



Briuselis, 2020 06 24  
SWD(2020) 115 final

**KOMISIJOS TARNYBŲ DARBINIS DOKUMENTAS**

[...]

*pridedamas prie*

**KOMISIJOS KOMUNIKATO EUROPOS PARLAMENTUI IR TARYBAI**

**Duomenų apsauga kaip daugiau galių suteikimo piliečiams ir ES požiūrio į perėjimą  
prie skaitmeninių technologijų pagrindas – dveji metai taikant Bendrąjį duomenų  
apsaugos reglamentą**

{COM(2020) 264 final}

## Turinys

1	Bendroji informacija.....	3
2	BDAR vykdymo užtikrinimas ir bendradarbiavimo ir nuoseklumo užtikrinimo mechanizmų veikimas.....	4
2.1	Naudojimas susitvirtais duomenų apsaugos institucijų įgaliojimais .....	4
	Konkrečiai su viešuoju sektoriumi susiję klausimai .....	5
	Bendradarbiavimas su kitomis reguliavimo institucijomis.....	5
2.2	Bendradarbiavimo ir nuoseklumo užtikrinimo mechanizmai .....	6
	Vieno langelio principas .....	7
	Savitarpio pagalba.....	8
	Nuoseklumo užtikrinimo mechanizmas.....	8
	Spręstinės problemos .....	9
2.3	Rekomendacijos ir gairės .....	10
	Informuotumo didinimas ir duomenų apsaugos institucijos rekomendacijos.....	10
	Europos duomenų apsaugos valdybos gairės.....	11
2.4	Duomenų apsaugos institucijų ištekliai.....	12
3	Taisyklės suderintos, bet vis dar esama susiskaidymo ir taikomi skirtingi metodai	14
3.1	BDAR įgyvendinimas valstybėse narėse .....	14
	Pagrindinės problemos, susijusios su įgyvendinimu nacionaliniu lygmeniu.....	15
	Teisės į asmens duomenų apsaugą derinimas su žodžio laisve ir teise į informaciją .....	16
3.2	Neprivalomos patikslinamosios nuostatos ir jų ribos.....	17
	Su neprivalomų patikslinamųjų nuostatų naudojimu susijęs susiskaidymas .....	17
4	Įgaliojimas fiziniams asmenims valdyti savo duomenis .....	20
5	Organizacijų, visų pirma mažųjų ir vidutinių įmonių, galimybės ir iššūkiai .....	23
	Įmonėms skirtų priemonių rinkinys .....	25
6	BDAR taikymas naujoms technologijoms .....	27
7	Tarptautinis duomenų perdavimas ir pasaulinis bendradarbiavimas.....	29
7.1	Privatumas. Pasaulio masto klausimas.....	29
7.2	Duomenų perdavimo pagal BDAR priemonių rinkinys.....	31
	Sprendimai dėl tinkamumo .....	32
	Tinkamos apsaugos priemonės .....	37
	Nukrypti leidžiančios nuostatos .....	42
	Užsienio teismų ar institucijų sprendimai: nėra pagrindas perduoti duomenis ...	43
7.3	Tarptautinis bendradarbiavimas duomenų apsaugos srityje.....	45

Dvišalis lygmuo .....	45
Daugiašalis aspektas .....	47

I priedas. Nuostatos dėl neprivalomų nacionalinės teisės aktuose įtvirtintų patikslinimų

II priedas. Duomenų apsaugos institucijų išteklių apžvalga

## 1 BENDROJI INFORMACIJA

Bendrasis duomenų apsaugos reglamentas<sup>1</sup> (toliau – BDAR) – aštuonerių metų paruošimo, rengimo ir tarpinstitucinių derybų rezultatas; jis pradėtas taikyti 2018 m. gegužės 25 d. praėjus dvejų metų pereinamajam laikotarpiui (2016 m. gegužės mėn. – 2018 m. gegužės mėn.). Pagal BDAR 97 straipsnį Komisija turi pateikti reglamento vertinimo ir peržiūros ataskaitą; pirmoji ataskaita teikiama praėjus dvejimėms metams ir vėliau kas ketverius metus.

Vertinimas taip pat yra daugialypio požiūrio, kurio Komisija laikėsi dar prieš pradėjus taikyti BDAR ir kurį vis dar aktyviai naudoja, dalis. Laikydamosi šio požiūrio Komisija dalyvavo su valstybėmis narėmis vykstančiuose dvišaliuose dialoguose dėl nacionalinės teisės aktų suderinamumo su BDAR, aktyviai prisidėjo prie Europos duomenų apsaugos valdybos (toliau – Valdyba) darbo dalydamasi savo patirtimi ir žiniomis, padėjo duomenų apsaugos institucijoms ir su daugeliu suinteresuotųjų subjektų palaikė glaudų ryšį dėl reglamento praktinio taikymo.

Vertinimas grindžiamas apžvalga, kurią Komisija parengė pirmaisiais BDAR taikymo metais ir kuri yra apibendrinta 2019 m. liepos mėn. paskelbtame komunikate<sup>2</sup>. Be to, jis atliktas atsižvelgiant į 2018 m. sausio mėn. paskelbtą komunikatą dėl BDAR taikymo<sup>3</sup>. 2018 m. rugsėjo mėn. Komisija taip pat priėmė asmens duomenų naudojimo rinkimuose gaires, o 2020 m. balandžio mėn. buvo paskelbtos duomenų apsaugos gairės dėl kovai su COVID-19 pandemija naudojamų programėlių.

Nors dėmesys sutelkiamas į du BDAR 97 straipsnio 2 dalyje pabrėžtus aspektus, t. y. duomenų perdavimą tarptautiniu lygmeniu ir bendradarbiavimo ir nuoseklumo užtikrinimo mechanizmus, šiame vertinime laikomasi bendresnio požiūrio siekiant spręsti problemas, kurias per pastaruosius dvejus metus iškėlė įvairūs subjektai.

Rengdama vertinimą Komisija atsižvelgė į šių šalių indėlius:

- Tarybos<sup>4</sup>;
- Europos Parlamento (Piliečių laisvių, teisingumo ir vidaus reikalų komiteto)<sup>5</sup>;
- Valdybos<sup>6</sup> ir pavienių duomenų apsaugos institucijų<sup>7</sup>, remiantis Komisijos išsiųstu klausimynu;

---

<sup>1</sup> 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 (OL L 119, 2016 5 4, p. 1–88).

<sup>2</sup> Komisijos komunikatas Europos Parlamentui ir Tarybai, Duomenų apsaugos taisyklių kaip priemonės pasitikėjimui didinti ES ir už ES ribų vertinimas, COM(2019) 374 *final*, 2019 m. liepos 24 d.

<sup>3</sup> Komisijos komunikatas Europos Parlamentui ir Tarybai „Didesnė apsauga, naujos galimybės. Komisijos gairės dėl tiesioginio Bendrojo duomenų apsaugos reglamento taikymo nuo 2018 m. gegužės 25 d.“, COM/2018/043 *final*.

<sup>4</sup> Tarybos pozicija ir išvados dėl Bendrojo duomenų apsaugos reglamento (BDAR) taikymo, 14994/2/19 Rev2, 2020 m. sausio 15 d.:

<https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-2/lt/pdf>

<sup>5</sup> 2020 m. vasario 21 d. Europos Parlamento LIBE komiteto raštas Komisijos nariui D. Reyndersui, IPOL-COM-LIBE D (2020)6525.

<sup>6</sup> Valdybos nuomonė dėl BDAR vertinimo pagal 97 straipsnį, priimta 2020 m. vasario 18 d.: [https://edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-evaluation-gdpr-under-article-97\\_en](https://edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-evaluation-gdpr-under-article-97_en).

- įvairių suinteresuotųjų subjektų grupės narių pateiktą grįžtamąją informaciją dėl BDAR taikymo<sup>8</sup>, taip pat remiantis Komisijos išsiųstu klausimynu;
- iš suinteresuotųjų subjektų gautus *ad hoc* indėlius.

## 2 BDAR VYKDYMO UŽTIKRINIMAS IR BENDRADARBIAVIMO IR NUOSEKLUMO UŽTIKRINIMO MECHANIZMŲ VEIKIMAS

BDAR sukurta novatoriška valdymo sistema ir tikrosios europinės duomenų apsaugos kultūros pagrindas siekiant užtikrinti ne tik vienodą aiškinimą, bet ir vienodą duomenų apsaugos taisyklių taikymą ir vykdymo užtikrinimą. Jo ramsčiai – nepriklausomos nacionalinės duomenų apsaugos institucijos ir neseniai įsteigta Valdyba.

Kadangi duomenų apsaugos institucijos yra itin svarbios visos ES duomenų apsaugos sistemos veikimui, Komisija įdėmiai stebi jų faktinį nepriklausomumą, taip pat kalbant apie pakankamus finansinius, žmogiškuosius ir techninius išteklius.

Dar per anksti išsamiai vertinti bendradarbiavimo ir nuoseklumo užtikrinimo mechanizmų veikimą, nes patirties sukaupta dar nedaug<sup>9</sup>. Be to, duomenų apsaugos institucijos dar nėra pasinaudojusios visomis BDAR priemonėmis, kuriomis siekiama toliau stiprinti jų bendradarbiavimą.

### 2.1 Naudojimas sustiprintais duomenų apsaugos institucijų įgaliojimais

BDAR įsteigiamos nepriklausomos duomenų apsaugos institucijos, kurioms suteikiami suderinti ir sustiprinti vykdymo užtikrinimo įgaliojimai. Nuo BDAR taikymo pradžios tos institucijos naudoja įvairius BDAR numatytus įgaliojimus imtis taisomųjų veiksmų, kaip antai skirti administracines baudas (22 ES ir EEE institucijos)<sup>10</sup>, įspėjimus ir papeikimus (23), nurodymus patenkinti duomenų subjekto prašymus (26), nurodymus suderinti duomenų tvarkymo operacijas su BDAR (27) ir nurodymus ištaisyti ar ištrinti asmens duomenis arba apriboti jų tvarkymą (17). Maždaug pusė duomenų apsaugos institucijų (13) yra nustačiusios laikiną arba galutinį duomenų tvarkymo apribojimą, įskaitant tvarkymo draudimą. Tai rodo, kad sąmoningai naudojamosi visomis BDAR numatytomis taisomosiomis priemonėmis; duomenų apsaugos institucijos nevengė skirti administracines baudas kartu taikydamos kitas taisomasias priemones arba užuot jas taikiusios, priklausomai nuo konkrečių atvejų aplinkybių.

<sup>7</sup> [https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities\\_en](https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_en).

<sup>8</sup> Komisijos sudarytą įvairių suinteresuotųjų subjektų grupę reglamento klausimais sudaro pilietinės visuomenės, verslo ir akademinio pasaulio atstovai ir srities specialistai: <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537>.

Įvairių suinteresuotųjų subjektų grupės ataskaita paskelbta šiuo adresu:

<https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=21356>.

<sup>9</sup> Tai taip pat pabrėžiama, visų pirma, Tarybos pozicijoje ir išvadose dėl BDAR taikymo bei Valdybos nuomonėje dėl vertinimo.

<sup>10</sup> Skaičiai skliausteliuose – tai ES ir EEE valstybių duomenų apsaugos institucijų, per laikotarpį nuo 2018 m. gegužės mėn. iki 2019 m. lapkričio mėn. pabaigos pasinaudojusių numatytais įgaliojimais, skaičius. Žr. Valdybos nuomonę, p. 32 ir 33.

### *Administracinės baudos*

2018 m. gegužės 25 d. – 2019 m. lapkričio 30 d. 22 ES ir EEE duomenų apsaugos institucijos skyrė maždaug 785 baudas. Tik kelios institucijos dar nėra skyrusios nė vienos administracinės baudos, nors užbaigus šiuo metu vykdomas procedūras tokios baudos gali būti skirtos. Dauguma baudų buvo susijusios su: teisėtumo principu; galiojančiu sutikimu; neskelbtinų duomenų apsauga; skaidrumo prievole ir duomenų subjektų teisėmis ir duomenų apsaugos pažeidimais.

Duomenų apsaugos institucijų skirtų baudų pavyzdžiai<sup>11</sup>:

- 200 000 EUR už teisės nesutikti dėl tiesioginės rinkodaros nepaisymą Graikijoje;
- 220 000 EUR bauda Lenkijos duomenų brokerių bendrovei už tai, kad neinformavo asmenų apie tai, kad buvo tvarkomi jų duomenys;
- 250 000 EUR bauda Ispanijos futbolo lygai „LaLiga“ už tai, kad rengiant išmaniajam telefonui skirtą programėlę stokota skaidrumo;
- 14,5 mln. EUR bauda Vokietijos nekilnojamojo turto įmonei už duomenų apsaugos principų pažeidimą, visų pirma neteisėtą saugojimą;
- 18 mln. EUR Austrijos pašto paslaugų įmonei už neteisėtą specialių kategorijų duomenų tvarkymą dideliu mastu;
- 50 mln. EUR bauda įmonei „Google“ Prancūzijoje dėl sąlygų naudotojų sutikimui gauti.

BDAR sėkmės nederėtų matuoti skirtų baudų skaičiumi, nes BDAR yra numatyta daugiau taisomųjų įgaliojimų. Priklausomai nuo aplinkybių, pavyzdžiui, draudimo tvarkyti duomenų srautus ar jų tvarkymo sustabdymo atgrasomasis poveikis gali būti daug didesnis.

### *Konkrečiai su viešuoju sektoriumi susiję klausimai*

Pagal BDAR valstybės narės gali nustatyti, ar ir koku mastu administracinės baudos gali būti skiriamos valdžios institucijoms ir įstaigoms. Jeigu valstybės narės pasinaudoja šia galimybe, duomenų apsaugos institucijoms tai netrukdo taikyti valdžios institucijoms ir įstaigoms visas kitas taisomąsias priemones<sup>12</sup>.

Dar vienas ypatingas klausimas yra teismų priežiūra: nors BDAR taip pat taikomas teismų veiklai, jiems vykdant teismines funkcijas jie yra atleidžiami nuo duomenų apsaugos institucijų vykdomos priežiūros. Tačiau pagal Chartiją ir SESV valstybės narės privalo patikėti tokių tvarkymo operacijų priežiūrą nepriklausomai įstaigai savo teismų sistemoje<sup>13</sup>.

### *Bendradarbiavimas su kitomis reguliavimo institucijomis*

Kaip paskelbta 2019 m. liepos mėn. komunikate, Komisija pritaria, kad reikalinga sąveika su kitomis reguliavimo institucijomis paisant visų atitinkamų kompetencijos

<sup>11</sup> Kai kurie sprendimai dėl baudų skyrimo vis dar peržiūrimi teisme.

<sup>12</sup> BDAR 83 straipsnio 7 dalis.

<sup>13</sup> Chartijos 8 straipsnio 3 dalis; SESV 16 straipsnio 2 dalis. BDAR 20 konstatuojamoji dalis.

ribų. Perspektyvios bendradarbiavimo sritys – vartotojų apsauga ir konkurencija. Valdyba išreiškė norą bendradarbiauti su kitomis reguliavimo institucijomis, visų pirma dėl koncentracijos skaitmeninėse rinkose<sup>14</sup>. Komisija pripažino privatumo ir duomenų apsaugos kaip kokybinio konkurencijos parametro svarbą<sup>15</sup>. Valdybos nariai dalyvavo bendruose seminaruose su Bendradarbiavimo vartotojų apsaugos srityje tinklu dėl bendradarbiavimo siekiant geriau užtikrinti ES vartotojų ir duomenų apsaugos teisės aktų vykdymą. Šio požiūrio bus laikomasi siekiant skatinti bendrą supratimą ir rasti praktinių būdų spręsti konkrečias problemas, su kuriomis susiduria vartotojai, visų pirma skaitmeninėje ekonomikoje.

Siekiant užtikrinti nuoseklų požiūrį į privatumą ir duomenų apsaugą, kol bus priimtas E. privatumo reglamentas, būtina glaudžiai bendradarbiauti su valdžios institucijomis, kompetentingomis užtikrinti E. privatumo direktyvos<sup>16</sup>, kuri yra *lex specialis* elektroninių ryšių srityje, vykdymą. Glaudesnis bendradarbiavimas su institucijomis, kompetentingomis pagal TIS direktyvą<sup>17</sup>, ir TIS bendradarbiavimo grupė būtų naudingas ir toms valdžios institucijoms, ir duomenų apsaugos institucijoms.

## 2.2 *Bendradarbiavimo ir nuoseklumo užtikrinimo mechanizmai*

BDAR buvo sukurtas bendradarbiavimo mechanizmas (vieno langelio sistema veiklos vykdytojams, bendroms operacijoms ir savitarpio pagalbai tarp duomenų apsaugos institucijų) ir nuoseklumo užtikrinimo mechanizmas siekiant skatinti vienodą duomenų apsaugos taisyklių taikymą Valdybai nuosekliai aiškinant ir sprendžiant galimą valdžios institucijų nesutarimą.

Valdyba, kurioje yra visų duomenų apsaugos institucijų atstovų, buvo įsteigta kaip ES įstaiga, turinti juridinio asmens statusą, ir veikia visu pajėgumu, padedama sekretoriato<sup>18</sup>. Ji yra itin svarbi abiejų pirmiau minėtų mechanizmų veikimui. Iki 2019 m. pabaigos Valdyba priėmė 67 dokumentus, įskaitant 10 naujų gairių<sup>19</sup> ir 43 nuomones<sup>20,21</sup>.

Svarbus Valdybos vaidmuo tapo akivaizdus, kai reikėjo greitai suformuoti nuoseklų BDAR aiškinimą ir rasti nedelsiant taikytinus sprendimus ES lygmeniu. Pavyzdžiui, įvykus COVID-19 protrūkiui, 2020 m. kovo mėn. Valdyba priėmė pareiškimą dėl asmens duomenų tvarkymo, kuriame, *inter alia*, kalbama apie duomenų tvarkymo

---

<sup>14</sup> Plg. Valdybos pareiškimą dėl ekonomikos santalkos poveikio duomenų apsaugai: [https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_statement\\_economic\\_concentration\\_lt.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_economic_concentration_lt.pdf).

<sup>15</sup> Žr. sprendimą byloje *COMP M. 8124 Microsoft / LinkedIn*.

<sup>16</sup> 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) (OL L 201, 2002 7 31, p. 0037–0047).

<sup>17</sup> 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (OL L 194, 2016 7 19, p. 1–30).

<sup>18</sup> Žr. išsamią informaciją apie sekretoriato veiklą Valdybos nuomonėje, p. 24–26.

<sup>19</sup> Be dešimties gairių, kurias prieš pradėjus taikyti BDAR priėmė 29 straipsnio darbo grupė ir kurias patvirtino Valdyba. Be to, nuo 2020 m. sausio mėn. iki gegužės mėn. pabaigos Valdyba priėmė 4 papildomas gaires ir atnaujino jau esamas.

<sup>20</sup> 42 iš tų nuomonių buvo priimta pagal BDAR 64 straipsnį ir viena, susijusi su Japonijai skirtu sprendimu dėl tinkamumo – pagal BDAR 70 straipsnio 1 dalies s punktą.

<sup>21</sup> Išsamią Valdybos veiklos apžvalgą žr. Valdybos nuomonėje, p. 18–23.

teisėtumą ir su tuo susijusį mobiliųjų buvimo vietos duomenų naudojimą<sup>22</sup>, o 2020 m. balandžio mėn. ji priėmė gaires dėl sveikatos duomenų tvarkymo su COVID-19 protrūkiu susijusių mokslinių tyrimų tikslais<sup>23</sup> ir gaires dėl buvimo vietos duomenų ir sąlytį turėjusių asmenų išaiškinimo priemonių naudojimo COVID-19 protrūkio aplinkybėmis<sup>24</sup>. Valdyba taip pat iš esmės prisidėjo prie Komisijos ir valstybių narių kuriamo ES požiūrio į sąlytį turėjusių asmenų išaiškinimo programėles.

Kasdienis bendradarbiavimas tarp duomenų apsaugos institucijų joms atliekant savo funkcijas arba einant Valdybos narių pareigas grindžiamas informacijos mainais ir pranešimais apie institucijų pradėtas bylas. Siekdama padėti institucijoms palaikyti ryšį Komisija suteikė joms didelę paramą, t. y. informacijos mainų sistemą<sup>25</sup>. Dauguma institucijų mano, kad ji yra pritaikyta bendradarbiavimo ir nuoseklumo užtikrinimo mechanizmų poreikiams, nors ją dar būtų galima patobulinti, pavyzdžiui, padarius ją patogesnę.

Nors reglamentas taikomas dar neilgai, jau dabar galima pažymėti kelis laimėjimus ir iššūkius. Jie pateikiami toliau. Iš jų matyti, kad duomenų apsaugos institucijos jau veiksmingai naudojami bendradarbiavimo priemonėmis ir renkasi lankstesnius sprendimus.

### *Vieno langelio principas*

Paprastai tirdama tarpvalstybines bylas valstybės narės duomenų apsaugos institucija gali dalyvauti kaip i) vadovaujanti institucija, kai veiklos vykdytojo pagrindinė buveinė yra šioje valstybėje narėje, arba ii) susijusi institucija, kai veiklos vykdytojo buveinė yra šios valstybės narės teritorijoje, kai daromas didelis poveikis šios valstybės narės asmenims arba kai yra pateiktas skundas.

Toks glaudus bendradarbiavimas tapo kasdiene praktika: nuo BDAR taikymo pradžios duomenų apsaugos institucijos visose valstybėse narėse jau yra buvusios vadovaujančia institucija arba susijusia institucija tarpvalstybinėse bylose, nors ir skirtingu mastu.

Nuo 2018 m. gegužės mėn. iki 2019 m. pabaigos Airijos duomenų apsaugos institucija buvo vadovaujanti institucija, tyrusi daugiausia tarpvalstybinių bylų (127), po jos – Vokietija (92), Liuksemburgas (87), Prancūzija (64) ir Nyderlandai (45). Tokia eilės tvarka, visų pirma, byloja apie ypatingą padėtį Airijoje ir Liuksemburge, kur yra įsisteigusios kelios didelės tarptautinės technologijų įmonės.

---

<sup>22</sup> [https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_statement\\_2020\\_processingpersonaldataandcovid-19\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf)

<sup>23</sup> [https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_guidelines\\_202003\\_healthdatascientific\\_researchcovid19\\_lt.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientific_researchcovid19_lt.pdf)

<sup>24</sup> [https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_guidelines\\_20200420\\_contact\\_tracing\\_covid\\_with\\_annex\\_lt.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_lt.pdf)

<sup>25</sup> Vidaus rinkos informacinė sistema (IMI).



Kalbant apie dalyvavimą susijusių duomenų apsaugos institucijų teisėmis, eilės tvarka yra kitokia: daugiausia bylų tiria Vokietijos institucijos (435), po jų – Ispanija (337), Danija (327), Prancūzija (332) ir Italija (306)<sup>26</sup>.

2018 m. gegužės 25 d. – 2019 m. gruodžio 31 d. taikant vieno langelio procedūrą buvo pateiktas 141 sprendimo projektas; iš jų dėl 79 buvo priimti galutiniai sprendimai. Šios ataskaitos paskelbimo dieną dar turi būti priimti keli svarbūs tarpvalstybinį aspektą turintys sprendimai naudojant vieno langelio sistemą. Keli iš šių sprendimų yra susiję su didelėmis tarptautinėmis technologijų įmonėmis<sup>27</sup>. Tikimasi, kad juos priėmus bus patikslintas BDAR aiškinimas ir tai padės jį aiškinti darniau.

### *Savitarpio pagalba*

Duomenų apsaugos institucijos daug naudojami savitarpio pagalbos priemone.

Iki 2019 m. pabaigos įvykdyta 115 savitarpio pagalbos<sup>28</sup> procedūrų, visų pirma, vykdant tyrimus, daugiausia iš kurių vykdė duomenų apsaugos institucijos Ispanijoje (26), Vokietijoje (20), Danijoje (13), Lenkijoje (12) ir Čekijoje (10). Kita vertus, daugiausia prašymų gavo Airija (19), Prancūzija (11), Austrija (10), Vokietija (10) ir Liuksemburgas (9)<sup>29</sup>.

Didžioji dauguma institucijų mano, kad savitarpio pagalba yra labai naudinga bendradarbiavimo priemonė, ir nėra susidūrusios su jokia konkrečia kliūtimi taikant savitarpio pagalbos procedūrą. Savanoriški savitarpio pagalbos mainai, kurių terminas nėra teisiškai nustatytas arba nėra griežtos prievolės atsakyti, buvo naudojami dažniausiai, vykdant 2 427 procedūras. Airijos duomenų apsaugos institucija išsiuntė ir gavo daugiausia savitarpio pagalbos (527 išsiuntė ir 359 gavo); antroje vietoje – Vokietijos institucijos (260 išsiuntė ir 356 gauta).

Kita vertus, bendrų operacijų<sup>30</sup>, kuriose kelių valstybių narių duomenų apsaugos institucijos galėtų dalyvauti jau tarpvalstybinių bylų tyrimo etape, dar nebuvo. Šiuo metu Valdyboje svarstomas praktinis šios priemonės įgyvendinimas ir kaip paskatinti jos naudojimą.

### *Nuoseklumo užtikrinimo mechanizmas*

Kol kas buvo tik atvejų, kai buvo įvykdytas pirmasis nuoseklumo užtikrinimo mechanizmo etapas, t. y. Valdybos nuomonių priėmimas<sup>31</sup>. Kita vertus, Valdybos lygmeniu dar neteko spręsti ginčų<sup>32</sup> arba taikyti skubos procedūros<sup>33</sup>.

<sup>26</sup> Žr. Valdybos nuomonę, p. 8.

<sup>27</sup> Pavyzdžiui, 2020 m. gegužės 22 d. Airijos duomenų apsaugos institucija kitoms susijusioms institucijoms pateikė sprendimo projektą pagal reglamento 60 straipsnį dėl su „Twitter International Company“ susijusio tyrimo dėl pranešimo apie duomenų saugumo pažeidimą. Tą pačią dieną Airijos duomenų apsaugos institucija taip pat paskelbė, kad pagal 60 straipsnį rengiamas teikti su „WhatsApp Ireland Limited“ susijusio sprendimo projektas dėl skaidrumo, be kita ko, dėl skaidrumo, susijusio su tuo, kokia informacija dalijamasi su „Facebook“.

<sup>28</sup> BDAR 61 straipsnis.

<sup>29</sup> Žr. Valdybos nuomonę, p. 12–14.

<sup>30</sup> BDAR 62 straipsnis.

<sup>31</sup> Remiantis BDAR 64 straipsniu.

<sup>32</sup> BDAR 65 straipsnis.

2018 m. gegužės 25 d. – 2019 m. gruodžio 31 d. Valdyba paskelbė 36 nuomones dėl vienos iš jos narių priimamų priemonių<sup>34</sup>. Dauguma jų (31) buvo susijusios su duomenų tvarkymo operacijų nacionalinių sąrašų sudarymu, kai reikia atlikti poveikio duomenų apsaugai vertinimą. Dvi nuomonės buvo susijusios su įmonei privalomomis taisyklėmis, dvi – su elgesio kodekso stebėsenos įstaigos akreditavimo reikalavimų projektu ir viena – su standartinėmis sutarčių sąlygomis<sup>35</sup>.

Be to, Valdyba priėmė šešias nuomones gavusi prašymų<sup>36</sup>. Trys iš jų buvo susijusios su nacionaliniais sąrašais, kuriuose nustatomos tvarkymo operacijoms, dėl kurių nereikia atlikti poveikio duomenų apsaugai vertinimo. Trys iš jų buvo atitinkamai susijusios su administraciniu susitarimu dėl asmens duomenų perdavimo tarp EEE ir EEE nepriklausančių finansų priežiūros institucijų, E. privatumo direktyvos ir BDAR sąveika ir priežiūros institucijos kompetencija pasikeitus aplinkybėms, susijusioms su pagrindine ar vienintele buveine<sup>37</sup>.

### *Spręstinos problemos*

Nors duomenų apsaugos institucijos labai aktyviai dirba kartu Valdyboje ir jau intensyviai naudoja savitarpio pagalbos priemone, tikrosios bendros duomenų apsaugos kultūros kūrimas vis dar vyksta.

Visų pirma, tiriant tarpvalstybines bylas reikia veiksmingesnio ir labiau suderinto požiūrio, reikia veiksmingai naudotis visomis BDAR numatytais bendradarbiavimo priemonėmis. Šiuo klausimu plačiai sutariama, nes jį įvairiomis aplinkybėmis kėlė Europos Parlamentas, Taryba, Europos duomenų apsaugos priežiūros pareigūnas, suinteresuotieji subjektai (įvairių suinteresuotųjų subjektų grupėje ir ne tik) ir duomenų apsaugos institucijos.

Atsižvelgiant į tai, pagrindinės spręstinos problemos yra susijusios su skirtumais:

- taikant nacionalines administracines procedūras, visų pirma susijusias su skundų nagrinėjimo procedūromis, skundų priimtinumui kriterijais, procedūrų trukme dėl skirtingų terminų ar terminų nebuvimo, procedūros momentu, kai suteikiama teisė būti išklausytam, skundo pateikėjų informavimu ir dalyvavimu procedūroje;
- aiškinant sąvokas, susijusias su bendradarbiavimo mechanizmu, kaip antai svarbios informacijos sąvoką, sąvoką „nedelsiant“, sąvoką „skundas“, dokumentą, kurį vadovaujanti duomenų apsaugos institucija apibrėžia kaip „sprendimo projektą“, draugišką sprendimą (visų pirma, procedūrą, kuri baigiasi draugišku sprendimu, ir teisinę sprendimo formą), ir
- dėl metodo, kada pradėti bendradarbiavimo procedūrą, įtraukti į ją susijusias duomenų apsaugos institucijas ir teikti joms informaciją. Skundo pateikėjams taip pat trūksta aiškumo, kaip jų bylos nagrinėjamos tarpvalstybiniais atvejais, kaip pabrėžė keli įvairių suinteresuotųjų subjektų grupės nariai. Be to, įmonės pažymi, kad tam tikrais atvejais nacionalinės duomenų apsaugos institucijos neperduoda

<sup>33</sup> BDAR 66 straipsnis.

<sup>34</sup> Pagal BDAR 64 straipsnio 1 dalį.

<sup>35</sup> BDAR 28 straipsnio 8 dalis.

<sup>36</sup> Pagal BDAR 64 straipsnio 2 dalį.

<sup>37</sup> Žr. Valdybos nuomonę, p. 15.

bylų vadovaujančiai duomenų apsaugos institucijai, o nagrinėja jas vietos lygmeniu.

Komisija palankiai vertina Valdybos pareiškimą, kad ji pradėjo mąstyti, kaip spręsti šias problemas. Visų pirma, Valdyba pažymėjo, kad patikslins procedūros etapus, susijusius su vadovaujančios duomenų apsaugos institucijos ir susijusių duomenų apsaugos institucijų bendradarbiavimu, išnagrinės nacionalinius administracinius procedūrinius įstatymus ir stiprins komunikaciją ir bendradarbiavimą (įskaitant bendras operacijas). Valdybai atlikus tokį vertinimą ir analizę turėtų būti sukurtos veiksmingesnės darbo procedūros tarpvalstybinėse bylose<sup>38</sup>, be kita ko, remiantis narių patirtimi ir stiprinant sekretoriato dalyvavimą. Be to, reikėtų pažymėti, kad Valdybos pareigos užtikrinti nuoseklų BDAR aiškinimą negalima įvykdyti tiesiog nustatant mažiausią bendrą vardiklį.

Galiausiai Valdyba kaip ES įstaiga taip pat turi taikyti ES administracinę teisę ir užtikrinti sprendimų priėmimo proceso skaidrumą.

### **2.3 Rekomendacijos ir gairės**

#### *Informuotumo didinimas ir duomenų apsaugos institucijos rekomendacijos*

Kelios duomenų apsaugos institucijos sukūrė naujas priemones, kaip antai pagalbos linijas fiziniams asmenims ir įmonėms, ir įmonėms skirtus priemonių rinkinius<sup>39</sup>. Daugelis veiklos vykdytojų palankiai vertina šių institucijų pragmatiškumą padedant taikyti BDAR. Visų pirma, keli aktyviai ir glaudžiai bendradarbiauja ir bendrauja su duomenų apsaugos pareigūnais, be kita ko, per duomenų apsaugos pareigūnų asociacijas. Daugelis institucijų taip pat parengė gaires dėl duomenų apsaugos pareigūnų vaidmens ir prievolių padedant duomenų apsaugos pareigūnams jų kasdienėje veikloje ir rengė specialiai jiems skirtus seminarus. Tačiau tai pasakytina ne apie visas duomenų apsaugos institucijas.

Iš suinteresuotųjų subjektų pateiktos grįžtamosios informacijos taip pat matyti kelios su gairėmis ir rekomendacijomis susijusios problemos:

- nėra nuoseklaus požiūrio ir gairių tarp nacionalinių duomenų apsaugos institucijų tam tikrais klausimais (pvz., dėl slapukų<sup>40</sup>, teisėto intereso principo taikymo, pranešimų apie duomenų saugumo pažeidimus ar poveikio duomenų apsaugai vertinimų) arba net tarp duomenų apsaugos institucijų vienos valstybės narės viduje (pvz., Vokietijoje – dėl duomenų valdytojo ir duomenų tvarkytojo sąvokų);
- nacionaliniu lygmeniu priimtų gairių nesuderinamumas su Valdybos priimtomis gairėmis;

---

<sup>38</sup> Kaip taip pat pažymėta Tarybos pozicijoje ir išvadose.

<sup>39</sup> Žr. toliau 7 punktą.

<sup>40</sup> Kol bus priimtas E. privatumo reglamentas, būtina glaudžiai bendradarbiauti su kompetentingomis institucijomis, atsakingomis už E. privatumo direktyvos vykdymo užtikrinimą valstybėse narėse. Pagal tą direktyvą kai kuriose valstybėse narėse valdžios institucijos, kompetentingos užtikrinti E. privatumo direktyvos 5 straipsnio 3 dalį (kurioje įtvirtinamos sąlygos, kuriomis gali būti nustatomi slapukai ir prie jų galima prieiti naudotojo galiniame įrenginyje), nėra tos pačios, kaip BDAR priežiūros institucijos.

- nėra rengiamos viešos konsultacijos dėl tam tikrų nacionaliniu lygmeniu priimamų gairių;
- skirtingi suinteresuotųjų subjektų dalyvavimo lygiai duomenų apsaugos institucijose;
- tenka ilgai laukti atsakymų į prašymus pateikti informaciją;
- sunku gauti vertingų praktinių rekomendacijų iš duomenų apsaugos institucijų;
- kai kuriose duomenų apsaugos institucijose reikia didinti sektoriaus žinių lygį (pvz., sveikatos priežiūros ir farmacijos sektoriuje).

Keli šie aspektai taip pat siejami su nepakankamais kelių duomenų apsaugos institucijų ištekliais (žr. toliau).

*Skirtinga praktika pranešant apie duomenų saugumo pažeidimus*<sup>41</sup>

Nors Taryba pabrėžia, kokia našta yra tokie pranešimai, tarp valstybių narių yra didelių su pranešimais susijusių skirtumų: nuo 2018 m. gegužės mėn. iki 2019 m. lapkričio mėn. pabaigos daugelyje valstybių narių bendras pranešimų apie duomenų saugumo pažeidimus skaičius neviršijo 2 000, 7 valstybėse narėse jis buvo nuo 2 000 iki 10 000, o Nyderlandų ir Vokietijos duomenų apsaugos institucijos pranešė, jog gavo atitinkamai 37 400 ir 45 600 pranešimus<sup>42</sup>.

Tai gali byloti apie tai, kad nėra nuoseklaus aiškinimo ir įgyvendinimo, nepaisant to, kad ES lygmeniu yra gairės dėl pranešimų apie duomenų saugumo pažeidimus.

*Europos duomenų apsaugos valdybos gairės*

Valdyba jau yra priėmusi daugiau nei 20 gairių dėl pagrindinių BDAR aspektų<sup>43</sup>. Gairės yra esminė nuoseklaus BDAR taikymo priemonė, tad suinteresuotieji subjektai iš esmės vertina jas palankiai. Suinteresuotieji subjektai yra patenkinti tuo, kad sistemingai (6–8 savaitės) rengiamos viešos konsultacijos. Tačiau jie prašo aktyvesnio dialogo su Valdyba. Atsižvelgiant į tai, reikėtų ir toliau (ir daugiau) organizuoti praktinius seminarus tikslinėmis temomis prieš rengiant gaires, kad būtų užtikrinamas Valdybos darbo skaidrumas, įtraukumas ir aktualumas. Suinteresuotieji subjektai taip pat prašo, kad gairėse būtų išaiškinti labiausiai ginčytini klausimai, nes dėl jų rengiamos viešos konsultacijos, o ne nuomonės pagal BDAR 64 straipsnio 2 dalį. Kai kurie suinteresuotieji subjektai taip pat prašo daugiau praktinių gairių, kuriose išsamiai paaiškinamas BDAR sąvokų ir nuostatų taikymas<sup>44</sup>. Įvairių suinteresuotųjų subjektų grupės nariai pabrėžia, kad reikia daugiau konkrečių pavyzdžių, kad būtų kuo mažiau galimybių duomenų apsaugos institucijoms aiškinti reglamentą skirtingai. Be to, dėl prašymų patikslinti, kaip taikyti BDAR, ir užtikrinti teisinį tikrumą neturėtų atsirasti papildomų reikalavimų arba sumažėti rizika pagrįsto metodo ir atskaitomybės principo teikiama nauda.

<sup>41</sup> BDAR 33 straipsnis.

<sup>42</sup> Žr. Valdybos nuomonę, p. 35.

<sup>43</sup> Darbas prie gairių jau pradėtas iki pradėtant taikyti BDAR 2018 m. gegužės 25 d. 29 straipsnio darbo grupėje. Išsamų gairių sąrašą žr. [https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices\\_lt](https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_lt).

<sup>44</sup> Tai taip pat pabrėžė Europos Parlamentas ir Taryba.

Temos, kuriomis suinteresuotieji subjektai norėtų papildomų Valdybos gairių yra, be kita ko, šios: duomenų subjektų teisių taikymo sritis (įskaitant užimtumo sritį); nuomonės dėl duomenų tvarkymo siekiant teisėtų interesų atnaujinimas; duomenų valdytojo, bendro duomenų valdytojo ir duomenų tvarkytojo sąvokos bei būtini susitarimai tarp šalių<sup>45</sup>; BDAR taikymas naujosioms technologijoms (kaip antai blokų grandinės ir dirbtinio intelekto atveju); duomenų tvarkymas atliekant mokslinius tyrimus (be kita ko, vykdant tarptautinį bendradarbiavimą); vaikų duomenų tvarkymas; pseudoniminimas ir anoniminimas; sveikatos duomenų tvarkymas.

Valdyba jau yra pranešusi, kad skelbs gaires daugeliu šių temų, ir jau pradėjo darbą prie kai kurių iš jų (pvz., dėl teisėtų interesų kaip duomenų tvarkymo teisinio pagrindo taikymo).

Suinteresuotieji subjektai taip pat prašo Valdybos tam tikrais atvejais atnaujinti ir peržiūrėti esamas gaires atsižvelgiant į nuo jų paskelbimo sukauptą patirtį ir pasinaudojant galimybę prireikus padaryti jas išsamesnes.

## **2.4 Duomenų apsaugos institucijų ištekliai**

Kiekvienos duomenų apsaugos institucijos aprūpinimas būtiniais žmogiškaisiais, techniniais ir finansiniais ištekliais, patalpomis ir infrastruktūra yra būtinoji sąlyga, kad ji veiksmingai atliktų savo užduotis ir naudotųsi savo įgaliojimais, tad tai esminė jos nepriklausomumo sąlyga<sup>46</sup>.

Daugumos duomenų apsaugos institucijų darbuotojų skaičius ir ištekliai po BDAR įsigaliojimo 2016 m. padidėjo<sup>47</sup>. Tačiau daugelis jų vis dar teigia, kad išteklių nepakanka<sup>48</sup>.

### *Nacionalinėse duomenų apsaugos institucijose dirbančių darbuotojų skaičius*

Bendras EEE valstybių duomenų apsaugos institucijose dirbančių darbuotojų skaičius 2016–2019 m. padidėjo iš viso 42 proc. (atsižvelgiant į 2020 m. prognozes – 62 proc.).

Darbuotojų skaičius per šį laikotarpį padidėjo daugelyje institucijų: daugiausia (procentais) jis padidėjo institucijose Airijoje (+169 proc.), Nyderlanduose (+145 proc.), Islandijoje (+143 proc.), Liuksemburge (+126 proc.) ir Suomijoje (+114 proc.). Kita vertus, keliose duomenų apsaugos institucijose darbuotojų skaičius sumažėjo: jis labiausiai sumažėjo Graikijoje (–15 proc.), Bulgarijoje (–14 proc.), Estijoje (–11 proc.), Latvijoje (–10 proc.) ir Lietuvoje (–8 proc.). Kai kuriose institucijose darbuotojų skaičius sumažėjo ir dėl duomenų apsaugos ekspertų perėjimo į privatųjį sektorių, kuriame siūlomos patrauklesnės sąlygos.

Apskritai, remiantis 2020 m. prognoze, palyginti su 2019 m. numatomas darbuotojų skaičiaus padidėjimas, išskyrus institucijas Austrijoje, Bulgarijoje, Italijoje, Švedijoje ir Islandijoje (kur, kaip tikimasi, darbuotojų skaičiai išliks tokie pat), Kipre ir Danijoje (kur, kaip tikimasi, darbuotojų skaičiai sumažės).

<sup>45</sup> Šiuo metu Valdyba rengia gaires dėl duomenų valdytojų ir tvarkytojų.

<sup>46</sup> Žr. BDAR 52 straipsnio 4 dalį.

<sup>47</sup> Reglamentas įsigaliojo 2016 m. gegužės mėn. ir buvo pradėtas taikyti 2018 m. gegužės mėn. po 2 metų pereinamojo laikotarpio.

<sup>48</sup> Žr. Valdybos nuomonę, p. 26–30.

Visose Vokietijos duomenų apsaugos institucijose<sup>49</sup> kartu dirba daugiausia darbuotojų (888 – 2019 m.; 2020 m. prognozuojamas skaičius – 1002); po jų – duomenų apsaugos institucijose Lenkijoje (238 ir 260), Prancūzijoje (215 ir 225), Ispanijoje (170 ir 220), Nyderlanduose (179 ir 188), Italijoje (170 ir 170) ir Airijoje (140 ir 176).

Mažiausia darbuotojų dirba duomenų apsaugos institucijose Kipre (24 ir 22), Latvijoje (19 ir 31), Islandijoje (17 ir 17), Estijoje (16 ir 18) ir Maltoje (13 ir 15).

#### *Nacionalinių duomenų apsaugos institucijų biudžetas*

Bendras EEE valstybių duomenų apsaugos institucijų biudžetas 2016–2019 m. padidėjo iš viso 49 proc. (atsižvelgiant į 2020 m. prognozes – 64 proc.).

Biudžetas per šį laikotarpį padidėjo daugelyje institucijų: daugiausia (procentais) jis padidėjo institucijose Airijoje (+223 proc.), Islandijoje (+167 proc.), Liuksemburge (+165 proc.), Nyderlanduose (+130 proc.) ir Kipre (+114 proc.). Kita vertus, kai kurių institucijų biudžetas padidėjo tik nedaug: mažiausias padidėjimas užfiksuotas duomenų apsaugos institucijose Estijoje (7 proc.), Latvijoje (4 proc.), Rumunijoje (3 proc.) ir Belgijoje (1 proc.), o Prancūzijos institucijoje biudžetas sumažėjo (– 2 proc.).

Apskritai, remiantis 2020 m. prognoze, numatoma, kad, palyginti su 2019 m., biudžetas padidės, išskyrus institucijas Austrijoje, Bulgarijoje, Estijoje ir Nyderlanduose (kurių biudžetai, kaip tikimasi, nesikeis).

Didžiausią biudžetą turi duomenų apsaugos institucijos Vokietijoje (76,6 mln. EUR 2019 m. ir 85,8 mln. EUR pagal 2020 m. prognozę), Italijoje (29,1 mln. EUR ir 30,1 mln. EUR), Nyderlanduose (18,6 mln. EUR ir 18,6 mln. EUR), Prancūzijoje (18,5 mln. EUR ir 20,1 mln. EUR) ir Airijoje (15,2 mln. EUR ir 16,9 mln. EUR).

Mažiausią biudžetą turi institucijos Kroatijoje (1,2 mln. EUR 2019 m. ir 1,4 mln. EUR pagal 2020 m. prognozę), Rumunijoje (1,1 mln. EUR ir 1,3 mln. EUR), Latvijoje (0,6 mln. EUR ir 1,2 mln. EUR), Kipre (0,5 mln. EUR ir 0,5 mln. EUR) ir Maltoje (0,5 mln. EUR ir 0,6 mln. EUR).

Lentelėje II priede pateikiama nacionalinių duomenų apsaugos institucijų žmogiškųjų ir biudžeto išteklių apžvalga.

Be poveikio institucijų gebėjimui užtikrinti taisyklių vykdymą nacionaliniu lygmeniu, dėl nepakankamų išteklių taip pat ribojamas duomenų apsaugos institucijų gebėjimas dalyvauti taikant bendradarbiavimo ir nuoseklumo užtikrinimo mechanizmus bei vykdant Valdybos darbą ir prie jų prisidėti. Kaip pabrėžė Valdyba, vieno langelio sistemos sėkmę lemia laikas ir pastangos, kurias duomenų apsaugos institucijos gali skirti konkrečių tarpvalstybinių bylų nagrinėjimui ir bendradarbiavimui jas nagrinėjant. Išteklių klausimas tampa dar svarbesnis atsižvelgiant į vis svarbesniu tampantį institucijų vaidmenį vykdant šiuo metu kuriamą didelio masto IT sistemų priežiūrą. Be to, Airijos ir Liuksemburgo duomenų apsaugos institucijos turi ypatingų

<sup>49</sup> Vokietijoje yra 18 institucijų, iš kurių viena yra federalinė institucija, o 17 – regioninės (įskaitant dvi Bavarijoje).



išteklų poreikių turint omenyje jų kaip vadovaujančių institucijų vaidmenį užtikrinant BDAR taikymą didelėms technologijų įmonėms, kurių daugiausia šiose valstybėse narėse.

Nors Taryba atkreipia dėmesį į bendradarbiavimo mechanizmo ir jo terminų poveikį duomenų apsaugos institucijų darbui<sup>50</sup>, pagal BDAR valstybės narės privalo aprūpinti savo nacionalines duomenų apsaugos institucijas pakankamais žmogiškaisiais, finansiniais ir techniniais ištekliais<sup>51</sup>.

Valdybos sekretoriatai, kurio paslaugas teikia Europos duomenų apsaugos priežiūros pareigūnas<sup>52</sup>, šiuo metu dirba 20 žmonių, įskaitant teisės, IT ir komunikacijos ekspertus. Reikia įvertinti, ar ateityje šis skaičius turėtų kisti, atsižvelgiant į veiksmingą analitinės, administracinės ir logistinės pagalbos Valdybai ir jos pogrupiams funkcijos įgyvendinimą, be kita ko, valdant informacijos mainų sistemą.

### **3 TAISYKLĖS SUDERINTOS, BET VIS DAR ESAMA SUSISKAIDYMO IR TAIKOMI SKIRTINGI METODAI**

BDAR yra numatytas nuoseklus požiūris į duomenų apsaugos taisykles visoje ES, pakeičiant skirtingus nacionalinius režimus, galiojusius pagal 1995 m. Duomenų apsaugos direktyvą.

#### **3.1 BDAR įgyvendinimas valstybėse narėse**

BDAR yra tiesiogiai taikytinas visose valstybėse narėse nuo 2018 m. gegužės 25 d. Pagal jį valstybės narės privalo priimti teisės aktus, visų pirma siekdamos įsteigti nacionalines duomenų apsaugos institucijas ir nustatyti bendrąsias sąlygas nariams, taip pat užtikrinti, kad kiekviena institucija veiktų visiškai nepriklausomai vykdydama savo užduotis ir naudodamasi savo įgaliojimais pagal BDAR. Teisinės prievolės ir viešosios užduotys gali būti asmens duomenų tvarkymo teisinis pagrindas tik jeigu tai numatyta (Sąjungos ar) nacionalinės teisės aktuose. Be to, valstybės narės turi nustatyti taisykles dėl nuobaudų, visų pirma dėl pažeidimų, už kuriuos nėra skiriamos administracinės baudos, bei privalo suderinti teisę į asmens duomenų apsaugą su teise į žodžio laisvę ir informaciją. Nacionalinės teisės aktais taip pat galima nustatyti teisinį pagrindą, pagal kurį būtų galima netaikyti bendrojo draudimo tvarkyti specialių kategorijų asmens duomenis, pavyzdžiui, dėl svarbaus viešojo intereso priešasčių visuomenės sveikatos srityje, įskaitant apsaugą nuo rimtų tarpvalstybinio pobūdžio grėsmių sveikatai. Be to, valstybės narės privalo užtikrinti sertifikavimo įstaigų akreditavimą.

Komisija stebi BDAR įgyvendinimą nacionalinės teisės aktais. Tuo metu, kai buvo rengiama ši ataskaita, visos valstybės narės, išskyrus Slovėniją, priėmė naujus duomenų apsaugos teisės aktus arba pritaikė savo įstatymus šioje srityje. Todėl

---

<sup>50</sup> BDAR 60 straipsnis.

<sup>51</sup> BDAR 52 straipsnio 4 dalis.

<sup>52</sup> BDAR 75 straipsnis.

Komisija paprašė Slovėnijos pateikti paaiškinimus dėl padarytos pažangos ir paragino ją užbaigti šį procesą<sup>53</sup>.

Be to, nacionalinės teisės aktų suderinamumas su duomenų apsaugos taisyklėmis pagal Šengeno *acquis* taip pat vertinamas taikant Komisijos koordinuojamą Šengeno vertinimo mechanizmą. Komisija ir valstybės narės kartu vertina, kaip šalyse Šengeno *acquis* įgyvendinamas ir taikomas keliose srityse; duomenų apsaugos srityje vertinamos didelio masto IT sistemos, kaip antai Šengeno informacinė sistema ir Vizų informacinė sistema bei duomenų apsaugos institucijų vaidmuo prižiūrint asmens duomenų tvarkymą tose sistemose.

Atskiriems sektoriams skirtų teisės aktų pritaikymo procesas nacionaliniu lygmeniu dar nesibaigęs. Įtraukus BDAR nuostatas į Europos ekonominės erdvės susitarimą jis pradėtas taikyti ir Norvegijai, Islandijai ir Lichtenšteinui. Šiose šalyse taip pat yra priimti nacionaliniai duomenų apsaugos įstatymai.

Komisija naudos visas turimas priemones, įskaitant pažeidimo nagrinėjimo procedūras, siekdama užtikrinti, kad visos valstybės narės laikytųsi BDAR.

#### *Pagrindinės problemos, susijusios su įgyvendinimu nacionaliniu lygmeniu*

Nuolat vertinant nacionalinės teisės aktus ir vykstant dvišaliams mainams su valstybėmis narėmis nustatytos šios pagrindinės problemos:

- BDAR taikymo apribojimai: kai kuriose valstybėse narėse, pavyzdžiui, jis visiškai netaikomas nacionalinio parlamento veiklai;
- specialių nacionalinių įstatymų taikomumo skirtumai. Kai kuriose valstybėse narėse jų nacionalinės teisės taikomumas siejamas su vieta, kurioje siūlomos prekės ar paslaugos; kitose – su duomenų valdytojo ar tvarkytojo įsisteigimo vieta. Tai nesuderinama su BDAR įtvirtintu suderinimo tikslu;
- nacionalinės teisės aktai, dėl kurių kyla klausimų dėl kišimosi į teisę į duomenų apsaugą proporcingumo. Pavyzdžiui, Komisija pradėjo pažeidimo nagrinėjimo procedūrą dėl valstybės narės, priėmusios teisės aktą, pagal kurį teisėjai privalo atskleisti konkrečią informaciją apie savo neprofesinę veiklą, ir tai nesuderinama su teise į privatų gyvenimą ir teise į asmens duomenų apsaugą<sup>54</sup>;
- nėra nepriklausomos įstaigos, kuri prižiūrėtų, kaip teismai tvarko duomenis vykdydami teismines funkcijas<sup>55</sup>;
- teisės aktai srityse, kurios yra visiškai reglamentuojamos BDAR, viršijant patikslinimo ar apribojimo ribą. Tai, visų pirma, pasakytina apie atvejus, kai nacionalinės teisės aktuose nustatomos duomenų tvarkymo dėl teisėtų interesų sąlygos ir siekiama užtikrinti atitinkamų duomenų valdytojo ir susijusių asmenų

---

<sup>53</sup> Pažymima, kad Slovėnijoje nacionalinė duomenų apsaugos institucija yra įsteigta remiantis galiojančiu nacionaliniu duomenų apsaugos įstatymu ir vykdo BDAR taikymo šioje valstybėje narėje priežiūrą.

<sup>54</sup> Ši pažeidimo nagrinėjimo procedūra yra susijusi su 2019 m. gruodžio 20 d. Lenkijos įstatymu dėl teisminių institucijų, kuris daro poveikį teisėjų nepriklausomumui ir yra susijęs, *inter alia*, su teisėjų dalyvavimu neprofesinėje veikloje atskleidimu:

[https://ec.europa.eu/commission/presscorner/detail/en/ip\\_20\\_772](https://ec.europa.eu/commission/presscorner/detail/en/ip_20_772).

<sup>55</sup> Žr. Chartijos 8 straipsnio 3 dalį, SESV 16 straipsnį ir BDAR 20 konstatuojamąją dalį.



interesų pusiausvyrą, o pagal BDAR visi duomenų valdytojai privalo patys užtikrinti tokią pusiausvyrą ir remtis tuo teisiniu pagrindu;

- patikslinimai ir papildomi reikalavimai, nesusiję su duomenų tvarkymo vykdant teisinę prievolę ar atliekant viešąją užduotį (pvz., vykdant stebėjimą vaizdo kameromis privačiajame sektoriuje ar tiesioginės rinkodaros tikslais), ir dėl BDAR vartojamų sąvokų (pvz., „didelis mastas“ arba „ištrinti“).

Kai kuriuos iš šių klausimų gali išspręsti Teisingumo Teismas šiuo metu nagrinėjamose bylose<sup>56</sup>.

#### *Teisės į asmens duomenų apsaugą derinimas su žodžio laisve ir teise į informaciją*

Kyla konkreti problema, susijusi su valstybių narių prievolės teisės aktais suderinti teisę į asmens duomenų apsaugą su žodžio laisve ir teise į informaciją įgyvendinimu<sup>57</sup>. Šis klausimas yra labai sudėtingas, nes vertinant šių pagrindinių teisių pusiausvyrą taip pat būtina atsižvelgti į spaudos ir žiniasklaidos įstatymų nuostatas ir juose numatytas apsaugos priemones.

Vertinant valstybių narių teisės aktus matyti skirtingi metodai, taikomi derinant teisę į asmens duomenų apsaugą su žodžio laisve ir teise į informaciją.

- Kai kuriose valstybėse narėse yra nustatytas žodžio laisvės pirmumo principas arba iš principo netaikomi ištisi BDAR 85 straipsnio 2 dalyje nurodyti skyriai, jeigu duomenys tvarkomi žurnalistikos tikslais ir jų tvarkymas yra susijęs su akademinė, menine ir literatūrine išraiška. Tam tikra prasme žiniasklaidos įstatymuose numatomos tam tikros apsaugos priemonės, susijusios su duomenų subjektų teisėmis.
- Kai kuriose valstybėse narėse pirmenybė suteikiama asmens duomenų apsaugai ir duomenų apsaugos taisyklės netaikomos tik konkrečiais atvejais, kaip antai susijusiais su visuomeninį statusą turinčiu asmeniu.
- Kitose valstybėse narėse numatoma, kad tam tikrą pusiausvyrą užtikrina teisės aktų leidėjas, ir (arba) nuostatų, leidžiančių nukrypti nuo tam tikrų BDAR nuostatų, vertinimas atliekamas kiekvienu konkrečiu atveju.

Komisija ir toliau vertins nacionalinės teisės aktus remdamasi Chartijos reikalavimais. Toks suderinimas turi būti numatytas įstatymuose, turi būti paisoma šių pagrindinių teisių esmės ir jis turi būti proporcingas ir būtinas (Chartijos 52 straipsnio 1 dalis). Duomenų apsaugos taisyklės neturėtų daryti poveikio naudojimuisi žodžio laisve ir teise į informaciją, ypač neturėtų turėti neigiamo poveikio arba būti aiškinamos kaip būdas daryti spaudimą žurnalistams, kad jie atskleistų savo šaltinius.

<sup>56</sup> Pavyzdžiui, šiuo metu Teisingumo Teismas nagrinėja bylą dėl prašymo priimti prejudicinį sprendimą dėl BDAR netaikymo parlamento komitetui (C-272/19).

<sup>57</sup> BDAR 85 straipsnis.

### 3.2 *Neprivalomos patikslinamosios nuostatos ir jų ribos*

Pagal BDAR valstybės narės gali papildomai patikslinti jo taikymą tam tikrose srityse. Šią veiksmų laisvę rengiant nacionalinės teisės aktus reikia atskirti nuo prievolės įgyvendinti tam tikras kitas BDAR nuostatas, kaip minėta pirmiau. Neprivalomos patikslinamosios nuostatos yra išvardytos I priede.

Valstybėms narėms priimant įstatymus veiksmų laisvei taikomos BDAR nustatytos sąlygos ir apribojimai; neleidžiama kurti lygiagretaus nacionalinio duomenų apsaugos režimo<sup>58</sup>. Valstybės narės privalo iš dalies pakeisti ar panaikinti nacionalinius duomenų apsaugos įstatymus, įskaitant sektorių teisės aktus, kuriuose įtvirtinami duomenų apsaugos aspektai.

Be to, susijusiuose valstybių narių teisės aktuose negali būti nuostatų, dėl kurių gali kilti painiava dėl tiesioginio BDAR taikymo. Taigi, kai BDAR numatoma galimybė valstybės narės teisėje konkrečiau apibrėžti reglamento taisykles ar numatyti jų apribojimus, valstybės narės, kiek tai būtina suderinamumui užtikrinti ir siekiant, kad nacionalinės nuostatos būtų suprantamos asmenims, kuriems jos taikomos, gali į savo nacionalinę teisę įtraukti šio reglamento elementus<sup>59</sup>.

Suinteresuotieji subjektai mano, kad valstybės narės turėtų mažiau naudotis arba visai nesinaudoti neprivalomomis patikslinamosiomis nuostatomis, nes jos neprisideda prie suderinimo. Dėl nacionalinių skirtumų įgyvendinant įstatymus ir duomenų apsaugos institucijoms juos išaiškinant visoje ES gerokai padidėja teisinių reikalavimų laikymosi išlaidos.

#### *Su neprivalomų patikslinamųjų nuostatų naudojimu susijęs susiskaidymas*

- Amžiaus riba dėl vaiko, kuriam siūlomos informacinės visuomenės paslaugos, sutikimo

Kai kurios valstybės narės pasinaudojo galimybe nustatyti jaunesnio nei 16 metų amžiaus ribą dėl sutikimo, susijusio su informacinės visuomenės paslaugomis (BDAR 8 straipsnio 1 dalis). Devyniose valstybėse narėse taikoma 16 metų amžiaus riba, aštuoniose valstybėse narėse buvo pasirinkta 13 metų riba, šešiose – 14 metų riba ir trijose – 15 metų riba<sup>60</sup>.

Taigi įmonė, teikianti informacinės visuomenės paslaugas nepilnamečiams visoje ES, turi laikytis skirtingų galimų naudotojų amžiaus ribų priklausomai nuo jų gyvenamosios vietos valstybės narės. Tai nesuderinama su pagrindiniu BDAR tikslu numatyti vienodo lygio asmenų apsaugą ir verslo galimybes visose valstybėse narėse.

Dėl tokių skirtumų susiklosto situacijos, kai valstybėje narėje, kurioje yra įsisteigęs duomenų valdytojas, nustatoma kitokia amžiaus riba nei valstybėse narėse, kuriose gyvena duomenų subjektai.

---

<sup>58</sup> Plačiau vartojamas terminas „įvadinės nuostatos“, reiškiantis patikslinimo nuostatas, yra klaidinantis, nes jį vartojant gali susidaryti įspūdis, kad valstybės narės turi veiksmų laisvę viršijant reglamento nuostatas.

<sup>59</sup> BDAR 8 konstatuojamoji dalis.

<sup>60</sup> 13 metų – Belgijoje, Danijoje, Estijoje, Latvijoje, Maltoje, Portugalijoje, Suomijoje ir Švedijoje; Austrijoje, Bulgarijoje, Ispanijoje, Italijoje, Kipre ir Lietuvoje – 14 metų; Čekijoje, Graikijoje ir Prancūzijoje – 15 metų; Airijoje, Kroatijoje, Lenkijoje, Liuksemburge, Nyderlanduose, Rumunijoje, Slovakijoje, Vengrijoje ir Vokietijoje – 16 metų.



- Sveikata ir moksliniai tyrimai

Įgyvendinant nuostatas, leidžiančias nukrypti nuo bendrojo draudimo tvarkyti specialių kategorijų asmens duomenis<sup>61</sup>, valstybių narių teisės aktuose laikomasi skirtingų požiūrių į patikslinamųjų nuostatų ir apsaugos priemonių lygį, be kita ko, sveikatos ir mokslinių tyrimų tikslais. Daugelyje valstybių narių buvo įtvirtintos ar liko galioti papildomos genetinių, biometrinių ar su sveikata susijusių duomenų tvarkymo sąlygos. Tai taip pat pasakytina apie nukrypti leidžiančias nuostatas, susijusias su duomenų subjektų teisėmis, taikomas mokslinių tyrimų tikslais<sup>62</sup>, ir dėl nukrypti leidžiančių nuostatų masto, ir dėl susijusių apsaugos priemonių.

Prie suderinto požiūrio šioje srityje prisidės ir Valdybos rengiamos gairės dėl asmens duomenų naudojimo mokslinių tyrimų tikslais. Komisija pateiks Valdybai savo nuomonę, visų pirma dėl su sveikata susijusių mokslinių tyrimų, be kita ko, kaip konkrečius iš mokslinių tyrimų bendruomenės gautus klausimus ir konkrečių scenarijų analizę. Būtų naudinga, jeigu šios gairės būtų priimtos prieš pradėdant įgyvendinti bendrąją programą „Europos horizontas“, siekiant suderinti duomenų apsaugos metodus ir sudaryti sąlygas dalytis duomenimis, kad mokslinių tyrimų srityje būtų daroma pažanga. Taip pat galėtų būti naudingos Valdybos gairės dėl asmens duomenų tvarkymo sveikatos srityje.

BDAR yra tvirtas pagrindas rengti nacionalinės teisės aktus visuomenės sveikatos srityje; jame yra aiškiai nurodytos tarpvalstybinės grėsmės sveikatai bei epidemijų ir jų plitimo stebėsenai<sup>63</sup>, kuri yra svarbi kovojant su COVID-19 pandemija.

ES lygmeniu 2020 m. balandžio 8 d. Komisija priėmė rekomendaciją dėl technologijų ir duomenų naudojimui skirtų priemonių rinkinio šioje srityje, įskaitant mobiliąsias programas ir anonimizintų judumo duomenų naudojimą<sup>64</sup>, o 2020 m. balandžio 16 d. – gaires dėl su duomenų apsauga susijusių programėlių kovai su pandemija<sup>65</sup>. 2020 m. kovo 19 d. Valdyba paskelbė pareiškimą dėl duomenų tvarkymo šioje srityje<sup>66</sup>, o 2020 m. balandžio 21 d. – gaires dėl duomenų tvarkymo mokslinių tyrimų tikslais ir dėl vietos nustatymo duomenų ir sąlytį turėjusių asmenų išaiškinimo priemonių naudojimo šioje srityje<sup>67</sup>. Tomis rekomendacijomis ir gairėmis patikslinama, kaip asmens duomenų apsaugos principai ir taisyklės taikomi kovojant su pandemija.

- Dideli duomenų subjektų teisių apribojimai

Daugelyje nacionalinės teisės aktų duomenų apsaugos srityje, kuriais apribojamos duomenų subjekto teisės, nėra nurodomi tokiais apribojimais apsaugomi bendro viešojo intereso tikslai ir (arba) jais nepakankamai tenkinamos BDAR 23 straipsnio 2 dalyje nustatytos sąlygos ir apsaugos priemonės<sup>68</sup>. Keliose valstybėse narėse

---

<sup>61</sup> BDAR 9 straipsnis.

<sup>62</sup> BDAR 89 straipsnio 2 dalis.

<sup>63</sup> Žr. BDAR 9 straipsnio 2 dalies i punktą ir 46 konstatuojamąją dalį.

<sup>64</sup> [https://ec.europa.eu/info/sites/info/files/recommendation\\_on\\_apps\\_for\\_contact\\_tracing\\_4.pdf](https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf).

<sup>65</sup> [https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:52020XC0417\(08\)&from=LT](https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:52020XC0417(08)&from=LT).

<sup>66</sup> [https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_statement\\_art\\_23gdpr\\_20200602\\_lt\\_1.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_art_23gdpr_20200602_lt_1.pdf).

<sup>67</sup> [https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices\\_en](https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en).

<sup>68</sup> Pavyzdžiui, tiesiog todėl, kad jais tiesiog pakartojama BDAR 23 straipsnio 1 dalies formuluotė.

nenumatoma galimybė atlikti proporcingumo patikrą arba išplėsti apribojimus net viršijant BDAR 23 straipsnio 1 dalies taikymo sritį. Pavyzdžiui, kai kuriuose nacionaliniuose įstatymuose dėl neproporcingų duomenų valdytojo pastangų nėra numatyta teisė susipažinti su asmens duomenimis, kurie yra saugojami vykdant saugojimo prievolę arba viešąsias užduotis, taikant tokį apribojimą ne tik bendro viešojo intereso tikslais.

- Papildomi reikalavimai įmonėms

Nors privalomo duomenų apsaugos pareigūno reikalavimas grindžiamas rizika pagrįstu metodu<sup>69</sup>, vienoje valstybėje narėje<sup>70</sup> jis yra išplėstas ir aprėpia kiekybinį kriterijų, kurį taikant įmonės, kuriose automatizuotu asmens duomenų tvarkymu nuolat užsiima 20 ar daugiau darbuotojų, yra įpareigojamos paskirti duomenų apsaugos pareigūną neatsižvelgiant į riziką, susijusią su duomenų tvarkymo veikla<sup>71</sup>. Dėl to susidarė papildoma našta.

#### 4 ĮGALIOJIMAS FIZINIAMS ASMENIMS VALDYTI SAVO DUOMENIS

Pagal BDAR įgyvendinamos pagrindinės teisės, visų pirma teisė į asmens duomenų apsaugą, taip pat kitos Chartijoje nustatytos pagrindinės teisės, įskaitant teisę į privatų ir šeimos gyvenimą, žodžio laisvę ir teisę į informaciją, teisę į nediskriminavimą, minties, sąžinės ir religijos laisvę, laisvę užsiimti verslu ir teisę į veiksmingą teisinę gynybą. Šios teisės turi būti tarpusavyje subalansuotos laikantis proporcingumo principo<sup>72</sup>.

Pagal BDAR fiziniams asmenims suteikiamos įgyvendinamos teisės, kaip antai teisė susipažinti su duomenimis, juos taisyti, ištrinti, dėl jų prieštarauti ir juos perkelti bei teisė į didesnę skaidrumą. Fiziniams asmenims taip pat suteikiama teisė pateikti skundą duomenų apsaugos institucijai, be kita ko, pareiškiant atstovaujамąjį ieškinį, ir apskųsti teismine tvarka.

Fiziniai asmenys vis geriau suvokia savo teises, kaip matyti iš 2019 m. liepos mėn. „Eurobarometro“ apklausos<sup>73</sup> ir Pagrindinių teisių agentūros atlikto tyrimo<sup>74</sup> rezultatų.

Remiantis Pagrindinių teisių agentūros atlikto pagrindinių teisių tyrimo rezultatais:

- 69 proc. 16 metų ir vyresnių ES gyventojų yra girdėję apie BDAR;
- 71 proc. ES respondentų yra girdėję apie jų nacionalinę duomenų apsaugos instituciją; šis skaičius svyruoja nuo 90 proc. Čekijoje iki 44 proc. Belgijoje;
- 60 proc. ES respondentų žino apie įstatymą, pagal kurį jie gali susipažinti su savo duomenimis, saugomais valdžios institucijose; tačiau privačiųjų įmonių atveju šis skaičius yra mažesnis – 51 proc.;

<sup>69</sup> BDAR 37 straipsnio 1 dalis.

<sup>70</sup> Vokietija.

<sup>71</sup> Naudojamosi BDAR 37 straipsnio 4 dalyje įtvirtinta patikslinamąja sąlyga.

<sup>72</sup> Plg. BDAR 4 konstatuojamąją dalį.

<sup>73</sup> [https://ec.europa.eu/commission/presscorner/detail/lt/IP\\_19\\_2956](https://ec.europa.eu/commission/presscorner/detail/lt/IP_19_2956).

<sup>74</sup> Europos Sąjungos pagrindinių teisių agentūra (FRA) (2020 m.). 2019 m. pagrindinių teisių tyrimas. Duomenų apsauga ir technologijos. <https://fra.europa.eu/en/publication/2020/fundamental-rights-survey-data-protection>.

- daugiau nei vienas iš penkių ES respondentų (23 proc.) nenori dalytis asmens duomenimis (kaip antai adresu, pilietybe ar gimimo data) su valdžios institucijomis, o 41 proc. nenori dalytis šiais duomenimis su privačiosiomis įmonėmis.

Fiziniai asmenys vis aktyviau naudojami savo teise pateikti skundą duomenų apsaugos institucijoms individualiai ar pareikšdami atstovaujамąjį ieškinį<sup>75</sup>. Tik keliose valstybėse narėse nevyriausybinėms organizacijoms leidžiama pareikšti ieškinius neturint įgaliojimų, kaip numatyta BDAR. Tikimasi, kad priėmus siūlomą direktyvą dėl atstovaujамųjų ieškinių siekiant apsaugoti kolektyvinius vartotojų interesus<sup>76</sup> atstovaujамųjų ieškinių sistema bus sustiprinta ir duomenų apsaugos srityje.

### *Skundai*

Valdybos duomenimis, bendras skundų, gautų nuo 2018 m. gegužės mėn. iki 2019 m. lapkričio mėn. pabaigos, skaičius yra maždaug 275 000<sup>77</sup>. Tačiau šį skaičių reikėtų vertinti labai atsargiai, nes institucijos vadovaujasi skirtingomis sąvokos „skundas“ apibrėžtimis. Absoliutinis duomenų apsaugos institucijų gautų skundų skaičius<sup>78</sup> valstybėse narėse labai skiriasi. Daugiausia skundų užregistruota Vokietijoje (67 000), Nyderlanduose (37 000), Ispanijoje ir Prancūzijoje (po 18 000), Italijoje (14 000), Lenkijoje ir Airijoje (po 12 000). Du trečdaliai institucijų pranešė, kad gauta nuo 8 000 iki 600 skundų. Mažiausia skundų užregistruota Estijoje ir Belgijoje (mažiau nei po 500), Maltoje ir Islandijoje (mažiau nei po 200).

Skundų skaičius nebūtinai sietinas su gyventojų skaičiumi ar BVP: pavyzdžiui, Vokietijoje beveik dvigubai daugiau skundų nei Nyderlanduose ir keturis kartus daugiau nei Ispanijoje ir Prancūzijoje.

Iš grįžtamosios informacijos iš įvairių suinteresuotųjų subjektų grupės matyti, kad organizacijos yra įgyvendinusios įvairias priemones, kad būtų sudarytos sąlygos naudotis duomenų subjektų teisėmis, įskaitant įgyvendinimo procesus, kuriais užtikrinama, kad duomenų valdytojas nagrinėtų prašymus ir atsakytų individualiai, būtų naudojami keli kanalai (paštas, specialiai skundams skirtas e. pašto adresas, interneto svetainė ir kt.), būtų atnaujinamos vidaus procedūros ir politika dėl prašymų tvarkymo vidaus lygmeniu laiku ir užtikrinamas darbuotojų mokymas. Kai kuriose įmonėse yra sukurti skaitmeniniai portalai, kuriais galima naudotis per įmonės interneto svetainę (arba įmonės darbuotojams skirtą intranetą), siekiant sudaryti sąlygas duomenų subjektams naudotis savo teisėmis.

Tačiau reikia toliau siekti pažangos dėl toliau išvardytų aspektų.

- Ne visi duomenų valdytojai laikosi savo prievolės sudaryti sąlygas duomenų subjektams naudotis savo teisėmis<sup>79</sup>. Jie turi užtikrinti, kad duomenų subjektai faktiškai galėtų kreiptis į kontaktinį asmenį, kuriam galėtų paaiškinti savo problemas. Tai gali būti duomenų apsaugos pareigūnas, kurių kontaktiniai duomenys turi būti aktyviai pateikiami duomenų subjektui<sup>80</sup>. Būdas susisiekti

<sup>75</sup> BDAR 80 straipsnis.

<sup>76</sup> COM(2018) 0184 *final* – 2018/089 (COD).

<sup>77</sup> Ir pagal BDAR 77 straipsnį, ir pagal 80 straipsnį.

<sup>78</sup> Žr. Valdybos nuomonę, p. 31 ir 32.

<sup>79</sup> BDAR 12 straipsnio 2 dalis.

<sup>80</sup> BDAR 13 straipsnio 1 dalies b punktas ir 14 straipsnio 1 dalies b punktas.

negali būti tik e. paštas; duomenų subjektai taip pat turi turėti galimybę kreiptis į duomenų valdytoją kitomis priemonėmis.

- Fiziniais asmenims vis dar kyla sunkumų prašant leisti susipažinti su duomenimis, pavyzdžiui, platformose, duomenų brokerių įmonėse ir reklamos technologijų įmonėse.
- Teise į duomenų perkeliamumą nėra naudojama visu pajėgumu. Europos duomenų strategijoje (toliau – Duomenų strategija)<sup>81</sup>, kurią Komisija priėmė 2020 m. vasario 19 d., pabrėžiamas poreikis sudaryti visas įmanomas sąlygas naudotis šia teise (pvz., nurodant sukurti technines sąsajas ir kompiuterio skaitomus formatus, kuriais užtikrinamas duomenų perkeliamumas (beveik) tikruoju laiku). Veiklos vykdytojai pažymi, kad kartais patiria sunkumų teikiant duomenis aiškios struktūros, plačiai naudojamu kompiuterio skaitomu formatu (nes nėra standarto). Tik tam tikrų sektorių, kaip antai bankininkystės, telekomunikacijų, vandens ir šilumos skaitiklių, organizacijos praneša, kad yra įgyvendinusios būtinas sąsajas<sup>82</sup>. Sukurtos naujos technologijų priemonės, kuriomis siekiama sudaryti sąlygas fiziniais asmenims naudotis savo teisėmis pagal BDAR, ne tik dėl duomenų perkeliamumo (pvz., dėl asmens duomenų saugyklų ir asmens informacijos valdymo paslaugų).
- Vaikų teisės: keli įvairių suinteresuotųjų subjektų grupės nariai pabrėžia, kad reikia teikti informaciją vaikams ir kad daugelis organizacijų neatsižvelgia į tai, jog jų vykdomas duomenų tvarkymas gali būti susijęs su vaikais. Taryba pabrėžė, kad rengiant elgesio kodeksus vaikų apsaugai būtų galima skirti ypatingą dėmesį. Duomenų apsaugos institucijos taip pat ypač rūpinasi vaikų apsauga<sup>83</sup>.
- Teisė į informaciją: kai kurios įmonės taiko labai teisišką požiūrį ir duomenų apsaugos pranešimus laiko teisiniu darbu: teikiama gana sudėtinga informacija, kurią sunku suprasti arba kuri nėra išsami, o pagal BDAR visa informacija turėtų būti glausta ir parengta aiškia ir paprasta kalba<sup>84</sup>. Kai kurios įmonės, atrodo, nesilaiko Valdybos rekomendacijų, pavyzdžiui, dėl subjektų, su kuriais jos dalijasi duomenimis, pavadinimų išvardijimo.
- Keliose valstybėse narėse duomenų subjektų teisės iš esmės ribojamos nacionalinės teisės aktais, o kai kuriose netgi viršijama veiksmų laisvė pagal BDAR 23 straipsnį.
- Fiziniai asmenys kartais susiduria su kliūtimis naudotis teisėmis dėl kelių didelių skaitmeninių įmonių taikomų metodų, dėl kurių fiziniais asmenims sunku pasirinkti geriausius privatumo apsaugos parametrus (pažeidžiant pritaikytosios ir standartizuotosios duomenų apsaugos reikalavimą<sup>85</sup>)<sup>86</sup>.

---

<sup>81</sup> [https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020\\_en.pdf](https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf).

<sup>82</sup> Žr. įvairių suinteresuotųjų subjektų grupės ataskaitą.

<sup>83</sup> Žr. viešų konsultacijų dėl vaikų duomenų apsaugos teisių, kurias surengė Airijos duomenų apsaugos institucija, rezultatus: [https://www.dataprotection.ie/sites/default/files/uploads/2019-09/Whose%20Rights%20Are%20They%20Anyway\\_Trends%20and%20Highlights%20from%20Stream%201.pdf](https://www.dataprotection.ie/sites/default/files/uploads/2019-09/Whose%20Rights%20Are%20They%20Anyway_Trends%20and%20Highlights%20from%20Stream%201.pdf). 2020 m. balandžio mėn. viešas konsultacijas pradėjo ir Prancūzijos duomenų apsaugos institucija: <https://www.cnil.fr/fr/la-cnil-lance-une-consultation-publique-sur-les-droits-des-mineurs-dans-lenvironnement-numerique>.

<sup>84</sup> BDAR 12 straipsnio 1 dalis.

<sup>85</sup> BDAR 25 straipsnis.



Suinteresuotieji subjektai labai laukia Valdybos gairių dėl duomenų subjektų teisių.

## **5 ORGANIZACIJŲ, VISŲ PIRMA MAŽŪJŲ IR VIDUTINIŲ ĮMONIŲ, GALIMYBĖS IR IŠŠŪKIAI**

### *Organizacijoms atsiveriančios galimybės*

BDAR skatinama konkurencija ir inovacijos. Kartu su Laisvo ne asmens duomenų judėjimo reglamentu<sup>87</sup>, juo užtikrinamas laisvas duomenų judėjimas ES viduje ir sukuriama vienodos sąlygos su įmonėmis, įsisteigusiomis už ES ribų. BDAR sukuriama suderintą asmens duomenų apsaugos sistemą užtikrinama, kad visi vidaus rinkos dalyviai laikytųsi vienodų taisyklių ir naudotųsi vienodomis galimybėmis, neatsižvelgiant į tai, kur jie yra įsisteigę ir kur vyksta duomenų tvarkymas. Užtikrinant BDAR technologinį neutralumą sukuriama duomenų apsaugos sistema, pritaikyta naujai technologinei plėtrai. Pritaikytosios ir standartizuotosios duomenų apsaugos principais skatinami novatoriški sprendimai, kuriuos kuriant iš pat pradžių atsižvelgiama į duomenų apsaugą ir gali būti sumažinamos duomenų apsaugos taisyklių laikymosi sąnaudos.

Be to, privatumas tampa svarbiu konkurencijos aspektu, į kurį vis dažniau atsižvelgiama renkantis paslaugas. Asmenys, kurie yra geriau informuoti ir labiau vertina duomenų apsaugą, ieško produktų ir paslaugų, kuriais užtikrinama veiksminga asmens duomenų apsauga. Įgyvendinant teisę į duomenų perkeliamumą gali būti mažinamos kliūtys įmonėms, siūlančioms novatoriškas duomenų apsaugos principais grindžiamas paslaugas, patekti į rinką. Galimo platesnio šios teisės naudojimo įvairiuose rinkos sektoriuose poveikį reikėtų stebėti. Laikantis duomenų apsaugos taisyklių ir skaidriai jas taikant bus užtikrinamas pasitikėjimas dėl žmonių asmens duomenų naudojimo ir įmonėms atsivers naujų galimybių.

Kaip visais reglamentavimo atvejais, dėl duomenų apsaugos taisyklių įmonės savaime patiria išlaidų. Tačiau tas išlaidas nusveria galimybės ir pranašumai, susiję su didesniu pasitikėjimu skaitmeninėmis inovacijomis ir nauda visuomenei dėl pagrindinės teisės laikymosi. Užtikrinant vienodas sąlygas ir aprūpinant duomenų apsaugos institucijas tuo, kas joms reikalinga siekiant veiksmingai užtikrinti taisyklių vykdymą, pagal BDAR užkertamas kelias įmonėms, kurios nesilaiko reikalavimų, piktnaudžiavimui pasitikėjimu, kurį užtikrina taisyklių besilaikančios įmonės.

### *Konkretūs mažosioms ir vidutinėms įmonėms (MVI) kylantys iššūkiai*

---

<sup>86</sup> Žr. Norvegijos vartotojų tarybos ataskaitą „Deceived by Design“, kurioje išdėstomi neskaidrūs modeliai, numatytieji parametrai ir kitos įmonių naudojamos priemonės ir būdai paraginti naudotojus rinktis įkyresnius variantus:

<https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/>.

Taip pat žr. tyrimą, kurį 2019 m. gruodžio mėn. paskelbė Transatlantinis vartotojų dialogas ir Briuselio Europos Sąjungos Heinrich-Böll-Stiftung ir kuriame nagrinėjama trijų pagrindinių pasaulio platformų metodai:

<https://eu.boell.org/en/2019/12/11/privacy-eu-and-us-consumer-experiences-across-three-global-platforms>.

<sup>87</sup> 2018 m. lapkričio 14 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1807 dėl laisvo ne asmens duomenų judėjimo Europos Sąjungoje pagrindų (OL L 303, 2018 11 28, p. 59–68).



Ir suinteresuotieji subjektai, ir Europos Parlamentas, Taryba ir duomenų apsaugos institucijos mano, kad BDAR taikymas kelia ypatingų sunkumų labai mažoms, mažosioms ir vidutinėms įmonėms bei mažoms savanoriškoms ir labdaros organizacijoms.

Remiantis rizika pagrįstu metodu nederėtų numatyti nukrypti leidžiančių nuostatų dėl veiklos vykdytojų dydžio, nes jų dydis savaime nėra rizikos, kuri jiems tvarkant asmens duomenis gali kilti asmenims, požymis. Taikant rizika pagrįstą metodą lankstumas derinamas su veiksminga apsauga. Jį taikant atsižvelgiama į MVI, kurių pagrindinė veikla nėra duomenų tvarkymas, poreikius ir kalibruojamos jų prievolės, visų pirma remiantis su konkrečiomis jų vykdomomis duomenų tvarkymo operacijomis susijusios rizikos tikimybe ir rimtumu<sup>88</sup>.

Nedidelio masto ir rizikos duomenų tvarkymo operacijų nereikėtų prilyginti prie dažnai vykdomo didelės rizikos duomenų tvarkymo, neatsižvelgiant į duomenis tvarkančios įmonės dydį. Taigi Valdyba padarė išvadą, kad „bet kuriuo atveju reikėtų ir toliau laikytis teisės aktų leidėjo šiame akte skatinamo rizika pagrįsto metodo, nes duomenų subjektams kylanti rizika nepriklauso nuo duomenų valdytojų dydžio“<sup>89</sup>. Užtikrinamos BDAR vykdymą duomenų apsaugos institucijos turėtų visiškai atsižvelgti į šį principą ir, pageidautina, taikyti bendrą europinį požiūrį, kad bendrojoje rinkoje nebūtų sudaromos kliūtys.

Duomenų apsaugos institucijos sukūrė kelias priemones ir pabrėžė savo ketinimą toliau jas tobulinti. Kai kurios institucijos pradėjo informuotumo didinimo kampanijas ir net rengs nemokamas MVI skirtas paskaitas apie BDAR.

*Gairių ir priemonių, kurias duomenų apsaugos institucijos nustato konkrečiai MVI, pavyzdžiai*

- MVI skirtos informacijos skelbimas;
- seminarai duomenų apsaugos pareigūnams ir renginiai MVI, kuriuose nereikia paskirti duomenų apsaugos pareigūno;
- interaktyvūs vadovai, skirti padėti MVI;
- karštosios linijos konsultacijoms;
- duomenų tvarkymo sutarčių ir duomenų tvarkymo veiklos įrašų šablonai.

Duomenų apsaugos institucijų veiklos aprašymas pateiktas Valdybos nuomonėje<sup>90</sup>.

Keliems veiksmams, kuriais konkrečiai remiamos MVI, buvo skirtas ES finansavimas. Komisija skyrė finansinę paramą per tris dotacijų raundus (bendra suma – 5 mln. EUR); du paskutiniai etapai buvo specialiai skirti remti nacionalines duomenų apsaugos institucijas joms stengiantis informuoti fizinius asmenis ir MVI. Todėl 2018 m. buvo skirta 2 mln. EUR devynioms duomenų apsaugos institucijoms 2018–2019 m. veiklai vykdyti (Belgijoje, Bulgarijoje, Danijoje, Vengrijoje, Lietuvoje,

<sup>88</sup> BDAR 24 straipsnio 1 dalis.

<sup>89</sup> Žr. Valdybos nuomonę, p. 35.

<sup>90</sup> Žr. Valdybos nuomonę, p. 35–45.

Latvijoje, Nyderlanduose, Slovėnijoje ir Islandijoje)<sup>91</sup>, o 2019 m. buvo skirta 1 mln. EUR keturioms duomenų apsaugos institucijoms 2020 m. veiklai vykdyti (Belgijoje, Maltoje, Slovėnijoje ir Kroatijoje partnerystės su Airija pagrindu)<sup>92</sup>. 2020 m. bus skirta dar 1 mln. EUR.

Nepaisant šių iniciatyvų MVĮ ir startuoliai neretai praneša, kad jiems sunku įgyvendinti BDAR numatytą atskaitomybės principą<sup>93</sup>. Jie, visų pirma, teigia, kad ne visada gauna pakankamai gairių ir praktinių patarimų iš nacionalinių duomenų apsaugos institucijų arba kad gauti tokias gaires ir rekomendacijas per ilgai užtrunka. Taip pat būta atvejų, kai institucijos nenorėjo užsiimti teisiniais klausimais. Susidūrusios su tokiomis situacijomis MVĮ neretai kreipiasi į išorės konsultantus ir teisininkus, kad įgyvendintų atskaitomybės principą ir rizika pagrįstą metodą (įskaitant skaidrumo reikalavimus, duomenų tvarkymo įrašus ir pranešimus apie duomenų saugumo pažeidimus). Dėl to jos gali patirti papildomų išlaidų.

Viena konkreti problema – tai duomenų tvarkymo veiklos dokumentavimas, kurį MVĮ ir mažos asociacijos laiko didele administracine našta. BDAR 30 straipsnio 5 dalyje numatytas leidimas nesilaikyti šios prievolės iš tikrųjų yra labai siauras. Tačiau su tos prievolės vykdymu susijusių pastangų nereikėtų pervertinti. Jeigu pagrindinė MVĮ veikla nėra susijusi su asmens duomenų tvarkymu, tokie įrašai gali būti paprasti ir nesudaryti naštos. Tas pats pasakytina apie savanoriškas ir kitas asociacijas. Tokius supaprastintus įrašus būtų lengviau rengti naudojant įrašų šablonus, kaip jau daro kai kurios duomenų apsaugos institucijos. Bet kuriuo atveju visi tvarkantys asmens duomenis turėtų parengti atliekamo duomenų tvarkymo apžvalgą; tai pagrindinis atskaitomybės principo reikalavimas.

Valdybos rengiamos ES lygmens praktinės priemonės, kaip antai suderintos pranešimų apie duomenų saugumo pažeidimus ir supaprastintų duomenų tvarkymo veiklos įrašų formos, gali būti naudingos MVĮ ir mažoms asociacijoms<sup>94</sup>, kurių pagrindinė veikla vykdančios prievolės nėra asmens duomenų tvarkymas.

Įvairios pramonės asociacijos deda pastangas, kad didintų informuotumą ir informuotų savo narius, pavyzdžiui, rengdamos konferencijas ir seminarus, teikdamos įmonėms informaciją apie turimas gaires ar teikdamos nariams pagalbos privatumo klausimais paslaugas. Jos taip pat praneša apie didėjantį idėjų kalvių ir MVĮ asociacijų rengiamų seminarų, susitikimų ir renginių su BDAR susijusiais klausimais skaičių.

Siekdama stiprinti laisvą visų duomenų judėjimą ES ir užtikrinti nuoseklų BDAR ir Laisvo ne asmens duomenų judėjimo reglamento taikymą Komisija taip pat parengė specialiai MVĮ skirtas praktines gaires dėl taisyklių, kuriomis reglamentuojamas mišrių asmens ir ne asmens duomenų rinkinių tvarkymas<sup>95</sup>.

### *Įmonėms skirtų priemonių rinkinys*

<sup>91</sup> <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai-ag-2017>.

<sup>92</sup> <https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supporting-implementation-gdpr-en>.

<sup>93</sup> Žr. įvairių suinteresuotųjų subjektų grupės ataskaitą.

<sup>94</sup> Žr. Tarybos nuomonę.

<sup>95</sup> Komisijos komunikatas Europos Parlamentui ir Tarybai „Gairės dėl Reglamento dėl laisvo ne asmens duomenų judėjimo Europos Sąjungoje pagrindų“, COM(2019) 250 *final*.

BDAR yra numatytos priemonės, padedančios įrodyti reikalavimų laikymąsi, kaip antai elgesio kodeksai, sertifikavimo mechanizmai ir standartinės sutarčių sąlygos.

- Elgesio kodeksai

Valdyba paskelbė gaires<sup>96</sup>, kuriomis siekiama teikti pagalbą ir sudaryti palankesnes sąlygas už kodeksą atsakingiems subjektams rengti, iš dalies pakeisti ar išplėsti kodeksus bei pateikti praktines gaires ir pagalbą aiškinant reglamentą. Tose gairėse taip pat paaiškinamos kodeksų pateikimo, patvirtinimo ir paskelbimo procedūros nacionaliniu ir ES lygmenimis nustatant minimaliuosius privalomus kriterijus.

Suinteresuotieji subjektai mano, kad elgesio kodeksai yra labai naudinga priemonė. Nors daugelis kodeksų įgyvendinama nacionaliniu lygmeniu, šiuo metu rengiami keli ES masto elgesio kodeksai (pavyzdžiui, dėl sveikatos srities mobiliųjų programėlių, sveikatos srities mokslinių genomikos tyrimų, debesijos kompiuterijos, tiesioginės rinkodaros, draudimo, prevencinio duomenų tvarkymo ir konsultacinių paslaugų vaikams)<sup>97</sup>. Veiklos vykdytojai mano, kad ES masto elgesio kodeksus reikėtų skatinti aktyviau, nes jie padeda užtikrinti nuoseklų BDAR taikymą visose valstybėse narėse.

Tačiau elgesio kodeksai taip pat reikalauja iš veiklos vykdytojų laiko ir investicijų juos rengiant ir įsteigiant privalomas nepriklausomas stebėsenos įstaigas. MVI atstovai pabrėžia jų padėčiai pritaikytų elgesio kodeksų, dėl kurių nepatiriama neproporcingų išlaidų, svarbą ir naudingumą.

Taigi keliuose sektoriuose verslo asociacijos įgyvendino kitų rūšių savireguliacijos priemones, kaip antai gerosios praktikos kodeksus arba gaires. Nors taikant tokias priemones galima gauti naudingos informacijos, jie nėra patvirtinti duomenų apsaugos institucijų ir negali būti naudojami kaip priemonė, padedanti įrodyti BDAR atitiktį.

Taryba pabrėžia, kad elgesio kodeksuose reikia skirti ypatingą dėmesį vaikų duomenų ir sveikatos duomenų tvarkymui. Komisija pritaria dėl elgesio kodekso (-ų), kuriuo (kuriais) būtų suderintas požiūris sveikatos ir mokslinių tyrimų srityse ir sudaromos palankesnės sąlygos tvarkyti asmens duomenis tarpvalstybiniu lygmeniu<sup>98</sup>. Šiuo metu Valdyba tvirtina elgesio kodeksų stebėsenos įstaigų akreditavimo reikalavimų projektą, kurį pateikė kelios duomenų apsaugos institucijos<sup>99</sup>. Kai tarpvalstybiniai ar ES elgesio kodeksai bus paruošti teikti tvirtinti duomenų apsaugos institucijoms, dėl jų vyks konsultacijos Valdyboje. Skubiai parengti tarpvalstybinius elgesio kodeksus ypač svarbu srityse, susijusiose su didelių duomenų kiekių tvarkymu (pvz., debesijos kompiuterijos) ar neskelbtinų duomenų tvarkymu (pvz., sveikatos ir mokslinių tyrimų).

- Sertifikavimas

Sertifikavimas gali būti naudinga priemonė siekiant įrodyti konkrečių BDAR reikalavimų laikymąsi. Taip galima padidinti teisinį tikrumą įmonėms ir populiarinti BDAR visame pasaulyje.

---

<sup>96</sup> [https://edpb.europa.eu/our-work-tools/our-documents/wytyczne/guidelines-12019-codes-conduct-and-monitoring-bodies-under\\_en](https://edpb.europa.eu/our-work-tools/our-documents/wytyczne/guidelines-12019-codes-conduct-and-monitoring-bodies-under_en).

<sup>97</sup> Žr. įvairių suinteresuotųjų subjektų grupės ataskaitą.

<sup>98</sup> Žr. veiksmus, paskelbtus Europos duomenų strategijoje, p. 30.

<sup>99</sup> Pagal BDAR 41 straipsnio 3 dalį. Žr. EDAV nuomonės šiuo adresu: [https://edpb.europa.eu/our-work-tools/consistency-findings/opinions\\_lt](https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_lt)

Kaip pažymėta 2019 m. balandžio mėn. paskelbtame tyrime dėl sertifikavimo<sup>100</sup>, tikslas turėtų būti palengvinti atitinkamų sistemų diegimą. Sertifikavimo sistemų kūrimas ES bus remiamas Valdybai parengiant gaires dėl sertifikavimo kriterijų<sup>101</sup> ir dėl sertifikavimo įstaigų akreditavimo<sup>102</sup>.

Saugumas ir pritaikytoji duomenų apsauga yra pagrindiniai elementai, į kuriuos reikia atsižvelgti sertifikavimo sistemose pagal BDAR ir dėl kurių visoje ES reikėtų taikyti bendrą plataus užmojo požiūrį. Komisija ir toliau remis palaikomus ryšius tarp Europos Sąjungos agentūros kibernetinio saugumo agentūros (ENISA), duomenų apsaugos institucijų ir Valdybos.

Kalbant apie kibernetinį saugumą, po Kibernetinio saugumo akto patvirtinimo Komisija paprašė ENISA parengti dvi sertifikavimo sistemas, įskaitant vieną, skirtą debesijos paslaugoms<sup>103</sup>. Šiuo metu svarstomos kitos sistemos, susijusios su paslaugų ir vartotojams skirtų produktų kibernetiniu saugumu. Nors tos sertifikavimo sistemos, sukurtos pagal Kibernetinio saugumo aktą, nėra konkrečiai susijusios su duomenų apsauga ir privatumu, jos padeda didinti vartotojų pasitikėjimą skaitmeninėmis paslaugomis ir produktais. Iš tokių sistemų galima gauti įrodymų, kad laikomasi pritaikytųjų saugumo principų ir įgyvendinamos tinkamos techninės ir organizacinės priemonės, susijusios su asmens duomenų tvarkymo saugumu.

- Standartinės sutarčių sąlygos

Komisija dirba prie standartinių sutarčių tarp duomenų valdytojų ir duomenų tvarkytojų sąlygų<sup>104</sup>, be kita ko, atsižvelgdama į standartinių sutarčių sąlygų dėl tarptautinio duomenų perdavimo modernizavimą (žr. 7.2 skirsnį). Komisijos priimtas Sąjungos aktas bus privalomas visoje ES ir taip bus užtikrinamas visiškas suderinimas ir teisinis tikrumas.

## 6 BDAR TAIKYMAS NAUJOMS TECHNOLOGIJOMS

### *Technologiškai neutrali sistema, atvira naujoms technologijoms*

BDAR yra technologiškai neutralus, pasitikėjimą skatinantis teisės aktas, grindžiamas principais<sup>105</sup>. Tie principai, įskaitant teisėtą ir skaidrų duomenų tvarkymą, jo tikslo apribojimą ir duomenų kiekio mažinimą, yra tvirtas asmens duomenų apsaugos pagrindas, neatsižvelgiant į vykdomas duomenų tvarkymo operacijas ir taikomus metodus.

---

<sup>100</sup> [https://ec.europa.eu/info/study-data-protection-certification-mechanisms\\_en](https://ec.europa.eu/info/study-data-protection-certification-mechanisms_en).

<sup>101</sup>

[https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_guidelines\\_201801\\_v3.0\\_certificationcriteria\\_annex2\\_lt.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_lt.pdf).

<sup>102</sup>

[https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_guidelines\\_201804\\_v3.0\\_accreditationcertificationbodies\\_annex1\\_lt.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_lt.pdf). Kelios priežiūros institucijos jau pateikė savo akreditavimo reikalavimus EDAV ir dėl elgesio kodeksų stebėsenos įstaigų, ir dėl sertifikavimo įstaigų. Apžvalgą žr. adresu [https://edpb.europa.eu/our-work-tools/consistency-findings/opinions\\_lt](https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_lt).

<sup>103</sup>

<https://ec.europa.eu/digital-single-market/en/news/towards-more-secure-and-trusted-cloud-europe>.

<sup>104</sup> BDAR 28 straipsnio 7 dalis.

<sup>105</sup> Kaip savo nuomonėse dėl vertinimo primena Taryba, Europos Parlamentas ir Valdyba.

Įvairių suinteresuotųjų subjektų grupės nariai pažymi, kad apskritai BDAR daro teigiamą poveikį naujų technologijų plėtrai ir yra geras pagrindas inovacijoms. BDAR laikomas esmine ir lanksčia priemone užtikrinti naujų technologijų plėtrą laikantis pagrindinių teisių. Tvarkant daug duomenų itin svarbu įgyvendinti jo pagrindinius principus. BDAR įtvirtintu rizika pagrįstu ir technologiškai neutraliu požiūriu užtikrinamas duomenų apsaugos lygis, kuris yra pakankamas siekiant pašalinti su tvarkymu susijusią riziką, be kita ko, pasitelkiant kuriamas technologijas.

Visų pirma, suinteresuotieji subjektai pažymi, kad BDAR įtvirtinti tikslo apribojimo ir tolesnio suderinamo duomenų tvarkymo, duomenų kiekio mažinimo, saugojimo trukmės apribojimo, skaidrumo ir atskaitomybės principai bei sąlygos, kuriomis gali būti teisiškai naudojami automatizuoti sprendimų priėmimo procesai<sup>106</sup>, iš esmės skirti išsklaidyti abejones dėl dirbtinio intelekto naudojimo.

Ateities iššūkiams parengtas ir rizika pagrįstas BDAR metodas taip pat bus taikomas galimoje būsimoje dirbtinio intelekto sistemoje ir įgyvendinant Duomenų strategiją. Duomenų strategijos tikslas – skatinti duomenų prieinamumą ir sukurti bendras Europos duomenų erdves, kuriose būtų teikiamos sietinės debesijos infrastruktūros paslaugos. Kalbant apie asmens duomenis, BDAR sukuriama pagrindinė teisinė sistema, kurioje kiekvienu konkrečiu atveju galima kurti veiksmingus sprendimus atsižvelgiant į kiekvienos duomenų erdvės pobūdį ir turinį.

Taikant BDAR padidėjo informuotumas apie asmens duomenų apsaugą ir ES viduje, ir už jos ribų, o įmonės buvo paskatintos pritaikyti savo metodus taip, kad diegiant inovacijas būtų atsižvelgiama į duomenų apsaugos principus. Tačiau pilietinės visuomenės organizacijos pažymi, kad, nors BDAR poveikis naujų technologijų plėtrai atrodo teigiamas, didelių skaitmeninės veiklos vykdytojų metodai dar iš esmės nepasikeitė taip, kad tvarkant duomenis būtų labiau orientuojamasi į privatumą. Patikimas ir veiksmingas BDAR vykdymo užtikrinimas jį taikant didelėms skaitmeninėms platformoms ir integruotoms įmonėms, įskaitant tokias sritis, kaip reklama internetu ir tikslus reklamos orientavimas, yra esminis elementas norint apsaugoti asmenis.

Komisija nagrinėja bendresnius klausimus, susijusius su didelių skaitmeninės veiklos vykdytojų elgesiu rinkoje, taikant Skaitmeninių paslaugų akto rinkinį<sup>107</sup>. Kalbant apie mokslinius tyrimus socialinės žiniasklaidos srityje, Komisija primena, kad socialinės žiniasklaidos platformos negali naudoti BDAR kaip pagrindo apriboti tyrėjų ir faktų tikrintojų prieigą prie ne asmens duomenų, kaip antai statistikos, kuriais remiantis nustatoma, kokia tikslinė reklama buvo išsiųsta kokių kategorijų asmenims, tokio tikslo orientavimo kriterijai, informacija apie netikras paskyras ir kt.

BDAR įtvirtintas technologiškai neutralus ir ateities iššūkiams pritaikytas metodas buvo išbandytas COVID-19 pandemijos sąlygomis ir užsirekomendavo kaip sėkmingas. Taikant jame nustatytas principais pagrįstas taisykles sudaromos sąlygos kurti priemones, skirtas kovoti su viruso plitimu ir jį stebėti.

### *Spręstinos problemos*

---

<sup>106</sup> Tačiau suinteresuotieji subjektai pažymi, kad ne visiems automatizuoto sprendimų priėmimo procesams pasitelkiant dirbtinį intelektą yra taikomas BDAR 22 straipsnis.

<sup>107</sup> [https://ec.europa.eu/commission/presscorner/detail/lt/ip\\_20\\_962](https://ec.europa.eu/commission/presscorner/detail/lt/ip_20_962).

Kuriant ir taikant naujas technologijas šie principai nėra kvestionuojami. Sunkumų kyla siekiant išsiaiškinti, kaip taikyti patvirtintus principus naudojant konkrečias technologijas, kaip antai dirbtinį intelektą, blokų grandinę, daiktų internetą, veido atpažinimą ar kvantinę kompiuteriją.

Atsižvelgdami į tai, Europos Parlamentas ir Taryba pabrėžė, jog reikia nuolat vykdyti stebėseną siekiant išsiaiškinti, kaip BDAR taikomas naujoms technologijoms ir didelėms technologijų įmonėms. Be to, suinteresuotieji subjektai įspėja, kad taip pat reikia nuolat stebėti vertinimą, ar BDAR ir toliau lieka tinkamas jo tikslams pasiekti.

Sektoriams atstovaujantys suinteresuotieji subjektai pabrėžia, kad BDAR yra taikomas remiantis jame įtvirtintais principais, o ne griežtai ir formaliai. Jie mano, kad Valdybos gairės dėl to, kaip taikyti BDAR principus, sąvokas ir taisykles naujoms technologijoms, kaip antai dirbtiniam intelektui, blokų grandinei ar daiktų internetui, atsižvelgiant į rizika pagrįstą metodą, padėtų viską išsiaiškinti ir užtikrinti teisinį tikrumą. Tokios privalomos teisinės galios neturintys teisinės priemonės tinka kartu su BDAR taikyti naujoms technologijoms, nes jomis užtikrinamas didesnis teisinis tikrumas ir jas galima peržiūrėti atsižvelgiant į technologinę plėtrą. Kai kurie suinteresuotieji subjektai taip pat teigia, kad galėtų būti naudingos konkrečioms sektoriams skirtos gairės dėl to, kaip taikyti BDAR naujoms technologijoms.

Valdyba pareiškė, kad ir toliau vertins naujų technologijų poveikį asmens duomenų apsaugai.

Suinteresuotieji subjektai taip pat pabrėžia, kaip svarbu, kad reguliavimo institucijos nuodugniai suprastų, kaip technologija naudojama, ir dalyvautų dialoge su sektoriumi dėl naujų technologijų kūrimo. Jie mano, kad įdomus būdas išbandyti naujas technologijas ir padėti įmonėms taikyti pritaikytosios ir standartizuotosios duomenų apsaugos principus naujoms technologijoms būtų vadinamasis reguliavimo smėliadėžės metodas, kuris yra būdas gauti gaires dėl taisyklių taikymo.

Kalbant apie tolesnius politikos veiksmus, suinteresuotieji subjektai rekomenduoja, kad visi būsimi politikos pasiūlymai dėl dirbtinio intelekto turėtų būti grindžiami esamomis teisinėmis sistemomis ir derėtų su BDAR. Galimus konkrečius klausimus reikėtų atidžiai įvertinti remiantis svarbiais įrodymais, prieš siūlant naujas normines taisykles.

Komisijos baltojoje knygoje dėl dirbtinio intelekto pateikiama daug politikos galimybių, dėl kurių suinteresuotųjų subjektų nuomonių buvo laukiama iki 2020 m. birželio 14 d. Kalbant apie veido atpažinimą, t. y. technologiją, kuri gali padaryti didelį poveikį asmenų teisėms, Baltojoje knygoje primenama apie galiojančią teisinę sistemą ir pradedamos viešos diskusijos dėl konkrečių aplinkybių (jeigu jų yra), kuriomis dirbtinio intelekto naudojimas veidui ir kitiems biometriniais tapatybės nustatymo duomenims atpažinti viešosiose vietose, ir bendrą apsaugos priemonių.

## **7 TARPTAUTINIS DUOMENŲ PERDAVIMAS IR PASAULINIS BENDRADARBIAVIMAS**

### **7.1 *Privatumas. Pasaulio masto klausimas***

Asmens duomenų apsaugos paklausa nepaiso sienų, nes visame pasaulyje vis labiau branginamas ir vertinamas privatumas ir duomenų saugumas.



Kita vertus, duomenų srautų svarba asmenims, vyriausybėms, įmonėms ir apskritai visuomenei yra neišvengiamas faktas mūsų tarpusavyje susijusiame pasaulyje. Jie yra neatsiejama prekybos, valdžios institucijų bendradarbiavimo ir socialinių ryšių dalis. Šiuo požiūriu dėl dabartinės COVID-19 pandemijos taip pat matyti, kaip svarbu perduoti asmens duomenis ir jais keistis atliekant daugelį esminių veiksmų, įskaitant vyriausybės ir verslo operacijų tęstinumo užtikrinimą, suteikiant galimybę dirbti nuotoliniu būdu ir pasitelkiant kitus sprendimus, kurie labai priklauso nuo informacinių ir ryšių technologijų – plėtoti bendradarbiavimą atliekant mokslinius tyrimus diagnostikos, gydymo ir vakcinų srityse ir kovojant su naujų formų kibernetiniais nusikaltimais, kaip antai sukčiavimo internetu schemomis, kai siūlomi padirbti vaistai, teigiant, jog jais galima užkirsti kelią COVID-19 arba jį išgydyti.

Atsižvelgiant į tai, dabar labiau nei bet kada anksčiau privatumo apsauga ir duomenų srautų palengvinimas turėtų būti užtikrinami lygiagrečiai. ES, kurioje galioja duomenų apsaugos režimas užtikrinant atvirumą tarptautiniam duomenų perdavimui esant aukšto lygio asmenų apsaugai, turi puikią galimybę skatinti saugius ir patikimus duomenų srautus. BDAR jau tapo atskaitos tašku tarptautiniu lygmeniu ir paskatino daugelį šalių visame pasaulyje apsvarstyti galimybę nustatyti šiuolaikines privatumo taisykles.

Tai iš tiesų pasaulinė tendencija, stebima (ir tai vos keli pavyzdžiai) nuo Čilės iki Pietų Korėjos, nuo Brazilijos iki Japonijos, nuo Kenijos iki Indijos, nuo Tuniso iki Indonezijos ir nuo Kalifornijos iki Taivano. Tokie pokyčiai yra nuostabūs ne tik kiekybiniu, bet ir kokybiniu požiūriu: daugelis neseniai priimtų arba šiuo metu priimamų privatumo teisės aktų yra pagrįsti pagrindinių bendrų apsaugos priemonių, teisių ir vykdymo užtikrinimo mechanizmų, kuriais dalijasi ES, rinkiniu. Šiame pasaulyje, kuriam pernelyg dažnai yra būdingi skirtingi ar net prieštaringi reguliavimo metodai, ši pasaulinės konvergencijos tendencija yra labai teigiamas pokytis, dėl kurio atsiveria naujų galimybių didinti asmenų apsaugą Europoje ir kartu palengvinti duomenų srautus bei sumažinti verslo subjektų patiriamas sandorių sąnaudas.

Siekdama išnaudoti šias galimybes ir įgyvendinti 2017 m. komunikate „Keitimasis asmens duomenimis ir jų apsauga globalizuotame pasaulyje“<sup>108</sup> nustatytą strategiją Komisija gerokai sustiprino savo darbą prie tarptautinio privatumo aspekto visiškai išnaudodama turimą duomenų perdavimo priemonių rinkinį, kaip paaiškinama toliau. Tai, be kita ko, aktyvus bendradarbiavimas su pagrindiniais partneriais siekiant prieiti prie išvados dėl tinkamumo, kuris davė svarbių rezultatų, pavyzdžiui, buvo sukurta didžiausią pasaulyje laisvų ir saugių duomenų srautų erdvė tarp ES ir Japonijos.

Be su tinkamumu susijusio darbo, Komisija glaudžiai bendradarbiauja su duomenų apsaugos institucijomis Valdyboje ir kitais suinteresuotaisiais subjektais siekdama išnaudoti visą lanksčių BDAR taisyklių potencialą tarptautinio duomenų perdavimo srityje. Tai susiję su priemonių, kaip antai standartinių sutarčių sąlygų, modernizavimu, sertifikavimo sistemų, elgesio kodeksų ar administracinių susitarimų dėl duomenų mainų tarp valdžios institucijų kūrimu ir pagrindinių sąvokų, susijusių, pavyzdžiui, su ES duomenų apsaugos taisyklių teritorine taikymo sritimi arba

<sup>108</sup> Komisijos komunikatas Europos Parlamentui ir Tarybai „Keitimasis asmens duomenimis ir jų apsauga globalizuotame pasaulyje“, 2017 m. sausio 10 d. (COM(2017) 7 final).

vadinamųjų nukrypti leidžiančių nuostatų naudojimu asmens duomenims perduoti, išaiškinimu.

Galiausiai Komisija sustiprino dialogą keliuose dvišaliuose, regioniniuose ir daugiašaliuose forumuose siekdama skatinti pasaulinę pagarbos privatumui kultūrą ir plėtoti skirtingų privatumo sistemų konvergencijos elementus. Dedama šias pastangas Komisija gali tikėtis aktyvios Europos išorės veikslių tarnybos ir ES delegacijų trečiosiose šalyse ir misijų tarptautinėse organizacijose tinklo pagalbos. Tai taip pat užtikrino įvairių ES politikos išorės dimensijos aspektų (nuo prekybos iki naujosios Afrikos ir ES partnerystės) nuoseklumą ir didesnę papildomumą.

## **7.2 Duomenų perdavimo pagal BDAR priemonių rinkinys**

Kadangi vis daugiau privačiųjų ir viešųjų veiklos vykdytojų pasitelkia tarptautinius duomenų srautus kasdienėje veikloje, tampa vis labiau reikalingos lanksčios priemonės, kurias būtų galima pritaikyti įvairiems sektoriams, verslo modeliams ir duomenų perdavimo situacijoms. Atsižvelgiant į šiuos poreikius, BDAR siūlomas modernizuotas priemonių rinkinys, kuriuo palengvinamas asmens duomenų perdavimas iš ES į trečiąją šalį ar tarptautinę organizaciją, kartu užtikrinant, kad duomenų apsaugos lygis ir toliau būtų aukštas. Toks apsaugos tęstinumas yra svarbus, atsižvelgiant į tai, kad šiame pasaulyje duomenys lengvai juda per sienas ir pagal BDAR garantuojama apsauga būtų neišsami, jeigu duomenų tvarkymas vyktų tik ES viduje.

BDAR V skyriumi teisės aktų leidėjas patvirtino duomenų perdavimo taisyklių struktūrą, jau įtvirtintą Direktyvoje 95/46: duomenys gali būti perduodami, jeigu Komisija priėjo prie išvados dėl tinkamumo trečiojoje šalyje ar tarptautinėje organizacijoje arba, jos nesant, jeigu duomenų valdytojas ar duomenų tvarkytojas ES (toliau – duomenų eksportuotojas) yra užtikrinęs pakankamas apsaugos priemones, pavyzdžiui, sudarydamas sutartį su duomenų gavėju (toliau – duomenų importuotojas). Be to, konkrečiais atvejais, kai teisės aktų leidėjas yra nusprendęs, jog dėl interesų balanso galima perduoti duomenis tam tikromis sąlygomis, ir toliau galioja teisiniai duomenų perdavimo pagrindai (vadinamosios nukrypti leidžiančios nuostatos). Kita vertus, atlikus reformą galiojančios taisyklės buvo patikslintos ir supaprastintos, pavyzdžiui, išsamiai nustatant išvados dėl tinkamumo priėmimo ar įmonei privalomų taisyklių sąlygas, apribojant leidimų suteikimo reikalavimus aprėpiant tik labai nedaug konkrečių atvejų ir visiškai panaikinant pranešimo reikalavimus. Be to, sukurtos naujos duomenų perdavimo priemonės, kaip antai elgesio kodeksai ar sertifikavimo sistemos, ir plečiamos galimybės naudoti esamas priemones (pvz., standartines sutarčių sąlygas).

Šiuo metu skaitmeninėje ekonomikoje užsienio veiklos vykdytojai turi galimybę (nuotoliniu būdu, bet) tiesiogiai dalyvauti ES vidaus rinkoje ir konkuruoti dėl Europos klientų ir jų asmens duomenų. Jeigu konkrečiai orientuojamasi į europiečius siūlant jiems prekes ar paslaugas arba stebint jų elgesį, jie turėtų laikytis ES teisės taip pat, kaip ES veiklos vykdytojai. Tai nustatyta BDAR 3 straipsnyje, pagal kurį išplečiamas tiesioginis ES duomenų apsaugos taisyklių taikomumas aprėpiant konkrečias duomenų valdytojų ir duomenų tvarkytojų už ES ribų vykdomas duomenų tvarkymo operacijas. Taip garantuojamos būtinos apsaugos priemonės ir sukuriamos vienodos sąlygos visoms ES rinkoje veikiančioms įmonėms.



Didelė aprėptis yra viena iš priežasčių, kodėl BDAR poveikis taip pat jaučiamas kitose pasaulio dalyse. Todėl, po išsamių viešų konsultacijų, išsamios Valdybos skelbiamos gairės dėl teritorinės BDAR taikymo srities yra svarbios siekiant padėti užsienio veiklos vykdytojams nustatyti, ar ir kuriems duomenų tvarkymo veiksams yra tiesiogiai taikytinos reglamente numatytos apsaugos priemonės, be kita ko, pateikiant konkrečių pavyzdžių<sup>109</sup>.

Tačiau vien ES duomenų apsaugos teisės taikymo srities išplėtimo savaimė nepakanka jos praktiniam laikymuisi užtikrinti. Kaip taip pat pabrėžė Taryba<sup>110</sup>, itin svarbu užtikrinti, kad užsienio veiklos vykdytojai laikytųsi reikalavimų ir kad jiems būtų veiksmingai taikomos vykdymo užtikrinimo priemonės. Šiuo požiūriu svarbų vaidmenį turėtų atlikti atstovo ES paskyrimas (BDAR 27 straipsnio 1 ir 2 dalys); į tokį atstovą, be užsienyje veikiančios atsakingos įmonės arba vietoj jos, galėtų kreiptis fiziniai asmenys ir priežiūros institucijos<sup>111</sup>. Tokio požiūrio, kuris vis dažniau taikomas ir kitomis aplinkybėmis<sup>112</sup>, reikėtų laikytis aktyviau siekiant aiškiai parodyti, kad neįsisteigę ES užsienio veiklos vykdytojai vis tiek privalo laikytis BDAR. Jeigu tokie veiklos vykdytojai neįvykdo savo prievolės paskirti atstovą<sup>113</sup>, priežiūros institucijos turėtų naudotis BDAR 58 straipsnyje numatytu išsamiau vykdymo užtikrinimo priemonių rinkiniu (pvz., vieši įspėjimai, laikinas ar galutinis draudimas tvarkyti duomenis ES, vykdymo užtikrinimo priemonės, taikomos ES įsteigtiems bendriems duomenų valdytojams).

Galiausiai labai svarbu, kad Valdyba užbaigtų savo darbą, kurio tikslas – papildomai patikslinti ryšį tarp 3 straipsnio dėl tiesioginio BDAR taikymo ir V skyriuje nustatytų tarptautinio duomenų perdavimo taisyklių<sup>114</sup>.

### *Sprendimai dėl tinkamumo*

Gautuose suinteresuotųjų subjektų atsakymuose patvirtinama, kad sprendimai dėl tinkamumo ir toliau yra esminė priemonė ES veiklos vykdytojams saugiai perduoti asmens duomenis į trečiąsias šalis<sup>115</sup>. Tokie sprendimai yra išsamiausias,

---

<sup>109</sup> EDAV gairės Nr. 2/2018 dėl teritorinės BDAR taikymo srities, 2019 m. lapkričio 12 d. Gairėse nagrinėjami keli per viešas konsultacijas iškelti klausimai, pavyzdžiui, dėl orientavimo ir stebėsenos kriterijų aiškinimo.

<sup>110</sup> Žr. Tarybos pozicijos ir išvadų 34, 35 ir 38 punktus.

<sup>111</sup> Žr. BDAR 27 straipsnio 4 dalį ir 80 konstatuojamąją dalį („Paskirtam atstovui turėtų būti taikomi reikalavimų laikymosi užtikrinimo veiksmai tais atvejais, kai duomenų valdytojas ar duomenų tvarkytojas nesilaiko reikalavimų“).

<sup>112</sup> Pasiūlymo dėl Europos Parlamento ir Tarybos direktyvos, kuria nustatomos teisinių atstovų skyrimo įrodymams baudžiamosiose bylose rinkti suderintos taisyklės (COM(2018) 226 *final*) 3 straipsnis; pasiūlymo dėl Europos Parlamento ir Tarybos reglamento dėl teroristinio turinio sklaidos internete prevencijos (COM(2018) 640 *final*) 16 straipsnio 2 ir 3 dalys.

<sup>113</sup> Remiantis vienu atsiliepimu, gautu per viešas konsultacijas, vienas iš pagrindinių aspektų, į kuriuos reikia atsižvelgti, yra „veiksmingas vykdymo užtikrinimas ir tikros pasekmės tiems, kas nusprendė nesilaikyti šio reikalavimo <...>. Reikėtų turėti omenyje, visų pirma, kad Sąjungoje įsisteigusios įmonės taip pat atsiduria nepalankioje konkurencinėje padėtyje, palyginti su tokiais reikalavimų nesilaikančiomis įmonėmis, įsisteigusiomis už Sąjungos ribų ir vykdančiomis prekybą su Sąjunga.“ Žr. „ES verslo partneriai“, 2020 m. balandžio 29 d. atsakymas.

<sup>114</sup> Šis klausimas buvo iškeltas keliuose atsiliepimuose, gautuose per viešas konsultacijas, pavyzdžiui, dėl asmens duomenų perdavimo gavėjams už ES ribų, kuriems vis dėlto taikomas BDAR.

<sup>115</sup> Tarybos pozicija ir išvados, 17 punktą; Valdybos nuomonė, p. 5 ir 6. Keliuose atsiliepimuose, gautuose per viešas konsultacijas, be kita ko, iš kelių verslo asociacijų (kaip antai Prancūzijos didelių įmonių asociacijos, „Digital Europe“, „Global Data Alliance“/BSA, Kompiuterių ir ryšių

paprasciausias ir ekonomiškai efektyviausias sprendimas duomenims perduoti, nes jie prilyginami duomenų perdavimui ES viduje, taip užtikrinant saugų ir laisvą asmens duomenų srautą nenustatant papildomų sąlygų ar nereikalaujant leidimo. Taigi pasitelkiant sprendimus dėl tinkamumo ES veiklos vykdytojams atsiveria komerciniai kanalai ir sudaromos palankesnės sąlygos valdžios institucijoms bendradarbiauti, kartu suteikiant privilegijuotą prieigą prie ES bendrosios rinkos. Remiantis 1995 m. direktyvoje įtvirtinta praktika, pagal BDAR aiškiai leidžiama nustatyti tam tikros trečiosios šalies teritorijos arba konkretaus sektoriaus ar pramonės trečiojoje šalyje tinkamumą (vadinamasis dalinis tinkamumas).

BDAR grindžiamas ankstesnių metų patirtimi ir Teisingumo Teismo pateiktais išaiškinimais; jame pateikiamas išsamus elementų, į kuriuos Komisija turi atsižvelgti atlikdama vertinimą, katalogas. Pagal tinkamumo standartą reikalaujama tokio apsaugos lygio, kurį būtų galima palyginti su ES užtikrinamu lygiu (arba kuris būtų jam iš esmės lygiavertis)<sup>116</sup>. Tai reiškia, kad reikia išsamiai įvertinti visą trečiosios šalies sistemą, įskaitant privatumo apsaugos priemonių esmę, jų veiksmingą įgyvendinimą ir vykdymo užtikrinimą bei taisykles dėl galimybės valdžios institucijoms susipažinti su asmens duomenimis, visų pirma, teisėsaugos ir nacionalinio saugumo tikslais<sup>117</sup>.

Tai taip pat pažymima buvusios 29 straipsnio darbo grupės priimtose (ir Valdybos patvirtintose) gairėse, visų pirma, kaip vadinamieji „tinkamumo pavyzdžiai“, toliau patikslinant elementus, į kuriuos Komisija privalo atsižvelgti atlikdama tinkamumo vertinimą, be kita ko, pateikdama esminių garantijų dėl galimybės valdžios institucijoms susipažinti su asmens duomenimis apžvalga<sup>118</sup>. Pastarasis aspektas grindžiamas, visų pirma, Europos Žmogaus Teisių Teismo jurisprudencija. Nors iš esmės lygiavertis standartas nesuponuoja, kad ES taisyklės turi būti visiškai nukopijuojamos (kaip fotokopija), atsižvelgiant į tai, kad skirtingose privatumo sistemose palyginamo apsaugos lygio užtikrinimo priemonės gali skirtis, neretai atspindint skirtingas teises tradicijas, vis dėlto reikalaujamas aukštas apsaugos lygis.

Toks standartas pagrindžiamas tuo, kad sprendimu dėl tinkamumo trečiajai šaliai iš esmės suteikiami bendrosios rinkos pranašumai, susiję su laisvu duomenų judėjimu. Tačiau, tai taip pat reiškia, kad tarp atitinkamoje trečiojoje šalyje užtikrinamo apsaugos lygio ir BDAR kartais bus svarbių skirtumų, kuriuos reikia pašalinti, pavyzdžiui, derantis dėl papildomų apsaugos priemonių. Tokias apsaugos priemones reikėtų vertinti teigiamai, nes jas taikant dar labiau stiprinama asmenų apsauga ES. Kartu Komisija pritaria Valdybai dėl to, kaip svarbu nuolat stebėti jų taikymą praktikoje, įskaitant veiksmingas vykdymo užtikrinimo priemones, kurių imasi trečiosios šalies duomenų apsaugos institucija<sup>119</sup>.

---

pramonės asociacijos (CCIA) ar JAV prekybos rūmų), raginama paspartinti darbą, susijusi su išvadomis dėl tinkamumo, ypač su svarbiais prekybos partneriais.

<sup>116</sup> 2015 m. spalio 6 d. Europos Sąjungos Teisingumo Teismo sprendimas *Maximilian Schrems / Data Protection Commissioner*, C-362/14 (toliau – Sprendimas *Schrems*), 73, 74 ir 96 punktai. Taip pat žr. BDAR 104 konstatuojamąją dalį, kurioje kalbama apie iš esmės lygiavertį standartą.

<sup>117</sup> BDAR 45 straipsnio 2 dalis ir 104 konstatuojamoji dalis. Taip pat žr. Sprendimo *Schrems* 75 ir 91 punktus.

<sup>118</sup> 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](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108)).

<sup>119</sup> Valdybos nuomonė, p. 5 ir 6.

BDAR paaiškinama, kad sprendimai dėl tinkamumo yra „gyvas“ dokumentas, kurį reikėtų nuolat stebėti ir reguliariai peržiūrėti<sup>120</sup>. Laikydamosi šių reikalavimų Komisija reguliariai keičiasi informacija su atitinkamomis institucijomis, kad aktyviai sektų naujus pokyčius. Pavyzdžiui, 2016 m. priėmus sprendimą dėl ES ir JAV privatumo skydo<sup>121</sup> Komisija kartu su Valdybos atstovais parengė tris metines apžvalgas, kad įvertintų visus sistemos veikimo aspektus<sup>122</sup>. Tos apžvalgos buvo parengtos remiantis informacija, gauta bendraujant su JAV institucijomis, ir kitų suinteresuotųjų subjektų, kaip antai ES duomenų apsaugos institucijų, pilietinės visuomenės ir prekybos asociacijų, pateiktais duomenimis. Tai leido pagerinti praktinį įvairių sistemos elementų veikimą. Žvelgiant plačiau, metinėmis apžvalgomis prisidėta prie bendresnio dialogo su JAV administracija dėl privatumo apskritai ir, visų pirma, dėl su nacionaliniu saugumu susijusių apribojimų ir apsaugos priemonių.

Atlikdama pirmąjį BDAR vertinimą Komisija taip pat turi peržiūrėti pagal 1995 m. direktyvą priimtus sprendimus dėl tinkamumo<sup>123</sup>. Komisijos tarnybos palaiko aktyvų dialogą su kiekviena iš 11 susijusių šalių ir teritorijų, kad įvertintų, kaip pasikeitė jų asmens duomenų apsaugos sistemos po sprendimo dėl tinkamumo priėmimo ir ar jos atitinka BDAR įtvirtintą standartą. Poreikis užtikrinti tokių sprendimų tęstinumą, nes jie yra pagrindinė prekybos ir tarptautinio bendradarbiavimo priemonė, yra vienas iš veiksnių, kurie paskatino kelias tokias šalis ir teritorijas modernizuoti ir griežtinti savo privatumo įstatymus. Tokie pokyčiai, žinoma, vertintini palankiai. Su kai kuriomis iš šių šalių ir teritorijų aptariamos papildomos apsaugos priemonės, kuriomis siekiama panaikinti svarbius su duomenų apsauga susijusius skirtumus.

Tačiau, atsižvelgiant į tai, kad sprendime, kuris turi būti paskelbtas liepos 16 d., Teisingumo Teismas gali pateikti paaiškinimų, kurie gali būti svarbūs tam tikriems tinkamumo standarto elementams, Komisija atskirai atsiskaitys dėl minėtų 11

---

<sup>120</sup> Pagal BDAR 45 straipsnio 4 ir 5 dalis Komisija turi nuolat stebėti pokyčius trečiojoje šalyje ir reguliariai, bent kas ketverius metus, peržiūrėti išvadą dėl tinkamumo. Pagal jas Komisija taip pat įgaliojama panaikinti, iš dalies pakeisti ar sustabdyti sprendimą dėl tinkamumo, jeigu nustato, kad atitinkamoje šalyje ar tarptautinėje organizacijoje nebeužtikrinama tinkamo lygio apsauga. Be to, pagal BDAR 97 straipsnio 2 dalies a punktą reikalaujama, kad iki 2020 m. Komisija pateiktų Europos Parlamentui ir Tarybai ataskaitą. Taip pat žr. 2015 m. spalio 6 d. Europos Sąjungos Teisingumo Teismo sprendimo *Maximilian Schrems / Data Protection Commissioner*, C-362/14, 76 punktą.

<sup>121</sup> 2016 m. liepos 12 d. Komisijos įgyvendinimo sprendimas (ES) 2016/1250 dėl ES ir JAV „privatumo skydo“ užtikrinamos apsaugos tinkamumo pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB. Šis sprendimas dėl tinkamumo yra ypatingas atvejis, nes JAV nesant bendrųjų duomenų apsaugos teisės aktų, remiamasi dalyvaujančių įmonių prisiimtais įsipareigojimais (kurių vykdymas užtikrinamas pagal JAV teisę) taikyti šiame susitarime nustatytus duomenų apsaugos standartus. Be to, privatumo skydas grindžiamas konkrečiais JAV vyriausybės pareiškimais ir patikinimais dėl prieigos nacionalinio saugumo tikslais, kuriais grindžiama išvada dėl tinkamumo.

<sup>122</sup> Peržiūra vyko 2017 m. (Komisijos ataskaita Europos Parlamentui ir Tarybai dėl pirmosios metinės ES ir JAV privatumo skydo veikimo peržiūros COM(2017) 611 *final*), 2018 m. (Komisijos ataskaita Europos Parlamentui ir Tarybai dėl antrosios metinės ES ir JAV privatumo skydo veikimo peržiūros, COM(2018) 860 *final*) ir 2019 m. (Komisijos ataskaita Europos Parlamentui ir Tarybai dėl trečiosios metinės ES ir JAV privatumo skydo veikimo peržiūros, COM(2019) 495 *final*).

<sup>123</sup> Tokie galiojantys sprendimai dėl tinkamumo yra susiję su šalimis, kurios yra glaudžiai integruotos su Europos Sąjunga ir jos valstybėmis narėmis (Šveicarija, Andora, Farerų salomis, Gernsiu, Džersiu, Meno Sala), svarbiomis prekybos partnerėmis (pvz., Argentina, Kanada, Izraeliu) ir šalimis, kurios atliko novatorišką vaidmenį rengdamos duomenų apsaugos įstatymus savo regione (Naująja Zelandija, Urugvajumi).

sprendimų dėl tinkamumo vertinimo po to, kai Teisingumo Teismas priims sprendimą toje byloje<sup>124</sup>.

Įgyvendindama 2017 m. komunikate „Keitimasis asmens duomenimis ir jų apsauga globalizuotame pasaulyje“ nustatytą strategiją Komisija taip pat dalyvavo naujuose dialoguose tinkamumo klausimais<sup>125</sup>. Šis darbas, dalyvaujant pagrindiniams ES partneriams, jau davė reikšmingų rezultatų. 2019 m. sausio mėn. Komisija priėmė sprendimą dėl tinkamumo dėl Japonijos, grindžiamą aukšto lygio konvergencija, be kita ko, įgyvendinant konkrečias apsaugos priemones, kaip antai tolesnio duomenų perdavimo srityje, ir sukuriant fizinių asmenų skundų dėl galimybės valdžios institucijoms susipažinti su asmens duomenimis teisėsaugos ir nacionalinio saugumo tikslais tyrimo ir tenkinimo mechanizmą.

Su Japonija suderinta sistema, patvirtinta priėmus pirmąją išvadą dėl tinkamumo pagal BDAR, yra naudingas precedentas būsimiems sprendimams<sup>126</sup>. Šiuo požiūriu svarbu ir tai, kad Japonija savo ruožtu priėmė išvadą dėl tinkamumo dėl ES. Šios išvados dėl abipusio tinkamumo kartu suformuoja didžiausią pasaulyje saugių ir laisvų asmens duomenų srautų erdvę; taip papildomas ES ir Japonijos ekonominės partnerystės susitarimas. Faktiškai susitarimu kasmet remiama maždaug 124 mlrd. EUR vertės prekyba prekėmis ir 42,5 mlrd. EUR vertės prekyba paslaugomis.

Taip pat yra pažengęs Pietų Korėjos tinkamumo vertinimo procesas. Vienas svarbus jo rezultatas – neseniai atlikta Pietų Korėjos teisėkūros reforma, po kurios buvo įsteigta nepriklausoma duomenų apsaugos institucija, kuriai yra suteikti dideli vykdymo užtikrinimo įgaliojimai. Tai rodo, kaip dialogas dėl tinkamumo gali prisidėti prie didesnės ES duomenų apsaugos taisyklių ir užsienio šalies taisyklių konvergencijos.

Komisija visiškai pritaria dėl suinteresuotųjų subjektų raginimo stiprinti dialogą su tam tikromis trečiosiomis šalimis siekiant galbūt priimti naujas išvadas dėl tinkamumo<sup>127</sup>. Ji aktyviai svarsto šią galimybę su kitais svarbiais partneriais Azijoje, Lotynų Amerikoje ir kaimynystės regione remdamasi dabartine tendencija didinti

<sup>124</sup> Sprendimas *Data Protection Commissioner / Facebook Ireland Limited, Maximillian Schrems* (toliau – Sprendimas *Schrems II*), C-311/18, yra susijęs su prašymu priimti prejudicinį sprendimą dėl vadinamųjų standartinių sutarčių sąlygų. Tačiau Teisingumo Teismas taip pat gali išsamiau paaiškinti tam tikrus tinkamumo standarto elementus. Teisingumo Teismo posėdis dėl šios bylos vyko 2019 m. liepos 9 d. ir sprendimas buvo paskelbtas 2020 m. liepos 16 d.

<sup>125</sup> Žr. 109 išnašą. Komisija paaiškino, kad vertinant, su kuriomis trečiosiomis šalimis turėtų būti vykdomas dialogas tinkamumo klausimais, bus atsižvelgiama į šiuos kriterijus: i) ES (faktinių ar galimų) komercinių santykių su trečiąja šalimi mastą, įskaitant laisvosios prekybos susitarimo buvimą ar vykstančias derybas; ii) asmens duomenų srautų iš ES mastą, atsižvelgiant į geografinius ir (arba) kultūrinius ryšius; iii) šalies novatorišką vaidmenį privatumo ir duomenų apsaugos srityje, kad ji galėtų būti pavyzdys kitoms to regiono šalims, ir iv) bendrus politinius santykius su šalimi, visų pirma susijusius su bendrų vertybių ir bendrų tikslų puoselėjimu tarptautiniu lygmeniu.

<sup>126</sup> 2018 m. gruodžio 13 d. Europos Parlamento rezoliucija „Japonijoje nustatytos asmens duomenų apsaugos tinkamumas“ (2018/2979(RSP)), 27 punktas; Valdybos nuomonė, p. 5 ir 6.

<sup>127</sup> Žr. 2017 m. gruodžio 12 d. Europos Parlamento rezoliucijos „Skaitmeninės prekybos strategijos kūrimas“ (2017/2065(INI)) 8 ir 9 punktus; Tarybos pozicijos ir išvadų dėl Bendrojo duomenų apsaugos reglamento (BDAR) taikymo, 2019 m. gruodžio 19 d., (14994/1/19), 17 punktą; Valdybos nuomonė, p. 5 ir 6.

duomenų apsaugos standartų konvergenciją visame pasaulyje. Pavyzdžiui, buvo priimti išsamūs privatumo srities teisės aktai arba teisėkūros procedūra jau yra pažengusi Lotynų Amerikoje (Brazilijoje, Čilėje), daug žadančių pokyčių yra Azijoje (pvz., Indijoje, Indonezijoje, Malaizijoje, Šri Lankoje, Taivane ir Tailande), Afrikoje (pvz., Etiopijoje, Kenijoje) ir Europos rytų ir pietų kaimynystės šalyse (pvz., Gruzijoje, Tunise). Kai įmanoma, Komisija sieks priimti išsamius sprendimus dėl tinkamumo ir dėl privačiojo, ir dėl viešojo sektoriaus<sup>128</sup>.

Be to, BDAR taip pat numatyta galimybė Komisijai priimti išvadas dėl tarptautinių organizacijų tinkamumo. Šiuo metu, kai tam tikros tarptautinės organizacijos modernizuoja savo duomenų apsaugos režimus įgyvendindamos išsamias taisykles ir mechanizmus, kuriais užtikrinama nepriklausoma priežiūra ir teisių gynimas, galima pirmą kartą apsvarstyti šią galimybę.

Tinkamumas taip pat atlieka svarbų vaidmenį santykiuose su Jungtine Karalyste po „Brexit’o“, jeigu tenkinamos taikytinos sąlygos. Tai svarbus veiksnys prekybai, įskaitant skaitmeninę prekybą, ir būtinoji sąlyga siekiant užtikrinti glaudų plataus užmojo bendradarbiavimą teisėsaugos ir saugumo srityje<sup>129</sup>. Be to, atsižvelgiant į duomenų srautų su Jungtine Karalyste mastą ir jos artumą ES rinkai, didelė duomenų apsaugos taisyklių konvergencija abiejose Lamanšo sąsiaurio pusėse yra svarbus elementas norint užtikrinti vienodas sąlygas. Remdamasi politine deklaracija dėl būsimų ES ir Jungtinės Karalystės santykių Komisija šiuo metu atlieka tinkamumo vertinimą ir pagal BDAR, ir pagal Teisėsaugos direktyvą<sup>130</sup>. Atsižvelgiant į autonominių ir vienašalį tinkamumo vertinimo pobūdį šios derybos vyksta atskirai nuo derybų dėl susitarimo dėl būsimų ES ir Jungtinės Karalystės santykių.

Galiausiai Komisija palankiai vertina tai, kad kitose šalyse yra diegiami duomenų perdavimo mechanizmai, panašūs į išvadą dėl tinkamumo. Taip jos dažnai pripažįsta ES ir šalis, dėl kurių Komisija yra priėmusi sprendimą dėl tinkamumo, saugiomis duomenų perdavimo paskirties šalimis<sup>131</sup>. Dėl didėjančio šalių, dėl kurių ES priima sprendimus dėl tinkamumo, skaičiaus ir tokios pripažinimo formos, kurių taiko kitos šalys, gali būti sukurtas šalių tinklas, kuriame duomenys gali judėti laisvai ir saugiai. Komisija mano, kad tai palankiai vertintinas pokytis, dėl kurio sprendimų dėl trečiųjų šalių tinkamumo nauda dar didės ir prisidės prie pasaulinės konvergencijos. Užtikrinant tokio pobūdžio sinergiją taip pat galima naudingai prisidėti prie saugių ir laisvų duomenų srautų sistemų plėtros, pavyzdžiui, įgyvendinant laisvo duomenų srauto užtikrinant pasitikėjimą iniciatyvą (žr. toliau).

---

<sup>128</sup> Kaip taip pat prašė Taryba, žr. Tarybos nuomonės ir išvadų dėl Bendrojo duomenų apsaugos reglamento (BDAR) taikymo, 2019 m. gruodžio 19 d. (14994/1/19), 17 ir 40 punktus. Tačiau tam reikia, kad būtų tenkinamos išvados dėl tinkamumo sąlygos, susijusios su duomenų perdavimu valdžios institucijoms, įskaitant nepriklausomą priežiūrą.

<sup>129</sup> Žr. derybinių nurodymų, pateiktų Tarybos sprendimo, kuriuo suteikiami įgaliojimai pradėti derybas dėl naujos partnerystės su Jungtine Didžiosios Britanijos ir Šiaurės Airijos Karalyste (ST 5870/20 ADD 1 REV 3), priede, 13 ir 118 punktus.

<sup>130</sup> Žr. peržiūrėtą politinės deklaracijos, kuria nustatoma būsimų Europos Sąjungos ir Jungtinės Karalystės santykių programa, tekstą, dėl kurio derybininkų lygmeniu buvo susitarta 2019 m. spalio 17 d., 8–10 punktus (paskelbta adresu [https://ec.europa.eu/commission/sites/beta-political/files/revised\\_political\\_declaration.pdf](https://ec.europa.eu/commission/sites/beta-political/files/revised_political_declaration.pdf)).

<sup>131</sup> Pavyzdžiui, Argentina, Kolumbija, Izraelis, Šveicarija ar Urugvajus.



### *Tinkamos apsaugos priemonės*

Be išsamaus išvados dėl tinkamumo sprendimo, BDAR yra numatyta įvairių kitų duomenų perdavimo priemonių. Apie tokio priemonių rinkinio lankstumą byloja BDAR 46 straipsnis, kuriuo reglamentuojamas duomenų perdavimas taikant tinkamas apsaugos priemones, įskaitant vykdytinas duomenų subjektų teises ir veiksmingas teisių gynimo priemones. Siekiant užtikrinti tinkamas apsaugos priemones galima naudoti įvairias priemones, kad būtų patenkinti ir komercinių veiklos vykdytojų, ir viešųjų įstaigų poreikiai.

- Standartinės sutarčių sąlygos (SSS)

Pirmoji tokių priemonių grupė yra susijusi su sutartinėmis priemonėmis, kurios gali būti specialiai parengtos *ad hoc* duomenų apsaugos sąlygos, dėl kurių susitaria ES duomenų eksportuotojas ir kompetentingos duomenų apsaugos institucijos įgaliojtas duomenų importuotojas už ES ribų (BDAR 46 straipsnio 3 dalies a punktas), arba standartinės sąlygos, kurias iš anksto patvirtina Komisija (BDAR 46 straipsnio 2 dalies c ir d punktai<sup>132</sup>). Svarbiausia iš šių priemonių yra vadinamosios standartinės sutarčių sąlygos (SSS), t. y. standartinės duomenų apsaugos sąlygos, kurias duomenų eksportuotojas ir duomenų importuotojas gali savanoriškai įtraukti į savo sutartis (pvz., paslaugų sutartį, pagal kurią reikia perduoti asmens duomenis) ir kuriose nustatomi su tinkamomis apsaugos priemonėmis susiję reikalavimai.

SSS yra labiausiai naudojamas duomenų perdavimo mechanizmas<sup>133</sup>. Tūkstančiai ES įmonių naudoja SSS teikdamos įvairias paslaugas savo klientams, tiekėjams, partneriams ir darbuotojams, įskaitant ekonomikos veikimui būtinas paslaugas. Toks platus jų naudojimas reiškia, kad jos yra labai naudingos įmonėms dedant pastangas laikytis reikalavimų ir ypač naudingos įmonėms, neturinčioms išteklių derėtis dėl individualių sutarčių su kiekvienu iš savo prekybos partnerių. Kadangi SSS yra standartinės ir iš anksto patvirtintos, jos yra lengvai įgyvendinama priemonė įmonėms įvykdyti duomenų apsaugos reikalavimus perduodant duomenis.

Galiojantys SSS rinkiniai<sup>134</sup> buvo priimti ir patvirtinti remiantis 1995 m. direktyva. Šios SSS galioja, kol prireikus nebus iš dalies pakeistos, pakeistos ar panaikintos Komisijos sprendimu (BDAR 46 straipsnio 5 dalis). Pagal BDAR išplečiamos galimybės naudoti SSS ir ES viduje, ir tarptautiniam duomenų perdavimui. Komisija

---

<sup>132</sup> Standartinės sutarčių sąlygas (SSS) dėl tarptautinio duomenų perdavimo turi visuomet tvirtinti Komisija, o parengti jas gali arba pati Komisija, arba nacionalinė DAI. Visos galiojančios SSS priklauso pirmajai kategorijai.

<sup>133</sup> Remiantis 2019 m. IAPP ir EY metine privatumo valdymo ataskaita, „populiariausios iš šių [duomenų perdavimo] priemonių jau daugelį metų yra standartinės sutarčių sąlygos: 88 proc. šių metų apklausos respondentų tvirtino, kad SSS yra pagrindinis eksteritorialių duomenų perdavimo operacijų metodas; antroje vietoje – ES ir JAV privatumo skydo susitarimas (60 proc.). Tarp respondentų, perduodančių duomenis iš ES į Jungtinę Karalystę (52 proc.), 91 proc. informavo, kad laikydamiesi duomenų perdavimo reikalavimų ketina naudoti SSS ir po „Brexit’o““.

<sup>134</sup> Šiuo metu yra trys Komisijos patvirtinti standartinės sutarčių sąlygų rinkiniai, skirti perduoti asmens duomenis į trečiąsias šalis: du – skirti perduoti duomenis iš EEE duomenų valdytojo EEE nepriklausančios šalies duomenų valdytojui ir vienas – skirtas perduoti duomenis iš EEE duomenų valdytojo EEE nepriklausančios šalies duomenų tvarkytojui. Jie buvo iš dalies pakeisti 2016 m. Teisingumo Teismui priėmus Sprendimą *Schrems I* (C-362/14), siekiant panaikinti bet kokius apribojimus kompetentingoms priežiūros institucijoms naudotis savo duomenų perdavimo priežiūros įgaliojimais. Žr. [https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en).

dirba kartu su suinteresuotaisiais subjektais, kad pasinaudotų šiomis galimybėmis ir atnaujintų galiojančias sąlygas<sup>135</sup>. Siekdama užtikrinti, kad būsimos SSS būtų parengtos tinkamai, Komisija renka grįžtamąją informaciją apie suinteresuotųjų subjektų patirtį naudojant SSS įvairių suinteresuotųjų subjektų grupėje BDAR klausimais ir 2019 m. rugsėjo mėn. surengtame specialiaame seminare, taip pat palaikydama ryšius su daugeliu SSS naudojančių įmonių ir pilietinės visuomenės organizacijų. Valdyba taip pat atnaujina keletą gairių, kurios galėtų būti svarbios peržiūrint SSS, pavyzdžiui, dėl sąvokų „duomenų valdytojas“ ir „duomenų tvarkytojas“.

Remdamosi gauta grįžtamąja informacija Komisijos tarnybos šiuo metu dirba prie SSS peržiūros. Atsižvelgiant į tai, nustatytos kelios tobulintinos sritys, visų pirma susijusios su šiais aspektais:

1. atnaujinti SSS atsižvelgiant į naujus BDAR nustatytus reikalavimus, kaip antai susijusius su duomenų valdytojo ir duomenų tvarkytojo santykiais pagal BDAR 28 straipsnį (visų pirma, duomenų tvarkytojo prievolėmis), duomenų importuotojo skaidrumo prievolės (susijusias su būtina informacija, kurią reikia teikti duomenų subjektui) ir kt.;
2. apsvarstyti kelis duomenų perdavimo scenarijus, kuriems nėra taikomos galiojančios SSS, kaip antai duomenų perdavimo iš ES duomenų tvarkytojo ES nepriklausančios šalies (pagalbiniam) duomenų tvarkytojui, bet taip pat atvejus, kai, pavyzdžiui, duomenų valdytojas yra už ES ribų<sup>136</sup>;
3. geriau perteikti duomenų tvarkymo operacijų realijas šiuolaikinėje skaitmeninėje ekonomikoje, kurioje tokiose operacijose dažnai dalyvauja keli duomenų importuotojai ir eksportuotojai, susidaro ilgos ir neretai sudėtingos duomenų tvarkymo grandinės, kuriami verslo ryšiai ir t. t. Siekiant atsižvelgti į tokias situacijas svarstomi tokie sprendimai, kaip galimybė daugeliui šalių pasirašyti SSS arba naujoms šalims prisijungti per visą sutarties galiojimo laikotarpį.

Sprendama šiuos klausimus Komisija taip pat svarsto būdus padaryti esamą SSS struktūrą patogesnę naudotojams, pavyzdžiui, pakeisdama daugelį SSS rinkinių vienu išsamiu dokumentu. Sunkumų kelia tai, kad reikia užtikrinti tinkamą pusiausvyrą, viena vertus, tarp poreikio viską išdėstyti aiškiai iki tam tikro laipsnio standartizuojant ir, kita vertus, būtino lankstumo, kuris leistų keliems veiklos vykdytojams naudoti sąlygas taikant skirtingus reikalavimus, skirtingomis aplinkybėmis ir dėl skirtingų duomenų perdavimo operacijų.

Dar vienas svarbus aspektas, kurį reikia turėti omenyje, – galimas poreikis, atsižvelgiant į Teisingumo Teisme nagrinėjamą bylą<sup>137</sup>, toliau patikslinti apsaugos

<sup>135</sup> Taip pat žr. Valdybos nuomonę, p. 6 ir 7. Taryba taip pat paragino Komisiją „artimiausiu metu peržiūrėti [SSS], kad būtų atsižvelgta į duomenų valdytojų ir duomenų tvarkytojų poreikius“. Žr. Tarybos poziciją ir išvadas.

<sup>136</sup> Keliuose atsakymuose, pateiktuose per viešas konsultacijas, buvo komentarų dėl šio paskutinio scenarijaus, daugiausia nuogąstaujant, kad, jeigu iš ES duomenų tvarkytojų būtų reikalaujama užtikrinti tinkamas apsaugos priemonės santykiuose su ES nepriklausančių šalių duomenų tvarkytojais, jie atsidurtų nepalankioje konkurencinėje padėtyje, palyginti su panašias paslaugas siūlančiais užsienio duomenų tvarkytojais.

<sup>137</sup> Žr. Sprendimą *Schrems II*.

priemonės dėl galimybės užsienio valdžios institucijoms susipažinti su duomenimis, perduodamais remiantis SSS, visų pirma nacionalinio saugumo tikslais. Tam, be kita ko, gali būti reikalaujama, kad duomenų importuotojas arba duomenų eksportuotojai ar jie abu imtųsi veiksmų ir patikslintų duomenų apsaugos institucijų vaidmenį šiame kontekste. Nors SSS peržiūra jau yra gerokai pažengusi, reikės laukti Teisingumo Teismo sprendimo, kad peržiūrėtose sąlygose būtų galima nustatyti galimą papildomą reikalavimą; tik po to sprendimo dėl naujo SSS rinkinio projektą galima teikti Valdybai, kad ši parengtų nuomonę, ir siūlyti ją tvirtinti pagal „komitologijos procedūrą“<sup>138</sup>.

Komisija taip pat palaiko ryšį su tarptautiniais partneriais, kuriančiais panašias priemones<sup>139</sup>. Šis dialogas, kurio metu galima pasikeisti patirtimi ir geriausia patirtimi, galėtų būti labai naudingas siekiant toliau didinti konvergenciją vietoje ir taip sudaryti palankesnes sąlygas įmonėms, vykdančioms veiklą įvairiuose pasaulio regionuose, laikytis tarpvalstybinio duomenų perdavimo taisyklių.

- Įmonei privalomos taisyklės (IPT)

Dar viena svarbi priemonė yra vadinamosios įmonei privalomos taisyklės (IPT). Tai teisiškai privaloma politika ir susitarimai, taikomi įmonių grupės nariams, įskaitant jų darbuotojus (BDAR 46 straipsnio 2 dalies b punktas ir 47 straipsnis). Taikant IPT galima užtikrinti laisvą asmens duomenų judėjimą tarp įvairių grupės narių visame pasaulyje ir nereikia sudaryti sutarčių tarp visų subjektų; kartu užtikrinama, kad visoje grupėje būtų laikomasi vienodai aukšto asmens duomenų apsaugos lygio. Tai ypač geras sprendimas sudėtingoms ir didelėms įmonių grupėms ir būdas įmonėms, kurios keičiasi duomenimis keliose jurisdikcijose, glaudžiai bendradarbiauti. Priešingai nei pagal 1995 m. direktyvą, pagal BDAR IPT gali naudoti jungtinę ekonominę veiklą vykdančių įmonių, kurios vis dėlto nepriklauso tai pačiai įmonių grupei, grupei.

Procedūriniu požiūriu IPT turi patvirtinti kompetentingos duomenų apsaugos institucijos vadovaudamosi neprivaloma Valdybos nuomone<sup>140</sup>. Siekdama nukreipti šį procesą tinkama linkme Valdyba peržiūrėjo IPT pavyzdžius (nustatė esminius standartus) duomenų valdytojams<sup>141</sup> ir duomenų tvarkytojams<sup>142</sup> remdamasi BDAR ir toliau atnaujina šiuos dokumentus vadovaudamasi priežiūros institucijų sukaupta praktine patirtimi. Ji taip pat priėmė įvairias gaires, kad padėtų pareiškėjams ir supaprastintų su IPT susijusį paraiškų teikimo ir patvirtinimo procesą<sup>143</sup>. Valdybos

---

<sup>138</sup> Pagal BDAR 46 straipsnio 2 dalies c punktą standartinės sutarčių sąlygos turi būti tvirtinamos vykdančią nagrinėjimo procedūrą, numatytą 2011 m. vasario 16 d. Europos Parlamento ir Tarybos reglamento (ES) Nr. 182/2011, kuriuo nustatomos valstybių narių vykdomos Komisijos naudojimosi įgyvendinimo įgaliojimais kontrolės mechanizmų taisyklės ir bendrieji principai (OL L 55, 2011 2 28, p. 13–18), 5 straipsnyje. Tam, visų pirma, reikalingas teigiamas komiteto, kurį sudaro valstybių narių atstovai, sprendimas.

<sup>139</sup> Tai, pavyzdžiui, darbas, kurį šiuo metu vykdo ASEAN valstybės narės kurdamos ASEAN tipines sutarčių sąlygas. Žr. ASEAN, „Pagrindiniai ASEAN tarpvalstybinių duomenų srautų mechanizmo metodai“ (paskelbta adresu <https://asean.org/storage/2012/05/Key-Approaches-for-ASEAN-Cross-Border-Data-Flows-Mechanism.pdf>).

<sup>140</sup> Iki šiol paskelbtų EDAV nuomonių apžvalgą žr. [https://edpb.europa.eu/our-work-tools/consistency-findings/opinions\\_lt](https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_lt).

<sup>141</sup> [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=614109](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109).

<sup>142</sup> [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=614110](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110).

<sup>143</sup> Šie dokumentai buvo patvirtinti (buvusios 29 straipsnio darbo grupės) po BDAR įsigaliojimo, bet iki pereinamojo laikotarpio pabaigos. Žr. WP263 (<https://ec.europa.eu/newsroom/article29/item->



duomenimis, daugiau nei 40 IPT šiuo metu ruošiami tvirtinti; tikimasi, kad pusė jų bus patvirtinta iki 2020 m. pabaigos<sup>144</sup>. Svarbu, kad duomenų apsaugos institucijos ir toliau dirbtų siekdamos dar labiau supaprastinti patvirtinimo procesą, nes suinteresuotieji subjektai dažnai mini tokių procedūrų trukmę kaip praktinę kliūtį naudoti IPT plačiau.

Galiausiai, kalbant konkrečiai apie Jungtinės Karalystės duomenų apsaugos institucijos Informacijos komisaro biuro patvirtintas IPT, įmonės galės ir toliau jas naudoti kaip galiojančią duomenų perdavimo mechanizmą pagal BDAR po pereinamojo laikotarpio pabaigos remdamosi ES ir Jungtinės Karalystės susitarimu dėl išstojimo, bet tik jeigu jos yra iš dalies pakeistos taip, kad visi ryšiai su Jungtinės Karalystės teisine tvarka būtų pakeisti tinkamomis nuorodomis į įmones ir kompetentingas institucijas ES. Patvirtinti bet kokias naujas IPT reikėtų prašyti vieną iš ES priežiūros institucijų.

- **Sertifikavimo mechanizmai ir elgesio kodeksai**

Be jau esamų duomenų perdavimo priemonių taikymo srities modernizavimo ir išplėtimo, BDAR taip pat diegiamos naujos priemonės, taip išplečiant tarptautinio duomenų perdavimo galimybes. Tai tam tikromis sąlygomis apima ir patvirtintų elgesio kodeksų ir sertifikavimo mechanizmų (kaip antai privatumo apsaugos ženklų ar žymenų) naudojimą siekiant užtikrinti tinkamas apsaugos priemones. Tai iš apačios į viršų taikomos priemonės, kurias naudojant galima kurti pritaikytus sprendimus kaip bendrąjį atskaitomybės mechanizmą (žr. BDAR 40–42 straipsnius) ir konkrečiai tarptautiniam duomenų perdavimui, pavyzdžiui, atsižvelgiant į konkrečias tam tikro sektoriaus ar pramonės arba tam tikrų duomenų srautų savybes ir poreikius. Elgesio kodeksai padeda suderinti įsipareigojimus su rizika, mažosioms ir vidutinėms įmonėms ir gali būti labai naudinga ir ekonomiškai efektyvi priemonė padėti mažosioms ir vidutinėms įmonėms vykdyti įsipareigojimus pagal BDAR.

Kalbant apie sertifikavimo mechanizmus, nors Valdyba priėmė gaires siekdama paskatinti jų naudojimą ES, darbas rengiant sertifikavimo mechanizmų patvirtinimo kriterijus tebevyksta. Tas pats pasakytina ir apie elgesio kodeksus, dėl kurių Valdyba šiuo metu rengia gaires, kad jie būtų naudojami kaip duomenų perdavimo priemonė.

Atsižvelgdama į tai, kaip svarbu veiklos vykdytojams suteikti daug įvairių jų poreikiams pritaikytų duomenų perdavimo priemonių, ir, visų pirma, sertifikavimo mechanizmų potencialą sudaryti palankesnes sąlygas duomenims perduoti, kartu užtikrinant aukštą duomenų apsaugos lygį, Komisija ragina Valdybą kuo greičiau užbaigti rengti šios srities gaires. Tai pasakytina ir apie esminius (kriterijai), ir apie procedūrinius aspektus (patvirtinimas, stebėseną ir kt.). Suinteresuotieji subjektai išreiškė didelį susidomėjimą dėl tokių duomenų perdavimo mechanizmų ir turėtų turėti galimybę išnaudoti visą BDAR numatytą priemonių rinkinį. Valdybos gairės taip pat padėtų populiarinti ES duomenų apsaugos modelį visame pasaulyje ir skatintų konvergenciją, nes pagal kitas privatumo apsaugos sistemas naudojamos panašios priemonės.

---

[detail.cfm?item\\_id=623056](https://detail.cfm?item_id=623056));

([https://edpb.europa.eu/sites/edpb/files/files/file2/wp264\\_art29\\_wp\\_bcr-c\\_application\\_form.pdf](https://edpb.europa.eu/sites/edpb/files/files/file2/wp264_art29_wp_bcr-c_application_form.pdf));

WP265 ([https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=623848](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623848)).

<sup>144</sup> Valdybos nuomonė, p. 7.

Iš vykdomo standartizavimo darbo privatumo srityje galima pasimokyti ir Europos, ir tarptautiniu lygmeniu. Vienas įdomus pavyzdys – neseniai paskelbtas tarptautinis standartas ISO 27701<sup>145</sup>, kurio tikslas – padėti įmonėms vykdyti privatumo reikalavimus ir valdyti su asmens duomenų tvarkymu susijusią riziką pasitelkiant „privatumo informacijos valdymo sistemas“. Nors sertifikavimas pagal standartą savaime nėra BDAR 42 ir 43 straipsnių reikalavimų vykdymas, taikant privatumo informacijos valdymo sistemas gali pavykti geriau užtikrinti atskaitomybę, be kita ko, perduodant duomenis tarptautiniu lygmeniu.

- Tarptautiniai susitarimai ir administraciniai susitarimai

Pagal BDAR taip pat galima užtikrinti tinkamas duomenų perdavimo tarp valdžios institucijų ar įstaigų apsaugos priemones naudojant tarptautinius susitarimus (46 straipsnio 2 dalies a punktas) ar administracinius susitarimus (46 straipsnio 3 dalies b punktas). Nors abi priemonės turi užtikrinti tą patį apsaugos su apsaugos priemonėmis susijusį rezultatą, įskaitant vykdytinas duomenų subjekto teises ir veiksmingas teisių gynimo priemones, jos skiriasi dėl savo teisinio pobūdžio ir priėmimo procedūros.

Priešingai nei tarptautinių susitarimų atveju, kai kyla pagal tarptautinę teisę privalomų įsipareigojimų, administraciniai susitarimai (pvz., susitarimo memorandumai) paprastai nėra privalomi, tad juos turi iš anksto patvirtinti kompetentinga duomenų apsaugos institucija (taip pat žr. BDAR 108 konstatuojamąją dalį). Vienas iš pirmųjų pavyzdžių yra administracinis susitarimas dėl asmens duomenų perdavimo tarp EEE ir EEE nepriklausančių šalių finansų priežiūros institucijų, bendradarbiaujančių Tarptautinėje vertybinių popierių komisijų organizacijoje (IOSCO), dėl kurio Valdyba buvo parengusi nuomonę<sup>146</sup> 2019 m. pradžioje. Per tą laiką Valdyba patikslino savo aiškinimą, kas yra minimaliosios apsaugos priemonės, kurios turi būti užtikrinamos tarptautiniuose (bendradarbiavimo) susitarimuose ir administraciniuose susitarimuose tarp valdžios institucijų ar įstaigų (įskaitant tarptautines organizacijas), kad būtų tenkinami BDAR 46 straipsnio reikalavimai. 2020 m. sausio 18 d. ji priėmė gairių projektą<sup>147</sup>, taip patenkindama valstybių narių prašymą pateikti papildomą paaiškinimą ir gaires, ką galima laikyti tinkamomis apsaugos priemonėmis perduodant duomenis tarp valdžios institucijų<sup>148</sup>. Valdyba primygtinai rekomenduoja valdžios institucijoms remtis šiomis gairėmis kaip pagrindu derybose su trečiosiomis šalimis<sup>149</sup>.

---

<sup>145</sup> Konkrečių šio ISO standarto reikalavimų sąrašas yra paskelbtas adresu <https://www.iso.org/standard/71670.html>.

<sup>146</sup> EDAV, Nuomonė Nr. 4/2019 dėl Administracinio susitarimo dėl Europos ekonominės erdvės (EEE) finansų priežiūros institucijų ne EEE finansų priežiūros institucijoms perduodamų asmens duomenų projekto, 2019 m. vasario 12 d.

<sup>147</sup> EDAV, Gairės Nr. 2/2020 dėl Reglamento 2016/679 dėl asmens duomenų perdavimo tarp EEE ir EEE nepriklausančių šalių valdžios institucijų ir įstaigų 46 straipsnio 2 dalies a punkto ir 46 straipsnio 3 dalies b punkto (projektas paskelbtas adresu [https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b\\_en](https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_en) ). EDAV nuomone, „[k]ompetentinga [priežiūros institucija] atlikdama vertinimą remsis šiose gairėse pateiktomis bendrosiomis rekomendacijomis, bet taip pat gali paprašyti suteikti daugiau garantijų priklausomai nuo konkretaus atvejo“. EDAV pateikė šį gairių projektą viešoms konsultacijoms, kurios pasibaigė 2020 m. gegužės 18 d.

<sup>148</sup> Tarybos pozicija ir išvados, 20 punktas.

<sup>149</sup> EDAV taip pat patikslina, kad valdžios institucijos „ir toliau gali naudotis kitomis svarbiomis priemonėmis, kuriomis užtikrinamos tinkamos apsaugos priemonės pagal BDAR 46 straipsnį“.

Gairėmis patvirtinamas tokių priemonių rengimo lankstumas, be kita ko, dėl tokių svarbių aspektų, kaip priežiūra<sup>150</sup> ir teisių gynimo priemonės<sup>151</sup>. Tai turėtų leisti valdžios institucijoms įveikti sunkumus, pavyzdžiui, užtikrinant vykdytiną duomenų subjektų teises neprivalomais susitarimais. Svarbus tokių susitarimų elementas yra nuolatinė kompetentingos duomenų apsaugos institucijos vykdoma stebėseną, remiantis informacijos ir įrašų saugojimo reikalavimais, ir prireikus duomenų srautų sustabdymas, jeigu praktiškai nebepavyksta užtikrinti tinkamų apsaugos priemonių.

#### *Nukrypti leidžiančios nuostatos*

Galiausiai BDAR paaiškinamas vadinamųjų nukrypti leidžiančių nuostatų taikymas. Tai konkretūs teisės aktais pripažįstami duomenų perdavimo pagrindai (pvz., aiškus sutikimas<sup>152</sup>, sutarties vykdymas arba svarbios viešojo intereso priežastys), kuriais subjektai gali remtis nesant kitų duomenų perdavimo priemonių ir tam tikromis sąlygomis.

Siekdama patikslinti tokių teisės aktuose įtvirtintų pagrindų naudojimą Valdyba paskelbė konkrečias gaires<sup>153</sup> ir išaiškino 49 straipsnį keliais atvejais, susijusiais su konkrečiais duomenų perdavimo scenarijais<sup>154</sup>. Valdyba mano, kad nukrypti leidžiančias nuostatas dėl jų išskirtinio pobūdžio reikia aiškinti siaurai, kiekvienu konkrečiu atveju. Nepaisant griežto aiškinimo, tokie pagrindai aprėpia daug įvairių duomenų perdavimo scenarijų. Tai, visų pirma, duomenų perdavimas, kurį vykdo ir valdžios institucijos, ir privatieji subjektai, kai tai būtina dėl „svarbių viešojo intereso priežasčių“, pavyzdžiui, tarp konkurencijos, finansų, mokesčių ar muitinės institucijų ir socialinės apsaugos ar visuomenės sveikatos srityse kompetentingų tarnybų

---

Kalbant apie priemonės pasirinkimą, EDAV pabrėžia, kad „[r]eikėtų kruopščiai įvertinti, ar naudoti teisiškai neprivalomus administracinius susitarimus apsaugos priemonėms užtikrinti viešajame sektoriuje ar ne, atsižvelgiant į duomenų tvarkymo tikslą ir tvarkomų duomenų pobūdį. Jeigu EEE asmenų duomenų apsaugos teisės ir teisių gynimo priemonės nėra įtvirtintos trečiosios šalies nacionalinėje teisėje, pirmenybę reikėtų teikti teisiškai privalomo susitarimo sudarymui. Neatsižvelgiant į priimtą priemonės rūšį, įdiegtos priemonės turi būti veiksmingos užtikrinant tinkamą įgyvendinimą, vykdymo užtikrinimą ir priežiūrą“ (67 punktas).

<sup>150</sup> Tai gali būti, pavyzdžiui, vidaus patikrinimų derinimas su įsipareigojimais informuoti kitą šalį apie bet kokį nepriklausomos priežiūros reikalavimų nesilaikymo atvejį naudojant išorės ar bent funkciniu požiūriu autonominius mechanizmus ir galimybe duomenis perduodančiai viešajai įstaigai sustabdyti ar nutraukti duomenų perdavimą.

<sup>151</sup> Tai gali būti, pavyzdžiui, iš dalies teisminiai, privalomi mechanizmai (pvz., arbitražas) ar alternatyvaus ginčų sprendimo mechanizmai, kartu užtikrinant galimybę duomenis perduodančiai valdžios institucijai sustabdyti ar nutraukti asmens duomenų perdavimą, jeigu šalims nepavyksta taikiai išspręsti ginčo, ir duomenis gaunančios viešosios įstaigos įsipareigojimas asmens duomenis grąžinti ar ištrinti. Renkantis alternatyvius teisių gynimo mechanizmus pasitelkiant privalomas ir vykdytiną priemonę, nes neįmanoma užtikrinti veiksmingų teisių gynimo priemonių, EDAV rekomenduoja siekti kompetentingos priežiūros institucijos patarimo prieš sudarant susitarimą.

<sup>152</sup> Tai pakeitimas, palyginti su Direktyva 95/46, pagal kurią buvo reikalaujamas tik „nedviprasmiškas“ sutikimas. Be to, taikomi bendrieji sutikimo reikalavimai pagal BDAR 4 straipsnio 11 punktą.

<sup>153</sup> EDAV, Gairės 2/2018 dėl leidžiančių nukrypti nuostatų pagal Reglamento 2016/679 49 straipsnį, 2018 m. gegužės 25 d. (paskelbtos adresu [https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_guidelines\\_2\\_2018\\_derogations\\_lt.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_lt.pdf)).

<sup>154</sup> Tai, pavyzdžiui, tarptautinis sveikatos duomenų perdavimas mokslinių tyrimų tikslais įvykus COVID-19 protrūkiui. Žr. EDAV gaires 03/2020 dėl sveikatos duomenų tvarkymo su COVID-19 protrūkiu susijusių mokslinių tyrimų tikslais, 2020 m. balandžio 21 d. (paskelbtos adresu [https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_guidelines\\_202003\\_healthdatascientificresearchcovid19\\_lt.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_lt.pdf)).

(pavyzdžiui, kai svarbu išaiškinti sąlytį turėjusius asmenis užkrečiamųjų ligų atveju arba siekiant panaikinti dopingą sporte)<sup>155</sup>. Dar vienas sritis – tarpvalstybinis bendradarbiavimas baudžiamosios teisės vykdymo tikslais, visų pirma sunkių nusikaltimų atveju<sup>156</sup>.

Valdyba patikslino, kad, nors atitinkamas viešasis interesas turi būti pripažintas ES arba valstybės narės teisėje, jį taip pat galima nustatyti taip: „Vertinant, ar esama viešojo intereso, kuriuo remiantis būtų galima taikyti 49 straipsnio 1 dalies d punktą, vienas iš rodiklių gali būti sudarytas tarptautinis susitarimas arba konvencija, kuriame (-ioje) pripažįstamas tam tikras tikslas ir numatoma palaikyti tarptautinį bendradarbiavimą siekiant to tikslo, jeigu ES arba valstybės narės yra to susitarimo arba konvencijos šalys“<sup>157</sup>.

*Užsienio teismų ar institucijų sprendimai: nėra pagrindas perduoti duomenis*

Be teigiamo duomenų perdavimo pagrindų nustatymo, BDAR V skyriaus 48 straipsnyje taip pat patikslinama, kad ES nepriklausančių šalių teismų nurodymai ir administracinių institucijų sprendimai *savime* nėra tokie pagrindai, nebent jie būtų pripažinti ar taptų vykdytini pagal tarptautinį susitarimą (pvz., pagal savitarpio teisinės pagalbos sutartį). Bet koks prašymą gavusio ES subjekto duomenų atskleidimas užsienio teisimui ar institucijai atsiliepiant į tokį nurodymą ar sprendimą laikomas tarptautiniu duomenų perdavimu, kuris turi būti grindžiamas viena iš minėtų duomenų perdavimo priemonių<sup>158</sup>.

BDAR nėra „blokavimo statusas“ ir pagal jį tam tikromis sąlygomis duomenis leidžiama perduoti atsiliepiant į atitinkamą trečiosios šalies teisėsaugos institucijų prašymą. Svarbu tai, kad tai būtų nustatyta ES teisėje ir būtent pagal ją būtų sprendžiama, kurių apsaugos priemonių pagrindu gali vykti toks duomenų perdavimas.

Komisija išaiškino BDAR 48 straipsnio taikymą, įskaitant galimą rėmimąsi nukrypti

<sup>155</sup> Žr. 112 konstatuojamąją dalį.

<sup>156</sup> Žr. Europos Komisijos informaciją Europos Sąjungos kaip *Amicus Curiae* vardu neremiant jokios šalies byloje *JAV / Microsoft*, p. 15: „Apskritai Sąjungos ir valstybių narių teisėje pripažįstama, kaip svarbu kovoti su sunkiais nusikaltimais (ir kokia svarbi yra baudžiamoji teisėsauga ir tarptautinis bendradarbiavimas šioje srityje), kaip bendrojo intereso tikslas. <...> SESV 83 straipsnyje yra nustatytos kelios ypač sunkių nusikaltimų, turinčių tarptautinį aspektą, sritys, kaip antai neteisėta prekyba narkotikais.“ (paskelbta adresu [https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791\\_17-2%20ac%20European%20Commission%20for%20filing.pdf](https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf)).

<sup>157</sup> EDAV, Gairės dėl nukrypti leidžiančių nuostatų (*supra* 153 išnaša), p. 10. EDAV taip pat patikslino, kad duomenų perdavimas taikant su viešuoju interesu susijusių nukrypti leidžiančių nuostatą negali būti „didelio masto“ ar „sistemiškas“, bet turi vykti „tik konkrečiais atvejais <...> [ir atitikti] griežtą būtinumo kriterijų“, bet nėra reikalavimo, kad jis vyktų „kartais“.

<sup>158</sup> Tai akivaizdu iš BDAR 48 straipsnio formuluotės („nedarant poveikio kitiems perdavimo pagrindams pagal šį skyrių“) ir su juo susijusios 115 konstatuojamosios dalies („Perduoti duomenis turėtų būti leidžiama tik jeigu įvykdytos duomenų perdavimui į trečiąsias valstybes taikomos šiame reglamente nustatytos sąlygos. Taip gali būti, *inter alia*, jeigu atskleisti duomenis būtina dėl svarbios Sąjungos ar valstybės narės teisėje, taikytinoje duomenų valdytojų, pripažintos viešojo intereso priežasties.“). Tai taip pat pripažįsta EDAV; žr. Gaires dėl nukrypti leidžiančių nuostatų (*supra* 153 išnaša), p. 5. Kalbant apie visas duomenų tvarkymo operacijas, reikia užtikrinti ir kitas reglamente numatytas apsaugos priemones (pvz., kad duomenys būtų perduodami konkrečiu tikslu, būtų tinkami ir tik tokie, kurių reikia siekiant tikslo, dėl kurių jie tvarkomi, ir t. t.).

leidžiančia nuostata dėl viešojo intereso, kai užsienio baudžiamosios teisėsaugos institucija JAV Aukščiausiojo Teismo byloje *Microsoft* pateikė įrodymų pateikimo orderį<sup>159</sup>. Savo nuomonėje Komisija pabrėžė, kad ES suinteresuota užtikrinti, kad teisėsaugos institucijų bendradarbiavimas vyktų „pagal teisinę sistemą, kurioje būtų vengiama teisės kolizijos ir kuri būtų grindžiama <...> abiejų šalių pagrindinių interesų ir privatumo, ir teisėsaugos srityse gerbimu“<sup>160</sup>. Visų pirma, „remiantis viešąja tarptautine teise, kai valdžios institucija prašo jos jurisdikcijoje įsteigtos įmonės pateikti elektroninius duomenis, saugomus užsienio jurisdikcijos serveryje, taikomi teritoriškumo ir pagarbos principai pagal viešąją tarptautinę teisę“<sup>161</sup>.

Tai taip pat pažymima Komisijos pasiūlyme dėl reglamento dėl Europos elektroninių įrodymų baudžiamosiose bylose pateikimo ir saugojimo orderių<sup>162</sup>, kuriame yra įtvirtinta konkreti „pagarbos sąlyga“, dėl kurios dėl įrodymų pateikimo orderio galima pareikšti prieštaravimą, jeigu jo vykdymas nėra suderinamas su trečiosios šalies įstatymais, pagal kuriuos draudžiama atskleisti informaciją, visų pirma remiantis pagrindu, kad ji yra būtina siekiant apsaugoti pagrindines suinteresuotųjų asmenų teises<sup>163</sup>.

Užtikrinti pagarbą yra svarbu, atsižvelgiant į tai, kad teisėsaugos veikla, kaip nusikaltimai ir, visų pirma, kibernetiniai nusikaltimai, įgyja vis didesnę tarptautinį aspektą, tad dažnai kyla klausimų dėl jurisdikcijos ir galima teisės kolizija<sup>164</sup>. Nenuostabu, kad geriausias būdas spręsti šiuos klausimus yra tarptautiniai susitarimai, kuriuose numatomi būtini apribojimai ir apsaugos priemonės suteikiant tarpvalstybinę

<sup>159</sup> Nuomonė dėl *Microsoft* (*supra* 156 išnaša). Taigi, kaip paaiškino Komisija, STPS pagal BDAR yra pageidautinas variantas perduodant duomenis, nes tokiose sutartyse „numatomas įrodymų rinkimas gavus sutikimą ir užtikrinama kruopščiai suderėta pusiausvyra tarp įvairių valstybių interesų, skirta mažinti jurisdikcijų koliziją, kuri galėtų kilti priešingu atveju“. Taip pat žr. EDAV gaires dėl nukrypti leidžiančių nuostatų (*supra* 153 išnaša), p. 5 („Tais atvejais, kai sudarytas tarptautinis susitarimas, pavyzdžiui, savitarpio teisinės pagalbos sutartis (*angl.* MLAT), ES įmonės paprastai turėtų atsakyti patenkinti tiesioginius prašymus ir nurodyti prašančiajai trečiosios valstybės institucijai galiojančią savitarpio teisinės pagalbos sutartį ar susitarimą.“).

<sup>160</sup> Nuomonė dėl *Microsoft* (*supra* 156 išnaša), p. 4.

<sup>161</sup> Nuomonė dėl *Microsoft* (*supra* 156 išnaša), p. 6.

<sup>162</sup> Europos Komisija, pasiūlymas dėl Europos Parlamento ir Tarybos reglamento dėl Europos elektroninių įrodymų baudžiamosiose bylose pateikimo ir saugojimo orderių, 2018 m. balandžio 17 d. (COM(2018) 225 *final*). Taryba priėmė bendrąjį požiūrį dėl siūlomo reglamento 2018 m. gruodžio 7 d. (paskelbta adresu <https://www.consilium.europa.eu/en/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-evidence-council-agrees-its-position/#>). Taip pat žr. EDAV nuomonę 7/19 dėl pasiūlymų dėl Europos elektroninių įrodymų baudžiamosiose bylose pateikimo ir saugojimo orderių (paskelbta adresu [https://edps.europa.eu/data-protection/ourwork/publications/opinions/electronic-evidence-criminal-matters\\_en](https://edps.europa.eu/data-protection/ourwork/publications/opinions/electronic-evidence-criminal-matters_en)).

<sup>163</sup> Aiškinamajame memorandume, p. 21, aiškiai pažymima, kad siekiant užtikrinti pagarbą suvereniems trečiųjų šalių interesams, apsaugoti atitinkamą asmenį ir panaikinti paslaugų teikėjų teisės aktų koliziją, vienas svarbus pagarbos sąlygos motyvas yra abipusiškumas, t. y. užtikrinama ES taisyklių pagarbą, be kita ko, dėl asmens duomenų apsaugos (BDAR 48 straipsnis). Taip pat žr. 2017 m. lapkričio 29 d. 29 straipsnio darbo grupės pareiškimą „Duomenų apsaugos ir privatumo aspektai tarpvalstybiniu lygmeniu suteikiant prieigą prie elektroninių įrodymų“ (29 straipsnio darbo grupės pareiškimas) (paskelbta adresu [file:///C:/Users/ralfs/AppData/Local/Packages/Microsoft.MicrosoftEdge\\_8wekyb3d8bbwe/TempState/Downloads/20171207\\_e-Evidence\\_Statement\\_FINAL.pdf%20\(1\).pdf](file:///C:/Users/ralfs/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/20171207_e-Evidence_Statement_FINAL.pdf%20(1).pdf)), p. 9.

<sup>164</sup> Žr. 29 straipsnio darbo grupės pareiškimą (*supra* 163 išnaša), p. 6.



prieigą prie asmens duomenų, be kita ko, prašančiajai institucijai užtikrinant aukšto lygio duomenų apsaugą.

Veikdama ES vardu Komisija šiuo metu dalyvauja daugiašalėse derybose dėl Europos Tarybos (Budapešto) konvencijos dėl elektroninių nusikaltimų Antrojo papildomo protokolo, kurio tikslas – sustiprinti galiojančias taisykles, pagal kurias suteikiama tarpvalstybinė prieiga prie elektroninių įrodymų atliekant baudžiamuosius tyrimus, kartu pagal protokolą užtikrinant tinkamas duomenų apsaugos priemones<sup>165</sup>. Be, to prasidėjo dvišalės derybos dėl ES ir Jungtinių Amerikos Valstijų susitarimo dėl tarpvalstybinės prieigos prie elektroninių įrodymų vykdant teisminį bendradarbiavimą baudžiamosiose bylose<sup>166</sup>. Šiose derybose Komisija tikisi Europos Parlamento ir Tarybos paramos bei EDAV rekomendacijų.

Apskritai svarbu užtikrinti, kad kai Europos rinkoje veikiančių įmonių remiantis teisėtu prašymu prašoma pasidalyti duomenimis teisėsaugos tikslais, jos gali tai daryti nesukeldamos teisės kolizijos ir visiškai paisydamos ES pagrindinių teisių. Tokiam duomenų perdavimui pagerinti Komisija yra išipareigojusi kartu su tarptautiniais partneriais kurti atitinkamas teises sistemas, kad būtų išvengta teisės kolizijos ir remiamos veiksmingos bendradarbiavimo formos, visų pirma numatant būtinas duomenų apsaugos priemones ir taip padedant veiksmingiau kovoti su nusikalstamumu.

### **7.3 Tarptautinis bendradarbiavimas duomenų apsaugos srityje**

Įvairių privatumo apsaugos sistemų konvergencijos skatinimas taip pat reiškia, kad šalys viena iš kitos mokosi keisdamosi žiniomis, patirtimi ir geriausia patirtimi. Tokie mainai yra labai svarbūs siekiant įveikti naujus iššūkius, kurių pobūdis ir mastas vis dažniau įgyja pasaulinį aspektą. Todėl Komisija sustiprino dialogą dėl duomenų apsaugos ir duomenų srautų su įvairiais subjektais ir įvairiuose forumuose dvišaliu, regioniniu ir daugiašaliu lygmenimis.

#### *Dvišalis lygmuo*

---

<sup>165</sup> Žr. rekomendaciją dėl Tarybos sprendimo, kuriuo suteikiami įgaliojimai dalyvauti derybose dėl Europos Tarybos konvencijos dėl elektroninių nusikaltimų (CETS Nr. 185) Antrojo papildomo protokolo, 2019 m. vasario 5 d. (COM(2019) 71 *final*). Taip pat žr. EDAV nuomonę 3/2019 dėl dalyvavimo derybose atsižvelgiant į Budapešto konvencijos dėl elektroninių nusikaltimų Antrąjį papildomą protokolą, 2019 m. balandžio 2 d. (paskelbta adresu [https://edps.europa.eu/sites/edp/files/publication/19-04-02\\_edps\\_opinion\\_budapest\\_convention\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/19-04-02_edps_opinion_budapest_convention_en.pdf)); EDAV nuomonė dėl konsultacijų dėl Europos Tarybos konvencijos dėl elektroninių nusikaltimų (Budapešto konvencijos) Antrojo papildomo protokolo projekto, 2019 m. lapkričio 13 d. (paskelbta adresu [https://edpb.europa.eu/sites/edpb/files/files/file1/edpbcontributionbudapestconvention\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpbcontributionbudapestconvention_en.pdf)).

<sup>166</sup> Žr. rekomendaciją dėl Tarybos sprendimo, kuriuo suteikiami įgaliojimai pradėti derybas dėl Europos Sąjungos ir Jungtinių Amerikos Valstijų susitarimo dėl tarpvalstybinės prieigos prie elektroninių įrodymų vykdant teisminį bendradarbiavimą baudžiamosiose bylose, 2019 m. vasario 5 d. (COM(2019) 70 *final*). Taip pat žr. EDAPP nuomonę 2/2019 įgaliojimų derėtis dėl ES ir JAV susitarimo dėl tarpvalstybinės prieigos prie elektroninių įrodymų (paskelbta adresu [https://edps.europa.eu/sites/edp/files/publication/19-04-02\\_edps\\_opinion\\_on\\_eu\\_us\\_agreement\\_on\\_e-evidence\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/19-04-02_edps_opinion_on_eu_us_agreement_on_e-evidence_en.pdf)).



Po BDAR priėmimo vis labiau domimasi ES patirtimi rengiant šiuolaikines privatumo apsaugos taisykles, dėl jų derantis ir jas įgyvendinant. Dialogas su šalimis, kuriose vyksta panašūs procesai, vyksta keliomis formomis.

Komisijos tarnybos yra pateikusios pastabų dėl įvairių viešų konsultacijų, kurias rengė užsienio vyriausybės svarstydamos privatumo apsaugos srities teisės aktus, pavyzdžiui, JAV<sup>167</sup>, Indijos<sup>168</sup>, Malaizijos ir Etiopijos. Kai kuriose trečiosiose šalyse Komisijos tarnyboms teko garbė kalbėti kompetinguose parlamento organuose, pavyzdžiui, Brazilijoje<sup>169</sup>, Čilėje<sup>170</sup>, Ekvadore ir Tunise<sup>171</sup>.

Be to, vykstant duomenų apsaugos įstatymų reformoms, buvo surengti specialūs susitikimai su daugelio pasaulio regionų (pvz., Gruzijos, Kenijos, Taivano, Tailando, Maroko) vyriausybių atstovais arba parlamentinėmis delegacijomis. Buvo, be kita ko, organizuojami seminarai ir mokomieji vizitai, pavyzdžiui, dalyvaujant Indonezijos vyriausybės atstovams ir JAV Kongreso darbuotojų delegacijai. Taip suteikta galimybių išaiškinti svarbias BDAR sąvokas, pagerinti abipusį supratimą apie privatumo klausimus; buvo pademonstruota, kokia naudinga konvergencija siekiant užtikrinti aukšto lygio asmenų teisių apsaugą, prekybą ir bendradarbiavimą. Kai kuriais atvejais taip pat pavyko užkirsti kelią neteisėtam duomenų apsaugos suvokimui, dėl kurio gali būti pradėtos taikyti protekcionistinės priemonės, kaip antai priverstinio vietos nustatymo reikalavimai.

Po BDAR priėmimo Komisija taip pat bendradarbiauja su keliomis tarptautinėmis organizacijomis, be kita ko, dėl duomenų mainų su šiomis organizacijomis svarbos įvairiose politikos srityse. Visų pirma, ypatingas dialogas pradėtas su Jungtinių Tautų Organizacija siekiant sudaryti palankesnes sąlygas diskutuoti su visais susijusiais suinteresuotaisiais subjektais ir užtikrinti sklandų duomenų perdavimą toliau plėtojant atitinkamų duomenų apsaugos režimų konvergenciją. Dalyvaudama šiame dialoge Komisija glaudžiai bendradarbiaus su EDAV, kad išsamiau paaiškintų, kaip ES

---

<sup>167</sup> Žr. 2018 m. lapkričio 9 d. Teisingumo ir vartotojų reikalų GD pastabas atsakant į JAV nacionalinės telekomunikacijų ir informacijos administracijos prašymą pateikti viešus komentarus dėl siūlomo vartotojų privatumo apsaugos metodo [dokumento Nr. 180821780-8780-01] (paskelbta adresu [https://ec.europa.eu/info/sites/info/files/european\\_commission\\_submission\\_on\\_a\\_proposed\\_approach\\_to\\_consumer\\_privacy.pdf](https://ec.europa.eu/info/sites/info/files/european_commission_submission_on_a_proposed_approach_to_consumer_privacy.pdf)).

<sup>168</sup> Žr. 2018 m. lapkričio 19 d. Teisingumo ir vartotojų reikalų GD pastabas elektroninių ir informacinių technologijų ministerijai dėl 2018 m. Indijos asmens duomenų apsaugos įstatymo projekto (paskelbta adresu [https://eeas.europa.eu/delegations/india/53963/submission-draft-personal-data-protection-bill-india-2018-directorate-general-justice\\_en](https://eeas.europa.eu/delegations/india/53963/submission-draft-personal-data-protection-bill-india-2018-directorate-general-justice_en)).

<sup>169</sup> Žr. 2018 m. balandžio 17 d. Brazilijos Senato plenarinio posėdžio protokolą (<https://www25.senado.leg.br/web/atividade/sessao-plenaria/-/pauta/23384>), 2019 m. balandžio 10 d. Brazilijos Kongreso jungtinio komiteto dėl MP 869/2018 posėdžio protokolą (<https://www12.senado.leg.br/ecidania/visualizacaoaudiencia?id=15392>) ir 2019 m. lapkričio 26 d. Brazilijos deputatų rūmų specialiojo komiteto posėdžio protokolą (<https://www.camara.leg.br/noticias/616579-comissao-discutira-protecao-de-dados-no-ambito-das-constituicoes-de-outros-paises/>).

<sup>170</sup> Žr. 2018 m. gegužės 29 d. ([https://senado.cl/appsenado/index.php?mo=comisiones&ac=asistencia\\_sesion&idcomision=186&idsession=12513&idpunto=15909&sesion=29/05/2018&listado=1](https://senado.cl/appsenado/index.php?mo=comisiones&ac=asistencia_sesion&idcomision=186&idsession=12513&idpunto=15909&sesion=29/05/2018&listado=1)) ir 2019 m. balandžio 24 d. ([https://www.senado.cl/appsenado/index.php?mo=comisiones&ac=sesiones\\_celebradas&idcomision=186&tipo=3&legi=485&ano=2019&desde=0&hasta=0&idsesion=13603&idpunto=17283&listado=2](https://www.senado.cl/appsenado/index.php?mo=comisiones&ac=sesiones_celebradas&idcomision=186&tipo=3&legi=485&ano=2019&desde=0&hasta=0&idsesion=13603&idpunto=17283&listado=2)) Čilės Senato konstitucinių, teisėkūros ir teisingumo reikalų komiteto posėdžių protokolus.

<sup>171</sup> Žr. 2018 m. lapkričio 2 d. Tuniso Atstovų Asamblėjos teisių, laisvių ir išorės santykių komiteto posėdžio protokolą (<https://www.facebook.com/1515094915436499/posts/2264094487203201/>).

viešieji ir privatieji veiklos vykdytojai gali vykdyti savo prievoles pagal BDAR keisdami duomenimis su tokiomis tarptautinėmis organizacijomis, kaip JT.

Komisija yra pasirengusi toliau dalytis reformų proceso metu įgyta patirtimi su suinteresuotomis šalimis ir tarptautinėmis organizacijomis, kaip ji pati mokėsi iš kitų sistemų, kai rengė pasiūlymą dėl naujų ES duomenų apsaugos taisyklių. Tokio pobūdžio dialogas yra abipusiai naudingas ES ir jos partneriams, nes leidžia geriau suprasti sparčiai besivystančią privatumo apsaugos aplinką ir keistis nuomonėmis apie naujus teisinius ir techninius sprendimus.

Būtent todėl Komisija steigia „Duomenų apsaugos akademiją“, kad paskatintų mainus tarp Europos ir trečiųjų šalių reguliavimo institucijų ir taip gerintų bendradarbiavimą vietoje.

Be to, reikia kurti tinkamas teises priemones glaudesniai bendradarbiavimui ir savitarpio pagalbai, be kita ko, numatant galimybę vykdyti būtinus informacijos mainus tyrimų tikslais. Taigi Komisija pasinaudos BDAR 50 straipsniu suteiktais šios srities įgaliojimais ir, visų pirma, sieks leidimo pradėti derybas dėl bendradarbiavimo vykdymo užtikrinimo srityje susitarimų sudarymo su atitinkamomis trečiosiomis šalimis. Tam ji taip pat atsižvelgs į Valdybos nuomonę dėl to, kurioms šalims turėtų būti teikiama pirmenybė atsižvelgiant į duomenų perdavimo mastą, dėl už trečiosiose šalyse privatumo apsaugos taisyklių vykdymo užtikrinimą atsakingos institucijos vaidmens ir įgaliojimų ir būtinybės bendradarbiauti vykdymo užtikrinimo tikslais bendro intereso atvejais.

### *Daugiašalis aspektas*

Be dvišalių mainų, Komisija taip pat aktyviai dalyvauja daugiašaliuose forumuose siekdama populiarinti bendras vertybes ir skatinti konvergenciją regioniniu ir pasauliniu lygmenimis.

Tai, kad vis daugiau šalių prisijungia prie Europos Tarybos konvencijos Nr. 108, kuri yra vienintelė teisiškai privaloma daugiašalė priemonė asmens duomenų apsaugos srityje, yra aiškus ženklas, kad judama link (didesnės) konvergencijos<sup>172</sup>. Konvenciją, prie kurios taip pat gali jungtis Europos Tarybos nariais nesančios šalys, ratifikavo jau 55 šalys, įskaitant kelias Afrikos ir Lotynų Amerikos valstybes<sup>173</sup>. Komisija labai prisidėjo prie sėkmingos derybų dėl konvencijos modernizavimo baigties<sup>174</sup> ir užtikrino, kad joje būtų laikomasi tokių pat principų, kaip ES duomenų apsaugos taisyklėse. Dauguma ES valstybių narių jau pasirašė protokolą, kuriuo iš dalies

<sup>172</sup> Svarbu tai, kad atnaujinta konvencija yra ne tik sutartis, kurioje nustatomos patikimos duomenų apsaugos priemonės; ja taip pat sukuriama priežiūros institucijų tinklas numatant bendradarbiavimo vykdymo užtikrinimo srityje priemonės, o Konvencijos komitetas yra forumas diskusijoms, keitimuisi geriausia patirtimi ir tarptautinių standartų rengimui.

<sup>173</sup> Žr. išsamų narių sąrašą: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures>. Tarp Afrikos šalių – Žaliasis Kyšulys, Mauricijus, Marokas, Senegalas ir Tunisas; Lotynų Amerikos – Argentina, Meksika ir Urugvajus. Prisijungti prie konvencijos buvo pakviestas Burkina Faso.

<sup>174</sup> Žr. atnaujintos konvencijos tekstą: [https://search.coe.int/cm/Pages/result\\_details.aspx?ObjectId=09000016807c65bf](https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf).

keičiama konvencija, bet Danija, Malta ir Rumunija to dar nepadarė. Protokolą, kuriuo iš dalies keičiama konvencija, ratifikavo tik keturios valstybės narės (Bulgarija, Kroatija, Lietuva ir Lenkija). Komisija ragina tris likusias valstybes nares pasirašyti atnaujintą konvenciją ir visas valstybes nares – skubiai pereiti prie ratifikavimo, kad protokolas įsigaliotų artimiausiu metu<sup>175</sup>. Be to, ji ir toliau aktyviai skatins jungtis trečiąsias šalis.

Duomenų srautus ir apsaugą pastaruoju metu nagrinėjo ir G 20 ir G 7. 2019 m. pasaulio vadovai pirmą kartą pritarė minčiai, kad duomenų apsauga prisidedama prie pasitikėjimo skaitmeninėje ekonomikoje ir sudaromos palankesnės sąlygos duomenų srautams. Komisijai aktyviai pritariant<sup>176</sup> vadovai patvirtino sąvoką „laisvas duomenų srautas užtikrinant pasitikėjimą“ (DFFT), kurią iš pradžių pasiūlė Japonija G 20 Osakos deklaracijoje<sup>177</sup> ir G 7 aukščiausiojo lygio susitikime Biarice<sup>178</sup>. Šis požiūris taip pat pateikiamas 2020 m. Komisijos komunikate „Europos duomenų strategija“<sup>179</sup>, kuriame pabrėžiamas jos ketinimas toliau skatinti keitimąsi duomenimis su patikimais partneriais kovojant su piktnaudžiavimu, kaip antai neproporcinga (užsienio) valdžios institucijų prieiga prie duomenų.

Taip ES galės naudotis keliomis priemonėmis įvairiose politikos srityse, kuriose vis labiau atsižvelgiama į poveikį privatumui: pavyzdžiui, pagal pirmąją ES užsienio investicijų tikrinimo sistemą, kuris bus taikoma visa nuo 2020 m. spalio mėn., suteikiama galimybė ES ir jos valstybėms narėms tikrinti investicinius sandorius, darančius poveikį „prieigai prie neskelbtinos informacijos, įskaitant asmens duomenis, arba gebėjimui kontroliuoti tokią informaciją“, jeigu dėl to daromas poveikis saugumui ar viešajai tvarkai<sup>180</sup>.

Komisija bendradarbiauja su panašiai mąstančiomis šalimis keliuose kituose daugiašaliuose forumuose, kad aktyviai propaguotų savo vertybes ir standartus. Vienas svarbus forumas yra neseniai įsteigta EBPO darbo grupė duomenų valdymo ir privatumo klausimais (DGP), įgyvendinanti kelias svarbias iniciatyvas, susijusias su

---

<sup>175</sup> Remdamasis 2018 m. gegužės 18 d. sprendimu Ministrų komitetas „paragino valstybes nares ir kitas Konvencijos šalis nedelsiant imtis būtinų priemonių, kad protokolas įsigaliotų per trejus metus nuo jo pasirašymo laikotarpio pradžios ir nedelsiant, tačiau bet kuriuo atveju ne vėliau kaip per vienus metus nuo protokolo pasirašymo laikotarpio pradžios pradėti ratifikavimo procesą pagal nacionalinę teisę...“ Jame taip pat „nurodoma, kad deputatai du kartus per metus ir pirmą kartą praėjus vieniems metams nuo protokolo pasirašymo įvertintų bendrą ratifikavimo pažangą remdamiesi informacija, kurią Generaliniam Sekretoriui ne vėliau kaip likus vienam mėnesiui iki svarstymo turi pateikti kiekviena valstybė narė ir kitos Konvencijos šalys“. Žr. [https://search.coe.int/cm/pages/result\\_details.aspx?objectid=09000016808a3c9f](https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016808a3c9f).

<sup>176</sup>

vaidmenį įgyvendinant abi iniciatyvas“.

<sup>177</sup> Žr. G 20 Osakos vadovų deklaracijos tekstą: [https://www.consilium.europa.eu/media/40124/final\\_g20\\_osaka\\_leaders\\_declaration.pdf](https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf)

<sup>178</sup> Žr. G 7 Biarico atviros, laisvos ir saugios skaitmeninės pertvarkos strategijos tekstą: <https://www.elysee.fr/admin/upload/default/0001/05/62a9221e66987d4e0d6ffcb058f3d2c649fc6d9d.pdf>.

<sup>179</sup> Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui „Europos duomenų strategija“, 2020 m. vasario 9 d. (COM(2011) 66 final) (<https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:52020DC0066&qid=1596691643564&from=EN>), p. 23 ir 24.

<sup>180</sup> 2019 m. kovo 19 d. Europos Parlamento ir Tarybos reglamento (ES) 2019/452, kuriuo nustatoma tiesioginių užsienio investicijų į Sąjungą tikrinimo sistema (OL L 79I, 2019 3 21), 4 straipsnio 1 dalies d punktas.

duomenų apsauga, dalijimusi duomenimis ir duomenų perdavimu. Atsižvelgiama ir į 2013 m. EBPO privatumo gairių vertinimą. Komisija taip pat aktyviai padėjo rengti EBPO Tarybos rekomendaciją dėl dirbtinio intelekto<sup>181</sup> ir užtikrino, kad galutiniame tekste būtų perteiktas į ES taikoma į žmogų orientuotą požiūrį, t. y. kad DI taikomosios programos turi atitikti pagrindines teises, visų pirma duomenų apsaugos srityje. Svarbu tai, kad rekomendacijoje dėl DI, kuri vėliau buvo įtraukta į G 20 DI principus, įtrauktus į G 20 Osakos vadovų deklaraciją<sup>182</sup>, nustatomi skaidrumo ir paaiškinamumo principai siekiant „suteikti galimybę tiems, kam DI sistema daro neigiamą poveikį, apskūsti jos veiklos rezultatus remiantis paprasta ir lengvai suprantama informacija apie veiksnius ir logiką, kuriais vadovautasi rengiant prognozę, teikiant rekomendaciją ar priimant sprendimą“, taip tiksliai perteikiant BDAR principus, susijusius su automatizuotu sprendimu priėmimu<sup>183</sup>.

Komisija taip pat stiprina dialogą su regioninėmis organizacijomis ir tinklais, kurie atlieka vis svarbesnį vaidmenį rengiant bendrus duomenų apsaugos standartus<sup>184</sup>, bei skatina keitimąsi geriausia patirtimi ir už vykdymo užtikrinimą atsakingų institucijų bendradarbiavimą. Tai, visų pirma, pasakytina apie Pietryčių Azijos valstybių asociaciją (ASEAN), be kita ko, vykstant darbui prie duomenų perdavimo priemonių, Afrikos Sąjungą, Azijos ir Ramiojo vandenyno šalių privatumo apsaugos institucijų (APPA) forumą ir Iberijos pusiasalio ir Lotynų Amerikos šalių duomenų apsaugos tinklą; jie visi yra pradėję svarbias iniciatyvas šioje srityje ir yra forumai naudingam privatumo reguliavimo institucijų ir kitų suinteresuotųjų subjektų dialogui.

Afrika yra puikus nacionalinių, regioninių ir pasaulinių privatumo aspektų papildomumo pavyzdys. Dėl skaitmeninių technologijų Afrikos žemynas transformuojasi greitai ir nuodugnai. Taip galima paspartinti darnaus vystymosi tikslų įgyvendinimą skatinant ekonomikos augimą, mažinant skurdą ir gerinant žmonių gyvenimą. Įdiegta šiuolaikinė duomenų apsaugos sistema, pritraukianti investicijas ir skatinanti konkurencingo verslo vystymąsi, kartu padedanti laikytis žmogaus teisių, demokratijos ir teisinės valstybės principų, yra esminis tokios pertvarkos elementas. Suderinus duomenų apsaugos taisykles visoje Afrikoje būtų sudarytos sąlygos skaitmeninei rinkos integracijai, o užtikrinus konvergenciją su pasauliniais standartais būtų lengviau keistis duomenimis su ES. Šie skirtingi duomenų apsaugos aspektai yra tarpusavyje susiję ir vienas kitą sustiprina.

Dabar vis aktyviau domimasi duomenų apsauga daugelyje Afrikos šalių, o Afrikos šalių, priėmusių ar siekiančių priimti šiuolaikinės duomenų apsaugos taisykles ir ratifikavusių Konvenciją Nr. 108<sup>185</sup> ar Malabo konvenciją<sup>186</sup>, skaičius ir toliau

<sup>181</sup> <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>.

<sup>182</sup> G 20 ministrų pareiškimas dėl prekybos ir skaitmeninės ekonomikos: [https://g20trade-digital.go.jp/dl/Ministerial\\_Statement\\_on\\_Trade\\_and\\_Digital\\_Economy.pdf](https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf).

<sup>183</sup> Žr. BDAR 13 straipsnio 2 dalies f punktą, 14 straipsnio 2 dalies g punktą ir 22 straipsnį.

<sup>184</sup> Žr., pavyzdžiui, Afrikos Sąjungos *konvenciją dėl kibernetinio saugumo ir asmens duomenų apsaugos* (toliau – Malabo konvencija) ir Iberijos pusiasalio ir Lotynų Amerikos šalių duomenų apsaugos tinklo parengtus *Iberijos pusiasalio ir Lotynų Amerikos šalių duomenų apsaugos standartus*.

<sup>185</sup> Europos Tarybos Konvencija dėl asmens apsaugos ryšium su asmens duomenų automatizuotu tvarkymu: [https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p\\_auth=DW5jevqD](https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=DW5jevqD).

<sup>186</sup> Afrikos Sąjungos konvencija dėl kibernetinio saugumo ir asmens duomenų apsaugos: <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>. Be to,

didėja<sup>187</sup>. Kita vertus, reglamentavimo sistema Afrikos žemyne išlieka labai netolygi ir susiskaidžiusi. Daugelyje šalių vis dar mažai duomenų apsaugos priemonių arba jų visai nėra. Vis dar paplitusios duomenų srautų ribojimo priemonės, kliudančios regioninės skaitmeninės ekonomikos plėtrai.

Siekdama pasinaudoti abipuse suderintų duomenų apsaugos taisyklių pranašumais Komisija bendradarbiaus su Afrikos partneriais ir dvišaliuose, ir regioniniuose forumuose<sup>188</sup>. Remiamasi ES ir AS specialios paskirties grupės skaitmeninės ekonomikos klausimais darbu Naujojoje Afrikos ir Europos skaitmeninės ekonomikos partnerystėje<sup>189</sup>. Pasiiekti tokius tikslus taip pat padeda tai, kad Komisijos partnerystės priemonės „Geresnė duomenų apsauga ir duomenų srautai“ taikymo sritis buvo išplėsta įtraukiant Afriką. Projektas bus vykdomas siekiant remti Afrikos šalis, ketinančias kurti šiuolaikines duomenų apsaugos sistemas arba norinčias tobulinti savo reguliavimo institucijų gebėjimus mokymo, dalijimosi žiniomis ir keitimosi geriausia patirtimi priemonėmis.

Galiausiai, skatindama duomenų apsaugos standartų konvergenciją tarptautiniu lygmeniu, taip siekdama sudaryti palankesnes sąlygas duomenų srautams ir atitinkamai – prekybai, Komisija taip pat yra pasiryžusi kovoti su skaitmeniniu protekcionizmu, kaip pabrėžiama neseniai priimtoje duomenų strategijoje<sup>190</sup>. Tam ji parengė konkrečias prekybos susitarimų nuostatas dėl duomenų srautų ir duomenų apsaugos, kurias ji nuolat siūlo dvišalėse (visai neseniai su Australija, Naująja Zelandija ir Jungtine Karalyste) ir daugiašalėse derybose, pavyzdžiui, vykstančiose su PPO dėl elektroninės prekybos. Šiomis horizontaliosiomis nuostatomis eliminuojami nepagrįsti apribojimai, kaip antai privalomi duomenų lokalizavimo reikalavimai, kartu išsaugant susitarimo šalių reguliavimo autonomiją, taip siekiant apsaugoti pagrindinę teisę į duomenų apsaugą.

Nors dialogai duomenų apsaugos ir prekybos derybų klausimais turi vykti atskiromis kryptimis, jie gali ir papildyti vienas kitą. Faktiškai konvergencija, pagrįsta aukštais standartais ir remiama veiksmingomis vykdymo užtikrinimo priemonėmis, yra patvariausias pagrindas keistis asmens duomenimis; tai vis labiau pripažįsta mūsų

---

duomenų apsaugos taisykles yra parengusios kelios regioninės ekonominės bendrijos (REB), pavyzdžiui, Vakarų Afrikos valstybių ekonominė bendrija (ECOWAS) ir Pietų Afrikos vystymosi bendrija (SADC). Atitinkamai žr. <http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED-Data-Protection-Act.pdf> ir [http://www.itu.int/ITU-D/projects/ITU\\_EC\\_ACP/hipssa/docs/SA4docs/data%20protection.pdf](http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/SA4docs/data%20protection.pdf).

<sup>188</sup> *Inter alia*, įgyvendinant Skaitmeninės Afrikos politikos ir reguliavimo iniciatyvą (PRIDA); žr. informaciją adresu <https://www.africa-eu-partnership.org/en/projects/policy-and-regulation-initiative-digital-africa-prida>.

<sup>189</sup> Žr. bendrą Europos Komisijos ir vyriausiojo įgaliojimo užsienio reikalams ir saugumo politikai komunikatą „Visapusiškos strategijos su Afrika kūrimas“ (paskelbta adresu <https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:52020JC0004&qid=1596694844607&from=EN>); Specialios paskirties grupė skaitmeninės ekonomikos klausimais, Naujoji Afrikos ir Europos skaitmeninės ekonomikos partnerystė „Darnaus vystymosi tikslų įgyvendinimo spartinimas“ (paskelbta adresu <https://www.africa-eu-partnership.org/sites/default/files/documents/finaldetfreportpdf.pdf>).

<sup>190</sup> <https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:52020DC0066&qid=1596691643564&from=EN>, p. 23.

tarptautiniai partneriai. Turint galvoje tai, kad įmonės vis dažniau veikia tarptautiniu mastu ir savo verslo operacijoms visame pasaulyje renkasi taikyti panašius taisyklių rinkinius, tokia konvergencija padeda kurti tiesioginėms investicijoms palankią aplinką, o kartu palengvina prekybą ir stiprina komercinių partnerių tarpusavio pasitikėjimą. Todėl reikėtų toliau nagrinėti prekybos ir duomenų apsaugos priemonių sinergiją siekiant užtikrinti laisvus ir saugius tarptautinius duomenų srautus, kurie yra būtini Europos įmonių, įskaitant MVI, verslo operacijoms, konkurencingumui ir augimui mūsų vis labiau skaitmeninamoje ekonomikoje.



**I priedas. Nuostatos dėl neprivalomų nacionalinės teisės aktuose įtvirtintų patikslinimų**

<b>Tema</b>	<b>Taikymo sritis</b>	<b>BDAR straipsniai</b>
Patikslinimai dėl teisinių prievolių ir viešosios užduoties	Nuostatų dėl duomenų tvarkymo siekiant įvykdyti teisinę prievolę ar viešąją užduotį taikymo pritaikymas, be kita ko, konkrečiose duomenų tvarkymo situacijose pagal IX skyrių	6 straipsnio 2 dalis ir 6 straipsnio 3 dalis
Amžiaus riba dėl sutikimo siūlant informacinės visuomenės paslaugas	Minimalaus amžiaus nuo 13 iki 16 metų nustatymas	8 straipsnio 1 dalis
Specialių kategorijų duomenų tvarkymas	Papildomų genetinių, biometrinių ar su sveikata susijusių duomenų tvarkymo sąlygų išlaikymas ar sukūrimas, įskaitant apribojimus	9 straipsnio 4 dalis
Nuo informacijos reikalavimų nukrypti leidžianti nuostata	Informacijos gavimas ar atskleidimas, aiškiai nustatytas teisės aktuose susijęs su įstatymais reglamentuojama profesine paslaptimi	14 straipsnio 5 dalies c ir d punktai
Automatizuotas individualių sprendimų priėmimas	Leidimas priimti automatinius sprendimus nukrypstant nuo bendrojo draudimo	22 straipsnio 2 dalies b punktas
Duomenų subjektų teisių apribojimai	Apribojimai taikant 12–22 straipsnius, 34 straipsnį ir atitinkamas 5 straipsnio nuostatas, kai tai būtina ir proporcinga siekiant apsaugoti į baigtinį sąrašą įtrauktus svarbius tikslus	23 straipsnio 1 dalis
Reikalavimas konsultuotis ir gauti leidimą	Reikalavimas duomenų valdytojams konsultuotis su duomenų apsaugos institucija ar gauti jos leidimą norint tvarkyti duomenis vykdant viešojo intereso užduotį	36 straipsnio 5 dalis
Duomenų apsaugos pareigūno paskyrimas papildomais atvejais	Duomenų apsaugos pareigūno paskyrimas kitais atvejais nei išvardyta 37 straipsnio 1 dalyje	37 straipsnio 4 dalis
Duomenų perdavimo apribojimai	Specialių kategorijų duomenų perdavimo apribojimas	49 straipsnio 5 dalis
Pačių organizacijų pateikiami skundai ir pareiškiama ieškiniai	Leidimas privatumo apsaugos organizacijoms teikti skundus ir pareikšti ieškinius nepriklausomai nuo joms suteiktų duomenų subjektų įgaliojimų	80 straipsnio 2 dalis

Galimybė susipažinti su oficialiaisiais dokumentais	Galimybės visuomenei susipažinti su oficialiaisiais dokumentais suderinimas su teise į asmens duomenų apsaugą	86 straipsnis
Nacionalinio asmens identifikavimo numerio tvarkymas	Nacionalinio asmens identifikavimo numerio tvarkymo specialiosios sąlygos	87 straipsnis
Duomenų tvarkymas užimtumo srityje	Konkretesnės darbuotojų asmens duomenų tvarkymo taisyklės	88 straipsnis
Nukrypti leidžiančios nuostatos tvarkant ir archyvuojant duomenis viešojo intereso, mokslinių tyrimų ar statistikos tikslais	Nuostatos, leidžiančios nukrypti nuo nurodytų duomenų subjektų teisių, jeigu dėl tokių teisių gali tapti neįmanoma arba labai sudėtinga įgyvendinti konkrečius tikslus	89 straipsnio 2 ir 3 dalys
Duomenų apsaugos suderinimas su prievolėmis saugoti paslaptį	Specialiosios taisyklės dėl duomenų apsaugos institucijų tyrimo įgaliojimų dėl duomenų valdytojų ar duomenų tvarkytojų vykdant prievolės saugoti profesinę paslaptį	90 straipsnis

## II PRIEDAS. Duomenų apsaugos institucijų išteklių apžvalga

Lentelėje toliau pateikiama kiekvienos ES ir EEE valstybės narės<sup>191</sup> duomenų apsaugos institucijų išteklių (darbuotojų ir biudžeto) apžvalga.

Lyginant valstybių narių skaičius svarbu turėti omenyje, kad institucijoms gali būti pavedamos užduotys ne tik pagal BDAR ir kad tos užduotys įvairiose valstybėse narėse gali skirtis. Institucijų darbuotojų skaičius vienam milijonui gyventojų ir institucijų biudžeto santykis su vienu milijonu eurų BVP pateikiami tik tam, kad būtų papildomų panašaus dydžio valstybių narių palyginimo elementų; šių skaičių nereikėtų vertinti atskirai. Vertinant tam tikros institucijos išteklius reikėtų kartu atsižvelgti į absoliutinius skaičius, santykius ir jų kitimą ankstesniais metais.

ES ir EEE valstybės narės	DARBUOTOJAI (etato ekvivalentas)					BUDŽETAS (EUR)				
	2019 m.	2020 m. prognozė	2016–2019 m. augimas %	2016–2020 m. augimas % (prognozė)	Darbuotojų skaičius vienam milijonui gyventojų (2019 m.)	2019 m.	2020 m. prognozė	2016–2019 m. augimas %	2016–2020 m. augimas % (prognozė)	Biudžetas vienam milijonui EUR BVP (2019 m.)
Austrija	34	34	48 %	48 %	3,8	2 282 000	2 282 000	29 %	29 %	5,7
Belgija	59	65	9 %	20 %	5,2	8 197 400	8 962 200	1 %	10 %	17,3
Bulgarija	60	60	-14 %	-14 %	8,6	1 446 956	1 446 956	24 %	24 %	23,8
Kroatija	39	60	39 %	114 %	9,6	1 157 300	1 405 000	57 %	91 %	21,5
Kipras	24	22	netaikytina	netaikytina	27,4	503 855	netaikytina	114 %	netaikytina	23,0
Čekija	101	109	0 %	8 %	9,5	6 541 288	6 720 533	10 %	13 %	29,7
Danija	66	63	106 %	97 %	11,4	5 610 128	5 623 114	101 %	101 %	18,0
Estija	16	18	-11 %	0 %	12,1	750 331	750 331	7 %	7 %	26,8
Suomija	45	55	114 %	162 %	8,2	3 500 000	4 500 000	94 %	150 %	14,6
Prancūzija	215	225	9 %	14 %	3,2	18 506 734	20 143 889	-2 %	7 %	7,7
Vokietija	888	1 002	52 %	72 %	10,7	76 599 800	85 837 500	48 %	66 %	22,3
Graikija	33	46	-15 %	18 %	3,1	2 849 000	3 101 000	38 %	50 %	15,2
Vengrija	104	117	42 %	60 %	10,6	3 505 152	4 437 576	102 %	155 %	24,4
Islandija	17	17	143 %	143 %	47,6	2 272 490	2 294 104	167 %	170 %	105,2
Airija	140	176	169 %	238 %	28,5	15 200 000	16 900 000	223 %	260 %	43,8
Italija	170	170	40 %	40 %	2,8	29 127 273	30 127 273	46 %	51 %	16,3
Latvija	19	31	-10 %	48 %	9,9	640 998	1 218 978	4 %	98 %	21,0
Lietuva	46	52	-8 %	4 %	16,5	1 482 000	1 581 000	40 %	49 %	30,6
Liuksemburgas	43	48	126 %	153 %	70,0	5 442 416	6 691 563	165 %	226 %	85,7
Malta	13	15	30 %	50 %	26,3	480 000	550 000	41 %	62 %	36,3
Nyderlandai	179	188	145 %	158 %	10,4	18 600 000	18 600 000	130 %	130 %	22,9
Norvegija	49	58	2 %	21 %	9,2	5 708 950	6 580 660	27 %	46 %	15,9
Lenkija	238	260	54 %	68 %	6,3	7 506 345	9 413 381	66 %	108 %	14,2
Portugalija	25	27	-4 %	4 %	2,4	2 152 000	2 385 000	67 %	86 %	10,1
Rumunija	39	47	-3 %	18 %	2,0	1 103 388	1 304 813	3 %	22 %	4,9
Slovakija	49	51	20 %	24 %	9,0	1 731 419	1 859 514	47 %	58 %	18,4
Slovėnija	47	49	42 %	48 %	22,6	2 242 236	2 266 485	68 %	70 %	46,7
Ispanija	170	220	13 %	47 %	3,6	15 187 680	16 500 000	8 %	17 %	12,2
Švedija	87	87	81 %	81 %	8,5	8 800 000	10 300 000	96 %	129 %	18,5
IŠ VISO	2 966	3 372	42 %	62 %	6,6	249 127 139	273 782 870	49 %	64 %	17,4

Neapdorotų skaičių šaltinis: Valdybos nuomonė. Komisijos skaičiavimai.

<sup>191</sup>

Išskyrus Lichtenšteiną.