzības līmeņa pietiekamības novērtējumu Korejas Republikā. EST tālāk izstrādāja "pietiekama aizsardzības līmeņa" jēdzienu, kas jau pastāvēja saskaņā ar Direktīvu 95/46. Ir svarīgi atcerēties EST lietā *Schrems* I izvirzīto standartu, proti, ka, lai arī "aizsardzības līmenim" trešā valstī ir jābūt "būtībā līdzvērtīgam" ES garantētajam līmenim, "*juridiskie līdzekļi, kas trešai valstij saistībā ar to ir pieejami ar mērķi nodrošināt šādu aizsardzības līmeni, var atšķirties no ES izmantotajiem*"[10]. Tāpēc mērķis nav punktu pa punktam atdarināt Eiropas tiesību aktus, bet gan iedibināt būtiskās un galvenās aplūkoto tiesību aktu prasības. Atbilstību var sasniegt, paredzot virkni datu subjektu tiesību, kā arī pienākumus personas datu apstrādātājiem vai struktūrām, kam ir kontroles tiesības pār šādu apstrādi un uzraudzību, ko īsteno neatkarīgas iestādes. Taču datu aizsardzības noteikumi ir efektīvi tikai tādā gadījumā, kad tie ir izpildāmi un tiek ievēroti praksē. Tāpēc ir jāapsver ne vien tādu noteikumu saturs, kas piemērojami personas datiem, kuri tiek nosūtīti uz trešo valsti vai starptautisku organizāciju, bet arī pastāvošā sistēma, kas nodrošina šādu noteikumu efektivitāti. Efektīvi piemērošanas mehānismi ir sevišķi svarīgi, lai panāktu datu aizsardzības noteikumu efektivitāti[11].

2.3. Vispārējas piezīmes un bažas

2.3.1. Starptautiskās saistības, ko uzņēmusies Korejas Republika

34. Saskaņā ar VDAR 45. panta 2. punkta c) apakšpunktu un VDAR pietiekamības atsaucēm[12], novērtējot trešās valsts aizsardzības līmeņa atbilstību, Eiropas Komisija cita starpā ņem vērā trešās valsts starptautiskās saistības vai citus pienākumus, kas izriet no trešās valsts dalības daudzpusējās vai reģionālās sistēmās, jo īpaši saistībā ar personas datu aizsardzību, kā arī šādu pienākumu izpildi.

35. Koreja ir līgumslēdzēja puse vairākos starptautiskos nolīgumos, kas garantē tiesības uz privātumu, piemēram, Starptautiskajā paktā par pilsoniskajām un politiskajām tiesībām (17. pants), Konvencijā par personu ar invaliditāti tiesībām (22. pants) un Konvencijā par bērnu tiesībām (16. pants). Turklāt

[10] C-362/14, *Maximilian Schrems v Data Protection Commissioner*, 2015. gada 6. oktobris, ECLI:EU:C:2015:650, 73.–74. punkts
[11] WP254, 2. lpp.
[12] WP254, 2. lpp.

Koreja kā ESAO dalībvalsts ievēro ESAO regulējumu attiecībā uz privātumu, jo īpaši vadlīnijas, kas reglamentē privātuma aizsardzību un personas datu pārrobežu plūsmas.

36. EDAK arī ņem vērā Korejas kā novērotājas valsts dalību Eiropas Padomes Konvencijas Nr. 108(+) Konsultatīvās komitejas darbā, lai gan nav vēl izlēmusi, vai tai pievienoties.

2.3.2. Lēmuma par aizsardzības līmeņa pietiekamību darbības joma

37. Saskaņā ar lēmuma projekta 5. apsvērumu Eiropas Komisija secina, ka Korejas Republika nodrošina pietiekamu aizsardzības līmeni personas datiem, kas no datu pārziņa vai apstrādātāja Eiropas Savienībā tiek nosūtīti personas datu pārziņiem (piemēram, fiziskām vai juridiskām personām, organizācijām, sabiedriskām iestādēm), uz kurām attiecas PDAL darbības joma, izņemot personas datu apstrādi misionāru darbībām, ko veic reliģiskās organizācijas, un politisko partiju kandidātu izvirzīšanu[13], vai personas kredītinformācijas apstrādi saskaņā ar CIP, ko veic Finanšu pakalpojumu komisijas uzraudzībai pakļauti datu pārziņi.

38. EDAK atzīmē, ka lēmums par aizsardzības līmeņa pietiekamību attieksies uz nosūtīšanas gadījumiem no EEZ tiesiskā regulējuma gan publiskiem, gan privātiem "personas datu pārziņiem", kas ietilpst PDAL darbības jomā. EDAK saprot, ka uz struktūrām, kas darbojas kā datu apstrādātāji VDAR izpratnē, attiecas arī termins "personas datu pārzinis", ņemot vērā, ka PDAL attieksies uz tām vienādi un ka konkrētas saistības ir piemērojamas, ja personas datu pārzinis ("ārpakalpojumu sniedzējs") iesaista kādu trešo pusi personas datu apstrādē ("ārpakalpojumu sniedzējs"), tomēr, lai izvairītos no pārpratumiem, EDAK aicina Eiropas Komisiju izteikties skaidrāk par to, ka lēmums par atbilstību attieksies arī uz nosūtīšanu "datu apstrādātājiem" Korejā un ka arī šajos gadījumos netiks apdraudēts no EEZ nosūtīto personas datu aizsardzības līmenis.

39. Bez tam ņemot vērā, ka lēmums par aizsardzības līmeņa pietiekamību attiecas arī uz personas datu nosūtīšanu valsts iestāžu starpā, EDAK saprot, ka tas attieksies arī uz nosūtīšanas gadījumiem starp datu aizsardzības uzraudzības iestādēm, un skaidrības labad aicina Eiropas Komisiju īpaši risināt šo jautājumu.

40. Turklāt attiecībā uz struktūrām, kas nav iekļautas lēmuma par aizsardzības līmeņa pietiekamību piemērošanas jomā, EDAK vēlas uzsvērt, ka lēmumā par aizsardzības līmeņa pietiekamību vajadzētu skaidrāk identificēt "komerciālās organizācijas", uz kurām attiecas PDAK uzraudzība (CIP 45. panta 3. punkts), lai EEZ datu pārziņi un apstrādātāji varētu viegli novērtēt, vai arī importētājs ir pakļauts lēmuma par aizsardzības līmeņa pietiekamību piemērošanas jomai, pirms datu nodošanas struktūrām, uz kurām attiecas CIP darbības joma, vai vismaz tiktu brīdināti par šī aspekta izvērtēšanas nepieciešamību.

41. Attiecībā uz lēmuma par aizsardzības līmeņa pietiekamību darbības jomu EDAK no Eiropas Komisijas papildu paskaidrojumiem ir sapratusi, ka arī Korejas Finanšu izlūkošanas vienība ("**KOFIV**"), kas ir izveidota Finanšu pakalpojumu komisijas pakļautībā un uzrauga nelikumīgi iegūtu līdzekļu legalizācijas un terorisma finansēšanas novēršanu saskaņā ar NFDIZIL[14], ir izslēgta no darbības jomas, jo tās kompetencē ir tikai finanšu iestādes, kas pašas nav iekļautas lēmuma projektā. Taču lēmuma projekta 1. panta 2. punkta c) apakšpunkts no tā darbības jomas izslēdz tikai tos personas datu pārziņus, kuri ir pakļauti Finanšu pakalpojumu komisijas pārraudzībai un apstrādā personas kredītinformāciju saskaņā ar CIP. Ņemot to vērā, EDAK lūdz Eiropas Komisiju precizēt, vai lēmuma projekts attiecas uz KOFIV un pašas KOFIV veiktās datu apstrādes darbībām.

[13] Plašāku kontekstu skatīt šī atzinuma 3.1.2. sadaļā.
[14] Skatīt II pielikuma 2.2.3.1. sadaļu.

3. VISPĀRĪGI DATU AIZSARDZĪBAS ASPEKTI

3.1. Saturiskie principi

42. VDAR pietiekamības atsauču 3. nodaļa ir veltīta "Saturiskajiem principiem". Tiem ir jābūt ietvertiem trešās valsts sistēmā, lai nodrošināto aizsardzības līmeni varētu uzskatīt par būtībā līdzvērtīgu tam, kas garantēts ES tiesību aktos.

43. Lai gan tiesības uz personas datu aizsardzību pašas par sevi nav skaidri noteiktas Korejas Konstitūcijā, tās tiek atzītas par pamattiesībām, kas izriet no konstitucionālajām tiesībām uz cilvēka cieņu un tiekšanos pēc laimes (10. pants), privāto dzīvi (17. pants) un komunikāciju privātumu (18. pants). To ir apstiprinājusi gan Augstākā tiesa, gan Satversmes tiesa, kā norādīts Eiropas Komisijas lēmuma projektā[15]. EDAK ņem vērā šo atzinumu, jo no tā izriet, ka datu aizsardzību kā pamattiesības saskaņā ar Korejas Konstitūcijas 37. pantu "*var ierobežot tikai ar likumu un gadījumos, kad tas ir nepieciešams valsts drošībai vai likuma un kārtības uzturēšanai, vai sabiedrības labklājībai*," un ka "*pat tad, ja tiek noteikti šādi ierobežojumi, tie nedrīkst ietekmēt brīvības vai tiesību būtību*".

44. Saskaņā ar Eiropas Komisijas[16] teikto Satversmes tiesa ir nolēmusi, ka arī ārvalstu pilsoņi ir pamattiesību subjekts. Saskaņā ar Korejas valdības oficiālajiem paziņojumiem[17], lai gan judikatūrā līdz šim nav īpaši aplūkotas trešo valstu pilsoņu privātuma tiesības, zinātnieku vidū ir plaši atzīts, ka Konstitūcijas 12.–22. pants nosaka "cilvēku tiesības". Turklāt Korejas Republika ir pieņēmusi virkni likumu datu aizsardzības jomā, kas nodrošina aizsardzību visām personām neatkarīgi no viņu valstspiederības, piemēram, PDAL. Šajā saistībā EDAK ņem vērā, ka Konstitūcijas 6. panta 2. punkts nosaka, ka ārvalstu pilsoņu statuss tiek garantēts, kā noteikts starptautiskajās tiesībās un līgumos, kā arī judikatūrā, kas minēta lēmuma projektā, saskaņā ar kuru "ārzemnieks" var būt "pamattiesību" nesējs. Ņemot vērā to, cik svarīgi ir atzīt tiesības uz datu aizsardzību "ārvalstu pilsoņiem", EDAK aicina Eiropas Komisiju pievērst uzmanību tam, ka ir jāturpina uzraudzīt judikatūra attiecībā uz datu aizsardzību kā pamattiesībām, kas tiek atzītas ne tikai Korejas pilsoņiem, bet visiem datu subjektiem, lai nodrošinātu, ka netiek apdraudēts VDAR garantētais fizisko personu aizsardzības līmenis, kad personas dati tiek nosūtīti uz Koreju saskaņā ar lēmumu par aizsardzības līmeņa pietiekamību.

3.1.1. Jēdzieni

45. Pamatojoties uz VDAR pietiekamības atsaucēm, vienkāršiem datu aizsardzības jēdzieniem un/vai principiem jābūt iekļautiem trešās valsts tiesiskajā regulējumā. Lai arī tiem nav pilnībā jāatspoguļo VDAR terminoloģija, tiem būtu jāatspoguļo un jāsaskan ar Eiropas datu aizsardzības tiesību aktos ietvertajiem jēdzieniem. Piemēram, VDAR ir iekļauti šādi svarīgi jēdzieni: "personas dati", "personas datu apstrāde", "datu pārzinis", "datu apstrādātājs", "saņēmējs" un "sensitīvi dati"[18].

46. PDAL ir iekļautas vairākas definīcijas, piemēram, "personas dati", "apstrāde" un "datu subjekts", kas ļoti līdzinās attiecīgajiem VDAR terminiem.

3.1.1.1. *Pseidonimizētu datu koncepts*

47. Starp PDAL sniegtajām definīcijām PDAL 2. panta 1. punkts jo īpaši definē personas datus kā jebkuru šādu informāciju, kas attiecas uz dzīvu fizisku personu: a) informāciju, kas identificē konkrētu fizisku personu ar pilnu vārdu, rezidenta reģistrācijas numuru, attēlu utt., un b) informāciju, kuru pat tad, ja tā pati par sevi neidentificē konkrētu personu, var viegli kombinēt ar citu informāciju, lai identificētu

[15] Skatīt lēmuma projekta 8. apsvērumu un attiecīgo judikatūru, kas minēta lēmuma projekta 10. vērē, un kam ir pieejami tikai kopsavilkumi angļu valodā.
[16] Skatīt lēmuma projekta 9. apsvērumu.
[17] Lēmuma projekta II pielikuma 1.1. sadaļa.
[18] WP254, 4. lpp.

konkrētu fizisku personu. Pēdējos no šiem gadījumiem to, vai kombinēšana ir vienkārša, nosaka, pamatoti ņemot vērā fiziskas personas identificēšanai patērēto laiku, izmaksas, tehnoloģijas u.c., piemēram, citas informācijas iegūšanas varbūtību.

48. Turklāt saskaņā ar PDAL 2. panta 1. punkta c) apakšpunktu arī "pseidonimizēta informācija" tiek uzskatīta par personas datiem. Pseidonimizēta informācija tiek definēta kā informācija saskaņā ar iepriekš minēto a) vai b) apakšpunktu, kas ir pseidonimizēta saskaņā ar 1.–2. apakšpunktu un tādējādi to nevar izmantot konkrētas fiziskas personas identificēšanai, neizmantojot vai nekombinējot informāciju, lai to atjaunotu sākotnējā stāvoklī. Informācija, kas ir pilnībā anonimizēta, ir izslēgta no PDAL piemērošanas jomas. Saskaņā ar PDAL 58. panta 2. punktu likums neattiecas uz informāciju, kas vairs neidentificē noteiktu fizisku personu, ja to kombinē ar citu informāciju, pamatoti ņemot vērā laiku, izmaksas, tehnoloģiju utt.

49. Eiropas Komisija lēmuma projekta 17. apsvērumā norāda, ka tas atbilst VDAR materiālajai piemērošanas jomai un tās jēdzieniem "personas dati", "pseidonimizācija" un "anonimizēta informācija".

50. Tomēr saskaņā ar PDAL 28. panta 7. punktu 20., 21., 27. pants, 34. panta 1. punkts, 35.–37. pants, 39. panta 3. punkts, 39. panta 4. punkts un 39. panta 6.–8. punkts neattiecas uz pseidonimizētiem personas datiem.

51. Eiropas Komisija savā lēmuma projektā norāda, ka PDAL 28. panta 7. punkts ir piemērojams tikai pseidonimizētiem personas datiem, ja tie tiek apstrādāta statistikas, zinātniskās izpētes vai arhivēšanas nolūkos sabiedrības interesēs[19]. Tomēr tas neizriet tieši no likuma burta, bet gan no Paziņojumā Nr. 2021-1 sniegtajiem paskaidrojumiem[20]. Lai gan EDAK atzīst, ka, pamatojoties uz PDAL struktūru un pamatojumu, var izvirzīt argumentu, ka PDAL 28. panta 2. punkts ir jāsaprot un loģiski jāinterpretē kā piemērojams arī PDAL 28. panta 7. punktam, ņemot vērā Paziņojuma Nr. 2021-1 nozīmīgumu Eiropas Komisijas novērtējumā par personas datu aizsardzības līmeņa atbilstību Korejas Republikā un lai izvairītos no jebkādām šaubām, EDAK aicina Eiropas Komisiju sniegt papildinformāciju par Paziņojuma Nr. 2021-1 saistošo raksturu, izpildāmību un derīgumu un uzraudzīt tā piemērošanu šajā konkrētajā kontekstā.

52. Šajā kontekstā EDAK vēlas atgādināt, ka saskaņā ar VDAR pseidonimizācija ir saprotama kā ieteicams drošības pasākums. Citiem vārdiem sakot, saskaņā ar VDAR pseidonimizēti dati joprojām ir personas dati, uz kuriem pilnībā attiecas VDAR. Pamatojoties uz iepriekšminēto, EDAK pauž bažas, ka, nosūtot personas datus uz Koreju, var tikt apdraudēts VDAR aizsardzības līmenis pseidonimizētiem personas datiem. Tāpēc EDAK aicina Eiropas Komisiju turpmāk izvērtēt pseidonimizācijas ietekmi saskaņā ar PDAL un, kas ir vissvarīgāk, kā tā var ietekmēt to datu subjektu pamattiesības un brīvības, kuru personas dati tiks nosūtīti uz Korejas Republiku, pamatojoties uz lēmumu par aizsardzības līmeņa pietiekamību. Tāpēc EDAK aicina Eiropas Komisiju sniegt garantijas, ka EEZ datu subjektu personas datu aizsardzības līmenis nepazemināsies pēc nosūtīšanas uz Korejas Republiku, pat ja pārsūtītie personas dati ir pseidonimizēti.

3.1.1.2. *Personas datu pārziņa koncepts*

53. PDAL 2. panta 5. punktā ir iekļauta "personas datu pārziņa" definīcija, kur šis termins nozīmē valsts iestādi, juridisku personu, organizāciju vai fizisku personu utt., kas tieši vai netieši apstrādā personas datus, lai rīkotos ar personas datu failiem "*savas darbības ietvaros*". Tomēr papildu drošības pasākumos, kas izklāstīti Paziņojumā Nr. 2021-1, termins "personas datu pārzinis" ir definēts kā valsts

[19] Cita starpā skatīt arī lēmuma projekta 82. apsvērumu.
[20] Lēmuma projekta I pielikuma 4. sadaļa.

iestāde, juridiska persona, organizācija, fiziska persona utt., kas tieši vai netieši apstrādā personas datus, lai rīkotos ar personas datu failiem "*uzņēmējdarbības nolūkos*". Savukārt lēmuma projekta 272. zemsvītras piezīmē par personas datu pārziņa jēdzienu ir norādīts šādi: "*Kā noteikts PDAL 2. pantā, proti, valsts iestāde, juridiska persona, organizācija, fiziska persona utt., kas tieši vai netieši apstrādā personas datus, lai rīkotos ar personas datu failiem "oficiālos vai uzņēmējdarbības nolūkos"*."

54. EDAK atzīst, ka šīs neatbilstības var būt saistītas ar oriģinālā teksta tulkojumiem, ko nodrošinājušas Korejas iestādes, un aicina Eiropas Komisiju regulāri pārbaudīt tulkojumu kvalitāti un noteiktību. Tomēr EDAK uzsver faktu, ka, lai varētu novērtēt Korejas tiesiskā regulējuma datu aizsardzības līmeņa būtisku līdzvērtību, ir nepieciešama skaidra izpratne par apstrādes nolūkiem, kas ietilpst PDAL materiālajā piemērošanas jomā. Turklāt šajā kontekstā EDAK atzīmē, ka PDAL neizmanto vienu un to pašu VDAR terminoloģiju attiecībā uz jēdzienu "datu pārzinis" un "datu apstrādātājs", un aicina Eiropas Komisiju precizēt koncepta "personas datu pārzinis" pareizo definīciju un darbības jomu un īpaši pievērsties tam, vai šis termins VDAR nozīmē attiecas arī uz datu apstrādātājiem, jo tas tieši ietekmē lēmuma par aizsardzības līmeņa pietiekamību darbības jomu[21].

3.1.2. Daļēji atbrīvojumi, kas paredzēti PDAL

55. PDAL 58. panta 1. punkts izslēdz PDAL daļu (proti, 15.–57. panta) piemērošanu četrām personas datu apstrādes kategorijām, kā aprakstīts tālāk. Proti, atbrīvojumi attiecas uz PDAL nosacījumiem par konkrētiem apstrādes iemesliem, noteiktiem datu aizsardzības pienākumiem, sīki izstrādātiem noteikumiem par fiziskas personas tiesību izmantošanu, kā arī noteikumiem, kas reglamentē strīdu izšķiršanu. Tomēr EDAK ņem vērā, ka joprojām tiek piemēroti daži vispārīgi PDAL noteikumi, piemēram, tie, kas attiecas uz datu aizsardzības principiem (PDAL 3. pants) un fiziskas personas tiesībām (PDAL 4. pants). Turklāt PDAL 58. panta 4. punkts nosaka īpašus pienākumus attiecībā uz šīm četrām datu apstrādes kategorijām.

56. Pirmkārt, daļējais atbrīvojums attiecas uz personas datiem, kas tiek vākti saskaņā ar Statistikas likumu, lai tos apstrādātu valsts iestādes. Eiropas Komisija lēmuma projekta 27. apsvērumā norāda, ka saskaņā ar Korejas valdības saņemtajiem paskaidrojumiem šajā kontekstā apstrādātie personas dati parasti attiecas uz Korejas pilsoņiem un var tikai izņēmuma kārtā iekļaut informāciju par ārvalstniekiem, proti, statistikas gadījumā par ieceļošanu un izbraukšanu no teritorijas vai ārvalstu investīcijām. Tomēr saskaņā ar lēmuma projektu pat šādos gadījumos šādi dati parasti netiek saņemti no datu pārziņiem/apstrādātājiem EEZ, bet drīzāk tos tieši ievāc Korejas valsts iestādes.

57. EDAK atzīst Eiropas Komisijas argumentāciju par to, ka Statistikas likuma piemērošanas izņēmums attiecas uz tādu personas datu apstrādi, kas ir nosūtīti saskaņā ar lēmumu par aizsardzības līmeņa pietiekamību; tomēr tā atzinīgi vērtētu papildinformāciju un apliecinājumus par konkrētiem aizsardzības pasākumiem, kas tiktu piemēroti gadījumā, ja no EEZ nosūtītie personas dati tiktu vākti saskaņā ar Statistikas likumu, lai tos apstrādātu valsts iestādes, jo īpaši saistībā ar datu subjektu individuālo tiesību izmantošanu saskaņā ar VDAR 89. panta 2. punktu, ciktāl šādas tiesības var neļaut vai būtiski traucēt sasniegt konkrētos nolūkus, un šādas atkāpes nav vajadzīgas minēto nolūku sasniegšanai.

58. Šajā perspektīvā šķiet, ka PDAL 4. panta piemērošana arī šāda veida apstrādei sniedz pārliecību, tomēr EDAK labprāt saņemtu papildinformāciju un paskaidrojumus lēmumā par aizsardzības līmeņa atbilstību noteiktajiem pienākumiem saskaņā ar PDAL 58. panta 4. punktu, kas attiecas uz šīm apstrādes darbībām, proti, attiecībā uz datu apjoma samazināšanu, ierobežotu datu glabāšanu, drošības pasākumiem un sūdzību izskatīšanu.

59. Otrkārt, daļējais atbrīvojums attiecas uz personas datiem, kas tiek vākti vai pieprasīti, lai analizētu ar valsts drošību saistītu informāciju. EDAK apzinās faktu, ka valsts drošības jautājumos valstīm ir plaša

[21] Skatīt arī šī dokumenta 38. punktu.

rīcības brīvība, ko atzīst ECT. EDAK arī atzīmē, ka saskaņā ar Korejas Konstitūcijas 37. panta 2. punktu jebkurš brīvību un tiesību ierobežojums, piemēram, ja tas ir nepieciešams valsts drošības aizsardzībai, nedrīkst pārkāpt šīs brīvības vai tiesību būtisko aspektu. Turklāt EDAK atzīmē Paziņojuma Nr. 2021-1 6. sadaļā minētos drošības pasākumus attiecībā uz personas datu apstrādi valsts drošības nolūkos, tostarp pārkāpumu izmeklēšanu un izpildi. Tomēr šajā kontekstā EDAK aicina Eiropas Komisiju sīkāk precizēt atbrīvojumu darbības jomu, jo tai rodas jautājums, vai visi atbrīvojumi, kas paredzēti 58. panta 1. punkta 2. apakšpunktā PDAL (III–VII nodaļa), attiecas uz izlūkdienestu darbu un vai tie nodrošina līdzvērtību nepieciešamības un proporcionalitātes principiem. Jo īpaši EDAK aicina Eiropas Komisiju sniegt vairāk skaidrojumu par to, kādos apstākļos izlūkdienests varētu paļauties uz atbrīvojumiem. EDAK uzskata, ka praksē ir rūpīgi jāuzrauga šo ierobežojumu ietekme, jo īpaši attiecībā uz datu subjektu tiesību efektīvu izmantošanu un izpildi.

60. Treškārt, daļējais atbrīvojums attiecas uz "*personas datiem, kas tiek apstrādāti īslaicīgi, ja tas ir steidzami nepieciešams sabiedrības drošības un aizsardzības, sabiedrības veselības u.c. nolūkos*". Saskaņā ar Eiropas Komisijas lēmuma projekta 29. apsvērumu šo kategoriju PDAK interpretē stingri, un tā attiecas tikai uz ārkārtas situācijām, kad ir nepieciešama steidzama rīcība, piemēram, lai izsekotu infekcijas izraisītājus vai glābtu un palīdzētu dabas katastrofās cietušajiem.

61. EDAK arī uzsver, ka visas atkāpes no personas datu aizsardzības līmeņa ir jāinterpretē stingri. Vienlaikus EDAK atzīmē, ka nosacījums nav stingri definēts un nesniedz izsmeļošu piemēru sarakstu par situācijām, kad personas datu apstrādi varētu uzskatīt par "*steidzami nepieciešamu*". Piemēram, EDAK ir nobažījusies par to, vai starptautiskā veselības datu nosūtīšana pašreizējās COVID-19 pandēmijas laikā arī būtu šī atbrīvojuma piemērošanas jomā. Ņemot vērā iepriekš minēto, EDAK aicina Eiropas Komisiju sniegt turpmākus paskaidrojumus par šī atbrīvojuma darbības jomu un pilnībā pārraudzīt tā piemērošanu un darbības jomu, lai nodrošinātu, ka tas neizraisa EEZ personas datu aizsardzības līmeņa samazināšanos pēc nosūtīšanas uz Koreju, pamatojoties uz lēmumu par aizsardzības līmeņa pietiekamību.

62. Visbeidzot daļējs atbrīvojums attiecas uz personas datiem, kas tiek vākti vai izmantoti preses ziņojumiem, reliģisko organizāciju misionāru darbībām un politisko partiju kandidātu izvirzīšanai[22]. Attiecībā uz personas datu apstrādi, ko veic prese žurnālistikas darbību nolūkos, Eiropas Komisija lēmuma projekta 31. apsvērumā norāda, ka līdzsvars starp vārda brīvību un citām tiesībām, tostarp tiesībām uz privātumu, ir norādīts likumā par šķīrējtiesu un tiesiskās aizsardzības līdzekļiem utt. attiecībā uz preses ziņojumu radītajiem zaudējumiem (turpmāk — "**Preses likums**"), un tajā ir izklāstīti konkrēti drošības pasākumi, kas izriet no Preses likuma. Tomēr EDAK grib aicināt Eiropas Komisiju pilnībā uzraudzīt šo atbrīvojumu un attiecīgo judikatūru, lai nodrošinātu, ka līdzvērtīgs datu aizsardzības līmenis Korejas tiesiskajā regulējumā tiek nodrošināts arī praksē.

3.1.3. Likumīgas un godprātīgas apstrādes leģitīmiem mērķiem pamatojumi

63. Saskaņā ar VDAR pietiekamības atsaucēm un atbilstoši VDAR dati ir jāapstrādā likumīgi, godprātīgi un leģitīmi. Juridiskais pamats, saskaņā ar kuru personas datus var likumīgi, godprātīgi un leģitīmi apstrādāt, būtu jānosaka pietiekami skaidri. Eiropas sistēmā tiek atzīti vairāki šādi leģitīmi iemesli, tostarp, piemēram, valsts tiesību aktu normas, datu subjekta piekrišana, datu pārziņa vai trešās personas līgumsaistību izpilde vai leģitīmas intereses, kas nav svarīgākas par indivīda interesēm.

64. Ievērojot VDAR līdzīgu struktūru, PDAL sākumā ievieš likumības, taisnīguma un pārredzamības principu (PDAL 3. panta 1. un 2. punkts), izklāstot konkrētus noteikumus tā piemērošanai vēlāk (PDAL 15.–19. pants). Konkrētāk — PDAL 15. pants iekļauj juridisko pamatojumu katalogu, uz kuru personas datu pārziņi var balstīt personas datu vākšanu un to izmantot vākšanas nolūkiem. Šie juridiskie pamati ir 1)

[22] Attiecīgi no lēmuma par aizsardzības līmeņa pietiekamību darbības jomas tiek izslēgta arī personas datu apstrāde, ko veic reliģiskās organizācijas misionāru darbībām un politiskās partijas personas datu apstrādei saistībā ar kandidātu izvirzīšanu. Skatīt arī iepriekš 2.3.2. sadaļas 37. punktu.

datu subjekta informēta piekrišana; 2) ar likumu noteikta atļauja vai nepieciešamība ievērot juridisku pienākumu; 3) valsts iestādes pienākumu izpildes nepieciešamība; 4) nepieciešamība izpildīt līgumu ar datu subjektu; 5) nepieciešamība aizsargāt datu subjekta vai trešās personas dzīvību, fiziskās vai īpašuma intereses no nenovēršama apdraudējuma (un iepriekšēju piekrišanu nevar saņemt); 6) nepieciešamība ievērot personas datu pārziņa pamatotas intereses, kas ir pārākas par datu subjekta interesēm.

65. Turklāt PDAL 17. pantā ir uzskaitīti juridiskie pamati, kas ir piemērojami personas datu koplietošanai ar trešo personu, tostarp 1) datu subjekta informēta piekrišana; 2) likumīga atļauja vai nepieciešamība ievērot juridisku pienākumu; 3) valsts iestādes pienākumu izpildes nepieciešamība; 4) nepieciešamība aizsargāt datu subjekta vai trešās personas dzīvību, fiziskās vai īpašuma intereses no nenovēršama apdraudējuma (un iepriekšēju piekrišanu nevar saņemt). Pat ja nav datu subjekta piekrišanas, personas datu koplietošana ir atļauta, ja tas notiek apjomā, kas ir pamatoti saistīts ar nolūku, kādam personas dati sākotnēji tika vākti (PDAL 17. panta 4. punkts).

66. PDAL 18. pants paredz konkrētus noteikumus par personas datu izmantošanu un koplietošanu, ja tas notiek ārpus datu vākšanas vai nodrošināšanas sākotnējā nolūka. Cita starpā arī piekrišana ir viens no šādiem atļaujošiem noteikumiem.

67. Atzīstot Korejas tiesību aktu būtisko līdzību VDAR attiecībā uz likumības principu un pastāvošām vispārējām tiesībām uz apturēšanu (PDAL 37. pants), uz kurām var atsaukties arī tad, ja personas dati tiek apstrādāti, pamatojoties uz piekrišanu, EDAK vēlas atzīmēt, ka saskaņā ar PDAL nav vispārēju tiesību atsaukt piekrišanu[23]. Ņemot vērā piekrišanas kā juridiskā pamata nozīmi visos iepriekš aprakstītajos scenārijos un ņemot vērā individuālo tiesību lomu datu aizsardzības tiesību sistēmā, lai aizsargātu datu subjektu pamattiesības un brīvības, EDAK aicina Eiropas Komisiju papildus izvērtēt ietekmi, ko rada vispārēju tiesību uz piekrišanas atsaukšanu trūkums saskaņā ar Korejas tiesību aktiem, un sniegt papildu garantijas, lai nodrošinātu, ka vienmēr tiek garantēts būtisks datu aizsardzības līmenis, kāds ir paredzēts VDAR, nepieciešamības gadījumā arī noskaidrojot, kāda ir apturēšanas tiesību loma šajā konkrētajā kontekstā.

3.1.4. Nolūka ierobežošanas princips

68. VDAR pietiekamības atsauces saskaņā ar VDAR paredz, ka dati būtu jāapstrādā noteiktā nolūkā, un pēc tam tos var izmantot, ciktāl tas nav pretrunā apstrādes nolūkam.

69. Saskaņā ar PDAL 3. panta 1. un 2. punktu personas datu pārziņiem ir jāprecizē un skaidri jānosaka apstrādes nolūki, kā arī jānodrošina apstrādes atbilstība šiem nolūkiem. Lai gan šis princips ir apstiprināts citos nosacījumos (piemēram, PDAL 15. panta 1. punktā, 18. panta 1. punktā un 19. panta 1. punktā), noteiktos apstākļos ir atļauta apstrāde "saprātīgi saistītiem" nolūkiem (skatīt PDAL 17. panta 4. punktu)[24], kā arī personas datu izmantošana un nodrošināšana ārpus nolūka izmantošanas (skatīt PDAL 18. un 19. pantu)[25].

[23] Lai gan datu subjekti noteiktos apstākļos var atteikt dot piekrišanu, skatiet, piemēram, PDAL 18. panta 3. punkta 5. apakšpunktu. Turpretī tiesības atsaukt piekrišanu, šķiet, pastāv tikai konkrētos gadījumos; saskaņā ar PDAL 27. panta 1. punktu 2 datu subjektiem ir tiesības atsaukt piekrišanu, ja viņi nevēlas, lai viņu personas dati tiktu nodoti trešajai personai saistībā ar personas datu pārziņa uzņēmējdarbības nodošanu pilnībā vai daļēji, apvienošanos u.c.; saskaņā ar PDAL 39. panta 7. punktu lietotāji var jebkurā brīdī atsaukt piekrišanu personas datu vākšanai, izmantošanai un nodrošināšanai no informācijas un sakaru pakalpojumu sniedzējiem u.c.; un saskaņā ar CIP 37. pantu individuāls kredītinformācijas subjekts var atsaukt piekrišanu, kas tika sniegta kredītinformācijas sniedzējam/lietotājam.

[24] Tādējādi nolūka atbilstība ir jāpārbauda iepriekš, pamatojoties uz PDAL izpildes dekrēta 14-2. pantu.

[25] Skatīt iepriekš arī šī dokumenta 66. punktu.

70. EDAK saprot, ka tad, ja personas dati tiek nosūtīti no EEZ uz Korejas Republiku, pamatojoties uz lēmumu par aizsardzības līmeņa pietiekamību, datu vākšanas nolūks EEZ datu pārziņiem ir nolūks, kādam dati tiek nosūtīti un kas apstrādei jāpiemēro personas datus saņemošajam pārzinim Korejā. Datu pārzinis Korejā varētu mainīt nolūku tikai saskaņā ar PDAL 18. panta 2. punkta 1–3. apakšpunktu, "*ja vien ar šādu rīcību negodīgi netiek pārkāptas datu subjekta vai trešās personas intereses*"[26]. Šajā kontekstā EDAK atzīst Eiropas Komisijas lēmuma projekta 55. apsvērumā pausto, ka gadījumos, kad ar likumu ir atļautas nolūka izmaiņas, šādos tiesību aktos ir jāievēro pamattiesības uz privātumu un datu aizsardzību. Tomēr EDAK atzīmē, ka nav sniegta konkrēta informācija šī konkrētā apgalvojuma pamatošanai, piemēram, nav atsauces uz (Korejas) Konstitūcijas 37. pantu. Tāpēc EDAK aicina Eiropas Komisiju lēmuma projektā sniegt papildu apliecinājumus un garantijas, lai nodrošinātu, ka jebkuri likumi, kas atļauj mainīt apstrādes nolūku, ir nepieciešami, lai ievērotu datu subjektu pamattiesības un brīvības attiecībā uz privātumu un datu aizsardzību.

3.1.5. Datu kvalitātes un proporcionalitātes princips

71. VDAR pietiekamības atsauces norāda, ka datiem vajadzētu būt precīziem un nepieciešamības gadījumā atjauninātiem. Datiem vajadzētu būt adekvātiem, atbilstīgiem un ne pārmērīgiem, ņemot vērā nolūkus, kādos tos apstrādā.

72. Saskaņā ar PDAL personas datu pārziņiem ir jānodrošina, lai personas dati būtu precīzi, pilnīgi un atjaunināti, ciktāl tas ir nepieciešams saistībā ar nolūkiem, kādiem personas dati tiek apstrādāti (PDAL 3. panta 3. punkts). Personas datu pārziņiem ir jāievāc tik maz personas datu, cik ir nepieciešams noteiktā nolūka sasniegšanai. Viņi šajā ziņā uzņemas pierādīšanas pienākumu (PDAL 16. panta 1. punkts).

73. Ņemot to vērā, EDAK piekrīt Eiropas Komisijas novērtējumam attiecībā uz PDAL aizsardzības līmeņa būtisku līdzvērtību salīdzinājumā ar VDAR.

3.1.6. Datu saglabāšanas princips

74. Saskaņā ar VDAR pietiekamības atsaucēm parasti dati būtu jāglabā ne ilgāk, kā tas ir nepieciešams nolūkiem, kādos personas datus apstrādā. Atbilstoši PDAL 21. panta 1. punktam šis princips pastāv arī Korejas tiesību aktos. Saskaņā ar PDAL personas datu pārziņiem ir pienākums nekavējoties iznīcināt personas datus, ja tie kļūst nevajadzīgi pēc glabāšanas termiņa beigām vai paredzētā apstrādes nolūka sasniegšanas, ja vien netiek piemēroti likumā noteiktie glabāšanas termiņi.

75. Tomēr EDAK paužbažas par to, ka PDAL 21. panta 1. punkts nav piemērojams pseidonimizētiem personas datiem. EDAK ņem vērā to, ka saskaņā ar Paziņojuma Nr. 2021-1 4. sadaļas iii) apakšpunktu:"[ja]*personas datu pārzinis apstrādā pseidonimizētu informāciju, lai apkopotu statistiku, veiktu zinātnisku izpēti, saglabātu publiskus ierakstus utt., un ja pseidonimizētā informācija nav* [sic] *iznīcināta, tiklīdz ir sasniegts konkrētais apstrādes nolūks saskaņā ar Konstitūcijas 37. pantu un Likuma 3. pantu (Personas datu aizsardzības principi), tas anonimizē informāciju ar mērķi nodrošināt, ka tā vairs neidentificē konkrētu fizisku personu atsevišķi vai kombinācijā ar citu informāciju, pamatoti ņemot vērā laiku, izmaksas, tehnoloģijas utt., saskaņā ar PDAL 58. panta 2. punktu*." Arī šeit, ņemot vērā Paziņojuma 2021-1 nozīmi un juridisku noteiktību par datu aizsardzības līmeņa līdzvērtību personas datiem, kas uz Korejas Republiku nosūtīti saskaņā ar lēmumu par aizsardzības līmeņa pietiekamību, EDAK atkārtoti aicina Eiropas Komisiju sniegt papildinformāciju it īpaši par to, kā Paziņojums Nr. 2021-1 tiek padarīts saistošs un kā tiek nodrošināta tā izpildāmība un derīgums[27].

[26] PDAL 18. panta 2. punkts.

[27] Skatīt arī iepriekš 51. punktu šī atzinuma 3.1.1.1. sadaļā par EDAK vispārējām bažām attiecībā uz pseidonimizācijas ietekmi saskaņā Korejas tiesību aktiem.

3.1.7. Drošības un konfidencialitātes princips

76. Kā aprakstīts VDAR pietiekamības atsaucēs, drošības un konfidencialitātes princips nosaka, ka datu apstrādes vienībām, kuras apstrādā personas datus, būtu, izmantojot atbilstīgus tehniskus vai organizatoriskus pasākumus, jānodrošina, ka dati tiek apstrādāti tādā veidā, kas nodrošina personas datu drošību, tostarp aizsardzību pret neatļautu vai nelikumīgu apstrādi, kā arī pret nejaušu nozaudēšanu, iznīcināšanu vai sabojāšanu. Drošības pakāpē būtu jāņem vērā tehnikas līmenis un ar to saistītās izmaksas.

77. Eiropas Komisija ir identificējusi līdzīgu datu drošības principu PDAL 3. panta 4. punktā, kas ir sīkāk konkretizēts PDAL 29. pantā. Turklāt datu drošības nosacījumi tiek piemēroti gadījumos, kad personas datu pārzinis piesaista "ārpakalpojumu sniedzēju". Apstrādes drošība ir jānodrošina ar tehniskiem un pārvaldības aizsardzības pasākumiem, kas jāiekļauj arī saistošajā personas datu apstrādes līgumā (PDAL 26. pants un PDAL izpildes dekrēta 28. pants). Turklāt saskaņā ar PDAL datu pārkāpuma gadījumā tiek piemērotas konkrētas saistības, tostarp pienākums informēt ietekmētos datu subjektus un uzraudzības iestādi, ja skarto datu subjektu skaits pārsniedz piemērojamo slieksni (PDAL 34. pants saistībā ar PDAL prezidenta dekrēta 39. pantu), izņemot gadījumus, kad ietekmētie dati ir pseidonimizēti personas dati, kas tiek apstrādāti statistikas, zinātniskas izpētes vai arhivēšanas nolūkos sabiedrības interesēs (PDAL 28. panta 7. punkts). Arī šajā gadījumā[28] EDAK ir nobažījusies par plašajiem atbrīvojumiem, kas attiecas uz pseidonimizētiem datiem, un atkārtoti aicina Eiropas Komisiju turpināt izvērtēt šo aspektu, lai nodrošinātu būtībā līdzvērtīga aizsardzības līmeņa nodrošināšanu saskaņā ar Korejas tiesību aktiem[29].

78. Neraugoties uz to, EDAK ir apmierināta ar Eiropas Komisijas novērtējumu un secinājumu par Korejas tiesību aktu būtisko līdzvērtību attiecībā uz drošības un konfidencialitātes principu.

3.1.8. Pārredzamības princips

79. Pamatojoties uz VDAR 5. panta 1. punkta a) apakšpunktu, pārredzamība ir ES datu aizsardzības sistēmas pamatprincips. VDAR preambulas 39. apsvērumā ir izklāstīta šī principa ārkārtīgi svarīgā funkcija, norādot, ka "[]*fiziskām personām vajadzētu būt pārredzamam tam, ka viņu personas datus vāc, izmanto, aplūko vai citādi apstrādā, un tam, kādā apjomā personas dati tiek vai tiks apstrādāti. (...) Fiziskās personas būtu jāinformē par riskiem, noteikumiem, aizsardzības pasākumiem un tiesībām saistībā ar personas datu apstrādi un to, kā īstenot savas tiesības saistībā ar šādu apstrādi.*"

80. VDAR pietiekamības atsaucēs ir skaidri minēta "pārredzamība" kā viens no satura principiem, kas jāņem vērā, novērtējot, vai trešās valsts nodrošinātais aizsardzības līmenis ir būtībā līdzvērtīgs. Konkrētāk tajā ir teikts, ka "[i]*kviena persona būtu jāinformē par visiem galvenajiem viņa/viņas personas datu apstrādes elementiem skaidrā, viegli pieejamā, kodolīgā, pārredzamā un saprotamā veidā. Šādā informācijā būtu jāiekļauj apstrādes nolūks, personas datu pārziņa identitāte, personai pieejamās tiesības un cita informācija, ciktāl tas ir nepieciešams godprātības nodrošināšanai. Noteiktos apstākļos var pastāvēt daži izņēmumi no šīm tiesībām uz informāciju, piemēram, lai garantētu krimināllizmeklēšanu, valsts drošību, tiesu iestāžu neatkarību un tiesvedību vai citus svarīgus vispārējo sabiedrības interešu mērķus, kas minēti VDAR 23. pantā.*"

81. Līdzīgi kā minēts VDAR, saskaņā ar PDAL tiek izslēgts vispārējs pārredzamības princips, kas ietver prasību personas datu pārziņiem publiskot savu privātuma politiku un citus ar personas datu apstrādi saistītus jautājumus (PDAL 3. panta 5. punkts). Konkrēti pienākumi sniegt informāciju tiek piemēroti gadījumos, kad personas datu pārziņi vēlas saņemt datu subjektu piekrišanu personas datu vākšanai un apstrādei (PDAL 15. panta 2. punkts), lai koplietotu personas datus ar trešo personu (PDAL 17. panta 2. punkts) un apstrādei ārpus nolūka (PDAL 18. panta 3. punkts). Jāatzīmē, ka šie

[28] Kā iepriekš izklāstīts šī atzinuma 51.–52. punktā un 3.1.1.1. sadaļā.
[29] Skatīt arī šī atzinuma 3.1.6. un 3.1.10. sadaļu.

informācijas sniegšanas pienākumi *mutatis mutandis* attiecas arī uz ārpakalpojumu sniedzēju (PDAL 26. panta 7. punkts).

82. EDAK atzīst un atzinīgi vērtē Paziņojuma Nr. 2021-1[30] 3. sadaļas i) un ii) apakšpunktā minētos papildu aizsardzības pasākumus attiecībā uz informāciju, kas jāsniedz datu subjektiem, ja viņu datus pārsūta EEZ struktūra, ņemot vērā faktu, ka saskaņā ar PDAL 20. panta 1. punktu gadījumos, kad dati nav iegūti no datu subjekta, datu subjekti tiek informēti tikai pēc pieprasījuma, savukārt vispārējās tiesības tikt informētam tiek atzītas tikai saskaņā ar PDAL 20. panta 2. punktu, kad noteiktas apstrādes darbības pārsniedz PDAL izpildes dekrētā noteiktās robežas (15. panta 2. punkts).

83. Kopumā EDAK ir apmierināta, ka Korejas tiesību aktos noteiktais aizsardzības līmenis attiecībā uz pārredzamības principu būtībā ir līdzvērtīgs VDAR paredzētajam.

3.1.9. Īpašu kategoriju personas dati

84. Lai trešās valsts datu aizsardzības sistēma tiktu atzīta par tādu, kas nodrošina personas datu aizsardzības līmeni, kas būtībā ir līdzvērtīgs VDAR, būtu jāparedz īpaši aizsardzības pasākumi gadījumiem, kad ir iesaistītas īpašas personu kategorijas VDAR 9. un 10. panta izpratnē.

85. Saskaņā ar PDAL konkrēti nosacījumi attiecas uz tā dēvētās sensitīvās informācijas apstrādi, kas iekļauj personas datus, kuri atklāj ideoloģiju, pārliecību, uzņemšanu arodbiedrībā vai politiskajā partijā vai izstāšanos no tās, politiskos uzskatus, veselību, dzimumdzīvi un citus personas datus, kas varētu ievērojami apdraudēt jebkura datu subjekta privātumu, kā arī, atsaucoties uz PDAL izpildes dekrētu, DNS informāciju, kas iegūta, veicot ģenētisku pārbaudi, sodāmības vēstures ieraksta datus; personas datus, kas iegūti, veicot tādu datu specifisku tehnisku apstrādi, kas attiecas uz fiziskas personas fiziskajām, fizioloģiskajām vai uzvedības īpatnībām, šīs personas unikālai identificēšanai; personas datus, kas atklāj rases vai etnisko izcelsmi.

86. Līdzīgi VDAR Korejas datu aizsardzības likums aizliedz apstrādāt sensitīvu informāciju, ja vien netiek piemēroti īpaši izņēmumi, kas ietver: 1) datu subjekta informēšanu un konkrētas piekrišanas saņemšanu; 2) tiesību normas, kas atļauj apstrādi (PDAL 23. panta 2. punkts).

87. Pamatojoties uz to, EDAK principā piekrīt Eiropas Komisijas secinājumam par Korejas tiesību aktu būtisku līdzvērtību attiecībā uz īpašu kategoriju personas datu apstrādi. Tomēr EDAK vēlas atzīmēt, ka tai nav nodrošināta ne PDAL rokasgrāmata, ne arī PDAK precizējumi attiecībā uz terminu "dzimumdzīve", kas tiek interpretēts kā tāds, kurš aptver arī fiziskas personas seksuālo orientāciju vai vēlmes, kas ir iekļautas Paziņojumā Nr. 2021-1. Tāpēc EDAK aicina Eiropas Komisiju sniegt šo informāciju, lai tā varētu to neatkarīgi novērtēt. Turklāt EDAK aicina Eiropas Komisiju konkrēti citēt dokumentus, kuros var atrast informāciju, uz ko tā atsaucas par šo tēmu.

3.1.10. Piekļuves, labošanas, dzēšanas un iebildumu tiesības

88. Korejas tiesiskajā regulējumā datu subjekta tiesības ir atzītas PDAL 3. panta 5. punktā, saskaņā ar kuru personas datu pārzinis garantē datu subjekta tiesības, kas ir uzskaitītas PDAL 4. pantā un sīkāk noteiktas PDAL 35.–37., 39. pantā un 39. panta 2. punktā un attiecībā uz "personas kredītinformāciju" (proti, "kredītinformāciju, kas ir nepieciešamā informācija, lai noteiktu finanšu vai komerciālo darījumu pušu kredītspēju — skatīt Lēmuma projekta 3. apsvērumu") CIP 37., 38. un 38. panta 3. punktā.

89. EDAK atzīmē, ka piekļuves tiesības (arī labojumu un dzēšanas tiesības, ko var izmantot "*datu subjekts, kurš ir piekļuvis saviem personas datiem saskaņā ar PDAL 35. pantu*") var tikt ierobežotas vai liegtas, "*ja piekļuve ir aizliegta vai ierobežota ar likumiem*", "*ja piekļuve var radīt kaitējumu trešās personas dzīvībai vai ķermenim vai nepamatotu jebkuras citas personas īpašuma un citu interešu aizskārumu*",

[30] Lēmuma projekta I pielikums.

un papildus valsts iestādēm, kur piekļuves piešķiršana "*radītu nopietnas grūtības*", veicot noteiktas funkcijas, kā sīkāk noteikts PDAL 35. panta 4. punktā[31]. Līdzīgi nosacījumi ir ietverti arī PDAL 37. pantā attiecībā uz tiesībām apturēt personas datu apstrādi.

90. VDAR 23. pants atļauj Eiropas Savienības vai dalībvalsts tiesību aktos ierobežot individuālās tiesības, ja šāds ierobežojums respektē pamattiesību un brīvību būtību un ir nepieciešams un samērīgs pasākums demokrātiskā sabiedrībā, un paredz šādus ierobežojumus, lai cita starpā aizsargātu datu subjektu vai citu personu tiesības un brīvības, kā arī "*uzraudzības, pārbaudes vai regulatīvo funkciju, kas – pat, ja tikai epizodiski – ir saistīta ar oficiālu pilnvaru īstenošanu a) līdz e) un g) apakšpunktā minētajos gadījumos*".

91. Ņemot to vērā, EDAK atzinīgi vērtētu lēmuma projektā sniegtus vispārējus apliecinājumus par jebkāda tāda likuma vai statūta nepieciešamību, kas ierobežo datu subjektu tiesības, lai ievērotu Korejas Konstitūcijas prasības, ka pamattiesības var ierobežot tikai tad, ja tas ir nepieciešams valsts drošībai vai sabiedriskās labklājības uzturēšanai, un ka šis ierobežojums nedrīkst ietekmēt attiecīgās brīvības vai tiesību būtību (Korejas Konstitūcijas 37. panta 2. punkts).

92. Turklāt attiecībā uz izņēmumu, kas ir saistīts ar "*citu personu īpašuma vai citu interešu nepamatotu aizskārumu*", EDAK atzīst, ka tas "*nozīmē, ka, no vienas puses, ir jāpanāk līdzsvars starp fiziskas personas (no vienas puses) un citu personu (no otras puses) konstitucionāli aizsargātajām tiesībām un brīvībām*"[32], tomēr tā aicinātu Eiropas Komisiju pilnībā uzraudzīt šī izņēmuma un attiecīgās judikatūras piemērošanu, lai panāktu, ka līdzvērtīgs datu subjekta tiesību aizsardzības līmenis tiek nodrošināts arī praksē Korejas tiesiskajā regulējumā.

93. Tāpat EDAK atzinīgi vērtētu rūpīgu uzraudzību attiecībā uz izņēmuma piemērošanu valsts iestādēm, jo īpaši gadījumos, kad piekļuves piešķiršana būtu uzskatāma par "*nopietnu apgrūtinājumu*", veicot savus pienākumus, ņemot vērā, ka šī frāze šķiet plašāka par citos PDAL nosacījumos, piemēram, 18. panta 2. punkta 5. apakšpunktā, izmantoto [33], un ir jāinterpretē šauri, lai izvairītos no datu subjekta tiesību nepamatotas ierobežošanas.

94. Turklāt EDAK ir nobažījusies par to, vai izņēmumi, saskaņā ar kuriem nosacījumi par pārredzamību pēc pieprasījuma (PDAL 20. pants) un fiziskas personas tiesības (PDAL 35.–37. pants), kā arī tiem līdzīgie, kas attiecas uz prasībām informācijas un sakaru pakalpojumu sniedzējiem (PDAL 39. panta 2. punkts, 39. panta 6.–8. punkts) un CIP ietvertajiem pakalpojumiem (skatīt CIP 40. panta 3. punktā paredzētos izņēmumus), neattiecas uz pseidonimizētu informāciju, ja tā tiek apstrādāta statistikas, zinātniskās izpētes vai arhivēšanas nolūkos sabiedrības interesēs (PDAL 28. panta 7. punkts) atbilstoši Eiropas tiesiskajā regulējumā paredzētajiem aizsardzības pasākumiem.

95. Šķiet, šie noteikumi ievieš vispārēju atkāpi šāda veida apstrādei, kamēr VDAR paredz, ka gadījumos, kad personas dati (iekļaujot pseidonimizētus personas datus) tiek apstrādāti zinātniskas vai vēsturiskas izpētes vai statistikas nolūkos, Eiropas Savienības vai dalībvalsts tiesību akti var paredzēt atkāpes no datu subjekta tiesībām, bet tikai, "*ciktāl šādas tiesības var neļaut vai būtiski traucēt sasniegt konkrētos nolūkus, un šādas atkāpes ir vajadzīgas minēto nolūku sasniegšanai*", pseidonimizācija ir tikai viens no tehniskajiem un organizatoriskajiem pasākumiem, kas jāveic, lai nodrošinātu datu apjoma samazināšanas principa ievērošanu (VDAR 89. panta 1. punkts).

---

[31] Tie paši nosacījumi un izņēmumi attiecībā uz piekļuves un labojumu tiesībām, ko paredz PDAL, attiecas arī uz piekļuves un labojumu tiesībām, ko CIP ir paredzējis personas kredītinformācijai (lēmuma projekta 135. zemsvītras piezīme).

[32] Lēmuma projekta 76. apsvērums.

[33] Saistībā ar izņēmumiem, kas attiecas uz personas datu izmantošanas un sniegšanas ierobežošanu pretēji nolūkam, PDAL 18. panta 2. punkta 5. apakšpunkts attiecas uz situācijām, kad valsts iestādēm "*nav iespējams*" veikt savus pienākumus.

96. Eiropas Komisija uzskata, ka PDAL 28. panta 7. punktā paredzētā atkāpe ir pamatota, ņemot vērā arī PDAL 28. panta 5. punktu, ar kuru personas datu pārzinim ir skaidri aizliegts apstrādāt pseidonimizēto informāciju noteiktas fiziskas personas identificēšanas nolūkā, un atsaucas uz VDAR 11. panta 2. punkta pieeju apstrādei (saistībā ar VDAR preambulas 57. apsvērumu), kurai nav nepieciešama identifikācija[34].

97. Patiešām saskaņā ar VDAR 11. pantu datu pārzinim nav pienākuma "*saglabāt, iegūt vai apstrādāt papildu informāciju, lai identificētu datu subjektu*" tikai ar nolūk rīkoties atbilstoši VDAR, ja tas paredzētajos nolūkos var apstrādāt personas datus, kuriem nav vai vairs nav nepieciešama datu subjekta identifikācija; šādos gadījumos, kad datu pārzinis spēj pierādīt, ka nevar identificēt datu subjektu, datu subjekta tiesības netiek piemērotas. Kā atzinusi Eiropas Komisija[35], VDAR tādējādi šādos gadījumos datu pārzinim pieprasa "praktisku" neiespējamību un saskaņā ar datu apjoma samazināšanas principu atzīst, ka VDAR "dēļ" papildu dati nav jāapstrādā.

98. Tomēr EDAK uzskata, ka šī situācija atšķiras no situācijas, kurā datu pārzinis praktiski spēj identificēt datu subjektu, bet tas nav atļauts ar tādu tiesību normu kā PDAL 28. panta 5. punkts. Šajā saistībā EDAK atzinīgi vērtē PDAK sniegtos paskaidrojumus Paziņojumā Nr. 2021-1[36], kas apstiprina, ka PDAL 3. sadaļa (iekļaujot 28. panta 7. punktu) un CIP 40. panta 3. punkta izņēmums ir piemērojams tikai tad, ja tiek apstrādāta pseidonimizēta informācija zinātniskiem pētījumiem, statistikai vai arhivēšanai sabiedrības interesēs. Tomēr — un papildus jau minētajām bažām par paziņojuma Nr. 2021-1[37] efektīvo saistošo raksturu EDAK joprojām domā, vai atkāpes, kas ir paredzētas PDAL 28. panta 7. punktā un CIP 40. panta 3. punktā, varētu uzskatīt par nepieciešamām un proporcionālām demokrātiskā sabiedrībā, ciktāl tās ierobežo datu subjekta tiesības visos gadījumos, kad pseidonimizēta informācija tiek apstrādāta šādiem nolūkiem — t. i., pat tad, ja personas datu pārzinis praktiski spēj identificēt datu subjektu un tiesības un tas, visticamāk, padarīs neiespējamu vai nopietni traucēs konkrēto nolūku sasniegšanu.

99. Proti, EDAK pauž bažas par to, ka šīs atkāpes nebūtu attaisnojamas un tās būtu rūpīgi jāpārbauda jo īpaši tad, ja tās piemēro personas datu pārzinis, kurš pseidonimizē datus "*statistikas, zinātniskās izpētes un arhivēšanas nolūkos sabiedrības interesēs, utt.*" saskaņā ar PDAL 28. panta 2. punktu "*bez datu subjektu piekrišanas*" (un nesniedzot informāciju, kas paredzēta PDAL 20. pantā)[38], ciktāl šis datu pārzinis saglabā informāciju, kas ļauj veikt atkārtotu identificēšanu. Saskaņā ar VDAR fiziskām personām būtu jāspēj izmantot savas tiesības attiecībā uz jebkuru informāciju, kas spēj tās identificēt vai izcelt, pat ja informācija tiek uzskatīta par "pseidonimizētu", ja vien netiek piemērots jau minētais VDAR 11. pants. Šajā saistībā EDAK atzīmē, ka tikai tad, ja šie dati tiek sniegti trešai personai tādiem pašiem statistikas, zinātniskās izpētes un arhivēšanas nolūkiem, nebūtu jāiekļauj informācija, ko var izmantot noteiktas fiziskas personas identificēšanai, un tāpēc tikai personas datu pārzinis, kuram tiek nodrošināti pseidonimizēti dati saskaņā ar PDAL 28-2. panta 2. punktu, iespējams, "praktiski" nevarētu identificēt datu subjektu bez papildu informācijas.

---

[34] Jāatzīmē, ka tas pats pamatojums nebūtu piemērojams izņēmumam, kas ir paredzēts CIP 40. panta 3. punktā attiecībā uz pseidonimizētas kredītinformācijas apstrādi, jo 40. panta 2. punkta 6. apakšpunkts paredz, ka: "*Kredītinformācijas uzņēmums utt. nedrīkst apstrādāt pseidonimizētu informāciju tādā veidā, ka konkrēta fiziska persona varētu tikt identificēta peļņas gūšanas vai negodīgos nolūkos*", un tādējādi varētu atļaut atkārtotu identificēšanu godīgā nolūkā, piemēram, lai izpildītu datu subjekta pieprasījumu.

[35] Skatīt lēmuma projekta 82. apsvērumu.

[36] Lēmuma projekta I pielikuma 4. sadaļa.

[37] Skatiet iepriekš 3.1.1.1. sadaļu.

[38] Skatīt PDAL 28. panta 7. punktu, kā paskaidrots paziņojumā Nr. 2021-1, saskaņā ar kuru daži PDAL ietvertie aizsardzības pasākumi, piemēram, "*20., 21., 27. pants, 34. panta 1. punkts, 35.–37. pants, 39. panta 3. punkts, 39. panta 4. punkts, 39. panta 6.–8. punkts*", neattiecas uz pseidonimizētu informāciju, kas tiek apstrādāta statistikas apkopošanas, zinātnisko pētījumu, publisko ierakstu saglabāšanas u.c. nolūkā.

100. Īsumā, ņemot vērā, kā to ir atzinusi Eiropas Komisija, "*tā vietā, lai paļautos uz pseidonimizāciju kā iespējamu aizsardzības līdzekli, PDAL to izvirza kā priekšnosacījumu, lai veiktu noteiktas apstrādes darbības statistikas, zinātniskas izpētes un arhivēšanas nolūkos sabiedrības interesēs (piemēram, lai varētu apstrādāt datus bez piekrišanas vai kombinēt dažādas datu kopas)*"[39], bet šādos gadījumos tas paredz būtiskus datu subjektu tiesību ierobežojumus, EDAK aicina Eiropas Komisiju turpmāk izvērtēt atkāpes, kas ietvertas PDAL 28. panta 7. punktā un CIP 40. panta 3. punktā, un rūpīgi uzraudzīt to piemērošanu un attiecīgo judikatūru[40], lai nodrošinātu, ka datu subjektu tiesības netiks nepamatoti ierobežotas, kad personas dati, kas nosūtīti saskaņā ar lēmumu par aizsardzības līmeņa pietiekamību, tiek apstrādāti šiem nolūkiem, ņemot vērā, ka daudzos gadījumos šīs tiesības palīdz arī datu pārzinim nodrošināt apstrādāto datu kvalitāti.

3.1.11. Tālākas nosūtīšanas ierobežojumi

101. VDAR pietiekamības atsaucēs tiek paskaidrots, ka to fizisko personu aizsardzības līmeni, kuru personas dati tiek nosūtīti saskaņā ar lēmumu par aizsardzības līmeņa pietiekamību, nedrīkst apdraudēt tālāka nosūtīšana, un tāpēc jebkura tālāka nosūtīšana "*būtu jāatļauj tikai tad, ja turpmākajam saņēmējam (t. I., pārsūtīto datu saņēmējam) arī piemēro noteikumus (tostarp līguma noteikumus), kas nodrošina pietiekamu aizsardzības līmeni, un tas ievēro attiecīgus norādījumus, veicot datu apstrādi datu pārziņa uzdevumā*".

102. Attiecībā uz tālāku nosūtīšanu ārpakalpojumu sniedzējiem (piemēram, "apstrādātājiem"), kas reģistrēti citās trešajās valstīs, EDAK ņem vērā, ka Korejas tiesiskajā regulējumā nav īpašu noteikumu, kas aptvertu šos gadījumus, un ka, kā uzskata Eiropas Komisija[41], Korejas personas datu pārzinim ir jānodrošina atbilstība PDAL nosacījumiem par ārpakalpojumiem (PDAL 26. pants), izmantojot juridiski saistošu instrumentu, un tas būs atbildīgs par ārpakalpojumam nodotajiem personas datiem (PDAL 26. pants).

103. Attiecībā uz tālāku nosūtīšanu trešajām pusēm (piemēram, citiem personas datu pārziņiem) saskaņā ar PDAL 17. panta 3. punktu Korejas personas datu pārzinim ir jāinformē datu subjekti par nosūtīšanu uz ārzemēm un jāsaņem viņu piekrišana, un viņš "*nedrīkst slēgt līgumu par personas datu pārrobežu nosūtīšanu, pārkāpjot PDAL*". EDAK atzīmē, ka šis pēdējais nosacījums atbilstoši Eiropas Komisijas[42] uzskatiem nodrošinās, ka neviens līgums par pārrobežu nosūtīšanu nevarētu ietvert pienākumus, kas ir pretrunā ar PDAL izvirzītajām prasībām personas datu pārzinim, un tāpēc to varētu uzskatīt par drošības līdzekli, tomēr tas neuzliek nekādu pienākumu ieviest aizsardzības pasākumus, lai garantētu, ka saņēmējs nodrošinās tādu pašu aizsardzības līmeni, kādu nodrošina PDAL. Tāpēc EDAK atzīst, ka datu subjekta informēta piekrišana parasti tiks izmantota par pamatu datu nosūtīšanai no personas datu pārziņa Korejā saņēmējam trešajā valstī.

104. Šajā sakarā ir apsveicami papildu skaidrojumi, ko PDAK sniedza Paziņojumā Nr. 2021-1 par pienākumu informēt fiziskas personas par trešo valsti, kurai tiks sniegti personas dati[43], jo tas, kā uzsvēra Eiropas Komisija[44], palīdzētu datu subjektiem EEZ pieņemt pilnībā apzinātu lēmumu par to, vai piekrist ārvalstu nosacījumam.

105. Tomēr, kā norādīts arī Atzinumā 28/2018 attiecībā uz Eiropas Komisijas projektu īstenošanas lēmumam par pietiekamu personas datu aizsardzību Japānā, ir jāuzsver, ka saskaņā ar VDAR datu

[39] Lēmuma projekta 42. apsvērums.
[40] Skatīt, piemēram, *Open Net* konstitucionālās problēmas (informācija https://opennet.or.kr/19909 pieejama tikai korejiešu valodā).
[41] Lēmuma projekta 87. apsvērums.
[42] Lēmuma projekta 88. apsvērums.
[43] Turpat.
[44] Turpat.

subjekti ir skaidri jāinformē par šādu nosūtījumu iespējamiem riskiem, kas ir radušies tādēļ, ka trešajā valstī nav atbilstošas aizsardzības un nav piemērotu aizsardzības pasākumu pirms piekrišanas sniegšanas. Šādā paziņojumā ir jāiekļauj informācija par to, ka, iespējams, trešā valstī var nebūt uzraudzības iestādes un/vai datu apstrādes principu, un/vai datu subjektu tiesību[45]. Pēc EDAK ieskatiem šīs informācijas sniegšana ir būtiska, lai datu subjektam ļautu sniegt informētu piekrišanu, pilnībā apzinoties šos konkrētos nosūtīšanas faktus[46]. Tāpēc EDAK pauž bažas par Eiropas Komisijas konstatējumiem lēmuma par aizsardzības līmeņa pietiekamību projektā attiecībā uz šāda veida nosūtīšanas gadījumiem. Datu subjekti parasti nav informēti par datu aizsardzības sistēmu trešās valstīs. Tādējādi nevar secināt, ka datu subjekts varētu novērtēt nosūtīšanas risku, tikai uzzinot konkrēto galamērķa valsti. Pirms datu subjekta piekrišanas drīzāk ir jābūt skaidrai informācijai par konkrētiem riskiem, ko rada šāda personas datu nosūtīšana uz valsti ārpus Korejas Republikas.

106. Tādējādi EDAK aicina Eiropas Komisiju nodrošināt, ka datu subjektam sniedzamajā informācijā "*par apstākļiem, kas saistīti ar nosūtīšanu*", ir iekļauta arī informācija par iespējamiem nosūtīšanas riskiem, kas rodas, ja trešajā valstī nav pietiekamas aizsardzības un piemērotu aizsardzības pasākumu. EDAK tas ir svarīgi, lai novērtētu, vai piekrišanas prasības būtībā ir līdzvērtīgas VDAR.

107. Turklāt ņemot vērā, ka piekrišana ir jāsniedz brīvi, informēti, konkrēti un nepārprotami, EDAK lēmumā par aizsardzības līmeņa pietiekamību atzinīgi vērtētu atkārtotus apliecinājumus, ka personas dati netiks nosūtīti no Korejas personas datu pārziņiem uz trešo valsti situācijā, kurā saskaņā ar VDAR nevarētu sniegt derīgu piekrišanu, piemēram, varas nestabilitātes dēļ.

108. Attiecībā uz gadījumiem, kad personas datu pārzinis var sniegt personas informāciju trešai pusei ārvalstīs bez datu subjekta piekrišanas, t. i., 1) ja personas dati tiek sniegti apjomā, kas ir pamatoti saistīts ar sākotnējo vākšanas nolūku saskaņā ar PDAL 17. panta 4. punktu; 2) ja personas datus var sniegt trešai pusei izņēmuma gadījumos, kas minēti PDAL 18. panta 2. punktā — EDAK ņem vērā PDAK sniegtos precizējumus Paziņojuma Nr. 2021-1 2. sadaļā (un atzinīgi vērtē paredzēto pienākumu, kas tiek piemērots datu pārzinim Korejā un ārvalsts saņēmējam, izmantojot juridiski saistošu instrumentu (piemēram, līgumu), nodrošināt PDAL līdzvērtīgu aizsardzības līmeni, tostarp attiecībā uz datu subjekta tiesībām).

3.1.12. Tiešā tirgvedība

109. Saskaņā ar VDAR 21. panta 2. punktu un 21. panta 3. punktu, kā arī VDAR pietiekamības atsaucēm datu subjektam jebkurā brīdī būtu jāspēj bez maksas iebilst pret savu datu apstrādi profilēšanas un tiešās tirgvedības nolūkos.

110. Attiecībā uz PDAL 37. pantā paredzētajām tiesībām uz apturēšanu EDAK atzīst, ka Eiropas Komisija uzskata — šīs tiesības attiecas arī uz gadījumiem, kad dati tiek izmantoti tiešās tirgvedības nolūkos[47]. Tomēr EDAK atzinīgi vērtētu papildu informāciju un paskaidrojumus lēmuma projektā saistībā ar šo novērtējumu un jo īpaši par apturēšanas tiesību praktisko piemērošanu tiešā mārketinga kontekstā (piemēram, atsauces uz attiecīgo judikatūru). Šajā saistībā EDAK arī uzsver, ka CIP ir skaidri noteiktas tiesības lūgt kredītinformācijas sniedzēju/lietotāju pārtraukt ar viņu saziņu, kuras mērķis ir ieviest vai pieprasīt preču vai pakalpojumu iegādi CIP (37. panta 2. punkts).

[45] EDAK Pamatnostādnes 2/2018 par 49. panta izņēmumiem saskaņā ar Regulu 2016/679, 2018. gada 25. maijs, 8. lpp.
[46] EDAK Pamatnostādnes 2/2018 par 49. panta izņēmumiem saskaņā ar Regulu 2016/679, 2018. gada 25. maijs, 7. lpp.
[47] Lēmuma projekta 79. apsvērums.

111. Turklāt, kā atzinusi Eiropas Komisija[48], Korejas tiesiskajā regulējumā šādai apstrādei parasti ir nepieciešama datu subjekta konkrēta (papildu) piekrišana (skatīt PDAL 15. panta 1. punkta 1. apakšpunktu, 17. panta 2. punkta 1. apakšpunktu.

112. Tā kā nevar izslēgt, ka no EEZ nosūtītie personas dati var tikt apstrādāti Korejā šādiem nolūkiem, EDAK arī vēlētos saņemt paskaidrojumus lēmumā par aizsardzības līmeņa pietiekamību par to, vai datu subjektam ir tiesības atsaukt piekrišanu[49] un par tiesībām uz to, lai viņa/viņas personas dati tiktu izdzēsti un vairs netiktu apstrādāti, ja apstrāde ir balstīta uz piekrišanu (piemēram, ja apstrāde tiek veikta tirgvedības vajadzībām) un datu subjekts to ir atsaucis.

3.1.13. Automatizēta lēmumu pieņemšana un profilēšana

113. Kā Eiropas Komisija ir atzinusi savā lēmuma projektā[50], PDAL un tās izpildes dekrēts neietver vispārīgus nosacījumus, kas risina jautājumu par lēmumiem, kuri ietekmē datu subjektu un ir balstīti tikai uz personas datu automatizētu apstrādi. Tomēr Korejas tiesiskā sistēma paredz šādas tiesības CIP, kas ietver noteikumus par automatizētiem lēmumiem (36. panta 2. punkts), pat ja šķiet, ka to piemērošana neietilpst PDAK uzraudzības jomā (un kā tāda ir ārpus šī lēmuma projekta piemērošanas — skatīt iepriekš 2.3.2. sadaļu par lēmuma projekta piemērošanas jomu).

114. Kā uzskatīja 29. panta darba grupa[51] savā atzinumā 1/2016 privātuma vairoga lietā un EDAK savā iepriekšējā atzinumā attiecībā uz lēmumu par aizsardzības līmeņa pietiekamību saistībā ar Japānu[52], automatizētās lēmumu pieņemšanas, profilēšanas un mākslīgā intelekta augošā nozīme rosinātu šajā ziņā izmantot vairāk aizsargājošu pieeju. Pretēji Eiropas Komisijas argumentiem[53], saskaņā ar kuriem PDAL konkrēto noteikumu trūkums attiecībā uz automatizētu lēmumu pieņemšanu, visticamāk, neietekmēs aizsardzības līmeni Eiropas Savienībā vāktajiem personas datiem (jo jebkuru lēmumu, kas balstīts uz automatizētu apstrādi, parasti pieņem datu pārzinis Eiropas Savienībā, kuram ir tieša saistība ar attiecīgo datu subjektu), EDAK uzskata, ka nevar izslēgt, ka datu nosūtīšanas gadījumā personas datu pārzinis Korejā varētu izmantot automatizētu lēmumu pieņemšanu saskaņā ar lēmumu par aizsardzības līmeņa pietiekamību (piemēram, saistībā ar nodarbinātību, lai novērtētu darba rezultātus, uzticamību, uzvedību).

115. Jaunu tehnoloģiju izstrāde ļauj uzņēmumiem vieglāk ieviest vai apsvērt automatizētu lēmumu pieņemšanas sistēmu ieviešanu, kas var izraisīt fizisku personu stāvokļa pasliktināšanos. Ja lēmumi, ko pieņem tikai šīs automatizētās sistēmas, ietekmē fizisku personu tiesisko stāvokli vai būtiski ietekmē fiziskas personas (piemēram, iekļaujot melnajā sarakstā un tādējādi atņemot fizisko personu tiesības), ir būtiski nodrošināt pietiekamus aizsardzības pasākumus, tostarp tiesības saņemt informāciju par lēmuma pamatojuma konkrētajiem iemesliem un iesaistīto loģiku, lai labotu neprecīzu vai nepilnīgu informāciju un apstrīdētu lēmumu, ja tas ir pieņemts, pamatojoties uz nepareizu faktu pamata[54].

---

[48] Turpat.

[49] Skatīt iepriekš arī šī dokumenta 67. punktu. Lai gan iespēja atsaukt piekrišanu ir skaidri paredzēta CIP 37. panta 1. punktā, šīs tiesības PDAL ir minētas tikai divreiz konkrētos apstākļos 27. panta 1. punkta 2. apakšpunktā un 39. panta 7. punktā.

[50] Skatīt lēmuma projekta 81. apsvērumu.

[51] Šī darba grupa tika izveidota saskaņā ar Direktīvas 95/46/EK 29. pantu. Tā bija neatkarīga Eiropas padomdevēja institūcija datu aizsardzības un privātuma jautājumos. Tās uzdevumi ir aprakstīti Direktīvas 95/46/EK 30. pantā un Direktīvas 2002/58/EK 15. pantā. Tagad WP29 ir kļuvusi par EDAK.

[52] Atzinums 28/2018 par Eiropas Komisijas Īstenošanas lēmuma projektu par personas datu pietiekamu aizsardzību Japānā pieņemts 2018. gada 5. decembrī.

[53] Lēmuma projekta 81. apsvērums.

[54] WP 254., 7. lpp.

116. Šajā kontekstā EDAK pauž bažas par to, ka PDAL nav tiesisku normu par automatizētu lēmumu pieņemšanu, un tāpēc aicina Eiropas Komisiju pievērsties šai problēmai un turpināt uzraudzīt Korejas tiesiskā regulējuma attīstību šajā sakarā.

3.1.14. Pārskatatbildība

117. Korejas tiesiskajā regulējumā ir vairāki noteikumi, kuru mērķis ir nodrošināt, lai personas datu pārzinis ieviestu atbilstošus tehniskus un organizatoriskus pasākumus savu datu aizsardzības jomas saistību efektīvas izpildes nolūkā un spētu parādīt šādu atbilstību, tostarp kompetentajai uzraudzības iestādei. Jo īpaši EDAK atzinīgi vērtē to, ka pastāv noteikumi, kas paredz iekšējās pārvaldības plāna pieņemšanu (PDAL 29. pants), pienākumu veikt tā saucamo ietekmes uz privātumu novērtējumu ("**IPN**") gadījumos, kad apstrāde rada lielāku iespējamo privātuma pārkāpuma risku (PDAL 33. panta 1. punkts un PDAL izpildes dekrēta 35. pants), noteikumi par personāla apmācību un uzraudzību (PDAL 28. pants), kā arī pienākums iecelt privātuma aizsardzības inspektoru (PDAL 31. pants saistībā ar PDAL Izpildes dekrēta 32. pantu).

118. EDAK piekrīt Eiropas Komisijas viedoklim par būtībā līdzvērtīgu aizsardzību, ko tie nodrošina — pat gadījumos, kad noteikumi, šķiet, salīdzinoši atšķiras no VDAR paredzētajiem, piemēram, nav nosacījuma, kas paredz, ka privātuma aizsardzības speciālistam ir jābūt neatkarīgam, tomēr ir skaidri noteikts, ka viņam/viņai ir jāatskaitās personas datu pārziņa vadībai (PDAL 31. panta 4. punkts) un viņš/viņa nedrīkst nonākt nepamatoti neizdevīgā stāvoklī šo funkciju izpildes rezultātā (PDAL 31. panta 5. punkts) — un ierosina Eiropas Komisijai, pārskatot lēmumu par aizsardzības līmeņa pietiekamību, uzraudzīt šo nosacījumu faktisko piemērošanu, lai novērtētu to efektīvu īstenošanu.

3.2. Procesuālie un izpildes mehānismi

119. Pamatojoties uz VDAR pietiekamības atsaucēs izvirzītajiem kritērijiem, EDAK ir analizējusi turpmākos Korejas datu aizsardzības aspektus, kas ir ietverti lēmuma projektā: neatkarīgas uzraudzības iestādes esamība un efektīva darbība; tādas sistēmas esamība, kas nodrošina labu atbilstības līmeni, un sistēma, kas nodrošina piekļuvi piemērotiem tiesiskās aizsardzības mehānismiem, sniedzot EEZ pilsoņiem iespējas izmantot savas tiesības un vērsties pēc palīdzības, nesaskaroties ar apgrūtinošiem šķēršļiem tiesiskās aizsardzības procesā administratīvā kārtā un tiesā.

120. Saskaņā ar VDAR VI nodaļu un VDAR pietiekamības atsauču 3. nodaļu vajadzētu būt vienai vai vairākām neatkarīgām uzraudzības iestādēm, kurām ir pienākums uzraudzīt, nodrošināt un panākt atbilstību trešās valsts datu aizsardzības un privātuma noteikumiem, lai garantētu EEZ līdzvērtīgu aizsardzības līmeni.

121. Šajā kontekstā trešās valsts uzraudzības iestādei jādarbojas pilnīgi neatkarīgi un objektīvi, pildot savus pienākumus un īstenojot savas pilnvaras, un, to darot, tai nav jāprasa un jāpieņem norādījumi. Turklāt uzraudzības iestādei vajadzētu būt visām nepieciešamajām un pieejamajām pilnvarām un misijām, lai nodrošinātu datu aizsardzības tiesību ievērošanu, kā arī veicinātu informētību. Jāņem vērā arī uzraudzības iestādes personāls un budžets. Uzraudzības iestāde pēc savas iniciatīvas var arī veikt izmeklēšanu.

3.2.1. Kompetenta neatkarīga uzraudzības iestāde

122. Korejas Republikā neatkarīgā iestāde, kas atbild par PDAL uzraudzību un izpildi, ir PDAK. PDAK sastāvā ir viens priekšsēdētājs, priekšsēdētāja vietnieks un septiņi komisāri. Priekšsēdētāju un priekšsēdētāja vietnieku ieceļ prezidents pēc ministru prezidenta ieteikuma. Divus no komisāriem ieceļ pēc priekšsēdētāja ieteikuma, divus — pēc tās politiskās partijas pārstāvju ieteikuma, kurai pieder prezidents, bet trīs pārējos komisārus pēc citu politisko partiju pārstāvju ieteikuma (PDAL 7. panta 2. punkta 2. apakšpunkts). PDAK palīdz sekretariāts (7. panta 13. punkts), un tas var izveidot

apakškomisijas (trīs komisāru sastāvā), lai izskatītu nelielus pārkāpumus un atkārtotus jautājumus (PDAL 7. panta 12. punkts).

123. Šajā ziņā EDAK atzīst, ka, neraugoties uz neseno reorganizāciju, kas būtiski mainīja tās statusu un pilnvaras, PDAK ir daudz darījusi vajadzīgās infrastruktūras izveidē, lai pielāgotos PDAL un tā jaunāko grozījumu īstenošanai. Te var minēt PDAK noteikumu izveidi, vadlīniju izstrādi, lai sniegtu norādījumus par PDAL interpretāciju, palīdzības līnijas izveidi, lai konsultētu uzņēmējdarbības veicējus un personas par datu aizsardzības nosacījumiem, kā arī sniegtu starpniecības pakalpojumu sūdzību izskatīšanā. Jo īpaši PDAK uzdevumos ietilpst konsultācijas par tiesību un normatīvajiem aktiem, kas saistīti ar datu aizsardzību, datu aizsardzības politikas un vadlīniju izstrāde, individuālo tiesību pārkāpumu izmeklēšana, sūdzību izskatīšana un starpniecība strīdu risināšanā, PDAL ievērošanas nodrošināšana, izglītības un atbalsta nodrošināšana datu aizsardzības jomā, kā arī apmaiņa un sadarbība ar trešo valstu datu aizsardzības iestādēm[55].

124. PDAK iecelšana un sastāvs ir noteikts PDAL 7. panta 2. punktā. Lai gan PDAK ir ministru prezidenta jurisdikcijā (un priekšsēdētāju un priekšsēdētāja vietnieku ieceļ prezidents pēc ministru prezidenta ieteikuma), tiesiskais regulējums paredz, ka komisāri savus pienākumus pilda neatkarīgi, saskaņā ar likumu un viņu sirdsapziņu. EDAK atzīst institucionālos un procesuālos aizsardzības pasākumus, kas ir ietverti PDAL un jo īpaši 7. panta 4.–7. punktā. Tomēr EDAK vēlētos, lai Eiropas Komisija uzraudzītu notikumus, kas varētu ietekmēt Dienvidkorejas uzraudzības iestādes pārstāvju neatkarību.

125. Turklāt lēmuma projektā vēl nav iekļauta PDAK budžeta analīze, tostarp finansējuma avoti un budžeta pārredzamība. EDAK uzskata, ka šis elements, kas ir minēts gan VDAR 56. panta 1. punktā, gan procesuālajos un izpildes datu aizsardzības principos un mehānismos, kuri jāizskata saskaņā ar VDAR pietiekamības atsaucēm, izvērtējot kādas valsts vai starptautiskas organizācijas sistēmu, ir pilnībā jāņem vērā, jo tas ir tādu ekonomikas un cilvēkresursu rādītājs, kas ir pieejami uzraudzības iestādei, lai neatkarīgi pildītu savas datu aizsardzības likumā noteiktās saistības un uzdevumus, un tādēļ ieteiktu Eiropas Komisijai to sīkāk ņemt vērā lēmuma projektā.

3.2.2. Datu aizsardzības sistēmai ir jānodrošina labs atbilstības līmenis

126. Izpildes jomā EDAK atzīst PDAK izpildes pilnvaru un sankciju klāstu, kas ir nodrošināts ar PDAL un CIP, un ņem vērā Paziņojumā Nr. 2021-1 ietvertos skaidrojumus, saskaņā ar kuriem PDAL 64. panta 1. punktā un CIP 45. panta 4. punktā norādītie nosacījumi[56] būs piemērojami ikreiz, kad tiks pārkāpts kāds likumā iekļautais princips, tiesības un pienākumi, kas paredzēti personas datu aizsardzībai. Tomēr tā ieteiktu Eiropas Komisijai cieši uzraudzīt PDAK pilnvaru piemērošanu praksē, lai pārkāpējam liktu veiktu pasākumus, ko tā uzskata par piemērotiem saskaņā ar CIP 64. panta 1. punktā vai 45. panta 4. punktā uzskaitīto.

127. Turklāt attiecībā uz PDAL 64. panta 1. punktā paredzētajiem korekcijas pasākumiem — korekcijas pasākuma neievērošanas gadījumā PDAK ir pilnvarota piemērot naudas sodu, kas nepārsniedz 50 miljonus Korejas vonu (PDAL 75. panta 2. punkta 13. apakšpunkts). Šī summa ir līdzvērtīga 36 564 EUR. EDAK uzskata un pauž bažas, ka šādam ierobežotam finansiālo sankciju klāstam varētu nebūt īpaši spēcīga preventīva ietekme uz pārkāpējiem, kā paredzēts likumā, lai nodrošinātu datu aizsardzības noteikumu izpildi, jo nešķiet, ka tas būtu pietiekami, lai no šādas rīcības atturētu, it īpaši lielas organizācijas vai uzņēmumus ar ievērojamiem finanšu resursiem.

128. Attiecībā uz iespēju, ka PDAK var pieprasīt, lai centrālās administratīvās aģentūras vadītājs veic personas datu pārziņa izpēti vai kopīgi iesaistās PDAL pārkāpumu izmeklēšanā un pat piemēro

[55] PDAK uzdevumi un pilnvaras galvenokārt ir paredzētas PDAL 7. panta 8. un 9. punktā, kā arī PDAL 61.–66. pantā.

[56] Piemēram, "*tiek uzskatīts, ka likuma pārkāpums, iespējams, aizskar fizisku personu tiesības un brīvību attiecībā uz personas datiem un, ja netiek veiktas nekādas darbības, var radīt grūti novēršamu kaitējumu".*

korekcijas pasākumus attiecībā uz tās jurisdikcijā esošajiem personas datu pārziņiem (PDAL 63. panta 4.–5. punkts), EDAK atzīmē, ka, lai gan lēmuma projekta 122. apsvērumā ir sniegta zināma informācija, kopumā šo pārējo aģentūru būtība un to tiesiskās attiecības ar PDAK joprojām ir diezgan neskaidras. Turklāt PDAL 68. panta 1. punkts attiecas uz daudzām struktūrām, kurām būtu iespējams deleģēt PDAK pilnvaras. Pat ja šķiet, ka šis nosacījums ir piemērots tikai attiecībā uz Korejas Interneta un drošības aģentūru[57], EDAK labprāt saņemtu skaidrojumus par iespējamo mijiedarbību starp šīm struktūrām un šī nosacījuma piemērošanas rūpīgu uzraudzību nākotnē, lai nodrošinātu to struktūru neatkarību, kuru uzdevumos ietilpst datu aizsardzības noteikumu piemērošana.

129. Attiecībā uz sankcijām Korejas sistēma, šķiet, kombinē dažādu veidu sankcijas no korekcijas pasākumiem un administratīviem naudas sodiem līdz krimināl sankcijām, kurām var būt spēcīga preventīva ietekme, un Korejas iestādes ir sniegušas vairākus piemērus par PDAK nesen piemērotajiem sodiem, tostarp viens no tiem bija 6,7 miljardu Korejas vonu apmērā, kas 2020. gada decembrī tika uzlikts uzņēmumam par dažādu PDAL noteikumu pārkāpšanu, un vēl viens naudas sods 103,3 miljonu Korejas vonu apmērā 2021. gada 28. aprīlī, kas tika piemērots uzņēmumam AI Technology par apstrādes likumības noteikumu pārkāpšanu, jo īpaši par piekrišanu un pseidonimizētas informācijas apstrādi.

130. Lai gan iepriekš minētajām summām var būt preventīvs efekts, EDAK labprāt saņemtu papildinformāciju par metodi, ko PDAK izmantoja, lai aprēķinātu administratīvo soda naudu apmēru, piemēram, attiecībā uz naudas sodiem, kas tika piemēroti par norādītā korekcijas pasākuma neievērošanu saskaņā ar PDAL 64. panta 1. punktu (skatīt PDAL 75. panta 2. punkta 13. apakšpunktu). Tas jo īpaši attiecas uz krimināl sankcijām un (Korejas) Krimināllikuma piemērošanu.

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

131. Attiecībā uz tiesisko aizsardzību Korejas sistēma, šķiet, piedāvā dažādus veidus, kā nodrošināt adekvātu aizsardzību un jo īpaši fizisko personu tiesību īstenošanu ar efektīvu administratīvo un tiesisko aizsardzību, tostarp zaudējumu atlīdzināšanu.

132. Papildus administratīvajiem un tiesu līdzekļiem Korejas sistēma piedāvā arī alternatīvus mehānismus, pie kuriem privātpersonas var vērsties, lai saņemtu tiesisko aizsardzību, kā paskaidrots lēmuma projekta 132. un 133. apsvērumā, kas attiecīgi ir saistīti ar Privātuma zvanu centru un Strīdu starpniecības komiteju. Tā kā šīs ir papildu tiesiskās aizsardzības iespējas, EDAK labprāt saņemtu sīkākus paskaidrojumus par to, kā tie papildina PDAK un tiesu datu aizsardzības iespējas datu subjektiem, kuru personas dati tiek nosūtīti uz Koreju saskaņā ar lēmumu par aizsardzības līmeņa pietiekamību.

4. DIENVIDKOREJAS PUBLISKO IESTĀŽU PIEKĻUVE PERSONAS DATIEM, KO NOSŪTA NO EIROPAS SAVIENĪBAS, UN TO IZMANTOŠANA

133. Attiecībā uz datu aizsardzības līmeņa novērtējumu tiesībaizsardzības un valsts drošības jomās Eiropas Komisija savā lēmuma projektā un pielikumos sniedza vispusīgu informāciju. Tāpēc EDAK vēlreiz neatkārtos lielāko daļu no šajā atzinumā ietvertajiem faktu konstatējumiem un novērtējumiem.

134. Eiropas Komisija secina, ka iepriekšminētajās jomās pastāv datu aizsardzības līmenis, kas atbilst EST judikatūrā noteiktajām prasībām, un tāpēc to var uzskatīt par būtībā līdzvērtīgu Eiropas Savienības līmenim.

[57] Skatīt lēmuma projekta 117. apsvērumu un Izpildes dekrēta 62. pantu.

135. Kā vispārīgu piezīmi EDAK vēlas uzsvērt, ka pat gadījumos, kad šķiet vai kad Eiropas Komisija apgalvo, ka no ES uz Dienvidkoreju nosūtītus datus, visticamāk, neietekmēs attiecīgie Korejas tiesību akti, joprojām būtu jānovērtē Korejas datu aizsardzības līmeņa atbilstība šādiem gadījumiem. To aktualitāti parāda arī fakts, ka Eiropas Komisija pati tos ir izskatījusi lēmuma projektā.

4.1. Vispārīga datu aizsardzības sistēma valdības piekļuves kontekstā

136. Runājot par valsts iestāžu piekļuvi personas datiem, ir jāizskata dažādi Korejas likumi, lai novērtētu aizsardzības līmeni tiesībām uz privātumu un datu aizsardzību. Pirmkārt, EDAK atzīmē, ka PDAL kā galvenais datu aizsardzības likums pieprasa plašu piemērojamību. Tomēr, lai gan PDAL ir pilnībā piemērojams tiesībaizsardzības jomā, tā piemērošana datu apstrādei valsts drošības nolūkos ir ierobežota. Saskaņā ar PDAL 58. panta 1. punkta 2. apakšpunktu III–VII nodaļa neattiecas uz personas datu apstrādi valsts drošības nolūkos. Tomēr I, II, IX un X nodaļa joprojām ir piemērojama valsts drošības jomā. Tādējādi PDAL pamatprincipi, kā arī datu subjekta tiesību pamatgarantijas un nosacījumi par uzraudzību, izpildi un tiesiskās aizsardzības līdzekļiem attiecas uz valsts drošības iestāžu piekļuvi personas datiem un to izmantošanu.

137. Arī Dienvidkorejas konstitūcija nosaka būtiskus datu aizsardzības principus, proti, likumības, nepieciešamības un samērīguma principus. Šie principi attiecas arī uz Dienvidkorejas valsts iestāžu piekļuvi personas datiem tiesībaizsardzības un valsts drošības jomās[58].

138. Tiesībaizsardzības jomā policija, prokurori, tiesas un citas valsts iestādes var ievākt personas datus, pamatojoties uz konkrētiem tiesību aktiem, piemēram, Kriminālprocesa likumu ("**KPL**"), Komunikāciju privātuma aizsardzības likumu ("**KPAL**"), Telekomunikāciju uzņēmējdarbības likumu ("**TUL**") un Likumu par noteiktas finanšu darījumu informācijas ziņošanu un izmantošanu ("**NFDIZIL**"), kas attiecas uz naudas atmazgāšanas un terorisma finansēšanas kriminālvajāšanu un novēršanu. Šie konkrētie likumi nosaka papildu ierobežojumus, aizsardzības pasākumus un izņēmumus.

139. Valsts drošības jomā, pamatojoties uz Nacionālā izlūkošanas dienesta likumu ("**NIDL**") un citiem "valsts drošības likumiem"[59], Nacionālais izlūkošanas dienests ("**NID**") var ievākt personas datus un pārtvert sakarus. Izmantojot savas pilnvaras, EDAK saprot, ka NID ir jāievēro iepriekš minētās tiesību normas, kā arī PDAL.

140. EDAK lūdz Komisiju precizēt, vai Korejā bez NID ir arī citas iestādes, kas atbild par valsts drošības jomu, jo pēc norādēm I pielikuma 6. sadaļā Eiropas Komisijai rodas iespaids par NID kā valsts drošības aģentūru piemēru.

4.2. Komunikācijas apliecinājuma datu aizsardzība un aizsardzības pasākumi saistībā ar valdības piekļuvi tiesībaizsardzības nolūkos

141. Pamatojoties uz attiecīgajiem likumiem, KPAL, tiesībaizsardzības iestādes var veikt divu veidu pasākumus, lai piekļūtu komunikācijas informācijai. KPAL nošķir komunikāciju ierobežojošus pasākumus, kas attiecas uz parastā pasta satura vākšanu un tiešu telekomunikāciju satura pārtveršanu[60], un tā dēvēto komunikācijas apliecinājuma datu vākšanu. Pēdējais no minētajiem iekļauj telekomunikāciju datumu, to sākuma un beigu laiku, izejošo un ienākošo zvanu skaitu, kā arī otras puses abonenta numuru, lietošanas biežumu, žurnālfailus par telekomunikāciju pakalpojumu izmantošanu un atrašanās vietas informāciju[61].

[58] Skatīt lēmuma projekta 145. apsvērumu.
[59] Valsts drošības likumi iekļauj, piemēram, Komunikāciju privātuma aizsardzības likumu, Likumu par terorisma novēršanu pilsoņu un sabiedrības drošības aizsardzībai un Telekomunikāciju uzņēmējdarbības likumu.
[60] KPAL 3. panta 2. punkts, 2. panta 6. punkts un 2. panta 7. punkts.
[61] KPAL 2. panta 11. punkts.

142. EDAK atzīmē, ka komunikācijas apliecinājuma datiem, šķiet, netiek piemēroti tādi paši aizsardzības pasākumi kā datiem, kas vākti, izmantojot komunikāciju ierobežojošus pasākumus, piemēram, satura datiem. Patiešām EDAK atzīmē, ka satura vākšana ir vairāk aizsargāta nekā komunikācijas apliecinājuma datu vākšana tiesībaizsardzības nolūkos: Pirmkārt, atšķirībā no satura datu vākšanas komunikācijas apliecinājuma datu vākšana neaprobežojas tikai ar noteiktu smagu noziegumu izmeklēšanu, bet to var veikt, ja tas tiek uzskatīts par nepieciešamu, lai veiktu "jebkuru izmeklēšanu vai izpildītu jebkādu sodu" (KPAL 13. panta 1. punkts). Otrkārt, komunikācijas apliecinājuma datu vākšana principā nav strukturēta kā pēdējais līdzeklis un būtu jāizmanto tikai gadījumos, kad ir grūti citādi novērst nozieguma izdarīšanu, aizturēt noziedznieku vai savākt pierādījumus[62]. Komunikācijas apliecinājuma dati var tikt ievākti ikreiz, kad prokurors vai tiesu policijas darbinieks "to uzskata par nepieciešamu" nozieguma izmeklēšanai vai soda izpildei. Tomēr šajā saistībā ir izņēmums attiecībā uz reāllaika izsekošanas datiem un komunikācijas apliecinājuma datiem par konkrētu bāzes staciju saskaņā ar KPAL 13. panta 2. punktu. Treškārt, tiesībaizsardzības iestādēm, kas ievāc komunikācijas saturu, šī darbība ir nekavējoties jāpārtrauc, tiklīdz turpmāka piekļuve vairs netiek uzskatīta par nepieciešamu[63]. Attiecībā uz komunikācijas apliecinājuma datiem tas vismaz nav skaidri atrunāts KPAL vai tā izpildes dekrētā.

143. EDAK ņem vērā, ka komunikācijas apliecinājuma datus var ievākt, tikai pamatojoties uz tiesas izdotu orderi. Turklāt KPAL pieprasa sniegt detalizētu informāciju gan pieteikumā par orderi, gan pašā orderī[64]. Šādas iepriekšējas tiesas atļaujas mērķis ir ierobežot tiesībaizsardzības iestāžu rīcības brīvību, piemērojot tiesību aktus, un pārbaudīt, vai katrā gadījumā pastāv pietiekami iemesli komunikācijas apliecinājuma datu vākšanai. EDAK arī atzīst, ka Korejas Republikas likumi, šķiet, neparedz komunikācijas apliecinājuma datu vispārēju un neierobežotu saglabāšanu. Tādējādi valdības piekļuve šādiem datiem vienmēr attiecas uz datiem, kas tiek saglabāti, lai izrakstītu rēķinus un sniegtu pašus sakaru pakalpojumus.

144. Tomēr EDAK uzsver, ka EST ir apšaubījis faktu par to, ka informācijas plūsmas dati ir mazāk jutīgi nekā citi, jo īpaši satura dati[65]. Ņemot vērā, ka komunikācijas apliecinājuma datiem vairākos aspektos tiek nodrošināts zemāks aizsardzības līmenis nekā satura datiem, EDAK aicina Eiropas Komisiju rūpīgi uzraudzīt, vai Korejas tiesību aktos noteiktie aizsardzības pasākumi šādai personas datu kategorijai nodrošina būtībā līdzvērtīgu aizsardzības līmeni ES garantētajam, jo īpaši attiecībā uz tiesību aktu samērīgumu un paredzamību.

1.3. Korejas valsts iestāžu piekļuve komunikācijas informācijai valsts drošības nolūkos

145. Attiecībā uz tiesisko regulējumu par valsts drošības iestāžu piekļuvi komunikācijas informācijai, kas tiek nosūtīta no EEZ uz Koreju, EDAK ir identificējusi divus bažas raisošus jautājumus, kas abi ir saistīti ar piekļuves režīmu komunikācijai starp personām, kuras nav Korejas valstspiederīgie un ietilpst konkrētā lietošanas gadījumu kopumā (skatīt 29. punktu). Šādos gadījumos attiecībā uz komunikācijas apliecinājuma datiem un satura datiem nav piemērojami daži citkārt paredzētie drošības pasākumi.

---

[62] Tas attiecas uz satura datiem saskaņā ar KPAL 3. panta 2. punktu un 5. panta 1. punktu.

[63] KPAL izpildes dekrēta 2. pants.

[64] Skatīt lēmuma projekta 156. apsvērumu.

[65] Skatīt EST, C-623/17, *Privacy International*, 2020. gada 6. oktobris, ECLI:EU:C:2020:790, 71. punkts: " *Iejaukšanās Hartas 7. pantā paredzētajās tiesībās, ko rada informācijas plūsmas datu un atrašanās vietas datu nosūtīšana drošības un izlūkošanas aģentūrām, ir jāuzskata par īpaši nopietnu, cita starpā paturot prātā informācijas sensitīvo raksturu, ko šie dati var sniegt, un jo īpaši iespēju izveidot attiecīgo personu profilu, pamatojoties uz šiem datiem, un šāda informācija nav mazāk sensitīva par saziņas faktisko saturu. Turklāt tas, iespējams, ieinteresēto personu prātos radīs sajūtu, ka viņu privātā dzīve tiek pastāvīgi uzraudzīta (pēc analoģijas skat. 2014. gada 8. aprīļa spriedumus Digital Rights Ireland and Others lietā C-293/12 un C-594/12, EU:C:2014:238, 27. un 37. punkts, un 2016. gada 21. decembra spriedumus Tele2 lietā C-203/15 un C-698/15, EU:C:2016:970, 99. un 100. punkts)*."

Citiem vārdiem sakot, šajos konkrētajos gadījumos uz datiem neattiecas tie paši drošības pasākumi, kas tiek piemēroti tad, ja komunikācijā ir iesaistīts vismaz viens Korejas pilsonis.

4.3.1. Nav pienākuma informēt fiziskas personas par valdības piekļuvi saziņai starp ārvalstu pilsoņiem

146. Saskaņā ar iepriekš aprakstīto scenāriju, piemēram, ja neviena no komunikācijas pusēm nav Korejas pilsonis, valsts drošības iestādēm nav pienākuma informēt fiziskas personas par viņu datu vākšanu un apstrādi. EDAK atzīst, ka šī problēma skar tikai atsevišķus gadījumus. Pirmkārt, kā jau tika norādīts, ja vismaz viens Korejas pilsonis ir iesaistīts komunikācijā, paziņojuma prasības saskaņā ar KPAL attiecas uz visām komunikācijas pusēm neatkarīgi no viņu valstspiederības[66]. Otrkārt, personas datu vākšana, kas izriet no komunikācijas tikai starp ārvalstu pilsoņiem, ir pakļauta konkrētam lietošanas gadījumu kopumam. Jo īpaši piekļuves tiesības šādos gadījumos attiecas uz komunikāciju ar: a) Korejas Republikai naidīgām valstīm, b) ārvalstu aģentūrām, grupām vai valstspiederīgajiem, kas tiek turēti aizdomās par iesaistīšanos pret Koreju vērstās darbībās[67], c) tādu grupu dalībniekiem, kas darbojas Korejas pussalā, bet faktiski pārsniedz Korejas Republikas suverenitāti, un to jumta organizācijas grupām, kas atrodas ārvalstīs. Tādējādi komunikācija starp ES personām, kas nosūtīta no EEZ uz Koreju, var tikt vākta tikai valsts drošības nolūkos, ja tā ietilpst vienā no trim iepriekš minētajām kategorijām[68]. EDAK no Eiropas Komisijas papildu paskaidrojumiem saprata, ka papildu ierobežojošs faktors ir tāds, ka piemērojamais tiesiskais regulējums neparedz datu pārtveršanu tranzītā ārpus Korejas.

147. Līdz ar to kritiku par paziņojuma prasības trūkumu, ņemot vērā tā praktisko ietekmi, var uzskatīt par ierobežotu. Tomēr EDAK uzsver, cik svarīgi ir (vēlāk) paziņot par valdības piekļuvi, jo īpaši attiecībā uz efektīvu tiesiskās aizsardzības līdzekļu nodrošināšanu. Saskaņā ar EST paziņošana ir "*nepieciešama, lai ļautu šīm personām īstenot savas tiesības, kas izriet no Hartas 7. un 8. panta, lūgt piekļuvi saviem personas datiem, kas ir šo pasākumu priekšmets, un vajadzības gadījumā panākt to labošanu vai dzēšanu, kā arī saskaņā ar Hartas 47. panta pirmo daļu izmantot tiesības uz efektīvu tiesību aizsardzību*"[69]. Valdības piekļuve valsts drošības nolūkos bieži iekļauj slepenus novērošanas pasākumus, proti, novērošanas objekti — datu subjekti — nav informēti par savu datu apstrādi. Tādējādi "*attiecīgajai personai principā ir maz iespēju vērsties tiesā, ja vien persona netiek informēta par pasākumiem, kas tiek īstenoti bez viņas ziņas, un tādējādi var apstrīdēt to likumību retrospektīvi, vai alternatīvi —, ja vien persona, kurai ir aizdomas, ka tās saziņa tiek pārtverta vai ir tikusi pārtverta, nevar vērsties tiesā tā, ka tiesas piekritība nav atkarīga no pārtveršanas subjekta informēšanas par viņa saziņas pārtveršanu*"[70]. Šajā kontekstā un saskaņā ar to EDAK daudzkārt ir paudusi bažas par efektīviem tiesiskās aizsardzības līdzekļiem uzraudzības lietās. EDAK uzsver, ka valdības pasākumu slepenība nedrīkst novest pie tā, ka šādi pasākumi faktiski nav apstrīdami. Ņemot vērā iepriekšminēto, neatkarīgi no tā, vai paziņojuma prasības trūkums attiecībā uz komunikāciju starp ārvalstu pilsoņiem ietekmē lēmuma projektā novērtēto datu aizsardzības līmeni, tas ir jāizvērtē kā daļa no vispārējā novērtējuma, īpaši ņemot vērā pārraudzības un tiesiskās aizsardzības mehānismus, kas paredzēti Korejas tiesību aktos (skatīt 4.7. un 4.8. sadaļu).

---

[66] Skatīt lēmuma projekta 192. apsvērumu.

[67] Skatīt II pielikuma 244. zemsvītras piezīmi, saskaņā ar kuru pret Koreju vērstas darbības jēdziens attiecas uz darbībām, kas apdraud valsts pastāvēšanu un drošību, demokrātisko kārtību vai tautas izdzīvošanu un brīvību.

[68] Skatīt lēmuma projekta 187. apsvērumu.

[69] EST, apvienotās lietas C-511/18, C-512/18 un C-520/18, *La Quadrature du Net and others*, 2020. gada 6. oktobris, ECLI:EU:C:2020:791, 190. punkts.

[70] ECT, *Big Brother Watch and others v. UK*, 2021. gada 25. maijs, ECLI:CE:ECHR:2021:0525JUD005817013, 337. punkts, un ECT, *Case of Roman Zakharov v. Russia*, 2015. gada 4. decembris, ECLI:CE:ECHR:2015:1204JUD004714306, 234. punkts.

148. Turklāt EDAK šajā kontekstā atzīmē, ka likums atsaucas uz diezgan plašiem terminiem, piemēram, pret Koreju vērstām vai antinacionālām darbībām[71], un ir grūti paredzēt, kā šie jēdzieni tiek interpretēti saskaņā ar Korejas tiesību aktiem. EDAK aicina Eiropas Komisiju uzraudzīt, kā šie termini ir atspoguļoti Korejas tiesību aktos un vai to piemērošana praksē atbilst proporcionalitātes prasībām, kas izriet no ES tiesību aktiem.

4.3.2. Nav iepriekšējas neatkarīgas atļaujas ārvalstu pilsoņu savstarpējās komunikācijas informācijas vākšanai

149. Gadījumos, kad EEZ personas dati, kas iegūti no komunikācijas starp personām, kuras nav Korejas pilsoņi (un kas ietilpst kādā no iepriekšminētajiem lietošanas gadījumiem), tiks apstrādāti Korejā valsts drošības nolūkos, šādu datu vākšanai nav nepieciešams iepriekšējs neatkarīgas iestādes apstiprinājums (kā tad, ja komunikācijā vismaz viena no attiecīgajām fiziskajām personām ir Korejas pilsonis)[72].

150. It īpaši ņemot vērā nesenos Eiropas Cilvēktiesību tiesas ("**ECT**") nolēmumus "Big Brother Watch and Others v. UK" un "Centrum för Rättvisa v. Sweden", EDAK uzskata par nepieciešamu izpētīt, vai tas ir Korejas datu aizsardzības sistēmas kritisks trūkums. Šajā saistībā EDAK atsaucas uz norādi tās atjauninātajos ieteikumos attiecībā uz Eiropas būtiskajām garantijām uzraudzības pasākumiem,[73] Līguma par Eiropas Savienību 6. panta 3. punkts nosaka, ka ECTK noteiktās pamattiesības veido ES tiesību vispārējos principus, bet, kā atgādina EST savā judikatūrā, kamēr Eiropas Savienība tam nav pievienojusies, tas nav juridisks instruments, kas ir oficiāli iekļauts ES tiesību aktos[74]. Tādējādi VDAR 45. pantā prasītais pamattiesību aizsardzības līmenis ir jānosaka, pamatojoties uz šīs regulas noteikumiem, ko interpretē saskaņā ar Hartā noteiktajām pamattiesībām. Tomēr saskaņā ar Hartas 52. panta 3. punktu tajā ietvertajām tiesībām, kas atbilst ECTK garantētajām tiesībām, ir tāda pati nozīme un darbības joma kā minētajā Konvencijā. Līdz ar to attiecībā uz tiesībām, kas arī paredzētas Hartā, ECT judikatūra ir jāņem vērā kā minimālais aizsardzības slieksnis, lai interpretētu atbilstīgās tiesības Hartā, piemēram, tajā ziņā, ka Harta, kā to interpretē EST, neparedz augstāku aizsardzības līmeni[75].

151. EDAK atzīmē, ka, lai gan iepriekšēja (neatkarīga) uzraudzības pasākumu apstiprināšana tiek uzskatīta par svarīgu aizsarglīdzekli pret patvaļu, šādu apstiprinājumu nevar atvasināt no EST jurisprudences kā absolūtu prasību uzraudzības pasākumu samērībai. Tomēr ECT tagad ir skaidri noteikusi prasību pēc iepriekšējas neatkarīgas atļaujas masveida pārtveršanai[76]. Lai gan lēmuma projektā tas nav skaidri pateikts, EDAK saprot, ka Korejas Republikas tiesiskais regulējums neparedz masveida, bet tikai mērķtiecīgu telesakaru pārtveršanu.[77]. Eiropas Komisija ir apstiprinājusi šo izpratni.

---

[71] Eiropas Komisija ir paskaidrojusi, ka saskaņā ar Korejas valdības paskaidrojumiem tas attiecas uz "darbībām, kas apdraud valsts pastāvēšanu un drošību, demokrātisko kārtību vai tautas izdzīvošanu un brīvību"; skatīt arī projekta lēmuma par aizsardzības līmeņa pietiekamību 319. zemsvītras piezīmi.

[72] Skatīt lēmuma projekta 190. apsvērumu.

[73] Skatīt EDAK ieteikumus 02/2020 attiecībā uz Eiropas būtiskajām garantijām uzraudzības pasākumiem, 10. 11. punkts.

[74] Skatīt EST, C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd. and Maximilian Schrems*, 2020. gada 16. jūlijs, ECLI:EU:C:2020:559 (turpmāk — "*Schrems II*"), 98. punkts.

[75] Skatīt EST, apvienotās lietas C-511/18, C-512/18 un C-520/18, *La Quadrature du Net and others*, 2020. gada 6. oktobris, 124. punkts.

[76] Skatīt ECT, *Big Brother Watch and others v. UK*, 2021. gada 25. maijs, ECLI:CE:ECHR:2021:0525JUD005817013, 351. punkts: "Masveida pārtveršanai jau pašā sākumā ir nepieciešama neatkarīga atļauja", "masveida pārtveršanas būtu jāatļauj neatkarīgai iestādei, proti, no izpildvaras neatkarīgai iestādei".

[77] Tikai II pielikuma 3.2. sadaļā ir ietverta skaidra deklarācija valsts drošības nolūkos, ja ir noteikts, ka ierobežojumi un aizsardzības pasākumi "*nodrošina, ka informācijas vākšana un apstrāde ir ierobežota un attiecas*

152. Tas nozīmē, ka iepriekšminētie ECT lēmumi saskaņā ar EST judikatūru[78] un iepriekšējo ECT judikatūru[79] vēlreiz parāda neatkarīgu uzraudzības iestāžu vispusīgas uzraudzības nozīmi. EDAK uzsver, ka neatkarīga pārraudzība visos valdības piekļuves procesa posmos tiesībaizsardzības un valsts drošības nolūkos ir svarīgs nodrošinājums pret patvaļīgiem uzraudzības pasākumiem un datu aizsardzības adekvāta līmeņa novērtēšanai. Uzraudzības iestāžu neatkarības garantija Hartas 8. panta 3. punkta nozīmē ir paredzēta, lai nodrošinātu efektīvu un uzticamu atbilstības uzraudzību, kā tiek ievēroti noteikumi par fizisku personu aizsardzību attiecībā uz personas datu apstrādi. Tas jo īpaši attiecas uz apstākļiem, kad slepenas novērošanas rakstura dēļ fiziskai personai ir liegts pieprasīt pārskatu vai tieši piedalīties jebkādās pārskata procedūrās pirms uzraudzības pasākuma vai tā laikā.

153. Iepriekšēja neatkarīga apstiprinājuma trūkums pats par sevi nevar tikt uzskatīts par būtisku trūkumu Korejas tiesību aktos attiecībā uz būtībā līdzvērtīga datu aizsardzības līmeņa novērtējumu. Atbilstības novērtējums tātad ir atkarīgs no visiem lietas apstākļiem, jo īpaši no *ex post* pārskata efektivitātes un tiesiskās aizsardzības, kā paredzēts Korejas tiesiskajā regulējumā (skatīt 4.7. un 4.8. sadaļu tālāk).

4.4. Brīvprātīga informācijas atklāšana

154. Saskaņā ar TUL 83. panta 3. punktu telekomunikāciju pakalpojumu sniedzēji pēc pieprasījuma var brīvprātīgi nodot valsts drošības un tiesībaizsardzības iestādēm tā sauktos "abonenta datus"[80]. Lai gan EDAK atzīmē, ka lietas, kas ietver no EEZ uz Koreju nosūtītos personas datus, visticamāk, ir retas, tās joprojām ir jāanalizē, lai novērtētu datu aizsardzības līmeni, kā jau minēts iepriekš.

155. EDAK saprot, ka šajos gadījumos tiek piemēroti PDAL datu aizsardzības pasākumi un valsts iestādēm, kā arī telekomunikāciju pakalpojumu sniedzējiem ir jāievēro šīs prasības[81] un tos abus var saukt pie atbildības par jebkādiem attiecīgo datu subjektu tiesību un brīvību pārkāpumiem[82]. Turklāt EDAK saprot, ka telekomunikāciju pakalpojumu sniedzējiem nav jāievēro šādi pieprasījumi.

156. Tomēr attiecībā uz koncepciju par valsts iestāžu piekļuvi abonenta datiem tiesībaizsardzības nolūkos, kā arī un jo īpaši valsts drošības nolūkos, izmantojot telekomunikāciju uzņēmumu operatoru veiktu "brīvprātīgu izpaušanu", pastāv bažas par paaugstinātu tiesību un brīvību risku datu subjektiem, jo īpaši saistībā ar viņu tiesībām uz informāciju.

157. Saskaņā ar PDAL 58. panta 1. punkta 2. apakšpunktu III–VII nodaļas noteikumi neattiecas ne uz kādiem pieprasītajiem personas datiem, kas ir jāsniedz saistībā ar valsts drošību. Šajā saistībā, piemēram, PDAL 18. panta (Izmantošanas pretēji nolūkam un personas datu sniegšanas ierobežojums) un 20. panta (Paziņojums par personas datu avotiem u.c., kas ievākti no trešajām personām) nosacījumi nav piemērojami šādiem pieprasījumiem. Gadījumos, kad pieprasījumu iesniedz valsts drošības iestāde, tas, no vienas puses, rada jautājumu, vai 58. panta 1. punkta 2. apakšpunkts novērš PDAL piemērošanu arī telekomunikāciju pakalpojumu sniedzējiem. No otras puses, rodas jautājums, vai PDAL 20. panta piemērošanas izslēgšana šādos gadījumos attiecas arī uz atbilstīgo nosacījumu no I pielikuma 3. sadaļas (Paziņojums par datiem, ja personas dati nav iegūti no datu subjekta) (Likuma 20. pants)). Ja tā būtu un ja 58. panta 1. punkta 2. apakšpunkts tiktu attiecināts arī uz telekomunikāciju

---

tikai uz to, kas ir absolūti nepieciešams leģitīmā mērķa sasniegšanai. Tas izslēdz jebkādu masveida un nekritisku personas datu vākšanu valsts drošības nolūkos".

[78] Skatīt, piemēram, EST apvienotās lietas C-203/15 un C-698/15, *Tele2 Sverige AB and others*, ECLI:EU:C:2016:970.

[79] Skatīt, piemēram, ECT, *Roman Zakharov v. Russia*, 2015. gada 4. decembris, ECLI:CE:ECHR:2015:1204JUD004714306.

[80] Attiecīgās datu kopas būtu: lietotāja vārds, uzvārds, rezidenta reģistrācijas numurs, adrese un tālruņa numurs, abonēšanas sākuma un beigu datums, kā arī lietotāja identifikācijas kods (izmanto, lai identificētu datorsistēmu vai sakaru tīkla likumīgo lietotāju).

[81] Skatīt lēmuma projekta 164. un 194. apsvērumu.

[82] Skatīt lēmuma projekta 166. apsvērumu.

pakalpojumu sniedzējiem, saskaņā ar pieejamo informāciju pastāvētu risks, ka nebūtu juridiska pienākuma informēt datu subjektus par brīvprātīgu izpaušanu.

158. Tāpēc EDAK pauž bažas par efektivitāti, proti, ka informācijas prasības varētu tikt padarītas neefektīvas, ievērojami apgrūtinot datu subjektu iespējas aizstāvēt savas tiesības uz datu aizsardzību, jo īpaši attiecībā uz tiesisko aizsardzību. Šajā saistībā EDAK aicina Eiropas Komisiju precizēt attiecīgo nosacījumu darbības jomu.

4.5. Informācijas turpmāka izmantošana

159. Nolūka ierobežojuma princips ir datu aizsardzības tiesiskā pamatprasība. Saskaņā ar to personas dati tiek vākti konkrētos, skaidros un leģitīmos nolūkos, un to turpmāku apstrādi neveic ar minētajiem nolūkiem nesavietojamā veidā. Turklāt saskaņā ar ES tiesību aktiem valsts iestādēm ir atļauts apstrādāt personas datus noziedzīgu nodarījumu novēršanai, izmeklēšanai vai lietas ierosināšanai, pat ja šie dati sākotnēji tika vākti citam nolūkam, ja šīm iestādēm ir juridisks pamats šādu datu apstrādei saskaņā ar attiecīgajiem tiesību aktiem un ja turpmāka apstrāde nav nesamērīga[83].

160. Saskaņā ar šo EDAK norāda, ka Korejas datu aizsardzības sistēma paredz aizsardzības pasākumus un ierobežojumus, kas ir līdzīgi ES tiesību aktos paredzētajiem attiecībā uz savāktās informācijas turpmāku izmantošanu tiesībaizsardzības un valsts drošības nolūkos, piemēram, PDAL 3. panta 1.–2. punkta nolūka ierobežojuma princips.

4.6. Tālāka nosūtīšana un informācijas apmaiņa

161. VDAR 44. pants paredz, ka personas datu nosūtīšana un tālāka nosūtīšana notiek tikai tad, ja nemazinās VDAR garantētais aizsardzības līmenis. Tādējādi no EEZ uz Koreju nosūtīto personas datu aizsardzības līmenis nedrīkst samazināties, nosūtot datus saņēmējiem trešā valstī, t. i., tālāka nosūtīšana būtu jāatļauj tikai uz vietām, kur ir pastāvīgs aizsardzības līmenis, kas būtībā ir līdzvērtīgs saskaņā ar ES tiesību aktiem nodrošinātajam. Līdz ar to, novērtējot, vai trešā valsts nodrošina pienācīgu datu aizsardzības līmeni, ir jāņem vērā valsts tiesiskais regulējums tālākai nosūtīšanai. Tas ir neapstrīdami un atbilst gan Eiropas Komisijas[84], gan EDAK viedoklim.

162. Šajā kontekstā EDAK ņem vērā, ka ECT savos nesenajos lēmumos "Big Brother Watch and Others v UK" un "Centrum för Rättvisa v. Sweden" ir sniegusi norādījumus[85] par datu aizsardzības piesardzības pasākumiem, kas ir jāievēro līgumslēdzējās valstīs, paziņojot personas datus citām pusēm tiesībaizsardzības un valsts drošības nolūkos masveida vākšanas gadījumos: "*Pirmkārt, valsts tiesību aktos ir skaidri jānosaka apstākļi, kādos šāda nosūtīšana var notikt. Otrkārt, nosūtošajai valstij ir jānodrošina, ka saņēmējvalstī datu apstrādei ir ieviesti aizsardzības pasākumi, kas spēj novērst ļaunprātīgu izmantošanu un nesamērīgu iejaukšanos. Saņēmējai valstij jo īpaši ir jāgarantē materiāla droša glabāšana un jāierobežo tā izpaušana. [..] Treškārt, būs nepieciešami pastiprināti aizsardzības pasākumi, ja ir skaidrs, ka tiek nosūtīts materiāls, kam ir nepieciešama īpaša konfidencialitāte, piemēram, konfidenciāls žurnālistikas materiāls*."[86]

---

[83] Skatīt Direktīvas par tiesībaizsardzību 4. panta 2. punktu.

[84] Skatīt lēmuma projekta 84. un turpmākos apsvērumus.

[85] Tālāk minētie elementi tika noteikti saistībā ar lietām *Big Brother Watch* un *Centrum för Rättvisa*, kas attiecas uz masveida pārtveršanas režīmiem. Prasība par piesardzības pasākumiem, kas jāievēro, paziņojot materiālu citām pusēm, jau bija daļa no kritērijiem, ko ECT izstrādāja mērķtiecīgas pārtveršanas kontekstā, un ECT to nebija sīkāk precizējusi (skatīt *Big Brother Watch and Others v. UK*, 335., 362. punkts).

[86] ECT, *Big Brother Watch and others v. UK*, 2021. gada 25. maijs, ECLI:CE:ECHR:2021:0525JUD005817013, 362. punkts.

163. Piemērojot šos standartus, ECT lietā "Centrum för Rättvisa v. Sweden" konstatēja, ka pārtveršanas režīmā nav skaidras juridiskas prasības novērtēt informācijas apmaiņas nepieciešamību un samērīgumu, jo tās iespējamā ietekme uz privātuma tiesībām ir ECTK 8. panta pārkāpums. ECT kritizēja, ka tiesību aktu vispārīguma līmeņa dēļ pārtveršanas materiālus parasti var nosūtīt uz ārzemēm, kad vien tas tiek uzskatīts par valsts interesēm noderīgu, neatkarīgi no tā, vai ārvalsts saņēmējs piedāvā pieņemamu minimālo aizsardzības līmeni[87].

164. Atzīstot, ka Dienvidkorejas tiesiskais regulējums neļauj veikt masveida pārtveršanu, tomēr ņemot vērā iepriekš minēto ECT judikatūras ietekmi, EDAK uzskata, ka papildus prasībām, kas izriet no ES tiesību aktiem, kā to interpretējusi EST, būtu jāņem vērā ECT argumenti, lai novērtētu, vai tiesiskais regulējums tālākai nosūtīšanai uz trešo valsti paredz atbilstošus datu aizsardzības standartus.

4.6.1. Piemērojamais tiesiskais regulējums tālākai nosūtīšanai, ko veic tiesībaizsardzības iestādes

165. Attiecībā uz tālāku nosūtīšanu, ko veic kompetentās iestādes tiesībaizsardzības nolūkos, EDAK no Eiropas Komisijas paskaidrojumiem saprot, ka ir piemērojama lēmuma projekta I pielikuma 2. sadaļa par tālākas nosūtīšanas ierobežošanu, tostarp tad, kad nosūtīšana tiek veikta pamatojoties uz citiem likumiem, nevis PDAL. Saskaņā ar šo noteikumu "*ja personas dati tiek sniegti trešajai pusei ārzemēs, tie var nesaņemt aizsardzības līmeni, ko garantē Korejas likums par personas datu aizsardzību dažādu valstu personas datu aizsardzības sistēmu atšķirību dēļ. Šādi gadījumi tiks attiecīgi uzskatīti par likuma 17. panta 4. punktā minētajiem "gadījumiem, kad datu subjektam var tikt radīti neizdevīgi apstākļi", vai likuma 18. panta 2. punktā un tā paša likuma Izpildes dekrēta 14. panta 2. punktā minētajiem "gadījumiem, kad datu subjekta vai trešās puses intereses tiek negodīgi aizskartas". Lai izpildītu šo nosacījumu prasības, personas datu pārzinim un trešai pusei ir skaidri jānodrošina Likumam līdzvērtīgs aizsardzības līmenis, tostarp garantija, ka datu subjekts īsteno savas tiesības juridiski saistošos dokumentos, piemēram, līgumos, pat pēc personas datu nosūtīšanas uz ārzemēm"*[88].

166. EDAK atzinīgi vērtē šo nosacījumu, kas, pieņemot, ka datu aizsardzības līmenis Korejā ir atbilstošs šim nolūkam, nodrošina tāda aizsardzības līmeņa nepārtrauktību, kāds būtībā ir paredzēts ES tiesību aktos attiecībā uz tālāku nosūtīšanu. Komisija ir apstiprinājusi, ka EDAK izpratne ir pareiza, proti, šī I pielikuma sadaļa attiecas uz visiem tālākas nosūtīšanas gadījumiem, ko veic kompetentās iestādes tiesībaizsardzības nolūkos. Tomēr EDAK norāda, ka ir jānodrošina, lai šis noteikums praksē nodrošinātu nepārtrauktu aizsardzības līmeni, jo var rasties neskaidrības par to, kādus līgumsaistību aizsardzības pasākumus un pienākumus vai citus līdzīgus mehānismus var izmantot, lai sasniegtu šādu aizsardzības līmeni gadījumā, kad apstrāde notiek tiesībaizsardzības nolūkos. Šajā saistībā papildus būtu jānorāda, ka, piemēram, personas datus drīkst koplietot tikai ar trešās valsts attiecīgajām kompetentajām iestādēm.

167. Ievērojot iepriekš pieprasīto precizējumu par to, vai uz KOFIV attiecas lēmuma projekts, EDAK norāda, ka oficiālā pārstāvniecība par valdības piekļuvi[89] paskaidro, ka saskaņā ar NFDIZIL 8. panta 1. punktu KOFIV komisārs var sniegt ārvalstu finanšu izlūkošanas dienestiem konkrētu informāciju par finanšu darījumiem, ja tas tiek uzskatīts par nepieciešamu NFDIZIL mērķa sasniegšanai[90]. NFDIZIL 8. pants pats par sevi neparedz pienākumu noteikt, vai ārvalsts nodrošina atbilstošus datu aizsardzības pasākumus.

---

[87] Skatīt ECT, *Centrum för Rättvisa v. Sweden*, 2021. gada 25. maijs, ECLI:CE:ECHR:2021:0525JUD005817013, 326. punkts.

[88] Lēmuma projekts, I pielikums, 7. lpp.

[89] Skatīt lēmuma projekta II pielikumu.

[90] Skatīt lēmuma projekta II pielikuma 2.2.3.2. sadaļu. Lai gan šāda apmaiņa var notikt tikai ar nosacījumu, ka ārvalsts dienests nedrīkst izmantot informāciju citiem mērķiem, izņemot sākotnējo izpaušanas mērķi, un jo īpaši ne kriminālizmeklēšanai vai tiesai (NFDIZIL 8. panta 2. punkts), KOFIV komisārs, saņemot ārvalsts pieprasījumu, ar tieslietu ministra iepriekšēju piekrišanu var sniegt piekrišanu šādu datu izmantošanai kriminālizmeklēšanā vai tiesvedībā par noziedzīgiem nodarījumiem (NFDIZIL 8. panta 3 punkts).

Šajā saistībā II pielikumā nav atsauces uz I pielikuma jauno sadaļu. Tāpēc EDAK aicina Eiropas Komisiju precizēt savstarpējo saistību starp I pielikuma attiecīgo sadaļu, kas attiecas uz tālākas nosūtīšanas ierobežojumu un tālākas nosūtīšanas juridisko pamatu saskaņā ar NFDIZIL.

4.6.2. Piemērojamais tiesiskais regulējums tālākai nosūtīšanai valsts drošības nolūkos

168. Lēmuma projektā nav nekādas informācijas par tiesisko regulējumu turpmākai nosūtīšanai valsts drošības jomā. Šim nolūkam EDAK saprot, ka atšķirībā no tiesībaizsardzības mērķiem I pielikuma 2. sadaļa nav piemērojama tālākai nosūtīšanai valsts drošības nolūkos. PDAL 17. un 18. pants, uz ko attiecas I pielikuma atbilstošā sadaļa, ir daļa no PDAL III nodaļas, kas savukārt nav piemērojama personas datu apstrādei valsts drošības nolūkos (PDAL 58. panta 1. punkts).

169. Tomēr EDAK pieņem, ka Korejai valsts drošības nolūkos var būt nepieciešams nosūtīt personas datus ārvalstu izlūkdienestiem un tā tos arī nosūta, piemēram, lai sadarbotos cīņā pret valsts drošības pārrobežu apdraudējumiem, brīdinātu par to ārvalstu valdības vai lūgtu to palīdzību šādu apdraudējumu identificēšanā.

170. EDAK ir sapratusi, ka, pēc Eiropas Komisijas domām, tālāku nosūtīšanu Korejas tiesību aktos pietiekami reglamentē aizsardzības pasākumi, kas izriet no visaptverošā konstitucionālā regulējuma, jo īpaši nepieciešamības un proporcionalitātes principi, kā arī PDAL regulētie datu aizsardzības pamatprincipi, piemēram, apstrādes likumība un godīgums, nolūka ierobežojums, datu apjoma samazināšana, drošība un vispārējie pienākumi novērst personas datu ļaunprātīgu un nepareizu izmantošanu.

171. EDAK atzīst un ņem vērā šo galveno (datu aizsardzības) principu vispārējo piemērojamību, taču pauž bažas, ka šiem aizsardzības pasākumiem ir ļoti vispārējs raksturs un tie, ar juridisku pamatu, īpaši neatsaucas uz konkrētiem apstākļiem un nosacījumiem, lai veiktu EEZ nosūtīto datu tālāku nosūtīšanu valsts drošības nolūkos. Lai gan šie vispārīgie un visaptverošie principi ir plaši piemērojami, EDAK apšauba, vai tos varētu uzskatīt par atbilstošiem noteikumu skaidrības un precizitātes kritērijiem un vai tie paredz pietiekami efektīvus un izpildāmus aizsardzības pasākumus. Jo īpaši gadījumos, kad valdības piekļuve personas datiem un to apstrāde tiek veikta slepenībā un no datiem izrietošie secinājumi ir īpaši smagi, ir svarīgi, lai būtu skaidri un sīki izstrādāti noteikumi. Likumā būtu pietiekami skaidri jānorāda kompetentajām iestādēm piešķirtās rīcības brīvības apjoms un tās izmantošanas veids, lai nodrošinātu pienācīgu aizsardzību fiziskai personai. Spriedumā *Schrems II* EST atgādina, ka juridiskajam pamatam, kas pieļauj iejaukšanos pamattiesībās, lai izpildītu nepieciešamības un samērīguma principu prasības, ir pašam jānosaka attiecīgo tiesību ierobežojuma apjoms un jānosaka skaidri un precīzi noteikumi, kas reglamentē attiecīgā pasākuma darbības jomu un piemērošanu, un nosaka minimālos aizsardzības pasākumus[91]. Tāpēc EDAK pauž bažas, ka nepietiek ar to, ka šādi aizsardzības pasākumi parasti ir ietverti augstāka līmeņa tiesību aktos, īpaši neieviešot, piemēram, samērīguma jēdzienu, attiecīgajā juridiskajā pamatā.

172. Šīs bažas apstiprina iepriekš minētais ECT lēmums, kurā tiesa konstatēja, ka vispārējs noteikums bez skaidras prasības izvērtēt nepieciešamību un samērīgumu vai apsvērt bažas par privātumu, nav saderīgs ar tiesībām uz privātumu saskaņā ar ECTK 8. pantu. Šajā saistībā EDAK norāda, ka attiecīgās lietas tiesību aktos (kā arī Korejas tiesību aktos) pastāv visaptveroši (konstitucionāli garantēti) nepieciešamības un proporcionalitātes principi, piemēram, saskaņā ar Hartu un pievienojoties ECTK.

173. EDAK aicina Eiropas Komisiju precizēt juridisko pamatu, kā un cik lielā mērā un ar kādiem īpašiem nosacījumiem izlūkdienestu pienākums ir apsvērt bažas par privātumu un datu aizsardzības pasākumus pirms personas datu izpaušanas ārvalstu partneriem valsts drošības nolūkos. Ja šāds pienākums izriet tieši no konstitucionālajiem principiem, Eiropas Komisijai būtu turpmāk jāizvērtē

[91] Skatīt *Schrems II*, 175. un 180. punkts.

attiecīgā likuma precizitātes un skaidrības prasības un jāapstiprina, ka vispārējie konstitucionālie un datu aizsardzības principi ir pienācīgi piemēroti un īstenoti.

4.6.3. Starptautiski nolīgumi

174. EDAK norāda, ka Eiropas Komisija, veicot atbilstības novērtējumu, nav ņēmusi vērā starptautisku nolīgumu esamību starp Koreju un trešām valstīm vai starptautiskām organizācijām, kas varētu paredzēt konkrētus nosacījumus par personas datu starptautisku nosūtīšanu uz trešajām valstīm, ko veic tiesībaizsardzības iestādes un/vai izlūkdienesti. EDAK uzskata, ka divpusēju vai daudzpusēju nolīgumu noslēgšana ar trešajām valstīm tiesībaizsardzības vai izlūkošanas sadarbības nolūkā, visticamāk, ietekmēs Korejas datu aizsardzības tiesisko sistēmu.

175. Tāpēc EDAK aicina Eiropas Komisiju precizēt, vai šādi nolīgumi pastāv un ar kādiem nosacījumiem tos var noslēgt, un izvērtēt, vai starptautisko nolīgumu nosacījumi var ietekmēt aizsardzības līmeni, ko tiesiskais regulējums nodrošina personas datiem, kas tiek nosūtīti no EEZ uz Koreju, un praksi saistībā ar informācijas izpaušanu ārvalstīm tiesībaizsardzības un valsts drošības nolūkos.

4.7. Uzraudzība

176. EDAK atzīmē, ka krimināltiesību izpildes, kā arī valsts drošības iestāžu uzraudzību nodrošina dažādu iekšējo un ārējo struktūru kombinācija.

177. Šajā kontekstā jāatzīmē, ka EST ir vairākkārt uzsvērusi nepieciešamību pēc neatkarīgas uzraudzības, kas ir būtiska fizisko personu aizsardzības sastāvdaļa attiecībā uz viņu personas datu apstrādi. Neatkarības jēdziens ietver institucionālo autonomiju, brīvību neuzklausīt norādījumus un materiālo neatkarību. Lai nodrošinātu datu aizsardzības tiesību aktu konsekventu uzraudzību un izpildi, uzraudzības iestādēm ir nepieciešamas efektīvas pilnvaras, tostarp korekcijai un labošanai.

178. EDAK piekrīt Eiropas Komisijas secinājumam, ka vispārējā novērtējumā var uzskatīt — Korejai ir neatkarīga un efektīva uzraudzības sistēma, lai gan vairākas uzraudzības sistēmas struktūras pašas par sevi neatbilst iepriekšminētajām prasībām. Piemēram, to lielākajai daļai nav izpildvaras, bet tās aprobežojas ar vienkāršiem ieteikumiem, ko sniedz, piemēram, Valsts cilvēktiesību komisija vai Revīziju un inspekciju padome. Turklāt lielākā daļa attiecīgo valsts iestāžu nav tikai datu aizsardzības iestādes, bet tām parasti tiek uzticēti citi uzdevumi pamattiesību aizsardzības jomā.

179. Tomēr saskaņā ar Eiropas Komisijas paskaidrojumiem EDAK atzīmē, ka tiesībaizsardzības iestāžu uzraudzību visaptveroši un bez izņēmuma garantē PDAK. Tāpēc PDAK ir izmeklēšanas, labošanas un izpildes pilnvaras saskaņā ar PDAL un citiem datu aizsardzības tiesību aktiem (piemēram, KPAL), kas attiecas uz visu tiesībaizsardzības un valsts drošības iestāžu piekļuves jomu personas datiem.

180. Šajā kontekstā EDAK vēlas vēlreiz uzsvērt, ka, lai īstenotu savus uzdevumus un pilnvaras, uzraudzības iestādēm ir nepieciešami pietiekami cilvēku, tehniskie un finanšu resursi. Šajā saistībā diemžēl trūkst informācijas par izraudzītajām uzraudzības struktūrām, jo īpaši PDAK. Tādēļ EDAK atkārtoti lūdz Eiropas Komisijai sniegt papildu informāciju šajā jautājumā.

181. Kopumā EDAK vēlas atzīmēt, ka lēmuma projektā gandrīz nav paziņojumu, piemēru vai skaitļu par uzraudzības darbībām, kā arī par datu aizsardzības tiesību aktu tiesisko izpildi, ko veic uzraudzības iestādes tiesībaizsardzības un valsts drošības jomā. To būtu noderīgi zināt, lai novērtētu uzraudzības iestāžu efektivitāti.

4.8. Tiesību aizsardzības līdzeklis un tiesiskā aizsardzība

182. EDAK atgādina, ka pienācīgam datu aizsardzības līmenim ir būtiski datu subjektiem nodrošināt vispusīgus tiesiskās aizsardzības līdzekļus un tiesisko aizsardzību pret neatļautu piekļuvi datiem vai to

apstrādi. Šiem tiesiskās aizsardzības līdzekļiem ir jābūt pietiekamiem, lai datu subjektam ļautu piekļūt par viņu glabātajiem datiem un pieprasīt to labošanu vai dzēšanu.

183. Ņemot vērā EST spriedumus *Schrems I* un *Schrems II*, ir skaidrs, ka papildus tiesībām vērsties kompetentajās iestādēs efektīvai tiesiskai aizsardzībai Hartas 47. panta 1. punkta izpratnē būtiska nozīme ir pieņēmumam par trešās valsts tiesību aktu atbilstību.

184. EDAK atzīst, ka Koreja ir iedibinājusi dažādus līdzekļus, kā īstenot fizisku personu tiesības piekļūt datiem, tos saglabāt, dzēst un apturēt apstrādi saskaņā ar PDAL. Šīs tiesības var īstenot attiecībā uz pašu datu pārzini vai izmantojot sūdzību, kas iesniegta PDAK vai citās uzraudzības iestādēs, piemēram, Valsts cilvēktiesību komisijā. Turklāt EDAK atzīst iespēju apstrīdēt datu pārziņu vai valsts iestāžu lēmumu, atbildot uz viņu pieprasījumu, pamatojoties uz Administratīvās tiesvedības likumu.

185. Turklāt EDAK no Eiropas Komisijas sniegtajiem paskaidrojumiem saprot, ka fiziskas personas var apstrīdēt tiesībaizsardzības un valsts drošības iestāžu rīcību kompetentās tiesās saskaņā ar Administratīvās tiesvedības likumu un Satversmes tiesas likumu, un tām ir iespēja saņemt kompensāciju par zaudējumiem, kas izriet no likuma par valsts kompensāciju[92].

186. Tomēr šajā kontekstā EDAK pauž bažas par efektīvu tiesisko aizsardzību ES fiziskajām personām valsts drošības lietās, kurās nav iesaistīts neviens Korejas pilsonis. Kā norādīts 33. un turpmākajos punktos, valsts drošības iestādēm nav pienākuma informēt datu subjektus par viņu personas datu vākšanu un apstrādi. Tā kā šādos gadījumos ir ievērojami grūtāk iegūt efektīvu tiesisko aizsardzību, EDAK vēlas norādīt, ka tad, ja tiek iesaistīti no EEZ nosūtīti dati, ir nepieciešami noteikti tiesiskās aizsardzības pasākumi. Šiem aizsardzības pasākumiem ir jānodrošina iespēja datu subjektiem efektīvi rīkoties pret nelikumīgu datu apstrādi juridiski drošā veidā, tos netraucējot ar pārmērīgi ierobežotām procesuālajām prasībām, piemēram, uzliekot pierādījuma pienākumu, ko viņi nevar izpildīt, nezinot par apstrādi. Turklāt datu subjektiem ir jābūt iespējai vērsties kompetentā iestādē, kas atbilst ES Pamattiesību hartas 47. panta prasībām, proti, kuras kompetencē ir noteikt, ka notiek datu apstrāde, lai pārbaudītu apstrādes likumību, un kurai ir izmantojamas tiesiskās aizsardzības pilnvaras, ja datu apstrāde ir nelikumīga. Ņemot vērā iepriekš minēto, nav pietiekamas, piemēram, tikai tiesības iesniegt sūdzību Valsts cilvēktiesību komisijā. Tāpēc EDAK aicina Komisiju sīkāk paskaidrot, kā šīs prasības tiek īstenotas procesuāli un pēc būtības, piemēram, vai datu subjekti var vērsties PDAK, kā arī tiesā, nepierādot attiecīgo datu apstrādi.

187. Turklāt EDAK atzīmē, ka lēmuma projektā ir paredzēts sūdzību nosūtīšanas mehānisms, proti, ka ES fiziskās personas var iesniegt sūdzību PDAK, izmantojot savas valsts datu aizsardzības iestādi vai EDAK. Kad izmeklēšana būs pabeigta, PDAK informēs fizisko personu, izmantojot to pašu kanālu[93]. EDAK atzinīgi vērtē centienus atvieglot piekļuvi tiesiskajai aizsardzībai pret Korejas valsts drošības iestādēm. Tajā pašā laikā EDAK iestājas par to, lai šāds atsauces mehānisms tiktu virzīts caur Eiropas valstu datu aizsardzības iestādēm, nevis caur EDAK, jo tās ir kompetentas un tām ir tuvāks fizisko personu sūdzību izskatīšanas process.

188. Turklāt EDAK atzīmē iespējamo pretrunu attiecībā uz brīvprātīgu informācijas izpaušanu. No vienas puses, lēmuma projektā ir teikts, ka fiziskas personas var saņemt kompensāciju, ja to dati tiek izpausti nelikumīgi pēc pieprasījuma par brīvprātīgu izpaušanu, tostarp prasību iesniedzot pret tiesībaizsardzības iestādi, kas izsniegusi pieprasījumu[94]. Savukārt lēmuma projektā ir atsauce uz tiešas ietekmes prasību attiecībā uz fiziskas personas tiesībām apstrīdēt valsts iestāžu rīcību, kā piemēru uzskaitot (tikai) saistošus informācijas izpaušanas pieprasījumus gadījumam, kad administratīvā darbība uzskatāma par tiešu ietekmi uz privātuma tiesībām[95]. EDAK no Eiropas Komisijas

[92] Skatīt II pielikuma 3.2.4. punktu saistībā ar 2.4.3. punktu.
[93] Skatīt lēmuma projekta 205. apsvērumu un I pielikuma 19. pantu.
[94] Skatīt lēmuma projekta 166. apsvērumu.
[95] Skatīt lēmuma projekta 181. apsvērumu (tiesībaizsardzība) un 208. un 181. apsvērumu (valsts drošība).

paskaidrojumiem saprot, ka faktiski tiesiskās aizsardzības iespējām nav nekādu ierobežojumu attiecībā uz brīvprātīgas izpaušanas pieprasījumiem, un tāpēc lūdz Eiropas Komisiju to sīkāk paskaidrot lēmumā gan tiesībaizsardzības, gan valsts drošības jomā (atšķirībā no sadaļas par tiesībaizsardzību sadaļa par brīvprātīgu informācijas izpaušanu valsts drošības nolūkos šajā kontekstā nesatur nekādu skaidru paziņojumu par tiesisko aizsardzību).