



Eiropas Savienības
Padome

Briselē, 2024. gada 22. janvārī
(OR. en)

5454/24

DATAPROTECT 23
JAI 62
RELEX 42

PAVADVĒSTULE

Sūtītājs:	Eiropas Komisijas ģenerālsēkretāre, parakstījusi direktore <i>Martine DEPREZ</i>
Saņēmējs:	Eiropas Savienības Padomes ģenerālsēkretāre <i>Thérèse BLANCHET</i>
K-jas dok. Nr.:	COM(2024) 7 final
Temats:	KOMISIJAS ZIŅOJUMS EIROPAS PARLAMENTAM UN PADOMEI, par to lēmumu par aizsardzības līmeņa pietiekamību darbības pirmo pārskatīšanu, kuri pieņemti saskaņā ar Direktīvas 95/46/EK 25. panta 6. punktu

Pielikumā ir pievienots dokuments COM(2024) 7 *final*.

Pielikumā: COM(2024) 7 *final*



Briselē, 15.1.2024.
COM(2024) 7 final

KOMISIJAS ZIŅOJUMS EIROPAS PARLAMENTAM UN PADOMEI,
par to lēmumu par aizsardzības līmeņa pietiekamību darbības pirmo pārskatīšanu, kuri
pieņemti saskaņā ar Direktīvas 95/46/EK 25. panta 6. punktu

{SWD(2024) 3 final}

1. PIRMĀ PĀRSKATĪŠANA — PAMATINFORMĀCIJA UN KONTEKSTS

Šajā ziņojumā ir ietverti Komisijas konstatējumi par pirmo pārskatīšanu attiecībā uz lēmumiem par aizsardzības līmeņa pietiekamību, kuri pieņemti, pamatojoties uz Direktīvas 95/46/EK¹ (Datu aizsardzības direktīva) 25. panta 6. punktu.

Šajos lēmumos Komisija noteica, ka pienācīgu aizsardzības līmeni personas datiem, kas tiek nosūtīti no Eiropas Savienības (ES), nodrošina vienpadsmit valstis vai teritorijas²: Andora³, Argentīna⁴, Kanāda (komerciālajiem operatoriem)⁵, Fēru Salas⁶, Gērnsija⁷, Menas Sala⁸, Izraēla⁹, Džērsija¹⁰, Jaunzēlande¹¹, Šveice¹² un Urugvaja¹³. Tādējādi datu nosūtīšanu no ES uz šīm valstīm un teritorijām var veikt bez papildu prasībām.

2018. gada 25. maijā stājoties spēkā Regulai (ES) 2016/679¹⁴ (VDAR), nemainīgi palika spēkā arī lēmumi par aizsardzības līmeņa pietiekamību, kas pieņemti saskaņā ar Datu aizsardzības direktīvu¹⁵. Turklāt VDAR ir precizēts, ka pietiekamības atzinumi ir “adaptīvi instrumenti”, norādot, ka Komisijai trešās valstīs ir pastāvīgi jāuzrauga norises, kas varētu ietekmēt esošo

¹ Eiropas Parlamenta un Padomes Direktīva 95/46/EK (1995. gada 24. oktobris) par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (OV L 281, 23.11.1995., 31. lpp.).

² VDAR piemēro arī Norvēģijai, Islandei un Lihtenšteinai pēc to iekļaušanas Līgumā par Eiropas Ekonomikas zonu (EEZ). Atsauces uz ES šajā ziņojumā būtu jāsaprot arī kā atsauces uz EEZ valstīm.

³ Komisijas 2010. gada 19. oktobra Lēmums 2010/625/ES par personas datu pienācīgu aizsardzību Andorā atbilstīgi Eiropas Parlamenta un Padomes Direktīvai 95/46/EK (OV L 277, 21.10.2010., 27. lpp.).

⁴ Komisijas 2003. gada 30. jūnija Lēmums 2003/490/EK atbilstīgi Eiropas Parlamenta un Padomes Direktīvai 95/46/EK par personas datu pienācīgu aizsardzību Argentīnā (OV L 168, 5.7.2003., 19. lpp.).

⁵ Komisijas 2001. gada 20. decembra Lēmums 2002/2/EK par personas datu pienācīgu aizsardzību, kas noteikta Kanādas likumā par personas datu un elektronisko dokumentu aizsardzību, atbilstīgi Eiropas Parlamenta un Padomes Direktīvai 95/46/EK (OV L 2, 4.1.2002., 13. lpp.).

⁶ Komisijas 2010. gada 5. marta Lēmums 2010/146/ES atbilstīgi Eiropas Parlamenta un Padomes Direktīvai 95/46/EK par personas datu pienācīgu aizsardzību saskaņā ar Fēru salu likumu par personas datu apstrādi (OV L 58, 9.3.2010., 17. lpp.).

⁷ Komisijas 2003. gada 21. novembra Lēmums 2003/821/EK par atbilstīgu personas datu aizsardzību Gērnsijā (OV L 308, 25.11.2003., 27. lpp.).

⁸ Komisijas 2004. gada 28. aprīļa Lēmums 2004/411/EK par pietiekamu personas datu aizsardzību Menas salā (OV L 151, 30.4.2004., 48. lpp.).

⁹ Komisijas 2011. gada 31. janvāra Lēmums 2011/61/ES par personas datu pienācīgu aizsardzību Izraēlā atbilstīgi Eiropas Parlamenta un Padomes Direktīvai 95/46/EK attiecībā uz personas datu automatizētu apstrādi (OV L 27, 1.2.2011., 39. lpp.).

¹⁰ Komisijas 2008. gada 8. maija Lēmums 2008/393/EK atbilstīgi Eiropas Parlamenta un Padomes Direktīvai 95/46/EK par personas datu pienācīgu aizsardzību Džērsijā (OV L 138, 28.5.2008., 21. lpp.).

¹¹ Komisijas 2012. gada 19. decembra Īstenošanas lēmums 2013/65/ES par personas datu pienācīgu aizsardzību Jaunzēlandē atbilstīgi Eiropas Parlamenta un Padomes Direktīvai 95/46/EK attiecībā uz personas datu automatizētu apstrādi (OV L 28, 30.1.2013., 12. lpp.).

¹² Komisijas 2000. gada 26. jūlija Lēmums 2000/518/EK atbilstīgi Eiropas Parlamenta un Padomes Direktīvai 95/46/EK par tādu personas datu pienācīgu aizsardzību Šveicē (OV L 215, 25.8.2000., 1. lpp.).

¹³ Komisijas 2012. gada 21. augusta Īstenošanas lēmums 2012/484/ES par personas datu pietiekamu aizsardzību Urugvajas Austrumu Republikā attiecībā uz personas datu automatizētu apstrādi atbilstīgi Eiropas Parlamenta un Padomes Direktīvai 95/46/EK (OV L 227, 23.8.2012., 11. lpp.).

¹⁴ Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp.).

¹⁵ Sk. VDAR 45. panta 9. punktu, kurā noteikts, ka lēmumi, ko Komisija pieņemusi, pamatojoties uz Direktīvas 95/46/EK 25. panta 6. punktu, ir spēkā, kamēr tos negroza, neizstāj vai neatceļ ar Komisijas lēmumu, kas pieņemts saskaņā ar 45. panta 3. vai 5. punktu.

lēmumu par aizsardzības līmeņa pietiekamību darbību¹⁶. Papildus tam VDAR 97. pantā ir noteikts, ka Komisijai periodiski — reizi četros gados — ir jāpārskata šie lēmumi, lai konstatētu, vai valstis un teritorijas, kas saņēmušas pietiekamības atzinumus, joprojām nodrošina pietiekamu personas datu aizsardzības līmeni.

Šī pirmā pārskatīšana attiecībā uz lēmumiem par aizsardzības līmeņa pietiekamību, kas pieņemti saskaņā ar iepriekšējo ES datu aizsardzības regulējumu, tika uzsākta kā daļa no plašāka novērtējuma par VDAR piemērošanu un darbību, par kuru konstatējumus Komisija sniedza savā paziņojumā “Datu aizsardzība kā iedzīvotāju tiesību nodrošināšanas un ES digitālās pārkārtošanās pīlārs — Vispārīgās datu aizsardzības regulas piemērošanas divi gadi”¹⁷. Tomēr secinājumu izdarīšana attiecībā uz šo pārskatīšanas aspektu tika atlikta, lai varētu ņemt vērā Tiesas spriedumu lietā *Schrems II*¹⁸, kurā Tiesa sniedza būtiskus precizējumus par pietiekamības standarta galvenajiem elementiem, kā arī citas saistītās norises. Savukārt tā rezultātā tika īstenota detalizēta informācijas apmaiņa ar attiecīgajām valstīm un teritorijām par viņu tiesiskā regulējuma, pārraudzības mehānismu un izpildes sistēmas saistītajiem aspektiem¹⁹. Šajā ziņojumā ir pilnībā ņemtas vērā visas minētās norises gan ES, gan attiecīgajās trešās valstīs un teritorijās.

Svarīgi atzīmēt, ka šī pirmā pārskatīšana tiek veikta arvien straujākas digitālo tehnoloģiju attīstības kontekstā. Pēdējās desmitgadēs ir ievērojami palielinājusies lēmumu par aizsardzības līmeņa pietiekamību nozīmīgums, jo datu plūsmas ir kļuvušas par sabiedrības digitālās pārkārtošanās un ekonomikas globalizācijas neatņemamu sastāvdaļu. Datu nosūtīšana ārpus Savienības robežām ir kļuvusi par daļu no ikdienas darbībām visu lielumu un nozaru Eiropas uzņēmumos. Vairāk nekā jebkad agrāk personas privātuma ievērošana ir nosacījums, kas ir jāievēro, lai nodrošinātu stabilas, drošas un konkurētspējīgas komerciālo datu plūsmas. Šajā kontekstā lēmumiem par aizsardzības līmeņa pietiekamību daudzējādā ziņā ir arvien nozīmīgāka loma. Nodrošinot nosūtīto datu aizsardzību, ar tiem tiek garantētas drošas datu plūsmas, tādējādi ievērojot personu tiesības saskaņā ar ES cilvēkorientēto pieeju, ko izmanto digitālās pārkārtošanās procesā. Atzīstot trešo valstu privātuma regulējumus, kas nodrošina aizsardzības līmeni, kurš būtībā ir līdzvērtīgs [ekvivalents] ES nodrošinātajam līmenim, ar tiem tiek veicināta uz augstiem aizsardzības standartiem balstītu privātuma sistēmu konverģence. Turklāt, kā paskaidrots šajā ziņojumā, lēmumi par aizsardzības līmeņa pietiekamību nav tikai galarezultāts, bet ar tiem ir arī likts pamats ciešākai sadarbībai un plašākai regulatīvajai konverģencei starp ES un līdzīgi domājošiem partneriem. Ar šiem lēmumiem, nodrošinot personas datu brīvu plūsmu, ES operatoriem ir pavērti komerciāli kanāli, citastarp papildinot un pastiprinot tirdzniecības nolīgumu sniegtos ieguvumus, kā arī ir atvieglota sadarbība ar

¹⁶ VDAR 45. panta 4. punkts. Sk. arī ES Tiesas 2015. gada 6. oktobra spriedumu *Maximilian Schrems / Data Protection Commissioner (Schrems I)*, C-362/14, ECLI:EU:C:2015:650, 76. punktu.

¹⁷ Paziņojums tika publicēts 2020. gada jūnijā un ir pieejams šādā saitē: https://ec.europa.eu/info/law/law-topic/data-protection/communication-two-years-application-general-data-protection-regulation_en

¹⁸ ES Tiesas 2020. gada 16. jūlija spriedumu lietā C-311/18 *Data Protection Commissioner / Facebook Ireland Ltd. un Maximilian Schrems* (“Schrems II”), ECLI:EU:C:2020:559.

¹⁹ Lēmums par aizsardzības līmeņa pietiekamību attiecībā uz Japānu tika pieņemts, pamatojoties uz VDAR, un tajā paredzēta atsevišķa periodiska pārskatīšana. Pirmo pārskatīšana tika pabeigta 2023. gada aprīlī ar Komisijas ziņojumu Eiropas Parlamentam un Padomei par pirmo pārskatīšanu attiecībā uz to, kā darbojas lēmums par aizsardzības līmeņa pietiekamību Japānā, COM(2023) 275 final, pieejams vietnē: <https://eur-lex.europa.eu/legal-content/LV/TXT/PDF/?uri=COM:2023:275:FIN>.

ārvalstu partneriem plašā regulatīvo jomu diapazonā. Nodrošinot vienkāršu un visaptverošu datu nosūtīšanas risinājumu, kas neprasa datu nosūtītājam sniegt papildu garantijas [aizsardzības pasākumus] vai iegūt kādas atļaujas, ar tiem tiek veicināta uzņēmumu — jo īpaši mazo un vidējo uzņēmumu — atbilstība VDAR noteiktajām starptautiskās nosūtīšanas prasībām. Visbeidzot, pateicoties to tīklveida darbībai, Eiropas Komisijas pieņemtie lēmumi par aizsardzības līmeņa pietiekamību kļūst arvien nozīmīgāki arī ārpus ES, jo ar tiem tiek nodrošināta brīva datu aprīte ne tikai ar 30 ES ekonomikām, bet arī ar daudzām citām tādām jurisdikcijām visā pasaulē²⁰, kas saskaņā ar saviem datu aizsardzības noteikumiem atzīst, ka valstis, attiecībā uz kurām ir pieņemts ES lēmums par aizsardzības līmeņa pietiekamību, ir droši galamērķi.

Visu iepriekš minēto iemeslu dēļ, kā apstiprināja arī aktīvais un auglīgais dialogs ar attiecīgajām trešām valstīm/teritorijām, uz kurām attiecas šī pārskatīšana, lēmumi par aizsardzības līmeņa pietiekamību ir kļuvuši par stratēģisku sastāvdaļu ES vispārējās attiecībās ar šiem ārvalstu partneriem un tiek atzīti par būtisku veicinošu faktoru sadarbības padziļināšanai dažādās jomās. Tādēļ ir īpaši svarīgi, lai šie lēmumi izturētu laika pārbaudi un tajos tiktu ņemtas vērā jaunas norises un problēmas.

2. PĀRSKATĪŠANAS MĒRĶIS UN METODIKA

Lēmumi par aizsardzības līmeņa pietiekamību, kas tiek aplūkoti šajā pārskatīšanā, ir pieņemti saskaņā ar ES datu aizsardzības regulējumu, kas bija spēkā pirms VDAR. Jaunākie lēmumi tika pieņemti aptuveni pirms 10 gadiem (piem., lēmums par Jaunzēlandi un lēmums par Urugvaju, abi pieņemti 2012. gadā), savukārt citi ir spēkā jau vairāk nekā 20 gadus (piem., par Kanādu un par Šveici, pieņemti attiecīgi 2001. un 2000. gadā). Kopš tā laika datu aizsardzības regulējumi visās 11 valstīs un teritorijās ir attīstījušies, piemēram, ar leģislatīvām vai regulatīvām reformām, norisēm datu aizsardzības iestāžu izpildes praksē vai judikatūrā.

Tādēļ, veicot šo novērtējumu, Komisija koncentrējās uz tādām norisēm attiecīgo valstu un teritoriju datu aizsardzības regulējumos, kas notikušas kopš attiecīgā lēmuma par aizsardzības līmeņa pietiekamību pieņemšanas. Komisija izvērtēja, kā šīs norises ir mainījušas attiecīgās valsts vai teritorijas datu aizsardzības ainu un vai, ņemot vērā minētās norises, dažādie režīmi joprojām nodrošina pietiekamu aizsardzības līmeni.

Šajā kontekstā tika rūpīgi aplūkoti arī pašas ES datu aizsardzības režīma attīstība, jo īpaši saistībā ar VDAR stāšanos spēkā. Konkrētāk, kopš šo lēmumu par aizsardzības līmeņa pietiekamību pieņemšanas Eiropas Savienības Tiesas judikatūrā un norādījumos, kurus pieņēma 29. panta darba grupa un apstiprināja tās pēctece Eiropas Datu aizsardzības kolēģija (EDAK)²¹, ir sniegti papildu precizējumi par juridisko standartu, kas piemērojams šādiem lēmumiem, kā arī par būtiskajiem elementiem, kuri ir jāņem vērā, izvērtējot, vai attiecīgā ārvalstu sistēma nodrošina pietiekamu aizsardzības līmeni.

²⁰ Piem., ar Argentīnu, Izraēlu, Kolumbiju, Maroku, Šveici un Urugvaju.

²¹ Eiropas Datu aizsardzības kolēģijā tiekas dalībvalstu datu aizsardzības uzraudzības iestāžu pārstāvji un Eiropas Datu aizsardzības uzraudzītājs.

Tiesa savā 2015. gada 6. oktobra spriedumā *Schrems I* konstatēja, ka, lai gan nevar prasīt, lai trešā valsts nodrošinātu aizsardzības līmeni, kas būtu identisks Savienības tiesiskajā kārtībā nodrošinātajam, pietiekamības pārbaude ir jāsaprot kā tāda, kurā nosaka būtībā ekvivalentu aizsardzības līmeni²². Konkrētāk, Tiesa precizēja, ka attiecīgās trešās valsts izmantotie līdzekļi personas datu aizsardzībai var atšķirties no Savienībā izmantotajiem, ja vien tie praksē efektīvi nodrošina pietiekamu aizsardzības līmeni²³. Tādējādi pietiekamības pārbaude ietver visaptverošu novērtējumu par trešās valsts sistēmu kopumā, t. sk. par privātuma aizsardzības līdzekļu būtību, to efektīvu īstenošanu un izpildi.

Turklāt Tiesa precizēja, ka Komisijas veiktajam novērtējumam nevajadzētu aprobežoties tikai ar trešās valsts vispārējo datu aizsardzības regulējumu, bet tajā vajadzētu ietvert arī noteikumus, ar kuriem reglamentē publisko iestāžu piekļuvi personas datiem, jo īpaši tiesībaizsardzības un valsts drošības nolūkos²⁴. Izmantojot Pamattiesību hartu kā etalonu, Tiesa noteica vairākas prasības, kurām šiem noteikumiem ir jāatbilst, lai tiktu izpildīts standarts “būtībā ekvivalents”. Piemēram, šīs jomas tiesiskajā regulējumā ir jāparedz skaidri un precīzi noteikumi, ar ko tiktu reglamentēts attiecīgā pasākuma apjoms un piemērošana un tiktu noteiktas minimālās prasības [garantijas] tādējādi, lai personām, kuru personas dati ir skarti, būtu pietiekamas garantijas, kas ļautu to personas datus efektīvi aizsargāt pret ļaunprātīgas izmantošanas risku, kā arī pret jebkādu nelikumīgu piekļuvi šiem datiem un to nelikumīgu izmantošanu²⁵. Tāpat tajā ir jāparedz iespējas indivīdiem [personām] likt lietā tiesību aizsardzības līdzekļus, lai piekļūtu personas datiem, kas uz tiem attiecas, vai panākt šādu datu labošanu vai dzēšanu²⁶.

VDAR ir izmantoti Tiesas sniegtie precizējumi, izveidojot detalizētu to elementu katalogu, kuri Komisijai jāņem vērā, veicot pietiekamības novērtējumu²⁷. Turklāt Tiesa 2020. gada 16. jūlija spriedumā *Schrems II* ir sīkāk aprakstījusi “būtībā ekvivalents” standartu, jo īpaši attiecībā uz noteikumiem par publisko iestāžu piekļuvi personas datiem tiesībaizsardzības un valsts drošības nolūkos. Konkrēti, tā ir precizējusi, ka “būtībā ekvivalents” standarts paredz, ka attiecīgais tiesiskais regulējums, kas ir saistošs publiskajām iestādēm attiecīgajās trešās valstīs un teritorijās, ietver minimālās garantijas, kas nodrošina, ka šādas iestādes var piekļūt tikai tiem datiem, kas ir nepieciešami un samērīgi, lai sasniegtu leģitīmus mērķus, un datu subjektiem ir faktiskas un izpildes ziņā panākamās tiesības pret šādām iestādēm²⁸.

Pietiekamības standarta interpretācijas attīstība ir atspoguļota arī norādījumos, kurus sākotnēji pieņēma 29. panta darba grupa un pēc tam apstiprināja EDAK²⁹. Šajos norādījumi, jo īpaši t. s. “pietiekamības atsaucēs”, ir sīkāk paskaidroti elementi, kuri Komisijai ir jāņem vērā, veicot aizsardzības līmeņa pietiekamības novērtējumu, t. sk., ir sniegts pārskats par būtiskajām garantijām saistībā ar publisko iestāžu piekļuvi personas datiem. Tajos jo īpaši tika izmantota

²² *Schrems I*, 73., 74. un 96. punkts. Sk. arī Regulas (ES) 2016/679 104. apsvērumu, kurā minēts standarts “pēc būtības ir līdzvērtīgs”.

²³ *Schrems I*, 74. punkts.

²⁴ *Schrems I*, 90. punkts.

²⁵ *Schrems I*, 91. punkts.

²⁶ *Schrems I*, 95. punkts.

²⁷ VDAR 45. panta 2. punkts.

²⁸ *Schrems II*, 180., 181. un 182. punkts.

²⁹ Pietiekamības atsaucēs, WP 254 rev. 01, 2018. gada 6. februāris (pieejamas šādā saitē: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108)

Eiropas Cilvēktiesību tiesas judikatūra, un tos vēlāk atjaunināja EDAK, lai ņemtu vērā Tiesas sniegtos precizējumus spriedumā *Schrems II*³⁰. Svarīgi atzīmēt, ka pietiekamības atsaucēs ir arī atzīts, ka standarts “būtībā ekvivalents” nenozīmē ES noteikumu precīzu atspoguļojumu (kopiju), jo līdzekļi līdzvērtīga aizsardzības līmeņa nodrošināšanai dažādās privātuma aizsardzības sistēmās var atšķirties, tādējādi bieži vien atspoguļojot to atšķirīgās tiesiskās tradīcijas.

Tādēļ, lai noteiktu, vai minētie 11 lēmumi par aizsardzības līmeņa pietiekamību, kas tika pieņemti saskaņā ar iepriekšējiem noteikumiem, joprojām atbilst VDAR noteiktajam standartam, Komisija ir ņēmusi vērā ne tikai datu aizsardzības regulējumu attīstību attiecīgajās valstīs un teritorijās, bet arī paša pietiekamības standarta interpretācijas attīstību saskaņā ar ES tiesību aktiem. Tas ietver arī novērtējumu par tiesisko regulējumu, ar ko reglamentē publisko iestāžu piekļuvi personas datiem, kuri nosūtīti no ES, un šādu datu izmantošanu valstīs un teritorijās, par kurām, pamatojoties uz Datu aizsardzības direktīvas 25. panta 6. punktu, tika sniegts atzinums, ka tās nodrošina pietiekamu aizsardzības līmeni.

3. PĀRSKATĪŠANAS PROCESS

Kā aprakstīts iepriekš, attiecībā uz katru minēto valsti vai teritoriju veiktais esošā lēmuma par aizsardzības līmeņa pietiekamību novērtējums aptver datu aizsardzības regulējumu un visas norises, kas attiecībā uz šo tiesisko regulējumu ir notikušas kopš pietiekamības atzinuma [lēmuma] pieņemšanas, kā arī noteikumus, ar kuriem reglamentē valdības piekļuvi datiem, jo īpaši tiesībaizsardzības un valsts drošības nolūkos. Pēdējos gados Komisijas dienesti ir īstenojuši vairākus pasākumus, lai veiktu šādu novērtējumu, ciešā sadarbībā ar katru no attiecīgajām valstīm vai teritorijām.

Lai palīdzētu Komisijai izpildīt tās uzraudzības pienākumus, katra no 11 valstīm vai teritorijām sniedza tai izsmeļošu informāciju par norisēm savā datu aizsardzības režīmā kopš lēmuma par aizsardzības līmeņa pietiekamību pieņemšanas. Papildus tam Komisija katrai no 11 valstīm vai teritorijām lūdza detalizētu informāciju par attiecīgajā valstī vai teritorijā piemērojamajiem noteikumiem attiecībā uz valdības piekļuvi personas datiem, jo īpaši tiesībaizsardzības un valsts drošības nolūkos. Informāciju par lēmumu darbību un norisēm, kas saistītas ar katras attiecīgās valsts un teritorijas tiesību aktiem un praksi gan attiecībā uz datu aizsardzības noteikumiem, kas piemērojami privātajiem operatoriem, gan attiecībā uz valdības piekļuvi, Komisija ieguva arī no publiskajiem avotiem, pārraudzības un izpildes iestādēm, kā arī vietējiem ekspertiem. Visbeidzot, attiecīgā gadījumā ir pienācīgi ņemtas vērā starptautiskās saistības, ko šīs valstis/teritorijas ir uzņēmušās saskaņā ar reģionāliem vai universālajiem instrumentiem.

Pamatojoties uz to, Komisija ir iesaistījusies intensīvā dialogā ar katru attiecīgo valsti un teritoriju. Saistībā ar šo dialogu daudzas minētās valstis un teritorijas ir modernizējušas un nostiprinājušas savus tiesību aktus privātuma jomā, veicot visaptverošas vai daļējas reformas (piemēram, Andora, Kanāda, Fēru Sala, Šveice, Jaunzēlande), ko cita starpā veicināja vajadzība

³⁰ Ieteikumi 02/2020 attiecībā uz Eiropas būtiskajām garantijām uzraudzības pasākumiem (pieejami šādā saitē: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_lv)

nodrošināt lēmumu par aizsardzības līmeņa pietiekamību nepārtrauktību. Dažas no šīm valstīm ir pieņēmušas vietējās datu aizsardzības iestādes izstrādātus noteikumus un/vai norādījumus, lai ieviestu jaunas datu aizsardzības prasības (piem., Izraēla, Urugvaja) vai, pamatojoties uz izpildes praksi vai judikatūru, precizētu noteiktus privātuma noteikumus (piem., Argentīna, Kanāda, Gērnsija, Džērsija, Menas Sala, Izraēla, Jaunzēlande). Turklāt, lai novērstu attiecīgās aizsardzības līmeņa atšķirības, ar dažām no šīm valstīm un teritorijām tika apspriestas un saskaņotas papildu garantijas no Eiropas nosūtītajiem personas datiem, ja tādas bija nepieciešamas pietiekamības lēmumu nepārtrauktības nodrošināšanai. Piemēram, Kanādas valdība paplašināja piekļuves un labošanas tiesības attiecībā uz personas datiem, kurus apstrādā publiskais sektors, lai tās aptvertu visas personas neatkarīgi no to valstspiederības vai dzīvesvietas (šādas tiesības iepriekš bija tikai Kanādas pilsoņiem, pastāvīgajiem iedzīvotājiem vai personām, kuras uzturas Kanādā)³¹. Vēl viens piemērs: Izraēlas valdība ieviesa īpašas garantijas, lai pastiprinātu no Eiropas Ekonomikas zonas nosūtīto personas datu aizsardzību, jo īpaši nosakot jaunus pienākumus datu precizitātes un datu saglabāšanas jomā, nostiprinot tiesības uz informācijas ieguvu un dzēšanu un ieviešot sensitīvo datu papildu kategorijas³².

Paralēli tam Komisijas dienesti apkopoja viedokļus par novērtējumu un par tajā panākto progresu regulāri informēja Eiropas Parlamentu (Pilsoņu brīvību, tieslietu un iekšlietu komiteju)³³, Padomi (ar Informācijas apmaiņas un datu aizsardzības jautājumu darba grupas starpniecību)³⁴, Eiropas Datu aizsardzības kolēģiju (EDAK)³⁵ un VDAR Daudzpusējo ekspertu grupu³⁶ (kas ietver pilsoniskās sabiedrības, nozaru, akadēmisko aprindu pārstāvjus un praktizējošus juristus).

Tādējādi šis ziņojums un tam pievienotais Komisijas dienestu darba dokuments (DDD) ir sagatavots, cieši sadarbojoties ar katru no attiecīgajām valstīm un teritorijām, kā arī apspriežoties ar saistītajām ES iestādēm un struktūrām un saņemot atsauksmes no tām. To sagatavošanā ir izmantoti dažādi avoti, t. sk. tiesību akti, regulatīvie akti, judikatūra, datu aizsardzības iestāžu lēmumi un norādījumi, (neatkarīgu) pārraudzības struktūru ziņojumi un ieinteresēto personu sniegtā informācija. Pirms šā ziņojuma pieņemšanas visām iepriekš minētajām valstīm un teritorijām tika dota iespēja pārbaudīt, vai DDD sniegtā informācija par viņu sistēmu ir faktu ziņā precīza.

³¹ Likuma par privātās dzīves aizsardzību 12. iedaļa, Likuma par privātās dzīves aizsardzību Paplašināšanas rīkojums Nr. 1 un Nr. 2.

³² Privātās dzīves aizsardzības noteikumi (Norādījumi attiecībā uz datiem, kas Izraēlai nosūtīti no Eiropas Ekonomikas zonas), 5783-2023, publicēti Izraēlas oficiālajā vēstnesī (*Reshumut*) 2023. gada 7. maijā.

³³ Sk., piem., Eiropas Parlamenta 2021. gada 25. marta rezolūciju par Komisijas izvērtēšanas ziņojumu par Vispārīgās datu aizsardzības regulas īstenošanu divus gadus pēc tās piemērošanas sākuma (2020/2717(RSP)), pieejama šādā saitē: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_LV.html

³⁴ Sk., piem., Padomes viedokli un atzinumus par Vispārīgās datu aizsardzības regulas (VDAR) piemērošanu, kas pieņemti 2019. gada 19. decembrī, pieejami šādā saitē: <https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-1/lv/pdf>

³⁵ Sk., piem., EDAK sagatavoto kopsavilkumu attiecībā uz VDAR novērtējumu saskaņā ar 97. pantu, kas pieņemts 2020. gada 18. februārī un pieejams šādā saitē: https://edpb.europa.eu/sites/default/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf

³⁶ Sk., piem., Daudzpusējās ekspertu grupas ziņojumu par VDAR novērtējumu, kas pieejams šādā saitē: <https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=en&do=groupDetail.groupMeeting&meetingId=21356>.

4. GALVENIE KONSTATĒJUMI UN SECINĀJUMI

Pirmā pārskatīšana parādīja, ka kopš lēmumu par aizsardzības līmeņa pietiekamību pieņemšanas spēkā esošie datu aizsardzības regulējumi katrā no minētajām 11 valstīm vai teritorijām ir vēl vairāk pieskaņoti ES regulējumam. Turklāt attiecībā uz valdības piekļuvi personas datiem pirmā pārskatīšana apliecināja, ka šo valstu vai teritoriju tiesību aktos ir paredzētas atbilstošas garantijas un ierobežojumi un ir nodrošināti pārraudzības un tiesiskās aizsardzības mehānismi šajā jomā.

Detalizēta informācija par konstatējumiem attiecībā uz katru no 11 valstīm vai teritorijām ir sniegta Komisijas dienestu darba dokumentā, kas pievienots šim ziņojumam. Balstoties uz šiem konstatējumiem, Komisija secina, ka katra no šīm 11 valstīm un teritorijām joprojām nodrošina VДАР izpratnē un atbilstoši Tiesas interpretācijai pietiekamu aizsardzības līmeni personas datiem, kas tiek nosūtīti no Eiropas Savienības. Tālāk apkopoti konstatējumi par katru no attiecīgajām valstīm un teritorijām.

4.1. *Andora*

Komisija atzinīgi vērtē norises saistībā ar Andoras tiesisko regulējumu, kas ir notikušas kopš lēmuma par aizsardzības līmeņa pietiekamību pieņemšanas, t. sk. grozījumus tiesību aktos un uzraudzības struktūru veiktās darbības. Konkrētāk, pieņemot Kvalificēto likumu Nr. 29/2021 par personas datu aizsardzību, kas stājās spēkā 2022. gada maijā, tika veicināts augstāks datu aizsardzības līmenis, jo Likums savas struktūras un galveno elementu ziņā ir cieši saskaņots ar VДАР.

Attiecībā uz valdības piekļuvi personas datiem ir noteikts, ka uz Andoras publiskajām iestādēm attiecas skaidri, precīzi un pieejami noteikumi, saskaņā ar kuriem šādas iestādes var piekļūt no ES nosūtītiem datiem un pēc tam tos izmantot sabiedrības interesēs esošu mērķu sasniegšanai, jo īpaši krimināltiesību aizsardzības un valsts drošības nolūkos. Šie ierobežojumi un garantijas izriet no visaptverošā tiesiskā regulējuma un starptautiskajām saistībām, jo īpaši no Andoras konstitūcijas, Eiropas Cilvēktiesību konvencijas (ECTK) un Eiropas Padomes Konvencijas par personu aizsardzību attiecībā uz personas datu automātisko apstrādi (Konvencija Nr. 108 un grozījumu protokols, ar ko izveido modernizēto Konvenciju 108+), kā arī no konkrētiem datu aizsardzības noteikumiem, ko piemēro personas datu apstrādei tiesībaizsardzības kontekstā un kuros būtībā atkārtoti Direktīvas (ES) 2016/680³⁷ galvenie elementi. Papildus tam Andoras tiesību aktos ir paredzēta virkne īpašu nosacījumu un ierobežojumu attiecībā uz publisko iestāžu piekļuvi personas datiem un to izmantošanu, kā arī ar tiem tiek nodrošināti pārraudzības un tiesiskās aizsardzības mehānismi šajā jomā.

Balstoties uz vispārējiem konstatējumiem, kas izklāstīti DDD, Komisija secina, ka Andora joprojām nodrošina pietiekamu aizsardzības līmeni personas datiem, kas tiek nosūtīti no ES.

³⁷ Eiropas Parlamenta un Padomes Direktīva (ES) 2016/680 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu kriminālsodus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI.

Attiecībā uz īpašajiem datu aizsardzības noteikumiem, kas pašlaik tiek piemēroti tiesībaizsardzības iestāžu veiktai datu apstrādei, Komisija atzinīgi vērtē Andoras likumdevēja nodomu šos noteikumus aizvietot ar visaptverošāku režīmu, kas būs vēl ciešāk saskaņots ar noteikumiem, kurus piemēro Eiropas Savienībā. Komisija cieši uzraudzīs turpmākās norises šajā jomā.

4.2. Argentīna

Komisija atzinīgi vērtē norises saistībā ar Argentīnas tiesisko regulējumu, kas ir notikušas kopš lēmuma par aizsardzības līmeņa pietiekamību pieņemšanas, t. sk. grozījumus tiesību aktos, judikatūru un pārraudzības struktūru veiktās darbības, kas ir veicinājušas augstāku datu aizsardzības līmeni. Konkrētāk, tika būtiski nostiprināta Argentīnas datu aizsardzības uzraudzības iestādes neatkarība, pieņemot Dekrētu Nr. 746/17, ar kuru *Agencia de Acceso a la Información Pública (AAIP)* tika uzticēts pienākums pārraudzīt atbilstību datu aizsardzības tiesību aktiem. Papildus tam *AAIP* izdeva virkni saistošu noteikumu un atzinumu, kuros precizēts, kā datu aizsardzības regulējums ir jāinterpretē un jāpiemēro praksē, tādējādi palīdzot nodrošināt, ka datu aizsardzības tiesību akti tiek regulāri atjaunināti. Argentīna arī pastiprināja savas starptautiskās saistības datu aizsardzības jomā, 2019. gadā pievienojoties Eiropas Padomes Konvencijai par personu aizsardzību attiecībā uz personas datu automātisko apstrādi un tās Papildu protokolam un 2023. gadā ratificējot Grozījuma protokolu, ar kuru izveido modernizēto Konvenciju Nr. 108+.

Attiecībā uz valdības piekļuvi personas datiem ir noteikts, ka uz Argentīnas publiskajām iestādēm attiecas skaidri, precīzi un pieejami noteikumi, saskaņā ar kuriem šādas iestādes var piekļūt no ES nosūtītiem datiem un pēc tam tos izmantot sabiedrības interesēs esošu mērķu sasniegšanai, jo īpaši krimināltiesību aizsardzības un valsts drošības nolūkos. Šie ierobežojumi un garantijas izriet no visaptverošā tiesiskā regulējuma un starptautiskajām saistībām, jo īpaši no Argentīnas Konstitūcijas, Amerikas Cilvēktiesību Konvencijas, Konvencijas Nr. 108 un Konvencijas Nr. 108+, kā arī no Argentīnas datu aizsardzības noteikumiem (2000. gada 4. oktobra Personas datu aizsardzības akts Nr. 25.326), kas attiecas arī uz Argentīnas publisko iestāžu veiktu personas datu apstrādi, citastarp tiesībaizsardzības un valsts drošības nolūkos. Papildus tam Argentīnas tiesību aktos ir paredzēta virkne īpašu nosacījumu un ierobežojumu attiecībā uz piekļuvi personas datiem un to izmantošanu krimināltiesību aizsardzības un valsts drošības nolūkos, kā arī ar tiem tiek nodrošināti pārraudzības un tiesiskās aizsardzības mehānismi šajā jomā.

Balstoties uz vispārējiem konstatējumiem, kas izklāstīti DDD, Komisija secina, ka Argentīna joprojām nodrošina pietiekamu aizsardzības līmeni personas datiem, kas tiek nosūtīti no ES.

Tomēr Komisija iesaka tiesību aktos iekļaut aizsardzības līdzekļus, kas jau ir noteikti zemāka līmeņa aktos, lai uzlabotu tiesisko noteiktību un konsolidētu šīs prasības. Ar datu aizsardzības likumprojektu, kas nesen tika iesniegts Argentīnas Kongresā, varētu tikt piedāvāta iespēja kodificēt šādas norises, tādējādi vēl vairāk nostiprinot Argentīnas privātuma regulējumu. Komisija cieši uzraudzīs turpmākās norises šajā jomā.

4.3. Kanāda

Komisija atzinīgi vērtē norises saistībā ar Kanādas tiesisko regulējumu, kas ir notikušas kopš lēmuma par aizsardzības līmeņa pietiekamību pieņemšanas, t. sk. vairākus grozījumus tiesību aktos, judikatūru un pārraudzības struktūru veiktās darbības, kas ir veicinājušas augstāku datu aizsardzības līmeni. Konkrētāk, ir nostiprināts Likums par personas datu un elektronisko dokumentu aizsardzību (*PIPEDA*), veicot dažādus grozījumus (piem., attiecībā uz nosacījumiem likumīgai piekrišanai un ziņošanu par datu pārkāpumiem), turklāt, izmantojot judikatūru, kā arī norādījumus, ko sagatavojusi Kanādas Federālā datu aizsardzības iestāde, t. i., Privātās dzīves aizsardzības komisāra birojs, ir precizētas galvenās datu aizsardzības prasības (piem., par sensitīvu datu apstrādi). Tomēr Komisija iesaka tiesību aktos iekļaut dažus no aizsardzības līdzekļiem, kas jau ir noteikti zemāka līmeņa aktos, lai uzlabotu tiesisko noteiktību un konsolidētu šīs prasības. Jo īpaši leģislatīvā reforma, kas pašlaik tiek veikta attiecībā uz *PIPEDA*, varētu piedāvāt iespēju kodificēt šādas norises, tādējādi vēl vairāk nostiprinot Kanādas privātuma regulējumu. Komisija cieši uzraudzīs turpmākās norises šajā jomā.

Attiecībā uz valdības piekļuvi personas datiem ir noteikts, ka uz Kanādas publiskajām iestādēm attiecas skaidri, precīzi un pieejami noteikumi, saskaņā ar kuriem šādas iestādes var piekļūt no ES nosūtītiem datiem un pēc tam tos izmantot sabiedrības interesēs esošu mērķu sasniegšanai, jo īpaši krimināltiesību aizsardzības un valsts drošības nolūkos. Šie ierobežojumi un garantijas izriet no visaptverošās konstitucionālās sistēmas (Kanādas Tiesību un brīvību harta), judikatūras, īpašiem tiesību aktiem, ar kuriem reglamentē piekļuvi datiem, kā arī no datu aizsardzības noteikumiem (piem., Likums par privātās dzīves aizsardzību vai līdzīgi provinču līmeņa likumi), kuri attiecas arī uz personas datu apstrādi, ko veic Kanādas publiskās iestādes, citastarp tiesībaizsardzības un valsts drošības nolūkos. Papildus tam Kanādas tiesību sistēma šajā jomā nodrošina efektīvus pārraudzības un tiesiskās aizsardzības mehānismus, arī ar nesen paplašinātajām datu subjekta tiesībām un tiesiskās aizsardzības iespējām attiecībā uz valstspiederīgajiem un iedzīvotājiem, kas nav Kanādas pilsoņi.

Balstoties uz vispārējiem konstatējumiem, kas izklāstīti DDD, Komisija secina, ka Kanāda joprojām nodrošina pietiekamu aizsardzības līmeni personas datiem, ko no ES nosūta saņēmējiem, uz kuriem attiecas *PIPEDA*. Kā norādīts iepriekš, attiecībā uz *PIPEDA* pašlaik tiek veikta leģislatīvā reforma, kas varētu vēl vairāk pastiprināt privātuma aizsardzības līdzekļus, arī jomās, kas attiecas uz pietiekamības atzinumu.

4.4. Fēru Salas

Komisija atzinīgi vērtē norises saistībā ar Fēru Salu tiesisko regulējumu, kas ir notikušas kopš lēmuma par aizsardzības līmeņa pietiekamību pieņemšanas, t. sk. grozījumus tiesību aktos, judikatūru un pārraudzības struktūru veiktās darbības, kas ir veicinājušas augstāku datu aizsardzības līmeni. Konkrētāk, Fēru Salas ir ievērojami modernizējušas savu datu aizsardzības regulējumu, pieņemot Datu aizsardzības likumu, kas stājās spēkā 2021. gadā un ar kuru Fēru Salu režīms tiek cieši saskaņots ar VDAR.

Attiecībā uz valdības piekļuvi personas datiem ir noteikts, ka uz Fēru Salas publiskajām iestādēm attiecas skaidri, precīzi un pieejami noteikumi, saskaņā ar kuriem šādas iestādes var piekļūt no ES nosūtītiem datiem un pēc tam tos izmantot sabiedrības interesēs esošu mērķu sasniegšanai, jo īpaši krimināltiesību aizsardzības un valsts drošības nolūkos. Šie ierobežojumi

un garantijas izriet no visaptverošā tiesiskā regulējuma un starptautiskajām saistībām, jo īpaši no konstitucionālās sistēmas un ECTK, kā arī no īpašiem tiesību aktiem, ar kuriem reglamentē valdības piekļuvi datiem, un datu aizsardzības noteikumiem, kas attiecas uz personas datu apstrādi krimināltiesību aizsardzības nolūkos (Likums par tiesībaizsardzības iestāžu veiktu personas datu apstrādi, kurš Fēru Salās stājās spēkā 2022. gadā un ar kuru transponē Dānijas pieņemto tiesību aktu Direktīvas (ES) 2016/680 īstenošanai Fēru Salās) un valsts drošības nolūkos (ietverti Likumā par Drošības un izlūkošanas dienestu). Papildus tam šajā jomā tiek nodrošināti efektīvi pārraudzības un tiesiskās aizsardzības mehānismi.

Balstoties uz vispārējiem konstatējumiem, kas izklāstīti DDD, Komisija secina, ka Fēru Salas joprojām nodrošina pietiekamu aizsardzības līmeni personas datiem, kas tiek nosūtīti no ES.

4.5. Gērnzija

Komisija atzinīgi vērtē norises saistībā ar Gērnzijas tiesisko regulējumu, kas ir notikušas kopš lēmuma par aizsardzības līmeņa pietiekamību pieņemšanas, t. sk. grozījumus tiesību aktos un pārraudzības struktūru veiktās darbības, kas ir veicinājušas augstāku datu aizsardzības līmeni. Konkrētāk, Gērnzija ir ievērojami modernizējusi savu datu aizsardzības regulējumu, pieņemot 2017. gada (*Bailiwick of Guernsey*) Datu aizsardzības likumu, kuru piemēro kopš 2019. gada un ar kuru Gērnzijas režīms tiek cieši saskaņots ar VDAR.

Attiecībā uz valdības piekļuvi personas datiem ir noteikts, ka uz Gērnzijas publiskajām iestādēm attiecas skaidri, precīzi un pieejami noteikumi, saskaņā ar kuriem šādas iestādes var piekļūt no ES nosūtītiem datiem un pēc tam tos izmantot sabiedrības interesēs esošu mērķu sasniegšanai, jo īpaši krimināltiesību aizsardzības un valsts drošības nolūkos. Šie ierobežojumi un garantijas izriet no visaptverošā tiesiskā regulējuma un starptautiskajām saistībām, jo īpaši no ECTK un Konvencijas Nr. 108, kā arī no Gērnzijas datu aizsardzības noteikumiem, t. sk. no īpašajiem noteikumiem par personas datu apstrādi tiesībaizsardzības nolūkos, kuri noteikti 2018. gada Datu aizsardzības rīkojumā (*Law Enforcement and Related Matters*) (*Bailiwick of Guernsey*). Papildus tam Gērnzijas tiesību aktos ir paredzēta virkne īpašu nosacījumu un ierobežojumu attiecībā uz piekļuvi personas datiem un to izmantošanu krimināltiesību aizsardzības un valsts drošības nolūkos, kā arī ar tiem tiek nodrošināti pārraudzības un tiesiskās aizsardzības mehānismi šajā jomā.

Balstoties uz vispārējiem konstatējumiem, kas izklāstīti DDD, Komisija secina, ka Gērnzija joprojām nodrošina pietiekamu aizsardzības līmeni personas datiem, kas tiek nosūtīti no ES.

4.6. Menas Sala

Komisija atzinīgi vērtē norises saistībā ar Menas Salas tiesisko regulējumu, kas ir notikušas kopš lēmuma par aizsardzības līmeņa pietiekamību pieņemšanas, t. sk. grozījumus tiesību aktos un pārraudzības struktūru veiktās darbības, kas ir veicinājušas augstāku datu aizsardzības līmeni. Konkrētāk, Menas Sala 2018. gadā pieņēma jaunu tiesību aktu (2018. gada Datu aizsardzības likums, kuru papildina 2018. gada Datu aizsardzības rīkojums (VDAR piemērošana)), ar kuru lielākā daļa ES datu aizsardzības regulējuma noteikumu tiek iestrādāta

Menas Salas tiesību sistēmā, veicot vien nelielas korekcijas noteiktos aspektos, lai šo regulējumu pielāgotu vietējam kontekstam.

Attiecībā uz valdības piekļuvi personas datiem ir noteikts, ka uz Menas Salas publiskajām iestādēm attiecas skaidri, precīzi un pieejami noteikumi, saskaņā ar kuriem šādas iestādes var piekļūt no ES nosūtītiem datiem un pēc tam tos izmantot sabiedrības interesēs esošu mērķu sasniegšanai, jo īpaši krimināltiesību aizsardzības un valsts drošības nolūkos. Šie ierobežojumi un garantijas izriet no visaptverošā tiesiskā regulējuma un starptautiskajām saistībām, jo īpaši no ECTK un Konvencijas Nr. 108, kā arī no Menas Salas datu aizsardzības noteikumiem, t. sk. no īpašajiem noteikumiem personas datu apstrādei tiesībaizsardzības nolūkos, kas noteikti 2018. gada Datu aizsardzības rīkojumā (Tiesībaizsardzības direktīvas (TAD) piemērošana) un 2018. gada TAD Īstenošanas noteikumos. Papildus tam Menas Salas tiesību aktos ir paredzēta virkne īpašu ierobežojumu attiecībā uz piekļuvi personas datiem un to izmantošanu krimināltiesību aizsardzības un valsts drošības nolūkos, kā arī ar tiem tiek nodrošināti pārraudzības un tiesiskās aizsardzības mehānismi šajā jomā.

Balstoties uz vispārējiem konstatējumiem, kas izklāstīti DDD, Komisija secina, ka Menas Sala joprojām nodrošina pietiekamu aizsardzības līmeni personas datiem, kas tiek nosūtīti no ES.

4.7. *Izraēla*

Komisija atzinīgi vērtē norises saistībā ar Izraēlas tiesisko regulējumu, kas ir notikušas kopš lēmuma par aizsardzības līmeņa pietiekamību pieņemšanas, t. sk. grozījumus tiesību aktos, judikatūru un pārraudzības struktūru veiktās darbības, kas ir veicinājušas augstāku datu aizsardzības līmeni. Konkrētāk, Izraēla ieviesa īpašas garantijas, lai pastiprinātu no Eiropas Ekonomikas zonas nosūtīto personas datu aizsardzību, pieņemot Privātās dzīves aizsardzības noteikumus 5783-2023 (Norādījumi attiecībā uz datiem, kas Izraēlai nosūtīti no Eiropas Ekonomikas zonas). Izraēla arī pastiprināja datu drošības prasības, pieņemot Privātās dzīves aizsardzības (datu drošības) noteikumus 5777-2017, un ar saistošu valdības rezolūciju nostiprināja savas datu aizsardzības uzraudzības iestādes neatkarību.

Attiecībā uz valdības piekļuvi personas datiem ir noteikts, ka uz Izraēlas publiskajām iestādēm attiecas skaidri, precīzi un pieejami noteikumi, saskaņā ar kuriem šādas iestādes var piekļūt no ES nosūtītiem datiem un pēc tam tos izmantot sabiedrības interesēs esošu mērķu sasniegšanai, jo īpaši krimināltiesību aizsardzības un valsts drošības nolūkos. Šie ierobežojumi un garantijas izriet no visaptverošā tiesiskā regulējuma, jo īpaši no Izraēlas Pamatlikuma, kā arī no Privātās dzīves aizsardzības likuma 5741-1981 un saskaņā ar to pieņemtajiem noteikumiem, kuri attiecas uz personas datu apstrādi, ko veic Izraēlas publiskās iestādes, citastarp tiesībaizsardzības un valsts drošības nolūkos. Papildus tam Izraēlas tiesību aktos ir paredzēta virkne īpašu ierobežojumu attiecībā uz piekļuvi personas datiem un to izmantošanu krimināltiesību aizsardzības un valsts drošības nolūkos, kā arī ar tiem tiek nodrošināti pārraudzības un tiesiskās aizsardzības mehānismi šajā jomā.

Balstoties uz vispārējiem konstatējumiem, kas izklāstīti DDD, Komisija secina, ka Izraēla joprojām nodrošina pietiekamu aizsardzības līmeni personas datiem, kas tiek nosūtīti no ES.

Tomēr Komisija iesaka tiesību aktos iekļaut aizsardzības līdzekļus, kas jau ir noteikti zemāka līmeņa aktos un judikatūrā, lai uzlabotu tiesisko noteiktību un konsolidētu šīs prasības. Ar Privātās dzīves aizsardzības likumprojektu 5722-2022 (grozījums Nr. 14), kas nesen tika iesniegts Izraēlas Parlamentā, tiek piedāvāta laba iespēja konsolidēt un kodificēt šādas norises, tādējādi vēl vairāk nostiprinot Izraēlas privātuma regulējumu. Komisija cieši uzraudzīs turpmākās norises šajā jomā.

4.8. Džērsija

Komisija atzinīgi vērtē norises saistībā ar Džērsijas tiesisko regulējumu, kas ir notikušas kopš lēmuma par aizsardzības līmeņa pietiekamību pieņemšanas, t. sk. grozījumus tiesību aktos, judikatūru un pārraudzības struktūru veiktās darbības, kas ir veicinājušas augstāku datu aizsardzības līmeni. Konkrētāk, Džērsija ir ievērojami modernizējusi savu datu aizsardzības regulējumu, pieņemot 2018. gada (Džērsijas) Datu aizsardzības likumu un 2018. gada (Džērsijas) Datu aizsardzības iestādes likumu, kuri stājās spēkā 2018. gadā un ar kuriem Džērsijas režīms tiek cieši saskaņots ar VDAR.

Attiecībā uz valdības piekļuvi personas datiem ir noteikts, ka uz Džērsijas publiskajām iestādēm attiecas skaidri, precīzi un pieejami noteikumi, saskaņā ar kuriem šādas iestādes var piekļūt no ES nosūtītiem datiem un pēc tam tos izmantot sabiedrības interesēs esošu mērķu sasniegšanai, jo īpaši krimināltiesību aizsardzības un valsts drošības nolūkos. Šie ierobežojumi un garantijas izriet no visaptverošā tiesiskā regulējuma un starptautiskajām saistībām, jo īpaši no ECTK un Konvencijas Nr. 108, kā arī no Džērsijas datu aizsardzības noteikumiem, t. sk. no īpašajiem noteikumiem personas datu apstrādei tiesībaizsardzības nolūkos, kuri noteikti 2018. gada (Džērsijas) Datu aizsardzības likumā un kuros grozījumi izdarīti ar šā likuma 1. sarakstu. Papildus tam Džērsijas tiesību aktos ir paredzēta virkne īpašu ierobežojumu attiecībā uz piekļuvi personas datiem un to izmantošanu krimināltiesību aizsardzības un valsts drošības nolūkos, kā arī ar tiem tiek nodrošināti pārraudzības un tiesiskās aizsardzības mehānismi šajā jomā.

Balstoties uz vispārējiem konstatējumiem, kas izklāstīti DDD, Komisija secina, ka Džērsija joprojām nodrošina pietiekamu aizsardzības līmeni personas datiem, kas tiek nosūtīti no ES.

4.9. Jaunzēlande

Komisija atzinīgi vērtē norises saistībā ar Jaunzēlandes tiesisko regulējumu, kas ir notikušas kopš lēmuma par aizsardzības līmeņa pietiekamību pieņemšanas, t. sk. grozījumus tiesību aktos, judikatūru un pārraudzības struktūru veiktās darbības, kas ir veicinājušas augstāku datu aizsardzības līmeni. Konkrētāk, attiecībā uz datu aizsardzības režīmu tika veiktas plašas reformas, pieņemot 2020. gada Privātās dzīves aizsardzības likumu, ar ko tika uzlabota konverģence ar ES datu aizsardzības regulējumu, jo īpaši attiecībā uz noteikumiem par personas datu starptautisku nosūtīšanu un datu aizsardzības iestādes (Privātās dzīves aizsardzības komisāra biroja) pilnvarām.

Attiecībā uz valdības piekļuvi personas datiem ir noteikts, ka uz Jaunzēlandes publiskajām iestādēm attiecas skaidri, precīzi un pieejami noteikumi, saskaņā ar kuriem šādas iestādes var

pieklūt no ES nosūtītiem datiem un pēc tam tos izmantot sabiedrības interesēs esošu mērķu sasniegšanai, jo īpaši krimināltiesību aizsardzības un valsts drošības nolūkos. Šie ierobežojumi un garantijas izriet no visaptverošā konstitucionālā regulējuma (piem., Tiesību likuma) un judikatūras, kā arī no īpašiem tiesību aktiem, ar kuriem tiek reglamentēta valdības piekļuve datiem, un no Privātās dzīves aizsardzības likuma noteikumiem, kas attiecas arī uz krimināltiesību aizsardzības un valsts drošības iestāžu veiktu personas datu apstrādi. Papildus tam Jaunzēlandes tiesību sistēma nodrošina dažādus pārraudzības un tiesiskās aizsardzības mehānismus šajā jomā.

Balstoties uz vispārējiem konstatējumiem, kas izklāstīti DDD, Komisija secina, ka Jaunzēlande joprojām nodrošina pietiekamu aizsardzības līmeni personas datiem, kas tiek nosūtīti no ES. Komisija atzinīgi vērtē arī likumprojektu, kuru Jaunzēlandes valdība nesen iesniedza Parlamentā ar mērķi grozīt 2020. gada Privātās dzīves aizsardzības likumu, lai pastiprinātu spēkā esošās pārraudzības prasības. Komisija cieši uzraudzīs turpmākās norises šajā jomā.

4.10. *Šveice*

Komisija atzinīgi vērtē norises saistībā ar Šveices tiesisko regulējumu, kas ir notikušas kopš lēmuma par aizsardzības līmeņa pietiekamību pieņemšanas, t. sk. grozījumus tiesību aktos, judikatūru un pārraudzības struktūru veiktās darbības, kas ir veicinājušas augstāku datu aizsardzības līmeni. Konkrētāk, ir modernizēts Federālais Datu aizsardzības likums, ar ko tika uzlabota konverģence ar ES datu aizsardzības regulējumu, jo īpaši attiecībā uz sensitīvo datu aizsardzības līdzekļiem un noteikumiem par starptautisku datu nosūtīšanu. Šveice arī pastiprināja savas starptautiskās saistības datu aizsardzības jomā, 2023. gada septembrī ratificējot Konvenciju Nr. 108+.

Attiecībā uz valdības piekļuvi personas datiem ir noteikts, ka uz Šveices publiskajām iestādēm attiecas skaidri, precīzi un pieejami noteikumi, saskaņā ar kuriem šādas iestādes var piekļūt no ES nosūtītiem datiem un pēc tam tos izmantot sabiedrības interesēs esošu mērķu sasniegšanai, jo īpaši krimināltiesību aizsardzības un valsts drošības nolūkos. Šie ierobežojumi un garantijas izriet no visaptverošā tiesiskā regulējuma un starptautiskajām saistībām, jo īpaši no Šveices Federālās Konstitūcijas, ECTK un Konvencijas Nr. 108+, kā arī no Šveices datu aizsardzības noteikumiem, t. sk. no Federālā Datu aizsardzības likuma un īpašiem datu aizsardzības noteikumiem, kas attiecas uz krimināltiesību aizsardzības līdzekļiem (piem., Kriminālprocesa kodekss) un valsts drošības iestādēm (piem., Izlūkošanas dienesta likums). Papildus tam Šveices tiesību aktos ir paredzēta virkne īpašu ierobežojumu attiecībā uz piekļuvi personas datiem un to izmantošanu krimināltiesību aizsardzības un valsts drošības nolūkos, kā arī ar tiem tiek nodrošināti pārraudzības un tiesiskās aizsardzības mehānismi šajā jomā.

Balstoties uz vispārējiem konstatējumiem, kas izklāstīti DDD, Komisija secina, ka Šveice joprojām nodrošina pietiekamu aizsardzības līmeni personas datiem, kas tiek nosūtīti no ES.

4.11. *Urugvaja*

Komisija atzinīgi vērtē norises saistībā ar Urugvajes tiesisko regulējumu, kas ir notikušas kopš lēmuma par aizsardzības līmeņa pietiekamību pieņemšanas, t. sk. vairākus grozījumus tiesību

aktos, judikatūru un pārraudzības struktūru veiktās darbības, kas ir veicinājušas augstāku datu aizsardzības līmeni. Konkrētāk, Urugvaja modernizēja un nostiprināja savu 2008. gada Likumu Nr. 18.331 par personas datu aizsardzību un “*Habeas Data*” procedūru, 2018. un 2020. gadā veicot tiesību akta grozījumus, ar kuriem tika paplašināts datu aizsardzības likuma teritoriālais tvērums, izveidotas jaunas pārskatatbildības prasības (piem., ietekmes novērtējumi, integrēta datu aizsardzība un datu aizsardzība pēc noklusējuma, datu pārkāpumu paziņošana un datu aizsardzības darbinieku iecelšana amatā) un ieviesti papildu aizsardzības līdzekļi biometriskajiem datiem. Urugvaja arī pastiprināja savas starptautiskās saistības datu aizsardzības jomā, 2019. gadā pievienojoties Konvencijai Nr. 108 un 2021. gadā ratificējot Konvenciju Nr. 108+.

Attiecībā uz valdības piekļuvi personas datiem ir noteikts, ka uz Urugvajas publiskajām iestādēm attiecas skaidri, precīzi un pieejami noteikumi, saskaņā ar kuriem šādas iestādes var piekļūt no ES nosūtītiem datiem un pēc tam tos izmantot sabiedrības interesēs esošu mērķu sasniegšanai, jo īpaši krimināltiesību aizsardzības un valsts drošības nolūkos. Šie ierobežojumi un garantijas izriet no visaptverošā tiesiskā regulējuma un starptautiskajām saistībām, jo īpaši no Urugvajas Konstitūcijas, Amerikas Cilvēktiesību Konvencijas, Konvencijas Nr. 108 un Konvencijas Nr. 108+, kā arī no datu aizsardzības noteikumiem, kas iekļauti Likumā Nr. 18.331 par personas datu aizsardzību un “*Habeas Data*” procedūru, kura attiecas uz Urugvajas publisko iestāžu veiktu personas datu apstrādi, jo īpaši tiesībaizsardzības un valsts drošības nolūkos. Papildus tam Urugvajas tiesību aktos ir paredzēta virkne īpašu nosacījumu un ierobežojumu attiecībā uz publisko iestāžu piekļuvi personas datiem un to izmantošanu, kā arī ar tiem tiek nodrošināti pārraudzības un tiesiskās aizsardzības mehānismi šajā jomā.

Balstoties uz vispārējiem konstatējumiem, kas izdarīti šīs pirmās pārskatīšanas ietvaros, Komisija secina, ka Urugvaja joprojām nodrošina pietiekamu aizsardzības līmeni personas datiem, kas tiek nosūtīti no ES.

5. TURPMĀKĀ UZRAUDZĪBA UN SADARBĪBA

Komisija atzinīgi un augstu vērtē teicamo sadarbību ar katras attiecīgās valsts un teritorijas atbildīgajām iestādēm šīs pārskatīšanas ietvaros. Komisija turpinās cieši uzraudzīt norises, kas skar attiecīgo valstu un teritoriju datu aizsardzības regulējumus un to reālo īstenošanas praksi. Ja attiecīgajā valstī vai teritorijā būs kādas norises, kas varētu negatīvi ietekmēt datu aizsardzības līmeni, kurš iepriekš atzīts par pietiekamu, Komisija nepieciešamības gadījumā izmantos savas VDAR 45. panta 5. punktā noteiktās pilnvaras apturēt, grozīt vai atcelt lēmumu par aizsardzības līmeņa pietiekamību.

Šī pārskatīšana apliecina, ka lēmuma par aizsardzības līmeņa pietiekamību pieņemšana nav tikai galarezultāts, bet nodrošina arī iespēju turpmāk pastiprināt dialogu un sadarbību ar līdzīgi domājošiem starptautiskajiem partneriem attiecībā uz datu plūsmām un digitālajiem jautājumiem kopumā. Saistībā ar to Komisija cer uz turpmāku informācijas apmaiņu ar atbildīgajām iestādēm, lai vēl vairāk pastiprinātu starptautiskā līmeņa sadarbību drošu un brīvu datu plūsmu veicināšanā, t. sk. nodrošinot spēcīgāku sadarbību izpildes panākšanas jomā. Lai pastiprinātu šo dialogu un veicinātu informācijas un pieredzes apmaiņu, Komisija plāno

2024. gadā organizēt augsta līmeņa sanāksmi, pulcējot pārstāvjus no ES un visām valstīm, kurām lēmums par aizsardzības līmeņa pietiekamību sniedz ieguvumus.