Europos Sąjungos
Taryba

Briuselis, 2024 m. sausio 22 d.
(OR. en)

5454/24

DATAPROTECT 23
JAI 62
RELEX 42

PRIDEDAMAS PRANEŠIMAS

nuo:	Europos Komisijos generalinės sekretorės, kurios vardu pasirašo direktorė Martine DEPREZ
kam:	Europos Sąjungos Tarybos generalinei sekretorei Thérèse BLANCHET
Komisijos dok. Nr.:	COM(2024) 7 final
Dalykas:	KOMISIJOS ATASKAITA EUROPOS PARLAMENTUI IR TARYBAI dėl pirmosios peržiūros vertinant, kaip veikia sprendimai dėl tinkamumo, priimti pagal Direktyvos 95/46/EB 25 straipsnio 6 dalį

Delegacijoms pridedamas dokumentas COM(2024) 7 final.

Pridedama: COM(2024) 7 final

EUROPOS
KOMISIJA

Briuselis, 2024 01 15
COM(2024) 7 final

KOMISIJOS ATASKAITA EUROPOS PARLAMENTUI IR TARYBAI

dėl pirmosios peržiūros vertinant, kaip veikia sprendimai dėl tinkamumo, priimti pagal Direktyvos 95/46/EB 25 straipsnio 6 dalį

{SWD(2024) 3 final}

1. PIRMOJI PERŽIŪRA. PAGRINDINĖS APLINKYBĖS IR KONTEKSTAS

Šioje ataskaitoje pateikiamos Komisijos išvados, padarytos atlikus pirmąją sprendimų dėl tinkamumo, priimtų remiantis Direktyvos 95/46/EB[1] (Duomenų apsaugos direktyva) 25 straipsnio 6 dalimi, peržiūrą.

Šiuose sprendimuose Komisija nustatė, kad tinkamą iš Europos Sąjungos (ES) perduodamų asmens duomenų apsaugos lygį užtikrina vienuolika šalių ar teritorijų[2]: Andora[3], Argentina[4], Kanada (komercinės veiklos vykdytojų atveju)[5], Farerų Salos[6], Gernsis[7], Meno sala[8], Izraelis[9], Džersis[10], Naujoji Zelandija[11], Šveicarija[12] ir Urugvajus[13]. Todėl duomenys iš ES į šias šalis ar teritorijas gali būti perduodami netaikant papildomų reikalavimų.

2018 m. gegužės 25 d. pradėjus taikyti Reglamentą (ES) 2016/679[14] (BDAR), pagal Duomenų apsaugos direktyvą priimti sprendimai dėl tinkamumo toliau galiojo[15]. Be to, BDAR paaiškinta, kad išvados dėl tinkamumo yra evoliucionuojantys dokumentai, t. y. Komisija turi nuolat stebėti trečiųjų šalių pokyčius, dėl kurių esamų sprendimų dėl tinkamumo veiksmingumas

[1] 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, OL L 281, 1995 11 23, p. 31.
[2] BDAR įtraukus į Europos ekonominės erdvės (EEE) susitarimą jis taip pat taikomas Norvegijai, Islandijai ir Lichtenšteinui. Šioje ataskaitoje nuorodos į ES turėtų būti suprantamos kaip apimančios ir EEE valstybes.
[3] 2010 m. spalio 19 d. Komisijos sprendimas 2010/625/ES dėl tinkamos asmens duomenų apsaugos Andoroje pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB, OL L 277, 2010 10 21, p. 27.
[4] 2003 m. birželio 30 d. Komisijos sprendimas 2003/490/EB dėl adekvačios asmens duomenų apsaugos Argentinoje, remiantis Europos Parlamento ir Tarybos direktyva 95/46/EB, OL L 168, 2003 7 5, p. 19.
[5] 2001 m. gruodžio 20 d. Komisijos sprendimas 2002/2/EB dėl Kanados asmens duomenų apsaugos ir elektroninių dokumentų įstatyme numatytos tinkamos asmens duomenų apsaugos pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB, OL L 2, 2002 1 4, p. 13.
[6] 2010 m. kovo 5 d. Komisijos sprendimas 2010/146/ES dėl Farerų salų Asmens duomenų tvarkymo įstatyme numatytos tinkamos asmens duomenų apsaugos pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB, OL L 58, 2010 3 9, p. 17.
[7] 2003 m. lapkričio 21 d. Komisijos sprendimas 2003/821/EB dėl tinkamos asmens duomenų apsaugos Guernsey, OL L 308, 2003 11 25, p. 27.
[8] 2004 m. balandžio 28 d. Komisijos sprendimas 2004/411/EB dėl tinkamos asmens duomenų apsaugos Meno saloje, OL L 151, 2004 4 30 p. 48.
[9] 2011 m. sausio 31 d. Komisijos sprendimas 2011/61/ES dėl Izraelio Valstybės užtikrinamos tinkamos asmens duomenų apsaugos automatizuoto asmens duomenų tvarkymo srityje pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB, OL L 27, 2011 2 1, p. 39.
[10] 2008 m. gegužės 8 d. Komisijos sprendimas 2008/393/EB dėl tinkamos asmens duomenų apsaugos Džersyje, priimtas remiantis Europos Parlamento ir Tarybos direktyva 95/46/EB, OL L 138, 2008 5 28, p. 21.
[11] 2012 m. gruodžio 19 d. Komisijos įgyvendinimo sprendimas 2013/65/ES dėl Naujosios Zelandijos užtikrinamos tinkamos asmens duomenų apsaugos pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB, OL L 28, 2013 1 30, p. 12.
[12] 2000 m. liepos 26 d. Komisijos sprendimas 2000/518/EB dėl Šveicarijoje teikiamos pakankamos asmens duomenų apsaugos pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB, OL L 215, 2000 8 25, p. 1.
[13] 2012 m. rugpjūčio 21 d. Komisijos įgyvendinimo sprendimas 2012/484/ES dėl Urugvajaus Rytų Respublikos užtikrinamos tinkamos asmens duomenų apsaugos automatizuoto asmens duomenų tvarkymo srityje pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB, OL L 227, 2012 8 23, p. 11.
[14] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas), OL L 119, 2016 5 4, p. 1.
[15] Žr. BDAR 45 straipsnio 9 dalį, kurioje nustatyta, kad Komisijos sprendimai, priimti remiantis Direktyvos 95/46/EB 25 straipsnio 6 dalimi, galioja tol, kol bus iš dalies pakeisti, panaikinti arba pakeisti Komisijos sprendimu, priimtu pagal 45 straipsnio 3 arba 5 dalį.

galėtų pakisti[16]. Be to, pagal BDAR 97 straipsnį Komisija privalo periodiškai, kas ketverius metus, peržiūrėti šiuos sprendimus ir įvertinti, ar šalys ir teritorijos, kurių atžvilgiu buvo priimta išvada dėl tinkamumo, ir toliau užtikrina tinkamą asmens duomenų apsaugos lygį.

Ši pirmoji sprendimų dėl tinkamumo, priimtų pagal ankstesnę ES duomenų apsaugos sistemą, peržiūra buvo inicijuota atliekant platesnį BDAR taikymo ir veikimo vertinimą, kurio išvadas Komisija pateikė komunikate „Duomenų apsauga kaip daugiau galių suteikimo piliečiams ir ES požiūrio į perėjimą prie skaitmeninių technologijų pagrindas – dveji metai taikant Bendrąjį duomenų apsaugos reglamentą“[17]. Tačiau šios peržiūros dalies išvados buvo atidėtos siekiant atsižvelgti į Teisingumo Teismo sprendimą *Schrems II*[18], kuriame Teisingumo Teismas pateikė svarbių paaiškinimų dėl pagrindinių tinkamumo standarto elementų ir kitų susijusių pokyčių. Šiuo pagrindu atitinkamų šalių ir teritorijų buvo paprašyta pateikti išsamios informacijos apie atitinkamus jų teisinės sistemos, priežiūros mechanizmų ir vykdymo užtikrinimo sistemos aspektus[19]. Šioje ataskaitoje visapusiškai atsižvelgiama į visus šiuos pokyčius – tiek ES, tiek atitinkamose trečiosiose šalyse ir teritorijose.

Svarbu pažymėti, kad ši pirmoji peržiūra atliekama atsižvelgiant į sparčią skaitmeninių technologijų plėtrą. Pastaraisiais dešimtmečiais sprendimų dėl tinkamumo svarba labai išaugo, nes duomenų srautai tapo neatsiejamu visuomenės skaitmeninės transformacijos ir ekonomikos globalizacijos aspektu. Tarpvalstybinis duomenų perdavimas tapo visų dydžių ir visų sektorių Europos įmonių veiklos kasdienybe. Privatumo užtikrinimas kaip niekad anksčiau yra stabilių, saugių ir konkurencingų komercinių srautų sąlyga. Todėl sprendimai dėl tinkamumo tapo daug svarbesni, įvairiais aspektais. Jie užtikrina, kad perduodant duomenis kartu būtų perduodami ir jų apsaugos standartai – taip sudaromos sąlygos saugiems duomenų srautams, t. y. gerbiamos žmogaus tesės ir įgyvendinamas į žmogų orientuotas ES požiūris į skaitmeninę transformaciją. Jais pripažįstama, kad trečiųjų šalių privatumo sistemų lygis iš esmės yra lygiavertis ES apsaugos lygiui, ir tokiu būdu skatinama aukšto lygio apsaugos standartais grindžiamų privatumo sistemų konvergencija. Be to, kaip paaiškinta šioje ataskaitoje, sprendimai dėl tinkamumo nėra galutiniai – jie yra pagrindas glaudesniam ES ir panašiai mąstančių partnerių bendradarbiavimui ir tolesnei teisinio reguliavimo konvergencijai. Šiais sprendimais sudarytos sąlygos laisvam asmens duomenų judėjimui, jie atvėrė ES prekiautojams komercinių galimybių – be kita ko, jie papildė prekybos susitarimus ir padidino jų naudą, taip pat palengvino bendradarbiavimą su užsienio partneriais įvairiose reguliavimo srityse. Jais nustačius paprastą ir visapusišką duomenų perdavimo sistemą, duomenų eksportuotojui nereikia imtis papildomų apsaugos priemonių ar prašyti leidimų; visų pirma mažosioms ir vidutinėms įmonėms jie

[16] BDAR 45 straipsnio 4 dalis. Taip pat žr. 2015 m. spalio 6 d. Europos Sąjungos Teisingumo Teismo sprendimo *Maximillian Schrems prieš Data Protection Commissioner*, C-362/14 (toliau – *Schrems I*), ECLI:EU:C:2015:650, 76 punktą.

[17] Komunikatas paskelbtas 2020 m. birželio mėn., jį galima rasti šiuo adresu: https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:52020DC0264.

[18] 2020 m. liepos 16 d. Teisingumo Teismo sprendimas *Data Protection Commissioner prieš Facebook Ireland Ltd ir Maximillian Schrems* (*Schrems II*), C-311/18, ECLI:EU:C:2020:559.

[19] Sprendimas dėl tinkamumo Japonijos atžvilgiu buvo priimtas remiantis BDAR; jame numatyta, kad bus reguliariai atliekama atskira peržiūra. Užbaigus pirmąją peržiūrą, 2023 m. balandžio mėn. pateikta Komisijos ataskaita Europos Parlamentui ir Tarybai dėl pirmosios Japonijos sprendimo dėl tinkamumo veikimo peržiūros, COM(2023) 275 *final*; ją galima rasti adresu https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=COM:2023:275:FIN.

padeda užtikrinti atitiktį BDAR nustatytiems tarptautinio duomenų perdavimo reikalavimams. Galiausiai, kadangi Europos Komisijos priimti sprendimai dėl tinkamumo turi labai platų poveikį, jie tampa vis aktualesni ir už ES ribų – jais sudaromos sąlygos laisvai keistis duomenimis ne tik su 30 ES šalių, bet ir su daug daugiau šalių ir teritorijų visame pasaulyje[20], kurios pagal savo duomenų apsaugos taisykles šalis, dėl kurių priimtas ES sprendimas dėl tinkamumo, pripažįsta saugiomis paskirties vietomis.

Dėl visų šių priežasčių (ką taip pat patvirtino intensyvus ir vaisingas dialogas su atitinkamomis trečiosiomis šalimis ir teritorijomis, kuriuo grindžiama ši peržiūra), sprendimai dėl tinkamumo tapo strateginiu elementu palaikant ES santykius su šiais užsienio partneriais apskritai, ir yra pripažįstami kaip svarbus veiksnys stiprinant bendradarbiavimą įvairiose srityse. Todėl ypač svarbu, kad šie sprendimai atitiktų šio laikmečio iššūkius ir kad jais būtų atsižvelgiama į naujausius pokyčius ir problemas.

2. PERŽIŪROS OBJEKTAS IR METODIKA

Sprendimai dėl tinkamumo, kurie yra šios peržiūros objektas, buvo priimti pagal ES duomenų apsaugos sistemą, galiojusią iki BDAR. Paskutinį kartą sprendimai priimti prieš maždaug dešimtmetį (pvz., 2012 m. sprendimai dėl Naujosios Zelandijos ir Urugvajaus), tačiau tam tikri sprendimai galioja jau daugiau kaip dvidešimt metų (pvz., sprendimas dėl Kanados, priimtas 2001 m., ir dėl Šveicarijos, priimtas 2000 m.). Per tą laiką duomenų apsaugos sistemos visose vienuolikoje šalių ir teritorijų keitėsi, pavyzdžiui, vykdant teisėkūros ar reguliavimo reformas, plėtojant duomenų apsaugos institucijų vykdymo užtikrinimo praktiką ir teismų praktiką.

Todėl atlikdama vertinimą Komisija daugiausia dėmesio skyrė atitinkamų šalių ir teritorijų duomenų apsaugos sistemų pokyčiams, įvykusiems po sprendimo dėl tinkamumo priėmimo. Ji įvertino, kaip šie pokyčiai toliau keitė atitinkamos šalies ar teritorijos duomenų apsaugos aplinką ir ar skirtingos sistemos, atsižvelgiant į šiuos pokyčius, vis dar užtikrina tinkamą apsaugos lygį.

Buvo visapusiškai atsižvelgta į pačios ES duomenų apsaugos tvarkos raidą, visų pirma pradėjus taikyti BDAR. Visų pirma, priėmus šiuos sprendimus dėl tinkamumo, tokiems sprendimams taikomas teisinis standartas ir elementai, svarbūs vertinant, ar užsienio šalies sistema užtikrina tinkamą apsaugos lygį, buvo išsamiau išaiškinti Teisingumo Teismo praktikoje ir 29 straipsnio darbo grupės ir ją pakeitusios Europos duomenų apsaugos valdybos[21] (EDAV) priimtose gairėse.

Konkrečiai, 2015 m. spalio 6 d. Sprendime *Schrems I* Teisingumo Teismas nustatė, kad nors iš trečiosios šalies negalima reikalauti užtikrinti tokį patį apsaugos lygį, koks garantuojamas ES, tinkamumo kriterijus turi būti suprantamas taip, kad turi būti užtikrintas „iš esmės lygiavertis“ apsaugos lygis[22]. Visų pirma Teisingumo Teismas išaiškino, kad priemonės, kurių siekdama

[20] Kaip antai Argentina, Kolumbija, Izraelis, Marokas, Šveicarija ir Urugvajus.
[21] Europos duomenų apsaugos valdyboje kartu dirba valstybių narių duomenų apsaugos priežiūros institucijos ir Europos duomenų apsaugos priežiūros pareigūnas.
[22] *Schrems I*, 73, 74 ir 96 punktai. Taip pat žr. Reglamento (ES) 2016/679 104 konstatuojamąją dalį, kurioje kalbama apie esminio lygiavertiškumo standartą.

apsaugoti asmens duomenis gali imtis atitinkama trečioji valstybė, gali skirtis nuo Sąjungoje taikomų priemonių, jeigu šios priemonės praktiškai padeda veiksmingai užtikrinti tinkamo lygio apsaugą[23]. Todėl atliekant tinkamumo patikrą reikia išsamiai įvertinti visą trečiosios šalies sistemą, įskaitant privatumo apsaugos priemonių esmę, jų veiksmingumą ir vykdymo užtikrinimą.

Be to, Teismas paaiškino, kad Komisijos vertinimas neturėtų apsiriboti trečiosios šalies bendra duomenų apsaugos sistema – jis taip pat turėtų apimti taisykles, reglamentuojančias valdžios institucijų prieigą prie asmens duomenų, ypač teisėsaugos ir nacionalinio saugumo tikslais[24]. Kaip etalonu remdamasis Pagrindinių teisių chartija, Teismas nustatė keletą reikalavimų šioms taisyklėms, kad jos atitiktų „esminio lygiavertiškumo“ standartą. Pavyzdžiui, šios srities teisės aktuose turėtų būti numatytos aiškios ir tikslios taisyklės, kuriomis reglamentuojama priemonės apimtis ir taikymas ir nustatomi minimalūs reikalavimai, kad asmenims, kurių duomenims tai turi įtakos, būtų suteikta pakankamai garantijų, leidžiančių veiksmingai apsaugoti jų asmens duomenis nuo piktnaudžiavimo pavojų, taip pat bet kokios neteisėtos prieigos prie jų ir neteisėto jų naudojimo[25]. Jais taip pat turėtų būti užtikrinta, kad asmenys galėtų pasinaudoti teisių gynimo priemonėmis tam, kad gautų prieigą prie su jais susijusių asmens duomenų arba galėtų juos taisyti ar ištrinti[26].

BDAR grindžiamas Teisingumo Teismo pateiktais išaiškinimais – jame pateiktas išsamus elementų, į kuriuos Komisija turi atsižvelgti atlikdama tinkamumo vertinimą, sąvadas[27]. Be to, 2020 m. liepos 16 d. Sprendime *Schrems II* Teisingumo Teismas išsamiau išdėstė „esminio lygiavertiškumo“ standartą, visų pirma taisyklių dėl valdžios institucijų prieigos prie asmens duomenų teisėsaugos ir nacionalinio saugumo tikslais aspektą. Visų pirma jis paaiškino, kad taikant „esminio lygiavertiškumo“ standartą atitinkamose teisinėse sistemose, privalomose valdžios institucijoms atitinkamose trečiosiose šalyse ir teritorijose, turi būti numatytos būtiniausios apsaugos priemonės, kuriomis užtikrinama, kad tokios institucijos negalėtų gauti prieigos prie duomenų, jei tai nėra būtina ir proporcinga siekiant teisėtų tikslų, o duomenų subjektai turėtų turėti veiksmingas ir įgyvendinamas teises šių institucijų atžvilgiu[28].

Tinkamumo standarto raida taip pat matyti iš gairių, kurių pirmąją versiją priėmė 29 straipsnio darbo grupė, o vėlesnę – EDAV[29]. Šiose gairėse, visų pirma vadinamajame tinkamumo pavyzdžių dokumente, išsamiau paaiškinami elementai, į kuriuos Komisija turi atsižvelgti atlikdama tinkamumo vertinimą, be kita ko, nustatyta pareiga apžvelgti esmines garantijas valdžios institucijų prieigos prie asmens duomenų srityje. Pastarasis dokumentas visų pirma grindžiamas Europos Žmogaus Teisių Teismo praktika, be to, EDAV jį atnaujino atsižvelgdama

[23] *Schrems I*, 74 punktas.
[24] *Schrems I*, 90 punktas.
[25] *Schrems I*, 91 punktas.
[26] *Schrems I*, 95 punktas.
[27] BDAR 45 straipsnio 2 dalis.
[28] *Schrems II*, 180–182 punktai.
[29] „Tinkamumo pavyzdžiai“, WP 254, 1-oji peržiūrėta versija, 2018 m. vasario 6 d. (paskelbta adresu https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108).

į Teisingumo Teismo sprendime *Schrems II* pateiktus paaiškinimus[30]. Svarbu pažymėti, kad tinkamumo pavyzdžių dokumente taip pat pripažįstama, kad „esminio lygiavertiškumo“ standarto įgyvendinimas nėra vien pažodinis ES taisyklių atkartojimas (kopija), nes panašaus apsaugos lygio užtikrinimo priemonės įvairiose privatumo sistemose gali skirtis ir dažnai yra nustatomos atsižvelgiant į skirtingas teisines tradicijas.

Todėl, siekdama nustatyti, ar vienuolika sprendimų dėl tinkamumo, priimti pagal ankstesnes taisykles, ir toliau atitinka BDAR nustatytą standartą, Komisija atsižvelgė ne tik į atitinkamų šalių ir teritorijų duomenų apsaugos sistemų pokyčius, bet ir į paties tinkamumo standarto aiškinimo pagal ES teisę raidą. Ji taip pat įvertino teisinę sistemą, reglamentuojančią šalių ar teritorijų valdžios institucijų prieigą prie iš ES perduodamų asmens duomenų ir jų naudojimą, kuri, kaip buvo nustatyta, užtikrina tinkamą apsaugos lygį pagal Duomenų apsaugos direktyvos 25 straipsnio 6 dalį.

3. PERŽIŪROS PROCESAS

Kaip aprašyta pirmiau, vertinant galiojančius sprendimus dėl tinkamumo kiekvienos susijusios šalies ar teritorijos atveju atsižvelgiama į duomenų apsaugos sistemą ir visus atitinkamos teisinės sistemos pokyčius nuo to laiko, kai buvo priimta išvada dėl tinkamumo, taip pat į taisykles, kuriomis reglamentuojama vyriausybės prieiga prie duomenų, visų pirma teisėsaugos ir nacionalinio saugumo tikslais. Tam Komisijos tarnybos, glaudžiai bendradarbiaudamos su kiekviena atitinkama šalimi ar teritorija, per pastaruosius keletą metų atliko tam tikrus veiksmus, padėsiančius atlikti šį vertinimą.

Sudarydamos sąlygas Komisijai vykdyti stebėsenos įsipareigojimus, kiekviena iš vienuolikos šalių ar teritorijų pateikė Komisijai išsamią informaciją apie savo duomenų apsaugos tvarkos pokyčius nuo sprendimo dėl tinkamumo priėmimo. Be to, kiekvienos iš vienuolikos šalių ar teritorijų Komisija paprašė išsamios informacijos apie vyriausybės prieigos prie asmens duomenų (visų pirma teisėsaugos ir nacionalinio saugumo tikslais) taisykles, taikomas atitinkamoje šalyje ar teritorijoje. Taip pat Komisija kreipėsi į viešuosius šaltinius, priežiūros ir vykdymo užtikrinimo institucijas bei vietos ekspertus, prašydama informacijos apie sprendimų veikimą ir atitinkamus kiekvienos susijusios šalies ir teritorijos teisės ir praktikos pokyčius taikant duomenų apsaugos taisykles – tiek taikomas privatiems veiklos vykdytojams, tiek susijusias su vyriausybės prieiga. Galiausiai, tam tikrais atvejais buvo deramai atsižvelgta į tarptautinius įsipareigojimus, kuriuos šios šalys (teritorijos) prisiėmė pagal regioninius ar visuotinius susitarimus.

Remdamasi šiais duomenimis Komisija užmezgė intensyvų dialogą su kiekviena iš susijusių šalių ir teritorijų. Vykstant šiam dialogui paaiškėjo, kad daugelyje minėtų šalių ir teritorijų (pvz., Andoroje, Kanadoje, Farerų salose, Šveicarijoje, Naujojoje Zelandijoje) privatumo teisės aktai buvo modernizuoti ir sugriežtinti atlikus visapusiškas arba dalines reformas, kurias, be kita ko, paskatino poreikis užtikrinti sprendimų dėl tinkamumo galiojimo pratęsimą. Kai

[30] Rekomendacijos Nr. 02/2020 dėl Europos pagrindinių garantijų taikant stebėjimo priemones (paskelbta adresu https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_lt).

kuriose iš šių šalių, remiantis vykdymo užtikrinimo arba teismų praktika, priimti duomenų apsaugos institucijų nuostatai ir (arba) gairės, kuriais nustatyti nauji duomenų apsaugos reikalavimai (pvz., Izraelyje, Urugvajuje) arba patikslintos tam tikros privatumo taisyklės (pvz., Argentinoje, Kanadoje, Gernsyje, Džersyje, Meno saloje, Izraelyje, Naujojoje Zelandijoje). Be to, siekiant pašalinti svarbius apsaugos lygio skirtumus, su kai kuriomis susijusiomis šalimis ir teritorijomis – kai to reikėjo siekiant užtikrinti sprendimų dėl tinkamumo galiojimo partęsimą – buvo derėtasi ir susitarta dėl papildomų apsaugos priemonių, taikomų iš Europos perduodamiems asmens duomenims. Pavyzdžiui, Kanados vyriausybė išplėtė teisę susipažinti su viešojo sektoriaus tvarkomais asmens duomenimis ir juos taisyti – ji suteikta visiems asmenims, neatsižvelgiant į jų pilietybę ar gyvenamąją vietą (anksčiau šiomis teisėmis galėjo naudotis tik Kanados piliečiai, jos nuolatiniai gyventojai arba Kanadoje esantys asmenys)[31]. Kitas pavyzdys: Izraelio vyriausybė nustatė konkrečias apsaugos priemones, kuriomis siekiama sustiprinti iš Europos ekonominės erdvės perduodamų asmens duomenų apsaugą – visų pirma nustatyti nauji duomenų tikslumo ir saugojimo įpareigojimai, sustiprintos teisės gauti informaciją ir ją ištrinti, taip pat nustatyta daugiau neskelbtinų duomenų kategorijų[32].

Be to, Komisijos tarnybos surinko Europos Parlamento (Piliečių laisvių, teisingumo ir vidaus reikalų komiteto)[33], Tarybos (per Duomenų apsaugos darbo grupę)[34], EDAV[35] ir BDAR daugiašalės suinteresuotųjų subjektų ekspertų grupės[36] (kurią be kita ko sudaro pilietinės visuomenės, pramonės, akademinės bendruomenės atstovai ir praktikuojantys teisininkai) nuomones ir reguliariai informavo šiuos subjektus apie vertinimo pažangą.

Taigi ši ataskaita ir prie jos pridedamas tarnybų darbinis dokumentas yra glaudaus bendradarbiavimo su kiekviena iš susijusių šalių ir teritorijų, konsultacijų su atitinkamomis ES institucijomis ir įstaigomis bei jų indėlio rezultatas. Šie dokumentai grindžiami įvairiais šaltiniais, įskaitant teisės aktus, norminius aktus, teismų praktiką, duomenų apsaugos institucijų sprendimus ir gaires, (nepriklausomų) priežiūros įstaigų ataskaitas ir suinteresuotųjų subjektų indėlį. Prieš priimant šią ataskaitą visoms minėtoms šalims ir teritorijoms buvo suteikta galimybė patikrinti Komisijos tarnybų darbiniame dokumente pateiktos informacijos faktinį tikslumą.

---

[31] Privatumo įstatymo 12 straipsnis, Privatumo įstatymo išplėtimo įsakymas Nr. 1 ir Privatumo įstatymo išplėtimo įsakymas Nr. 2.

[32] Privatumo apsaugos nuostatai (nurodymai dėl duomenų, perduotų Izraeliui iš Europos ekonominės erdvės) 5783-2023, paskelbti 2023 m. gegužės 7 d. Izraelio oficialiajame leidinyje (*Reshumut*).

[33] Žr., pavyzdžiui, 2021 m. kovo 25 d. Europos Parlamento rezoliuciją dėl Komisijos vertinimo ataskaitos dėl Bendrojo duomenų apsaugos reglamento įgyvendinimo praėjus dvejiems metams nuo jo taikymo pradžios (2020/2717(RSP), kuri paskelbta adresu: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_LT.html.

[34] Žr., pavyzdžiui., 2019 m. gruodžio 19 d. priimtą Tarybos poziciją ir išvadas dėl Bendrojo duomenų apsaugos reglamento (BDAR) taikymo, kurios paskelbtos adresu: https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-1/lt/pdf.

[35] Žr., pavyzdžiui, 2020 m. vasario 18 d. priimtą EDAV nuomonę, įtraukiamą į BDAR vertinimą pagal 97 straipsnį, kuri paskalbta adresu: https://edpb.europa.eu/sites/default/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf.

[36] Žr., pavyzdžiui, daugiašalės suinteresuotųjų subjektų ekspertų grupės ataskaitą dėl BDAR vertinimo, kuri paskelbta adresu: https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=lt&do=groupDetail.groupMeeting&meetingId=21356.

4. PAGRINGINIAI FAKTAI IR IŠVADOS

Pirmoji peržiūra parodė, kad nuo tada, kai buvo priimti sprendimai dėl tinkamumo, kiekvienoje iš vienuolikos šalių ar teritorijų taikomos duomenų apsaugos sistemos dar labiau priartėjo prie ES sistemos. Be to, dėl vyriausybės prieigos prie asmens duomenų, pirmoji peržiūra parodė, kad šių šalių ar teritorijų teisėje nustatytos tinkamos šios srities apsaugos priemonės ir apribojimai, taip pat numatyti priežiūros ir teisių gynimo mechanizmai.

Išsamios išvados dėl kiekvienos iš vienuolikos šalių ar teritorijų pateikiamos prie šios ataskaitos pridedamame Komisijos tarnybų darbiniame dokumente. Remdamasi šiomis išvadomis, Komisija laikosi nuomonės, kad kiekviena iš vienuolikos šalių ir teritorijų toliau užtikrina tinkamą iš Europos Sąjungos perduodamų asmens duomenų apsaugos lygį, kaip apibrėžta BDAR ir atsižvelgiant į Teisingumo Teismo išaiškinimą. Toliau pateikiama išvadų dėl kiekvienos iš atitinkamų šalių ir teritorijų santrauka.

4.1. Andora

Komisija palankiai vertina tai, kaip Andoros teisinė sistema buvo pakeista nuo sprendimo dėl tinkamumo priėmimo, įskaitant teisės aktų pataisas ir priežiūros įstaigų veiklos pokyčius. Visų pirma, 2022 m. gegužės mėn. įsigaliojęs kvalifikuota balsų dauguma priimtas Įstatymas Nr. 29/2021 dėl asmens duomenų apsaugos padėjo pakelti duomenų apsaugos lygį – šio įstatymo struktūra ir pagrindinės nuostatos yra glaudžiai suderintos su BDAR.

Vyriausybės prieigos prie asmens duomenų srityje Andoros valdžios institucijoms taikomos aiškios, tikslios ir paprastos taisyklės, pagal kurias jos gali susipažinti su duomenimis, perduodamais iš ES, ir vėliau juos naudoti viešojo intereso – visų pirma baudžiamosios teisėsaugos ir nacionalinio saugumo – tikslais. Šie apribojimai ir apsaugos priemonės grindžiami bendrąja teisine sistema ir tarptautiniais įsipareigojimais, visų pirma Andoros Konstitucija, Europos žmogaus teisių konvencija (EŽTK) ir Europos Tarybos konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (Konvencija Nr. 108 ir jos pakeitimo protokolu, kuriuo nustatyta atnaujinta Konvencija Nr. 108+), taip pat konkrečiomis duomenų apsaugos taisyklėmis, taikomomis asmens duomenų tvarkymui teisėsaugos tikslais, kurios iš esmės pakartoja pagrindines Direktyvos (ES) 2016/680[37] nuostatas. Be to, Andoros teisėje nustatytos tam tikros konkrečios valdžios institucijų prieigos prie asmens duomenų ir jų naudojimo sąlygos ir apribojimai, taip pat numatyti priežiūros ir teisių gynimo mechanizmai šioje srityje.

Remdamasi Komisijos tarnybų darbiniame dokumente pateiktomis bendromis išvadomis, Komisija laikosi nuomonės, kad Andora ir toliau užtikrina tinkamą iš ES perduodamų asmens duomenų apsaugos lygį.

[37] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuria panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR.

Kalbant apie konkrečias duomenų apsaugos taisykles, kurios šiuo metu taikomos teisėsaugos institucijų atliekamam duomenų tvarkymui, Komisija teigiamai vertina Andoros teisės aktų leidėjo ketinimą pakeisti šias taisykles išsamesne tvarka, kuri bus dar labiau suderinta su ES taikomomis taisyklėmis. Komisija atidžiai stebės būsimus pokyčius šioje srityje.

4.2. Argentina

Komisija palankiai vertina tai, kaip Argentinos teisinė sistema buvo pakeista nuo sprendimo dėl tinkamumo priėmimo, įskaitant teisės aktų pataisas, teismų praktiką ir priežiūros įstaigų veiklos pokyčius, kurie padėjo pakelti duomenų apsaugos lygį. Visų pirma Argentinos duomenų apsaugos priežiūros institucijos nepriklausomumas gerokai padidėjo priėmus Dekretą Nr. 746/17, kuriuo Prieigos prie viešosios informacijos agentūrai (*Agencia de Acceso a la Información Pública*, AAIP) pavesta prižiūrėti, kaip laikomasi duomenų apsaugos teisės. Be to, AAIP paskelbė keletą privalomų nuostatų ir nuomonių, kuriuose paaiškinama, kaip duomenų apsaugos sistema turi būti aiškinama ir taikoma praktikoje – tai padeda palaikyti duomenų apsaugos teisės aktų aktualumą. Argentina taip pat sustiprino savo tarptautinius įsipareigojimus duomenų apsaugos srityje 2019 m. prisijungusi prie Europos Tarybos konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu ir jos papildomo protokolo, o 2023 m. ratifikavusi jos pakeitimo protokolą, kuriuo nustatyta atnaujinta Konvencija Nr. 108+.

Vyriausybės prieigos prie asmens duomenų srityje Argentinos valdžios institucijoms taikomos aiškios, tikslios ir paprastos taisyklės, pagal kurias jos gali susipažinti su duomenimis, perduodamais iš ES, ir vėliau juos naudoti viešojo intereso – visų pirma baudžiamosios teisėsaugos ir nacionalinio saugumo – tikslais. Šie apribojimai ir apsaugos priemonės grindžiami bendrąja teisine sistema ir tarptautiniais įsipareigojimais, visų pirma Argentinos Konstitucija, Amerikos žmogaus teisių konvencija, Konvencija Nr. 108 ir Konvencija Nr. 108+, taip pat Argentinos duomenų apsaugos taisyklėmis (2000 m. spalio 4 d. Įstatymu Nr. 25.326 dėl asmens duomenų apsaugos), kurios taip pat taikomos Argentinos valdžios institucijų vykdomam asmens duomenų tvarkymui, be kita ko, teisėsaugos ir nacionalinio saugumo tikslais. Be to, Argentinos teisėje nustatytos tam tikros konkrečios prieigos prie asmens duomenų ir jų naudojimo baudžiamosios teisėsaugos ir nacionalinio saugumo tikslais sąlygos ir apribojimai, taip pat numatyti priežiūros ir teisių gynimo mechanizmai šioje srityje.

Remdamasi Komisijos tarnybų darbiniame dokumente pateiktomis bendromis išvadomis, Komisija laikosi nuomonės, kad Argentina ir toliau užtikrina tinkamą iš ES perduodamų asmens duomenų apsaugos lygį.

Be to, Komisija rekomenduoja neteisėkūros lygmens apsaugos priemones numatyti teisės aktuose, taip būtų padidintas teisinis tikrumas ir konsoliduoti šie reikalavimai. Neseniai Argentinos Kongrese pristatytas Duomenų apsaugos įstatymo projektas yra galimybė kodifikuoti tokius pokyčius ir taip dar labiau sustiprinti Argentinos privatumo sistemą. Komisija atidžiai stebės būsimus pokyčius šioje srityje.

4.3. Kanada

Komisija palankiai vertina tai, kaip Kanados teisinė sistema buvo pakeista nuo sprendimo dėl tinkamumo priėmimo, įskaitant keletą teisės aktų pataisų, teismų praktiką ir priežiūros įstaigų veiklos pokyčius, kurie padėjo pakelti duomenų apsaugos lygį. Visų pirma Asmens duomenų apsaugos ir elektroninių dokumentų įstatymas (*Personal Information Protection and Electronic Documents Act*, PIPEDA) buvo dar labiau sugriežtintas priėmus įvairių pakeitimų (pvz., dėl galiojančio sutikimo sąlygų ir pranešimų apie duomenų apsaugos pažeidimus), be to, teismų praktikoje ir Kanados federalinės duomenų apsaugos institucijos – Privatumo priežiūros pareigūno tarnybos – gairėse išsamiau išaiškinti pagrindiniai duomenų apsaugos reikalavimai (pvz., dėl neskelbtinų duomenų tvarkymo). Be to, Komisija rekomenduoja tam tikras neteisėkūros lygmens apsaugos priemones numatyti teisės aktuose – taip būtų padidintas teisinis tikrumas ir konsoliduoti šie reikalavimai. Šiuo metu vykdoma PIPEDA teisėkūros reforma visų pirma yra galimybė kodifikuoti šias pataisas ir taip dar labiau sustiprinti Kanados privatumo sistemą. Komisija atidžiai stebės būsimus pokyčius šioje srityje.

Vyriausybės prieigos prie asmens duomenų srityje Kanados valdžios institucijoms taikomos aiškios, tikslios ir paprastos taisyklės, pagal kurias jos gali susipažinti su duomenimis, perduodamais iš ES, ir vėliau juos naudoti viešojo intereso – visų pirma baudžiamosios teisėsaugos ir nacionalinio saugumo – tikslais. Šie apribojimai ir apsaugos priemonės grindžiami bendrąja konstitucine sistema (Kanados teisių ir laisvių chartija), teismų praktika, konkrečiais teisės aktais, kuriais reglamentuojama prieiga prie duomenų, taip pat duomenų apsaugos taisyklėmis (t. y. Privatumo įstatymu ir panašiais provincijų lygmens teisės aktais), kurios taip pat taikomos Kanados valdžios institucijoms vykdant asmens duomenų tvarkymą, be kita ko, teisėsaugos ir nacionalinio saugumo tikslais. Be to, Kanados teisinėje sistemoje numatyti veiksmingi priežiūros ir teisių gynimo mechanizmai šioje srityje, be kita ko, neseniai duomenų subjektų teisės ir teisių gynimo galimybės išplėstos įtraukus į jų taikymo sritį ne Kanados piliečius ir joje negyvenančius asmenis.

Remdamasi Komisijos tarnybų darbiniame dokumente pateiktomis bendromis išvadomis, Komisija laikosi nuomonės, kad Kanada ir toliau užtikrina tinkamą iš ES subjektams, kuriems taikomas PIPEDA, perduodamų asmens duomenų apsaugos lygį. Kaip jau minėta, šiuo metu vykdoma PIPEDA teisėkūros reforma, kuria būtų galima dar labiau sustiprinti privatumo apsaugą, be kita ko, srityse, kurios yra svarbios priimant išvadą dėl tinkamumo.

4.4. Farerų Salos

Komisija palankiai vertina Farerų Salų teisinės sistemos pokyčius nuo sprendimo dėl tinkamumo priėmimo, įskaitant teisės aktų pakeitimus, teismų praktiką ir priežiūros įstaigų veiksmus, kurie padėjo pakelti duomenų apsaugos lygį. Visų pirma Farerų Salos iš esmės atnaujino savo duomenų apsaugos sistemą – priėmė Duomenų apsaugos įstatymą, kuris įsigaliojo 2021 m., ir Farerų Salose taikomą tvarką glaudžiai suderino su BDAR.

Vyriausybės prieigos prie asmens duomenų srityje Farerų Salų valdžios institucijoms taikomos aiškios, tikslios ir paprastos taisyklės, pagal kurias jos gali susipažinti su duomenimis, perduodamais iš ES, ir vėliau juos naudoti viešojo intereso – visų pirma baudžiamosios teisėsaugos ir nacionalinio saugumo – tikslais. Šie apribojimai ir apsaugos priemonės grindžiami bendrąja teisine sistema ir tarptautiniais įsipareigojimais, visų pirma konstitucine

sistema ir EŽTK, taip pat konkrečiais įstatymais, kuriais reglamentuojama vyriausybės prieiga prie duomenų ir nustatomos duomenų apsaugos taisyklės, taikomos asmens duomenų tvarkymui baudžiamosios teisėsaugos tikslais (2022 m. Farerų Salose įsigaliojo Įstatymas dėl teisėsaugos institucijų vykdomo asmens duomenų tvarkymo, kuriuo į Farerų Salų teisę perkeliami Danijos priimti teisės aktai, kuriais įgyvendinama Direktyva (ES) 2016/680) ir nacionalinio saugumo tikslais (nustatytos Saugumo ir žvalgybos tarnybos įstatyme). Be to, šioje srityje taikomi veiksmingi priežiūros ir teisių gynimo mechanizmai.

Remdamasi Komisijos tarnybų darbiniame dokumente pateiktomis bendromis išvadomis, Komisija laikosi nuomonės, kad Farerų Salos ir toliau užtikrina tinkamą iš ES perduodamų asmens duomenų apsaugos lygį.

4.5. Gernsis

Komisija palankiai vertina Gernsio teisinės sistemos pokyčius nuo sprendimo dėl tinkamumo priėmimo, įskaitant teisės aktų pakeitimus ir priežiūros įstaigų veiksmus, kurie padėjo pakelti duomenų apsaugos lygį. Visų pirma Gernsis iš esmės atnaujino savo duomenų apsaugos sistemą – 2017 m. priėmė Gernsio Valdos Duomenų apsaugos įstatymą, kuris taikomas nuo 2019 m. ir kuriuo Gernsio tvarka glaudžiai suderinta su BDAR.

Vyriausybės prieigos prie asmens duomenų srityje Gernsio valdžios institucijoms taikomos aiškios, tikslios ir paprastos taisyklės, pagal kurias jos gali susipažinti su duomenimis, perduodamais iš ES, ir vėliau juos naudoti viešojo intereso – visų pirma baudžiamosios teisėsaugos ir nacionalinio saugumo – tikslais. Šie apribojimai ir apsaugos priemonės grindžiami bendrąja teisine sistema ir tarptautiniais įsipareigojimais, visų pirma EŽTK ir Konvencija Nr. 108, taip pat Gernsio duomenų apsaugos taisyklėmis, įskaitant konkrečias nuostatas dėl asmens duomenų tvarkymo teisėsaugos tikslais, išdėstytas 2018 m. Gernsio Valdos potvarkyje dėl duomenų apsaugos (teisėsaugos ir susijusiais tikslais). Be to, Gernsio teisėje nustatytos tam tikros konkrečios prieigos prie asmens duomenų ir jų naudojimo baudžiamosios teisėsaugos ir nacionalinio saugumo tikslais sąlygos ir apribojimai, taip pat numatyti priežiūros ir teisių gynimo mechanizmai šioje srityje.

Remdamasi Komisijos tarnybų darbiniame dokumente pateiktomis bendromis išvadomis, Komisija laikosi nuomonės, kad Gernsis ir toliau užtikrina tinkamą iš ES perduodamų asmens duomenų apsaugos lygį.

4.6. Meno Sala

Komisija palankiai vertina Meno Salos teisinės sistemos pokyčius nuo sprendimo dėl tinkamumo priėmimo, įskaitant teisės aktų pakeitimus ir priežiūros įstaigų veiksmus, kurie padėjo pakelti duomenų apsaugos lygį. Visų pirma, 2018 m. Meno Sala priėmė naują teisės aktą (2018 m. Duomenų apsaugos aktą, papildytą 2018 m. Duomenų apsaugos potvarkiu (dėl BDAR taikymo)), kuriuo dauguma ES duomenų apsaugos sistemos nuostatų perkeliamos į Meno Salos teisinę sistemą, padarius tik nedidelių konkrečių aspektų pakeitimų, visų pirma siekiant pritaikyti sistemą prie vietos aplinkybių.

Vyriausybės prieigos prie asmens duomenų srityje Meno Salos valdžios institucijoms taikomos aiškios, tikslios ir paprastos taisyklės, pagal kurias jos gali susipažinti su duomenimis, perduodamais iš ES, ir vėliau juos naudoti viešojo intereso – visų pirma baudžiamosios teisėsaugos ir nacionalinio saugumo – tikslais. Šie apribojimai ir apsaugos priemonės grindžiami bendrąja teisine sistema ir tarptautiniais įsipareigojimais, visų pirma EŽTK ir Konvencija Nr. 108, taip pat Meno Salos duomenų apsaugos taisyklėmis, įskaitant konkrečias nuostatas dėl asmens duomenų tvarkymo teisėsaugos tikslais, išdėstytas 2018 m. Duomenų apsaugos potvarkyje (dėl Teisėsaugos direktyvos taikymo), ir 2018 m. Teisėsaugos direktyvos įgyvendinimo nuostatuose. Be to, Meno Salos teisėje nustatyti tam tikri konkretūs prieigos prie asmens duomenų ir jų naudojimo baudžiamosios teisėsaugos ir nacionalinio saugumo tikslais apribojimai, taip pat numatyti priežiūros ir teisių gynimo mechanizmai šioje srityje.

Remdamasi Komisijos tarnybų darbiniame dokumente pateiktomis bendromis išvadomis, Komisija laikosi nuomonės, kad Meno Sala ir toliau užtikrina tinkamą iš ES perduodamų asmens duomenų apsaugos lygį.

4.7. Izraelis

Komisija palankiai vertina tai, kaip Izraelio teisinė sistema buvo pakeista nuo sprendimo dėl tinkamumo priėmimo, įskaitant teisės aktų pataisas, teismų praktiką ir priežiūros įstaigų veiklos pokyčius, kurie padėjo pakelti duomenų apsaugos lygį. Visų pirma Izraelis nustatė konkrečias apsaugos priemones, kuriomis sustiprinta iš Europos ekonominės erdvės perduodamų asmens duomenų apsauga – priimti Privatumo apsaugos nuostatai (Nurodymai dėl duomenų, perduotų Izraeliui iš Europos ekonominės erdvės) Nr. 5783-2023. Izraelis taip pat sugriežtino duomenų saugumo reikalavimus – priimti Privatumo apsaugos (duomenų saugumo) nuostatai Nr. 5777-2017 ir privaloma Vyriausybės rezoliucija, kuria įtvirtintas duomenų apsaugos priežiūros institucijos nepriklausomumas.

Vyriausybės prieigos prie asmens duomenų srityje Izraelio valdžios institucijoms taikomos aiškios, tikslios ir paprastos taisyklės, pagal kurias jos gali susipažinti su duomenimis, perduodamais iš ES, ir vėliau juos naudoti viešojo intereso – visų pirma baudžiamosios teisėsaugos ir nacionalinio saugumo – tikslais. Šie apribojimai ir apsaugos priemonės grindžiami bendrąja teisine sistema, visų pirma Izraelio Pagrindiniu įstatymu, taip pat Privatumo apsaugos įstatymu (Nr. 5741-1981) ir pagal jį priimtais nuostatais, kurie taikomi Izraelio valdžios institucijoms vykdant asmens duomenų tvarkymą, be kita ko, teisėsaugos ir nacionalinio saugumo tikslais. Be to, Izraelio teisėje nustatyti tam tikri konkretūs prieigos prie asmens duomenų ir jų naudojimo baudžiamosios teisėsaugos ir nacionalinio saugumo tikslais apribojimai, taip pat numatyti priežiūros ir teisių gynimo mechanizmai šioje srityje.

Remdamasi Komisijos tarnybų darbiniame dokumente pateiktomis bendromis išvadomis, Komisija laikosi nuomonės, kad Izraelis ir toliau užtikrina tinkamą iš ES perduodamų asmens duomenų apsaugos lygį.

Be to, Komisija rekomenduoja neteisėkūros lygmens ir remiantis teismų praktika nustatytas apsaugos priemones numatyti teisės aktuose, taip būtų padidintas teisinis tikrumas ir įtvirtinti šie reikalavimai. Neseniai Izraelio parlamentui pateiktas Privatumo apsaugos įstatymo

projektas Nr. 5722-2022 (pakeitimas Nr. 14) yra svarbi galimybė konsoliduoti ir kodifikuoti tokius pokyčius ir taip dar labiau sustiprinti Izraelio privatumo sistemą. Komisija atidžiai stebės būsimus pokyčius šioje srityje.

4.8. Džersis

Komisija palankiai vertina Džersio teisinės sistemos pokyčius nuo sprendimo dėl tinkamumo priėmimo, įskaitant teisės aktų pakeitimus, teismų praktiką ir priežiūros įstaigų veiksmus, kurie padėjo pakelti duomenų apsaugos lygį. Visų pirma Džersis iš esmės atnaujino savo duomenų apsaugos sistemą – priėmė 2018 m. Džersio Duomenų apsaugos įstatymą ir 2018 m. Džersio Duomenų apsaugos institucijos įstatymą, įsigaliojusius 2018 m., kuriais Džersio tvarka glaudžiai suderinta su BDAR.

Vyriausybės prieigos prie asmens duomenų srityje Džersio valdžios institucijoms taikomos aiškios, tikslios ir paprastos taisyklės, pagal kurias jos gali susipažinti su duomenimis, perduodamais iš ES, ir vėliau juos naudoti viešojo intereso – visų pirma baudžiamosios teisėsaugos ir nacionalinio saugumo – tikslais. Šie apribojimai ir apsaugos priemonės grindžiami bendrąja teisine sistema ir tarptautiniais įsipareigojimais, visų pirma EŽTK ir Konvencija Nr. 108, taip pat Džersio duomenų apsaugos taisyklėmis, įskaitant konkrečias nuostatas dėl asmens duomenų tvarkymo teisėsaugos tikslais, išdėstytas 2018 m. Džersio Duomenų apsaugos įstatyme, su pakeitimais, padarytais šio įstatymo pakeitimu Nr. 1. Be to, Džersio teisėje nustatyti tam tikri konkretūs prieigos prie asmens duomenų ir jų naudojimo baudžiamosios teisėsaugos ir nacionalinio saugumo tikslais apribojimai, taip pat numatyti priežiūros ir teisių gynimo mechanizmai šioje srityje.

Remdamasi Komisijos tarnybų darbiniame dokumente pateiktomis bendromis išvadomis, Komisija laikosi nuomonės, kad Džersis ir toliau užtikrina tinkamą iš ES perduodamų asmens duomenų apsaugos lygį.

4.9. Naujoji Zelandija

Komisija palankiai vertina tai, kaip Naujosios Zelandijos teisinė sistema buvo pakeista nuo sprendimo dėl tinkamumo priėmimo, įskaitant teisės aktų pataisas, teismų praktiką ir priežiūros įstaigų veiklos pokyčius, kurie padėjo pakelti duomenų apsaugos lygį. Visų pirma, 2020 m. priimtu Privatumo įstatymu buvo atlikta visapusiška duomenų apsaugos tvarkos reforma, kuria dar labiau padidinta konvergencija su ES duomenų apsaugos sistema, ypač kalbant apie tarptautinio asmens duomenų perdavimo taisykles ir duomenų apsaugos institucijos (Privatumo priežiūros pareigūno tarnybos) įgaliojimus.

Vyriausybės prieigos prie asmens duomenų srityje Naujosios Zelandijos valdžios institucijoms taikomos aiškios, tikslios ir paprastos taisyklės, pagal kurias jos gali susipažinti su duomenimis, perduodamais iš ES, ir vėliau juos naudoti viešojo intereso – visų pirma baudžiamosios teisėsaugos ir nacionalinio saugumo – tikslais. Šie apribojimai ir apsaugos priemonės grindžiami bendrąja konstitucinės teisės sistema (pvz., Teisių chartija) ir teismų praktika, taip pat konkrečiais įstatymais, kuriais reglamentuojama vyriausybės prieiga prie duomenų bei Privatumo įstatymo nuostatomis, kurios taip pat taikomos tvarkant asmens duomenis

baudžiamosios teisėsaugos ir nacionalinio saugumo tikslais. Be to, Naujosios Zelandijos teisinėje sistemoje numatyta įvairių priežiūros ir teisių gynimo mechanizmų šioje srityje.

Remdamasi Komisijos tarnybų darbiniame dokumente pateiktomis bendromis išvadomis, Komisija laikosi nuomonės, kad Naujoji Zelandija ir toliau užtikrina tinkamą iš ES perduodamų asmens duomenų apsaugos lygį. Komisija taip pat palankiai vertina Naujosios Zelandijos vyriausybės neseniai Parlamentui pateiktą įstatymo projektą, kuriuo, siekiant dar labiau sugriežtinti esamus skaidrumo reikalavimus, iš dalies keičiamas 2020 m. Privatumo įstatymas. Komisija atidžiai stebės būsimus pokyčius šioje srityje.

4.10. Šveicarija

Komisija palankiai vertina tai, kaip Šveicarijos teisinė sistema buvo pakeista nuo sprendimo dėl tinkamumo priėmimo, įskaitant teisės aktų pataisas, teismų praktiką ir priežiūros įstaigų veiklos pokyčius, kurie padėjo pakelti duomenų apsaugos lygį. Visų pirma atnaujintas Federalinis duomenų apsaugos įstatymas, taip dar labiau padidinant konvergenciją su ES duomenų apsaugos sistema, ypač neskelbtinų duomenų apsaugos ir tarptautinio duomenų perdavimo taisyklių srityse. Šveicarija taip pat sustiprino savo tarptautinius įsipareigojimus duomenų apsaugos srityje 2023 m. rugsėjo mėn. ratifikavusi Konvenciją Nr. 108+.

Vyriausybės prieigos prie asmens duomenų srityje Šveicarijos valdžios institucijoms taikomos aiškios, tikslios ir paprastos taisyklės, pagal kurias jos gali susipažinti su duomenimis, perduodamais iš ES, ir vėliau juos naudoti viešojo intereso – visų pirma baudžiamosios teisėsaugos ir nacionalinio saugumo – tikslais. Šie apribojimai ir apsaugos priemonės grindžiami bendrąja teisine sistema ir tarptautiniais įsipareigojimais, visų pirma Šveicarijos federaline konstitucija, EŽTK ir Konvencija Nr. 108+, taip pat Šveicarijos duomenų apsaugos taisyklėmis, įskaitant Federalinį duomenų apsaugos įstatymą ir konkrečias duomenų apsaugos taisykles, taikomas baudžiamosios teisėsaugos institucijoms (kaip antai Baudžiamojo proceso kodeksas) ir nacionalinėms saugumo institucijoms (kaip antai Žvalgybos tarnybos įstatymas). Be to, Šveicarijos teisėje nustatyti tam tikri konkretūs prieigos prie asmens duomenų ir jų naudojimo baudžiamosios teisėsaugos ir nacionalinio saugumo tikslais apribojimai, taip pat numatyti priežiūros ir teisių gynimo mechanizmai šioje srityje.

Remdamasi Komisijos tarnybų darbiniame dokumente pateiktomis bendromis išvadomis, Komisija laikosi nuomonės, kad Šveicarija ir toliau užtikrina tinkamą iš ES perduodamų asmens duomenų apsaugos lygį.

4.11. Urugvajus

Komisija palankiai vertina tai, kaip Urugvajaus teisinė sistema buvo pakeista nuo sprendimo dėl tinkamumo priėmimo, įskaitant keletą teisės aktų pataisų, teismų praktiką ir priežiūros įstaigų veiklos pokyčius, kurie padėjo pakelti duomenų apsaugos lygį. Visų pirma Urugvajus atnaujino ir sustiprino savo 2008 m. Asmens duomenų apsaugos ir *habeas data* proceso įstatymą Nr. 18.331 – 2018 ir 2020 m. priimti šio įstatymo pakeitimai, kuriais išplėsta duomenų apsaugos nuostatų teritorinė taikymo sritis, nustatyti nauji atskaitomybės reikalavimai (pvz., numatyti poveikio vertinimai, pritaikytosios ir standartizuotosios duomenų apsaugos

priemonės, pranešimo apie duomenų saugumo pažeidimus ir duomenų apsaugos pareigūnų skyrimo tvarka) ir papildomos biometrinių duomenų apsaugos priemonės. Urugvajus taip pat sustiprino savo tarptautinius įsipareigojimus duomenų apsaugos srityje 2019 m. prisijungęs prie Konvencijos Nr. 108 ir 2021 m. ratifikavęs Konvenciją Nr. 108+ .

Vyriausybės prieigos prie asmens duomenų srityje Urugvajaus valdžios institucijoms taikomos aiškios, tikslios ir paprastos taisyklės, pagal kurias jos gali susipažinti su duomenimis, perduodamais iš ES, ir vėliau juos naudoti viešojo intereso – visų pirma baudžiamosios teisėsaugos ir nacionalinio saugumo – tikslais. Šie apribojimai ir apsaugos priemonės grindžiami bendrąja teisine sistema ir tarptautiniais įsipareigojimais, visų pirma Urugvajaus Konstitucija, Amerikos žmogaus teisių konvencija, Konvencija Nr. 108 ir Konvencija Nr. 108+, taip pat duomenų apsaugos taisyklėmis, įtvirtintomis Asmens duomenų apsaugos ir *habeas data* proceso įstatymu Nr. 18.331, kurios taip pat taikomos Urugvajaus valdžios institucijoms tvarkant asmens duomenis, ypač teisėsaugos ir nacionalinio saugumo tikslais. Be to, Urugvajaus teisėje nustatytos tam tikros konkrečios valdžios institucijų prieigos prie asmens duomenų ir jų naudojimo sąlygos ir apribojimai, taip pat numatyti priežiūros ir teisių gynimo mechanizmai šioje srityje.

Remdamasi bendromis šios pirmosios peržiūros išvadomis, Komisija laikosi nuomonės, kad Urugvajus ir toliau užtikrina tinkamą iš ES perduodamų asmens duomenų apsaugos lygį.

5. BŪSIMA STEBĖSENA IR BENDRADARBIAVIMAS

Komisija pripažįsta ir labai vertina, kad atliekant šią peržiūrą buvo puikiai bendradarbiaujama su atitinkamomis kiekvienos susijusios šalies ir teritorijos valdžios institucijomis. Komisija toliau atidžiai stebės atitinkamų šalių ir teritorijų apsaugos sistemų pokyčius ir faktinę praktiką. Jei šalyje ar teritorijoje, kurios atžvilgiu priimtas tinkamumo sprendimas, įvyktų pokyčių, dėl kurių nukentėtų tinkamas duomenų apsaugos lygis, Komisija prireikus pasinaudos savo įgaliojimais pagal BDAR 45 straipsnio 5 dalį sustabdyti, iš dalies pakeisti arba atšaukti sprendimą dėl tinkamumo.

Šia peržiūra patvirtinama, kad sprendimo dėl tinkamumo priėmimas nėra galutinis – tai galimybė toliau intensyvinti dialogą duomenų srautų ir visais kitais skaitmeniniais klausimais ir plėsti bendradarbiavimą su panašiai mąstančiais tarptautiniais partneriais. Todėl Komisija tikisi ir ateityje keistis informacija su atitinkamomis valdžios institucijomis, kad toliau stiprėtų tarptautinis bendradarbiavimas skatinant saugius ir laisvus duomenų srautus, be kita ko, bendradarbiaujant vykdymo užtikrinimo srityje. Siekdama paspartinti šį dialogą ir skatinti keitimąsi informacija bei patirtimi, Komisija ketina 2024 m. surengti aukšto lygio susitikimą, kuriame dalyvautų ES ir visų šalių, dėl kurių priimti sprendimai dėl tinkamumo, atstovai.