Euroopa Liidu
Nõukogu

Brüssel, 22. jaanuar 2024
(OR. en)

5454/24

DATAPROTECT 23
JAI 62
RELEX 42

SAATEMÄRKUSED

Saatja:	Euroopa Komisjoni peasekretär, allkirjastanud Martine DEPREZ, direktor
Saaja:	Thérèse BLANCHET, Euroopa Liidu Nõukogu peasekretär
Komisjoni dok nr:	COM(2024) 7 final
Teema:	KOMISJONI ARUANNE EUROOPA PARLAMENDILE JA NÕUKOGULE, direktiivi 95/46/EÜ artikli 25 lõike 6 kohaselt vastu võetud kaitse piisavuse otsuste toimimise esimese läbivaatamise kohta

Käesolevaga edastatakse delegatsioonidele dokument COM(2024) 7 final.

Lisatud: COM(2024) 7 final

EUROOPA
KOMISJON

Brüssel, 15.1.2024
COM(2024) 7 final

KOMISJONI ARUANNE EUROOPA PARLAMENDILE JA NÕUKOGULE,

direktiivi 95/46/EÜ artikli 25 lõike 6 kohaselt vastu võetud kaitse piisavuse otsuste toimimise esimese läbivaatamise kohta

{SWD(2024) 3 final}

1. ESIMENE LÄBIVAATAMINE – TAUST JA KONTEKST

Käesolev aruanne sisaldab tähelepanekuid, mille komisjon tegi direktiivi 95/46/EÜ[1] (andmekaitsedirektiiv) artikli 25 lõike 6 alusel vastu võetud kaitse piisavuse otsuste esimese läbivaatamise käigus.

Neis otsustes leiab komisjon, et Euroopa Liidust (EL) edastatud isikuandmete kaitse piisava taseme tagavad üksteist riiki või territooriumi:[2] Andorra,[3] Argentina,[4] Kanada (ettevõtjatele),[5] Fääri saared,[6] Guernsey,[7] Mani saar,[8] Iisrael,[9] Jersey,[10] Uus-Meremaa,[11] Šveits[12] ja Uruguay[13]. Seetõttu ei kohaldata EList neisse riikidesse või neile territooriumidele andmete edastamise suhtes lisanõudeid.

Määruse (EL) 2016/679[14] (isikuandmete kaitse üldmäärus) jõustumisel 25. mail 2018 jäid andmekaitsedirektiivi alusel vastu võetud kaitse piisavuse otsused kehtima[15]. Samas on isikuandmete kaitse üldmääruses osutatud sellele, et kaitse piisavuse otsused on n-ö elavad dokumendid, ja sätestatud, et komisjon peab pidevalt jälgima kolmandates riikides esinevaid

[1] Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (EÜT L 281, 23.11.1995, lk 31).

[2] Pärast isikuandmete kaitse üldmääruse inkorporeerimist Euroopa Majanduspiirkonna (EMP) lepingusse kohaldatakse seda määrust ka Norra, Islandi ja Liechtensteini suhtes. Käesoleva aruande viiteid ELile tuleks mõista viidetena, mis hõlmavad kõiki EMP riike.

[3] Komisjoni 19. oktoobri 2010. aasta otsus 2010/625/EL isikuandmete piisava kaitse kohta Andorras vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ (ELT L 277, 21.10.2010, lk 27).

[4] Komisjoni 30. juuni 2003. aasta otsus 2003/490/EÜ isikuandmete piisava kaitse kohta Argentiinas vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ (ELT L 168, 5.7.2003, lk 19).

[5] Komisjoni 20. detsembri 2001. aasta otsus 2002/2/EÜ vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ isikuandmete piisava kaitse kohta, nagu on ette nähtud Kanada isikuandmete kaitse ja elektrooniliste dokumentide seadusega (EÜT L 2, 4.1.2002, lk 13).

[6] Komisjoni 5. märtsi 2010. aasta otsus 2010/146/EL, milles käsitletakse vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ piisavat kaitset, mida pakub Fääri saarte isikuandmete töötlemise seadus (ELT L 58, 9.3.2010, lk 17).

[7] Komisjoni 21. novembri 2003. aasta otsus 2003/821/EÜ isikuandmete piisava kaitse kohta Guernseyl (ELT L 308, 25.11.2003, lk 27).

[8] Komisjoni 28. aprilli 2004. aasta otsus 2004/411/EÜ isikuandmete piisava kaitse kohta Mani saarel (ELT L 151, 30.4.2004, lk 48).

[9] Komisjoni 31. jaanuari 2011. aasta otsus 2011/61/EL isikuandmete piisava kaitse kohta Iisraeli Riigis seoses isikuandmete automaatse töötlemisega vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ (ELT L 27, 1.2.2011, lk 39).

[10] Komisjoni 8. mai 2008. aasta otsus 2008/393/EÜ isikuandmete piisava kaitse kohta Jerseyl vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ (ELT L 138, 28.5.2008, lk 21).

[11] Komisjoni 19. detsembri 2012. aasta rakendusotsus 2013/65/EL isikuandmete piisava kaitse kohta Uus-Meremaal vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ (ELT L 28, 30.1.2013, lk 12).

[12] Komisjoni 26. juuli 2000. aasta otsus 2000/518/EÜ isikuandmete piisava kaitse kohta Šveitsis vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ (EÜT L 215, 25.8.2000, lk 1).

[13] Komisjoni 21. augusti 2012. aasta rakendusotsus 2012/484/EL isikuandmete piisava kaitse kohta Uruguay Idavabariigis seoses isikuandmete automaatse töötlemisega vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ (ELT L 227, 23.8.2012, lk 11).

[14] Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1).

[15] Vt isikuandmete kaitse üldmääruse artikli 45 lõige 9, milles on sätestatud, et otsused, mille komisjon on vastu võtnud direktiivi 95/46/EÜ artikli 25 lõike 6 alusel, jäävad jõusse, kuni nende muutmise, asendamise või kehtetuks tunnistamiseni artikli 45 lõike 3 või 5 kohaselt vastu võetud komisjoni otsusega.

suundumusi, mis võiksid mõjutada kehtivate otsuste toimimist[16]. Peale selle kohustab isikuandmete kaitse üldmääruse artikkel 97 komisjoni kaitse piisavuse otsused iga nelja aasta tagant läbi vaatama, et selgitada välja, kas riigid ja territooriumid, mille kohta on selline otsus tehtud, tagavad jätkuvalt isikuandmete kaitse piisava taseme.

ELi eelmise andmekaitseraamistiku kohaselt vastu võetud kaitse piisavuse otsuste esimene läbivaatamine algatati osana isikuandmete kaitse üldmääruse kohaldamise ja toimimise laiemast hindamisest, mille kohta komisjon esitas oma järeldused teatises „Andmekaitse kodanike võimestajana ja ELi valmistumine digiüleminekuks – isikuandmete kaitse üldmääruse kohaldamise kaks esimest aastat“[17]. Järelduste esitamine kaitse piisavuse otsuste kohta lükati siiski edasi, et võtta arvesse Euroopa Kohtu otsust kohtuasjas Schrems II,[18] kus kohus esitas olulisi selgitusi piisavuse nõude põhielementide ja muu seonduva arengu kohta. See otsus tõi kaasa üksikasjaliku teabevahetuse asjaomaste riikide ja territooriumidega nende õigusraamistiku, järelevalvemehhanismide ja täitmise tagamise süsteemi asjaomaste aspektide teemal[19]. Käesolevas aruandes võetakse igati arvesse kogu arengut nii ELis kui ka asjaomastes kolmandates riikides ja kolmandatel territooriumidel.

Oluline on märkida, et kõnealune esimene läbivaatamine toimus digitehnoloogia hoogsa arengu taustal. Viimastel kümnenditel on kaitse piisavuse otsuste tähtsus märkimisväärselt suurenenud, kuna andmevoogudest on saanud ühiskonna digiülemineku ja majanduse globaliseerumise lahutamatu element. Andmete edastamine üle piiri on muutunud igapäevategevuse osaks igas suuruses Euroopa ettevõtjate jaoks kõigis sektorites. Eraelu puutumatuse austamine on stabiilsete, turvaliste ja konkurentsipõhiste kaubandusvoogude eeltingimusena tähtsam kui kunagi varem. Selles kontekstis on kaitse piisavuse otsustel mitmes mõttes üha olulisem roll. Tagades, et andmetega käib kaasas andmete kaitse, võimaldavad need otsused turvalisi andmevooge, milles austatakse üksikisikute õigusi kooskõlas inimkeskse lähenemisviisiga, mida EL rakendab digiülemineku suhtes. Tunnistades, et kolmanda riigi eraelu puutumatuse raamistik tagab kaitsetaseme, mis on sisuliselt samaväärne ELis tagatuga, edendavad need otsused kõrgetel kaitsestandarditel põhinevate andmekaitsesüsteemide vahelist lähenemist. Peale selle – nagu selgitatakse käesolevas aruandes – ei kujuta kaitse piisavuse otsused endast finišijoont, vaid nendega on pandud alus ELi ja sarnaseid seisukohti jagavate partnerite tihedamale koostööle ja edasisele õigusnormide lähendamisele. Võimaldades isikuandmete vaba liikumist, on need otsused avanud ELi ettevõtjatele kaubanduskanaleid, sealhulgas täiendanud ja võimendanud kaubanduslepingutest tulenevaid eeliseid ning lihtsustanud koostööd välispartneritega mitmesugustes reguleeritavates valdkondades. Pakkudes andmeedastuseks lihtsat ja terviklikku lahendust, mille puhul andmeeksportija ei pea pakkuma

[16] Isikuandmete kaitse üldmääruse artikli 45 lõige 4. Vt ka kohtuotsus, Euroopa Liidu Kohus, 6. oktoober 2015, Maximillian Schrems *vs.* Data Protection Commissioner, C-362/14 (edaspidi „Schrems I“), ECLI:EU:C:2015:650, punkt 76.

[17] Teatis avaldati 2020. aasta juunis ja see on kättesaadav aadressil https://ec.europa.eu/info/law/law-topic/data-protection/communication-two-years-application-general-data-protection-regulation_en.

[18] Kohtuotsus, Euroopa Liidu Kohus, 16. juuli 2020, Data Protection Commissioner *vs.* Facebook Ireland Ltd ja Maximilian Schrems, C-311/18 (edaspidi „Schrems II“), ECLI:EU:C:2020:559.

[19] Jaapanit käsitlev kaitse piisavuse otsus võeti vastu isikuandmete kaitse üldmääruse põhjal ja selles on ette nähtud eraldi korrapärane läbivaatamine. Esimene läbivaatamine lõppes 2023. aasta aprillis komisjoni aruandega Jaapani pakutava kaitse piisavuse otsuse toimimise esimese läbivaatamise kohta (COM(2023) 275 final); kättesaadav aadressil https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=COM:2023:275:FIN.

täiendavaid kaitsemeetmeid ega hankima ühtki luba, hõlbustavad need otsused isikuandmete kaitse üldmääruses sätestatud andmete rahvusvahelise edastamise nõuete täitmist, eelkõige väikeste ja keskmise suurusega ettevõtjate jaoks. Samuti on Euroopa Komisjoni vastu võetud kaitse piisavuse otsused tänu võrguefektile aina olulisemad ka väljaspool ELi, kuna need ei võimalda andmete vaba liikumist üksnes 30 Euroopa riigi puhul, vaid ka paljude teiste jurisdiktsioonide puhul,[20] kes peavad riike, mille kohta EL on teinud kaitse piisavuse otsuse, oma andmekaitsenormide alusel turvaliseks sihtkohaks.

Kõigil neil põhjustel – nagu kinnitas ka läbivaatamist toetanud elav ja viljakas dialoog asjassepuutuvate kolmandate riikide ja territooriumidega – on kaitse piisavuse otsustest saanud ELi ja asjaomaste välispartnerite vaheliste suhete strateegiline komponent ja neid otsuseid peetakse väga oluliseks, et koostööd mitmesugustes valdkondades süvendada. Seetõttu on eriti oluline, et need otsused suudaksid ajaproovile – uutele suundumustele ja probleemidele – vastu pidada.

2. LÄBIVAATAMISE EESMÄRK JA METOODIKA

Kaitse piisavuse otsused, mis läbi vaadati, on vastu võetud isikuandmete kaitse määrusele eelnenud ELi andmekaitseraamistiku alusel. Kui kõige hilisemad otsused on umbes kümme aastat vanad (nt otsused Uus-Meremaa ja Uruguay kohta, mis võeti vastu 2012. aastal), siis teised on kehtinud üle kahekümne aasta (nt otsus Kanada kohta, mis võeti vastu 2001. aastal, ja otsus Šveitsi kohta, mis võeti vastu 2000. aastal). Kõigi üheteistkümne riigi ja territooriumi andmekaitseraamistik on sellest ajast saati arenenud, näiteks tulenevalt seadusandlikest või regulatiivsetest reformidest, muudatustest andmekaitseasutuste õigusnormide täitmise tagamise praktikas või kohtupraktikast.

Seepärast keskendus komisjon hindamisel asjaomaste riikide ja territooriumide andmekaitseraamistikus pärast kaitse piisavuse otsuse vastuvõtmist toimunud arengule. Komisjon hindas, kuidas see areng on kujundanud asjaomase riigi või territooriumi andmekaitsemaastikku ning kas riigis või territooriumil kehtestatud kord tagab selle arengu valguses jätkuvalt isikuandmete kaitse piisava taseme.

Hindamisel võeti täiel määral arvesse ELi enda andmekaitsekorra arenemist, eriti seoses sellega, et hakati kohaldama isikuandmete kaitse üldmäärust. Pärast kõnealuste kaitse piisavuse otsuste vastuvõtmist on selliste otsuste suhtes kohaldatavaid õiguslikke nõudeid ja elemente, mis on asjakohased selle hindamisel, kas ELi-väline süsteem tagab kaitse piisava taseme, täiendavalt selgitatud eelkõige Euroopa Kohtu praktikas ning artikli 29 töörühma ja selle järeltulija Euroopa Andmekaitsenõukogu[21] vastu võetud suunistes.

Eeskätt on Euroopa Kohus oma 6. oktoobri 2015. aasta otsuses kohtuasjas Schrems I sedastanud, et ehkki ei saa nõuda, et kolmas riik tagaks kaitsetaseme, mis on ELis tagatuga identne, tuleb piisavuse kriteeriumit mõista nõudena, et kaitse tase peab olema sisuliselt

[20] Nagu Argentina, Colombia, Iisrael, Maroko, Šveits ja Uruguay.

[21] Euroopa Andmekaitsenõukogusse kuuluvad liikmesriikide andmekaitse järelevalveasutuste esindajad ja Euroopa Andmekaitseinspektor.

samaväärne[22]. Kohus selgitab, et vahendid, mida asjaomane kolmas riik kasutab isikuandmete kaitsmiseks, võivad erineda nendest, mida rakendatakse liidus, seni kuni need osutuvad praktikas kaitse piisava taseme tagamisel tulemuslikuks[23]. Seetõttu tuleb kaitsetaseme piisavuse kontrollimiseks põhjalikult hinnata kolmanda riigi süsteemi kui tervikut, sealhulgas eraelu puutumatuse kaitse sisu, selle rakendamise tõhusust ja täitmise tagamist.

Lisaks on Euroopa Kohus selgitanud, et komisjon ei tohiks hindamisel piirduda üksnes kolmanda riigi üldise andmekaitseraamistikuga, vaid peaks vaatlema ka õigusnorme, millega reguleeritakse avaliku sektori asutuste juurdepääsu isikuandmetele, eelkõige õiguskaitse ja riikliku julgeoleku eesmärgil[24]. Kasutades võrdlusalusena põhiõiguste hartat, on kohus välja toonud mitu nõuet, millele need õigusnormid peaksid vastama, et sisulise samaväärsuse nõue oleks täidetud. Näiteks peaks asjaomane õigusakt sisaldama selgeid ja täpseid õigusnorme, mis reguleerivad meetme ulatust ja kohaldamist ning millega on kehtestatud minimaalsed kaitsemeetmed, nii et isikutel, kelle isikuandmed on asjassepuutuvad, on piisavad tagatised, mis võimaldavad nende andmeid tõhusalt kaitsta kuritarvitamise ohu ning ebaseadusliku juurdepääsu ja kasutamise eest[25]. Samuti peaks see võimaldama isikutel kasutada õiguskaitsevahendeid, et tutvuda teda puudutavate isikuandmetega või lasta neisse parandusi teha või need kustutada[26].

Isikuandmete kaitse üldmääruses on esitatud Euroopa Kohtu selgitustele tuginedes üksikasjalik loetelu elementidest, mida komisjon peab kaitse taseme piisavuse hindamisel arvesse võtma[27]. Lisaks on Euroopa Kohus vaadelnud sisulise samaväärsuse nõuet põhjalikumalt oma 16. juuli 2020. aasta otsuses kohtuasjas Schrems II, eelkõige seoses normidega, mis käsitlevad avaliku sektori asutuste juurdepääsu isikuandmetele õiguskaitse ja riikliku julgeoleku eesmärgil. Kohtu selgituse kohaselt tähendab sisulise samaväärsuse nõue seda, et asjaomase kolmanda riigi või territooriumi avaliku sektori asutustele siduv õigusraamistik peab sisaldama minimaalseid kaitsemeetmeid, millega tagatakse, et nende asutuste juurdepääs andmetele üksnes ulatuses, mis on vajalik seaduslike eesmärkide saavutamiseks ja sellega proportsionaalne, ning et andmesubjektidel peavad olema tõhusad ja kohtulikult kaitstavad õigused nende asutuste suhtes[28].

Kaitse piisavuse nõude arengut on käsitletud ka suunistes, mille võttis algselt vastu artikli 29 töörühm ja seejärel kinnitas Euroopa Andmekaitsenõukogu[29]. Neis suunistes ja eelkõige nn piisavuse võrdlusaluses on selgitatud täpsemalt elemente, mida komisjon peab arvesse võtma piisavuse hindamisel, mille raames tuleb muu hulgas koostada ülevaade olulistest tagatistest avalike asutuste juurdepääsul isikuandmetele. See võrdlusalus põhineb eelkõige Euroopa Inimõiguste Kohtu kohtupraktikal; Euroopa Andmekaitsenõukogu on võrdlusalust

[22] Schrems I, punktid 73, 74 ja 96. Vt ka määruse (EL) 2016/679 põhjendus 104, milles on osutatud sisulise samaväärsuse nõudele.
[23] Schrems I, punkt 74.
[24] Schrems I, punkt 90.
[25] Schrems I, punkt 91.
[26] Schrems I, punkt 95.
[27] Isikuandmete kaitse üldmääruse artikli 45 lõige 2.
[28] Schrems II, punktid 180–182.
[29] Piisavuse võrdlusalus, WP 254 rev. 01, 6.2.2018; kättesaadav aadressil https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

ajakohastanud, et võtta arvesse Euroopa Kohtu selgitusi Schrems II kohtuotsuses[30]. Oluline on, et piisavuse võrdlusaluses tunnistatakse, et sisulise samaväärsuse nõue ei eelda ELi õigusnormide punkt-punktilt kopeerimist, sest võrreldava kaitsetaseme tagamise vahendid võivad andmekaitsesüsteemide lõikes erineda, mis sageli kajastab erinevusi õigustavades.

Seepärast on komisjon selle kindlakstegemisel, kas varasemate õigusnormide alusel vastu võetud üksteist kaitse piisavuse otsust vastavad jätkuvalt isikuandmete kaitse üldmäärusega kehtestatud nõuetele, lisaks asjaomaste riikide ja territooriumide andmekaitseraamistiku arengule arvesse võtnud ka arengut piisavuse nõude tõlgendamisel liidu õiguses. Muu hulgas on hinnatud õigusraamistikku, millega reguleeritakse juurdepääsu EList edastatud isikuandmetele ja nende isikuandmete kasutamist selliste riikide või territooriumide avaliku sektori asutuste poolt, kelle puhul on andmekaitsedirektiivi artikli 25 lõike 6 kohaselt leitud, et tagatud on kaitse piisav tase.

3. LÄBIVAATAMISPROTSESS

Nagu eespool selgitatud, vaadeldi kehtivate kaitse piisavuse otsuste hindamisel iga asjaomase riigi või territooriumi andmekaitseraamistikku ja mis tahes arengut selles raamistikus pärast kaitse piisavuse otsuse vastuvõtmist ning õigusnorme, millega reguleeritakse valitsuse juurdepääsu andmetele, eelkõige õiguskaitse ja riikliku julgeoleku eesmärgil. Komisjoni talitused on astunud viimastel aastatel tihedas koostöös asjaomaste riikide ja territooriumidega mitmeid samme selle hindamise korraldamiseks.

Selleks et aidata komisjonil täita oma järelevalvekohustust, esitasid kõik üksteist riiki ja territooriumi komisjonile põhjalikku teavet arengu kohta, mis oli toimunud nende andmekaitsekorras pärast kaitse piisavuse otsuse vastuvõtmist. Peale selle küsis komisjon kõigilt üheteistkümnelt riigilt ja territooriumilt üksikasjalikku teavet õigusnormide kohta, millega reguleeritakse riigis või territooriumil valitsuse juurdepääsu isikuandmetele, eelkõige õiguskaitse ja riikliku julgeoleku eesmärgil. Samuti hankis komisjon avalikest allikatest, järelevalve- ja täitevasutustelt ning kohalikelt ekspertidelt teavet kõnealuste otsuste toimimise kohta ning asjassepuutuva arengu kohta asjaomase riigi või territooriumi õiguses ja tavades, pidades silmas nii eraettevõtjate suhtes kohaldatavaid andmekaitsenorme kui ka valitsuse juurdepääsu andmetele. Lõpetuseks võeti nõuetekohaselt arvesse rahvusvahelisi kohustusi, mille riik või territoorium on võtnud piirkondliku või üldise dokumendi alusel.

Eelnimetatule tuginedes on komisjon pidanud iga asjaomase riigi ja territooriumiga elavat dialoogi. Selle dialoogi raames on mitu riiki ja territooriumi ajakohastanud ja tugevdanud oma eraelu puutumatust käsitlevaid õigusakte, viies ellu ulatuslikke või osalisi reforme (nt Andorra, Kanada, Fääri saared, Šveits ja Uus-Meremaa), mis olid osaliselt tingitud vajadusest tagada, et kaitse piisavuse otsus jääb kehtima. Mõnes riigis ja mõnel territooriumil on vastu võetud andmekaitseasutuse eeskirjad ja/või suunised, et kehtestada uued andmekaitsenõuded (nt Iisrael ja Uruguay) või selgitada teatavaid eraelu puutumatust käsitlevaid õigusnorme (nt Argentina,

[30] Soovitused 02/2020 Euroopa oluliste tagatiste kohta jälgimismeetmete kontekstis; kättesaadav aadressil https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_en.

Kanada, Guernsey, Jersey, Mani saar, Iisrael ja Uus-Meremaa), tuginedes õigusnormide täitmise tagamise tavadele või kohtupraktikale. Lisaks on kaitse taseme erinevuste kaotamiseks peetud mõne riigi ja territooriumiga läbirääkimisi ja lepitud kokku täiendavates kaitsemeetmetes Euroopast edastatavate isikuandmete jaoks, kui see on olnud vajalik selle tagamiseks, et kaitse piisavuse otsus jääks kehtima. Näiteks Kanada valitsus laiendas õigust tutvuda avaliku sektori töödeldavate isikuandmetega ja õigust nõuda nende andmete parandamist kõigile isikutele, olenemata nende kodakondsusest ja elukohast (varem olid need õigused vaid Kanada kodanikel, alalistel elanikel ja Kanadas viibivatel isikutel)[31]. Teise näitena võib tuua Iisraeli, mille valitsus kehtestas EMPst edastatud isikuandmete kaitse tugevdamiseks spetsiaalsed kaitsemeetmed, millega tekitati andmete täpsuse ja andmete säilitamisega seotud uued kohustused, tugevdati õigust saada teavet ja lasta andmed kustutada ning loodi täiendavad tundlike andmete kategooriad[32].

Samal ajal kogusid komisjoni talitused seisukohti Euroopa Parlamendilt (kodanikuvabaduste, justiits- ja siseasjade komisjonilt),[33] nõukogult (andmekaitse töörühma kaudu),[34] Euroopa Andmekaitsenõukogult[35] ja mitut sidusrühma (kodanikuühiskond, tööstus, akadeemilised ringkonnad ja õiguspraktikud) hõlmavalt isikuandmete kaitse üldmääruse eksperdirühmalt[36] ning teavitasid neid korrapäraselt hindamise edenemisest.

Seega on käesolev aruanne ja sellele lisatud komisjoni talituste töödokument kõigi asjaomaste riikide ja territooriumidega tehtud tiheda koostöö ning asjaomaste ELi institutsioonide ja asutustega konsulteerimise ja neilt saadud tagasiside tulemus. Aruanne ja töödokument põhinevad mitmesugustel allikatel, mille hulka kuuluvad õigusaktid, kohtupraktika, andmekaitseasutuste otsused ja suunised, (sõltumatute) järelevalveasutuste aruanded ja sidusrühmadelt saadud teave. Enne käesoleva aruande vastuvõtmist anti kõigile asjaomastele riikidele ja territooriumidele võimalus kontrollida komisjoni talituste töödokumendis nende süsteemi kohta esitatud teabe faktilist täpsust.

4. PEAMISED TÄHELEPANEKUD JA JÄRELDUSED

Esimene läbivaatamine näitas, et üheteistkümne riigi ja territooriumi andmekaitseraamistik on pärast kaitse piisavuse otsuse vastuvõtmist veelgi enam lähenenud ELi raamistikule. Lisaks leiti läbivaatamise käigus, et mis puudutab valitsuse juurdepääsu isikuandmetele, on nende riikide

[31] Eraelu puutumatuse seaduse 12. jagu, eraelu puutumatuse seaduse laiendamise korraldused nr 1 ja 2.
[32] Eraelu puutumatuse kaitse eeskirjad nr 5783-2023 (juhised andmete jaoks, mis on Iisraeli edastatud Euroopa Majanduspiirkonnast), *Reshumut* (Iisraeli ametlik väljaanne), 7.5.2023.
[33] Vt näiteks Euroopa Parlamendi 25. märtsi 2021. aasta resolutsioon, mis käsitleb komisjoni hindamisaruannet isikuandmete kaitse üldmääruse rakendamise kohta kaks aastat pärast selle kohaldamise algust (2020/2717(RSP); kättesaadav aadressil https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_ET.html.
[34] Vt näiteks nõukogu seisukoht ja tähelepanekud isikuandmete kaitse üldmääruse kohaldamise kohta (vastu võetud 19. detsembril 2019); kättesaadav aadressil https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-1/et/pdf.
[35] Vt näiteks Euroopa Andmekaitsenõukogu panus isikuandmete kaitse üldmääruse artiklis 97 sätestatud hindamisse (vastu võetud 18. veebruaril 2020); kättesaadav aadressil https://edpb.europa.eu/sites/default/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf.
[36] Vt näiteks mitut sidusrühma hõlmava isikuandmete kaitse üldmääruse hindamise eksperdirühma aruanne; kättesaadav aadressil https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=et&do=groupDetail.groupMeeting&meetingId=21356.

ja territooriumide õiguses kehtestatud asjakohased kaitsemeetmed ja piirangud ning tagatud seonduvad järelevalve- ja õiguskaitsemehhanismid.

Üksikasjalikud tähelepanekud kõigi üheteistkümne riigi ja territooriumi kohta on esitatud käesolevale aruandele lisatud komisjoni talituste töödokumendis. Nende tähelepanekute põhjal järeldab komisjon, et kõik üksteist riiki ja territooriumi tagavad jätkuvalt Euroopa Liidust edastatud isikuandmete kaitse piisava taseme isikuandmete kaitse üldmääruse tähenduses, nagu seda on tõlgendanud Euroopa Kohus. Asjaomaste riikide ja territooriumide kohta tehtud tähelepanekud on kokku võetud allpool.

4.1. Andorra

Komisjonile valmistab heameelt areng, mis on toimunud Andorra õigusraamistikus pärast kaitse piisavuse otsuse vastuvõtmist, sealhulgas seadusandlikud muudatused ja järelevalveasutuste tegevus. Eelkõige on 2022. aasta mais jõustunud isikuandmete kaitse seadus nr 29/2021 aidanud tõsta andmekaitse taset, kuna selle seaduse ülesehitus ja põhikomponendid on heas kooskõlas isikuandmete kaitse üldmäärusega.

Mis puudutab valitsuse juurdepääsu isikuandmetele, siis kohaldatakse Andorra avaliku sektori asutuste suhtes selgeid, täpseid ja ligipääsetavaid õigusnorme, mille alusel need asutused EList edastatud andmetele juurde pääsevad ja saavad neid andmeid kasutada avaliku huvi eesmärkide saavutamiseks, eelkõige kriminaalõiguskaitse ja riikliku julgeoleku eesmärgil. Kehtestatud piirangud ja kaitsemeetmed tulenevad üldisest õigusraamistikust ja rahvusvahelistest kohustustest, eelkõige Andorra põhiseadusest, Euroopa inimõiguste konventsioonist ja Euroopa Nõukogu vastu võetud isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioonist (konventsioon nr 108 ja selle muutmisprotokoll, millega loodi ajakohastatud konventsioon nr 108+), ning andmekaitse erinormidest, mida kohaldatakse isikuandmete töötlemisel õiguskaitse kontekstis ja mis sisuliselt kattuvad direktiivi (EL) 2016/680[37] põhielementidega. Peale selle on Andorra õiguses kehtestatud mitu eritingimust ja -piirangut, mis käsitlevad avaliku sektori asutuste juurdepääsu isikuandmetele ja isikuandmete kasutamist neis asutustes, ning ette nähtud seonduvad järelevalve- ja õiguskaitsemehhanismid.

Komisjoni talituste töödokumendis esitatud üldiste tähelepanekute põhjal järeldab komisjon, et Andorra tagab jätkuvalt EList edastatud isikuandmete kaitse piisava taseme.

Mis puudutab andmekaitse erinorme, mida kohaldatakse õiguskaitseasutustes toimuva andmete töötlemise suhtes, siis komisjoni rõõmustab Andorra seadusandja kavatsus asendada kehtivad normid terviklikuma korraga, mis on veelgi paremini kooskõlas ELis kohaldatavate normidega. Komisjon jälgib tähelepanelikult selles valdkonnas toimuvat arengut.

4.2. Argentina

[37] Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta direktiiv (EL) 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK.

Komisjonile valmistab heameelt areng, mis on toimunud Argentina õigusraamistikus pärast kaitse piisavuse otsuse vastuvõtmist, sealhulgas seadusandlikud muudatused, kohtupraktika ja järelevalveasutuste tegevus, mis on aidanud tõsta andmekaitse taset. Eelkõige on dekreediga nr 746/17 suurendatud märkimisväärselt Argentina andmekaitse järelevalveasutuse sõltumatust, andes *Agencia de Acceso a la Información Públicale* ülesande teha järelevalvet andmekaitseõiguse järgimise üle. Lisaks on see asutus välja andnud mitu siduvat määrust ja arvamust, milles selgitatakse andmekaitseraamistiku tõlgendamist ja kohaldamist praktikas, aidates seega ajakohastada andmekaitseõigust. Samuti on Argentina tugevdanud oma andmekaitsealaseid rahvusvahelisi kohustusi, ühinedes 2019. aastal Euroopa Nõukogu konventsiooniga isikuandmete automatiseeritud töötlemisel isiku kaitse kohta ja selle lisaprotokolliga ning ratifitseerides 2023. aastal selle konventsiooni muutmisprotokolli, millega loodi ajakohastatud konventsioon nr 108+.

Mis puudutab valitsuse juurdepääsu isikuandmetele, siis kohaldatakse Argentina avaliku sektori asutuste suhtes selgeid, täpseid ja ligipääsetavaid õigusnorme, mille alusel need asutused EList edastatud andmetele juurde pääsevad ja saavad neid andmeid kasutada avaliku huvi eesmärkide saavutamiseks, eelkõige kriminaalõiguskaitse ja riikliku julgeoleku eesmärgil. Kehtestatud piirangud ja kaitsemeetmed tulenevad üldisest õigusraamistikust ja rahvusvahelistest kohustustest, eeskätt Argentina konstitutsioonist, Ameerika inimõiguste konventsioonist, konventsioonist nr 108 ja konventsioonist nr 108+, ning Argentina andmekaitsenormidest (4. oktoobri 2000. aasta seadus nr 25.326 isikuandmete kaitse kohta), mida kohaldatakse ka Argentina avaliku sektori asutustes isikuandmete töötlemise suhtes, sealhulgas õiguskaitse ja riikliku julgeoleku eesmärgil toimuva töötlemise suhtes. Peale selle on Argentina õiguses kehtestatud mitu eritingimust ja -piirangut, mis käsitlevad juurdepääsu isikuandmetele ja nende andmete kasutamist kriminaalõiguskaitse ja riikliku julgeoleku eesmärgil, ning ette nähtud seonduvad järelevalve- ja õiguskaitsemehhanismid.

Komisjoni talituste töödokumendis esitatud üldiste tähelepanekute põhjal järeldab komisjon, et Argentina tagab jätkuvalt EList edastatud isikuandmete kaitse piisava taseme.

Samal ajal soovitab komisjon sätestada mitteseadusandlikul tasandil välja töötatud kaitsemeetmed õigusaktides, et suurendada õiguskindlust ja need meetmed konsolideerida. Argentina kongressis hiljuti esitatud andmekaitseseaduse eelnõu võib anda võimaluse need meetmed kodifitseerida ja sellega veelgi tugevdada Argentina eraelu puutumatuse raamistikku. Komisjon jälgib tähelepanelikult selles valdkonnas toimuvat arengut.

4.3. Kanada

Komisjonile valmistab heameelt areng, mis on toimunud Kanada õigusraamistikus pärast kaitse piisavuse otsuse vastuvõtmist, sealhulgas mitu seadusandlikku muudatust, kohtupraktika ja järelevalveasutuste tegevus, mis on aidanud tõsta andmekaitse taset. Eelkõige on veelgi tugevdatud isikuandmete kaitse ja elektrooniliste dokumentide seadust, tehes sellesse mitmesuguseid muudatusi (mis puudutavad näiteks kehtiva nõusoleku tingimusi ja teavitamist isikuandmetega seotud rikkumistest), ning kohtupraktikas ja Kanada föderaalse andmekaitseasutuse (föderaalse eraelu puutumatuse kaitse voliniku büroo) välja antud suunistes on veelgi selgitatud peamisi andmekaitsenõudeid (nt tundlike andmete töötlemise kohta). Samal

ajal soovitab komisjon sätestada osa mitteseadusandlikul tasandil välja töötatud kaitsemeetmetest õigusaktides, et suurendada õiguskindlust ja need meetmed konsolideerida. Isikuandmete kaitse ja elektrooniliste dokumentide seaduse käimasolev reform võib anda võimaluse need meetmed kodifitseerida ja sellega veelgi tugevdada Kanada eraelu puutumatuse raamistikku. Komisjon jälgib tähelepanelikult selles valdkonnas toimuvat arengut.

Mis puudutab valitsuse juurdepääsu isikuandmetele, siis kohaldatakse Kanada avaliku sektori asutuste suhtes selgeid, täpseid ja ligipääsetavaid õigusnorme, mille alusel need asutused EList edastatud andmetele juurde pääsevad ja saavad neid andmeid kasutada avaliku huvi eesmärkide saavutamiseks, eelkõige kriminaalõiguskaitse ja riikliku julgeoleku eesmärgil. Kehtestatud piirangud ja kaitsemeetmed tulenevad üldisest põhiseaduslikust raamistikust (Kanada õiguste ja vabaduste harta), kohtupraktikast, andmetele juurdepääsu reguleerivatest eriõigusaktidest ja andmekaitsenormidest (st andmekaitseseadus ja sarnased seadused provintsi tasandil), mida kohaldatakse ka Kanada avaliku sektori asutustes isikuandmete töötlemise suhtes, sealhulgas õiguskaitse ja riikliku julgeoleku eesmärgil toimuva töötlemise suhtes. Peale selle on Kanada õigussüsteemis tagatud seonduvad tõhusad järelevalve- ja õiguskaitsemehhanismid, sealhulgas andmesubjektide õiguste ja õiguskaitsevõimaluste hiljutise laiendamisega isikutele, kes ei ole Kanada kodanikud või elanikud.

Komisjoni talituste töödokumendis esitatud üldiste tähelepanekute põhjal järeldab komisjon, et Kanada tagab jätkuvalt EList edastatud isikuandmete kaitse piisava taseme andmete edastamisel isikuandmete kaitse ja elektrooniliste dokumentide seaduse kohaldamisalasse kuuluvatele vastuvõtjatele. Nagu eespool märgitud, on praegu käsil selle seaduse reform, mille tulemusel võib eraelu puutumatuse kaitse veelgi tugevneda, sealhulgas kaitse piisavuse otsuse vaatenurgast olulistes valdkondades.

4.4. Fääri saared

Komisjonile valmistab heameelt areng, mis on toimunud Fääri saarte õigusraamistikus pärast kaitse piisavuse otsuse vastuvõtmist, sealhulgas seadusandlikud muudatused, kohtupraktika ja järelevalveasutuste tegevus, mis on aidanud tõsta andmekaitse taset. Eelkõige on Fääri saared märkimisväärselt ajakohastanud oma andmekaitseraamistikku, võttes vastu andmekaitseseaduse, mis jõustus 2021. aastal ja millega on Fääri saartel kohaldatav kord viidud heasse kooskõlla isikuandmete kaitse üldmäärusega.

Mis puudutab valitsuse juurdepääsu isikuandmetele, siis kohaldatakse Fääri saarte avaliku sektori asutuste suhtes selgeid, täpseid ja ligipääsetavaid õigusnorme, mille alusel need asutused EList edastatud andmetele juurde pääsevad ja saavad neid andmeid kasutada avaliku huvi eesmärkide saavutamiseks, eelkõige kriminaalõiguskaitse ja riikliku julgeoleku eesmärgil. Kehtestatud piirangud ja kaitsemeetmed tulenevad üldisest õigusraamistikust ja rahvusvahelistest kohustustest, eeskätt põhiseaduslikust raamistikust ja Euroopa inimõiguste konventsioonist, ning eriõigusaktidest, millega reguleeritakse valitsuse juurdepääsu andmetele, ja andmekaitsenormidest, mida kohaldatakse isikuandmete töötlemise suhtes andmete töötlemisel kriminaalõiguskaitse eesmärgil (õiguskaitseasutustes isikuandmete töötlemise seadus, mis jõustus Fääri saartel 2022. aastal ja millega võeti üle õigusakt, mille Taani oli vastu võtnud direktiivi (EL) 2016/680 rakendamiseks Fääri saartel) ja andmete töötlemisel riikliku

julgeoleku eesmärgil (luure- ja julgeolekuteenistuse seadus). Peale selle on olemas seonduvad tõhusad järelevalve- ja õiguskaitsemehhanismid.

Komisjoni talituste töödokumendis esitatud üldiste tähelepanekute põhjal järeldab komisjon, et Fääri saared tagavad jätkuvalt EList edastatud isikuandmete kaitse piisava taseme.

4.5. Guernsey

Komisjonile valmistab heameelt areng, mis on toimunud Guernsey õigusraamistikus pärast kaitse piisavuse otsuse vastuvõtmist, sealhulgas seadusandlikud muudatused ja järelevalveasutuste tegevus, mis on aidanud tõsta andmekaitse taset. Eelkõige on Guernsey märkimisväärselt ajakohastanud oma andmekaitseraamistikku, võttes vastu (Guernsey sõltkonna) 2017. aasta andmekaitseseaduse, mida kohaldatakse alates 2019. aastast ja millega on Guernseyl kohaldatav kord viidud heasse kooskõlla isikuandmete kaitse üldmäärusega.

Mis puudutab valitsuse juurdepääsu isikuandmetele, siis kohaldatakse Guernsey avaliku sektori asutuste suhtes selgeid, täpseid ja ligipääsetavaid õigusnorme, mille alusel need asutused EList edastatud andmetele juurde pääsevad ja saavad neid andmeid kasutada avaliku huvi eesmärkide saavutamiseks, eelkõige kriminaalõiguskaitse ja riikliku julgeoleku eesmärgil. Kehtestatud piirangud ja kaitsemeetmed tulenevad üldisest õigusraamistikust ja rahvusvahelistest kohustustest, eeskätt Euroopa inimõiguste konventsioonist ja konventsioonist nr 108, ning Guernsey andmekaitsenormidest, sealhulgas (õiguskaitsele ja seonduvatele küsimustele keskenduva) 2018. aasta (Guernsey sõltkonna) andmekaitsemääruse erisätetest, mis käsitlevad isikuandmete töötlemist õiguskaitse kontekstis. Peale selle on Guernsey õiguses kehtestatud mitu eritingimust ja -piirangut, mis käsitlevad juurdepääsu isikuandmetele ja nende andmete kasutamist kriminaalõiguskaitse ja riikliku julgeoleku eesmärgil, ning ette nähtud seonduvad järelevalve- ja õiguskaitsemehhanismid.

Komisjoni talituste töödokumendis esitatud üldiste tähelepanekute põhjal järeldab komisjon, et Guernsey tagab jätkuvalt EList edastatud isikuandmete kaitse piisava taseme.

4.6. Mani saar

Komisjonile valmistab heameelt areng, mis on toimunud Mani saare õigusraamistikus pärast kaitse piisavuse otsuse vastuvõtmist, sealhulgas seadusandlikud muudatused ja järelevalveasutuste tegevus, mis on aidanud tõsta andmekaitse taset. Eelkõige võttis Mani saar 2018. aastal vastu uued õigusaktid (2018. aasta andmekaitseseadus, mida täiendab isikuandmete kaitse üldmääruse kohaldamisele keskenduv 2018. aasta andmekaitsemäärus), millega on enamik ELi andmekaitseraamistiku sätteid inkorporeeritud Mani saare õiguskorda, tehes vaid väikesi muudatusi konkreetsetes aspektides, et kohandada raamistikku kohalikule kontekstile.

Mis puudutab valitsuse juurdepääsu isikuandmetele, siis kohaldatakse Mani saare avaliku sektori asutuste suhtes selgeid, täpseid ja ligipääsetavaid õigusnorme, mille alusel need asutused EList edastatud andmetele juurde pääsevad ja saavad neid andmeid kasutada avaliku huvi eesmärkide saavutamiseks, eelkõige kriminaalõiguskaitse ja riikliku julgeoleku eesmärgil. Kehtestatud piirangud ja kaitsemeetmed tulenevad üldisest õigusraamistikust ja

rahvusvahelistest kohustustest, eeskätt Euroopa inimõiguste konventsioonist ja konventsioonist nr 108, ning Mani saare andmekaitsenormidest, sealhulgas (õiguskaitsedirektiivi kohaldamise) 2018. aasta andmekaitsemääruse ja õiguskaitsedirektiivi 2018. aasta rakendusmääruste erisätetest, mis käsitlevad isikuandmete töötlemist õiguskaitse kontekstis. Peale selle on Mani saare õiguses kehtestatud mitu eripiirangut, mis käsitlevad juurdepääsu isikuandmetele ja nende andmete kasutamist kriminaalõiguskaitse ja riikliku julgeoleku eesmärgil, ning ette nähtud seonduvad järelevalve- ja õiguskaitsemehhanismid.

Komisjoni talituste töödokumendis esitatud üldiste tähelepanekute põhjal järeldab komisjon, et Mani saar tagab jätkuvalt EList edastatud isikuandmete kaitse piisava taseme.

4.7. Iisrael

Komisjonile valmistab heameelt areng, mis on toimunud Iisraeli õigusraamistikus pärast kaitse piisavuse otsuse vastuvõtmist, sealhulgas seadusandlikud muudatused, kohtupraktika ja järelevalveasutuste tegevus, mis on aidanud tõsta andmekaitse taset. Eelkõige on Iisrael kehtestanud EMPst edastatud isikuandmete kaitse tugevdamiseks spetsiaalsed kaitsemeetmed, võttes vastu eraelu puutumatuse kaitse eeskirjad nr 5783-2023 (juhised andmete jaoks, mis on Iisraeli edastatud Euroopa Majanduspiirkonnast). Iisrael on tugevdanud ka andmete turvalisusega seotud nõudeid, võttes vastu eraelu puutumatuse kaitse (andmeturbe) eeskirjad nr 5777-2017, ning suurendanud valitsuse siduva resolutsiooniga oma andmekaitse järelevalveasutuse sõltumatust.

Mis puudutab valitsuse juurdepääsu isikuandmetele, siis kohaldatakse Iisraeli avaliku sektori asutuste suhtes selgeid, täpseid ja ligipääsetavaid õigusnorme, mille alusel need asutused EList edastatud andmetele juurde pääsevad ja saavad neid andmeid kasutada avaliku huvi eesmärkide saavutamiseks, eelkõige kriminaalõiguskaitse ja riikliku julgeoleku eesmärgil. Kehtestatud piirangud ja kaitsemeetmed tulenevad üldisest õigusraamistikust, eeskätt Iisraeli põhiseadusest, ning eraelu puutumatuse kaitse seadusest nr 5741-1981 ja selle alusel vastu võetud eeskirjadest, mida kohaldatakse Iisraeli avaliku sektori asutustes isikuandmete töötlemise suhtes, sealhulgas õiguskaitse ja riikliku julgeoleku eesmärgil toimuva töötlemise suhtes. Peale selle on Iisraeli õiguses kehtestatud mitu eripiirangut, mis käsitlevad juurdepääsu isikuandmetele ja nende andmete kasutamist kriminaalõiguskaitse ja riikliku julgeoleku eesmärgil, ning ette nähtud seonduvad järelevalve- ja õiguskaitsemehhanismid.

Komisjoni talituste töödokumendis esitatud üldiste tähelepanekute põhjal järeldab komisjon, et Iisrael tagab jätkuvalt EList edastatud isikuandmete kaitse piisava taseme.

Samal ajal soovitab komisjon sätestada mitteseadusandlikul tasandil välja töötatud ja kohtupraktikal põhinevad kaitsemeetmed õigusaktides, et suurendada õiguskindlust ja need meetmed konsolideerida. Hiljuti Iisraeli parlamendile esitatud eraelu puutumatuse kaitse seaduse nr 5722-2022 eelnõu (muudatusettepanek nr 14) annab võimaluse need meetmed konsolideerida ja kodifitseerida ning sellega veelgi tugevdada Iisraeli eraelu puutumatuse raamistikku. Komisjon jälgib tähelepanelikult selles valdkonnas toimuvat arengut.

4.8. Jersey

Komisjonile valmistab heameelt areng, mis on toimunud Jersey õigusraamistikus pärast kaitse piisavuse otsuse vastuvõtmist, sealhulgas seadusandlikud muudatused, kohtupraktika ja järelevalveasutuste tegevus, mis on aidanud tõsta andmekaitse taset. Eelkõige on Jersey märkimisväärselt ajakohastanud oma andmekaitseraamistikku, võttes vastu 2018. aasta andmekaitseseaduse ja 2018. aasta seaduse andmekaitseasutuse kohta, mis jõustusid 2018. aastal ja millega on Jerseyl kohaldatav kord viidud heasse kooskõlla isikuandmete kaitse üldmäärusega.

Mis puudutab valitsuse juurdepääsu isikuandmetele, siis kohaldatakse Jersey avaliku sektori asutuste suhtes selgeid, täpseid ja ligipääsetavaid õigusnorme, mille alusel need asutused EList edastatud andmetele juurde pääsevad ja saavad neid andmeid kasutada avaliku huvi eesmärkide saavutamiseks, eelkõige kriminaalõiguskaitse ja riikliku julgeoleku eesmärgil. Kehtestatud piirangud ja kaitsemeetmed tulenevad üldisest õigusraamistikust ja rahvusvahelistest kohustustest, eeskätt Euroopa inimõiguste konventsioonist ja konventsioonist nr 108, ning Jersey andmekaitsenormidest, sealhulgas 2018. aasta andmekaitseseaduse erisätetest (mida on muudetud selle määruse 1. lisas sätestatud viisil), mis käsitlevad isikuandmete töötlemist õiguskaitse kontekstis. Peale selle on Jersey õiguses kehtestatud mitu eripiirangut, mis käsitlevad juurdepääsu isikuandmetele ja nende andmete kasutamist kriminaalõiguskaitse ja riikliku julgeoleku eesmärgil, ning ette nähtud seonduvad järelevalve- ja õiguskaitsemehhanismid.

Komisjoni talituste töödokumendis esitatud üldiste tähelepanekute põhjal järeldab komisjon, et Jersey tagab jätkuvalt EList edastatud isikuandmete kaitse piisava taseme.

4.9. Uus-Meremaa

Komisjonile valmistab heameelt areng, mis on toimunud Uus-Meremaa õigusraamistikus pärast kaitse piisavuse otsuse vastuvõtmist, sealhulgas seadusandlikud muudatused, kohtupraktika ja järelevalveasutuste tegevus, mis on aidanud tõsta andmekaitse taset. Eelkõige on reformitud põhjalikult andmekaitsekorda, võttes vastu 2020. aasta eraelu puutumatuse seaduse, millega on suurendatud veelgi kooskõla ELi andmekaitseraamistikuga, eriti isikuandmete rahvusvahelist edastamist käsitlevate õigusnormide ja andmekaitseasutuse (eraelu puutumatuse kaitse voliniku büroo) volituste osas.

Mis puudutab valitsuse juurdepääsu isikuandmetele, siis kohaldatakse Uus-Meremaa avaliku sektori asutuste suhtes selgeid, täpseid ja ligipääsetavaid õigusnorme, mille alusel need asutused EList edastatud andmetele juurde pääsevad ja saavad neid andmeid kasutada avaliku huvi eesmärkide saavutamiseks, eelkõige kriminaalõiguskaitse ja riikliku julgeoleku eesmärgil. Kehtestatud piirangud ja kaitsemeetmed tulenevad üldisest põhiseaduslikust raamistikust (nt õiguste deklaratsioon) ja kohtupraktikast ning eriõigusaktidest, millega reguleeritakse valitsuse juurdepääsu andmetele, ja eraelu puutumatuse seaduse sätetest, mida kohaldatakse ka isikuandmete töötlemise suhtes kriminaalasjadega tegelevates õiguskaitseasutustes ja riiklikes julgeolekuasutustes. Peale selle on Uus-Meremaa õigussüsteemis ette nähtud mitmesugused seonduvad järelevalve- ja õiguskaitsemehhanismid.

Komisjoni talituste töödokumendis esitatud üldiste tähelepanekute põhjal järeldab komisjon, et Uus-Meremaa tagab jätkuvalt EList edastatud isikuandmete kaitse piisava taseme. Komisjonile valmistab heameelt ka see, et Uus-Meremaa valitsus esitas hiljuti parlamendile 2020. aasta eraelu seaduse muutmise eelnõu, et veelgi tugevdada kehtivaid läbipaistvusnõudeid. Komisjon jälgib tähelepanelikult selles valdkonnas toimuvat arengut.

4.10. Šveits

Komisjonile valmistab heameelt areng, mis on toimunud Šveitsi õigusraamistikus pärast kaitse piisavuse otsuse vastuvõtmist, sealhulgas seadusandlikud muudatused, kohtupraktika ja järelevalveasutuste tegevus, mis on aidanud tõsta andmekaitse taset. Eelkõige on ajakohastatud föderaalse andmekaitseseadusega veelgi suurendatud kooskõla ELi andmekaitseraamistikuga, eeskätt tundlike andmete kaitse ja andmete rahvusvahelise edastamise eeskirjade osas. Samuti on Šveits tugevdanud oma andmekaitsealaseid rahvusvahelisi kohustusi, ratifitseerides septembris 2023 konventsiooni nr 108+.

Mis puudutab valitsuse juurdepääsu isikuandmetele, siis kohaldatakse Šveitsi avaliku sektori asutuste suhtes selgeid, täpseid ja ligipääsetavaid õigusnorme, mille alusel need asutused EList edastatud andmetele juurde pääsevad ja saavad neid andmeid kasutada avaliku huvi eesmärkide saavutamiseks, eelkõige kriminaalõiguskaitse ja riikliku julgeoleku eesmärgil. Kehtestatud piirangud ja kaitsemeetmed tulenevad üldisest õigusraamistikust ja rahvusvahelistest kohustustest, eeskätt Šveitsi föderaalsest põhiseadusest, Euroopa inimõiguste hartast ja konventsioonist nr 108+, ning Šveitsi andmekaitsenormidest, sealhulgas föderaalsest andmekaitseseadusest ja andmekaitse erinormidest, mida kohaldatakse kriminaalasjadega tegelevate õiguskaitseasutuste suhtes (nt kriminaalmenetluse seadustik) ja riiklike julgeolekuasutuste suhtes (nt luureteenistuse seadus). Peale selle on Šveitsi õiguses kehtestatud mitu eripiirangut, mis käsitlevad juurdepääsu isikuandmetele ja nende andmete kasutamist kriminaalõiguskaitse ja riikliku julgeoleku eesmärgil, ning ette nähtud seonduvad järelevalve- ja õiguskaitsemehhanismid.

Komisjoni talituste töödokumendis esitatud üldiste tähelepanekute põhjal järeldab komisjon, et Šveits tagab jätkuvalt EList edastatud isikuandmete kaitse piisava taseme.

4.11. Uruguay

Komisjonile valmistab heameelt areng, mis on toimunud Uruguay õigusraamistikus pärast kaitse piisavuse otsuse vastuvõtmist, sealhulgas mitu seadusandlikku muudatust, kohtupraktika ja järelevalveasutuste tegevus, mis on aidanud tõsta andmekaitse taset. Eelkõige on Uruguay ajakohastanud ja tugevdanud oma 2008. aasta seadust nr 18.331 isikuandmete kaitse ja õiguskaitsevahendi *habeas data* kohta, tehes sellesse 2018. ja 2020. aastal muudatused, millega suurendati andmekaitsealaste õigusaktide territoriaalset kohaldamisala, kehtestati uued vastutusega seotud nõuded (nagu mõjuhinnangud, lõimitud ja vaikimisi andmekaitse, teavitamine andmetega seotud rikkumistest ja andmekaitseametnike määramine) ja seati sisse lisakaitse biomeetriliste andmete jaoks. Samuti on Uruguay tugevdanud oma andmekaitsealaseid rahvusvahelisi kohustusi, ühinedes 2019. aastal konventsiooniga nr 108 ja ratifitseerides 2021. aastal konventsiooni nr 108+.

Mis puudutab valitsuse juurdepääsu isikuandmetele, siis kohaldatakse Uruguay avaliku sektori asutuste suhtes selgeid, täpseid ja ligipääsetavaid õigusnorme, mille alusel need asutused EList edastatud andmetele juurde pääsevad ja saavad neid andmeid kasutada avaliku huvi eesmärkide saavutamiseks, eelkõige kriminaalõiguskaitse ja riikliku julgeoleku eesmärgil. Kehtestatud piirangud ja kaitsemeetmed tulenevad üldisest õigusraamistikust ja rahvusvahelistest kohustustest, eeskätt Uruguay konstitutsioonist, Ameerika inimõiguste konventsioonist, konventsioonist nr 108 ja konventsioonist nr 108+, ning isikuandmete kaitset ja *habeas data* õiguskaitsevahendit käsitlevas seaduses nr 18.331 sätestatud andmekaitsenormidest, mida kohaldatakse Uruguay avaliku sektori asutustes isikuandmete töötlemise suhtes, eelkõige õiguskaitse ja riikliku julgeoleku eesmärgil toimuva töötlemise suhtes. Peale selle on Uruguay õiguses kehtestatud mitu eritingimust ja -piirangut, mis käsitlevad avaliku sektori asutuste juurdepääsu isikuandmetele ja nende andmete kasutamist neis asutustes, ning ette nähtud seonduvad järelevalve- ja õiguskaitsemehhanismid.

Esimese läbivaatamise raames tehtud üldiste tähelepanekute põhjal järeldab komisjon, et Uruguay tagab jätkuvalt EList edastatud isikuandmete kaitse piisava taseme.

5. EDASINE JÄRELEVALVE JA KOOSTÖÖ

Komisjon tunnistab ja hindab kõrgelt läbivaatamise raames toimunud suurepärast koostööd iga vaadeldud riigi ja territooriumi asjaomaste asutustega. Komisjon jälgib ka edaspidi tähelepanelikult asjaomaste riikide ja territooriumide andmekaitseraamistike ja tavade arengut. Kui riigis või territooriumil, mille andmekaitse tase on tunnistatud piisavaks, toimub areng, mis kaitse taset kahjustab, kasutab komisjon vajaduse korral isikuandmete kaitse üldmääruse artikli 45 lõikest 5 tulenevat õigust peatada kaitse piisavuse otsuse kehtivus, seda otsust muuta või see otsus kehtetuks tunnistada.

Läbivaatamine kinnitas, et kaitse piisavuse otsus ei kujuta endast finišijoont, vaid selle vastuvõtmine annab võimaluse veelgi elavdada dialoogi ja koostööd sarnaseid seisukohti jagavate rahvusvaheliste partneritega andmevoogude valdkonnas ja digiküsimustes üldisemalt. Sellega seoses jääb komisjon huviga ootama edasist suhtlust asjaomaste asutustega, et veelgi tugevdada rahvusvahelist koostööd turvaliste ja vabade andmevoogude edendamiseks, sealhulgas koostöö tugevdamisega õigusnormide täitmise tagamise valdkonnas. Selle dialoogi elavdamiseks ning teabe- ja kogemustevahetuse edendamiseks kavatseb komisjon korraldada 2024. aastal kõrgetasemelise kohtumise, mis toob kokku esindajad EList ja kõigist riikidest, mille kohta on tehtud kaitse piisavuse otsus.