Nuomonė Nr. 14/2021 dėl Europos Komisijos įgyvendinimo sprendimo pagal Reglamentą (ES) 2016/679 dėl tinkamos asmens duomenų apsaugos Jungtinėje Karalystėje projekto

Priimta 2021 m. balandžio 13 d.

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

TURINYS

1. SANTRAUKA 4

1.1. Konvergencijos sritys 5

1.2. Sunkumai 5

1.2.1. Bendrieji klausimai 5

1.2.2. Bendrieji duomenų apsaugos aspektai 6

1.2.3. Dėl valdžios institucijų teisės susipažinti su duomenimis, perduotais į JK 8

1.3. Išvada 9

2. ĮVADAS 10

2.1. JK duomenų apsaugos sistema 10

2.2. EDAV vertinimo sritis 11

2.3. Bendrosios pastabos ir susirūpinimą keliantys klausimai 12

2.3.1. JK prisiimti tarptautiniai įsipareigojimai 12

2.3.2. Galimi būsimi JK duomenų apsaugos sistemos skirtumai 13

3. BENDRIEJI DUOMENŲ APSAUGOS ASPEKTAI 14

3.1. Esminiai principai: 14

3.1.1. Teisė susipažinti su duomenimis, reikalauti juos ištaisyti, ištrinti ir nesutikti 15

3.1.2. Tolesnio duomenų perdavimo ribojimas 19

3.2. Procedūriniai ir vykdymo užtikrinimo mechanizmai 26

3.2.1 Kompetentinga nepriklausoma priežiūros institucija 26

3.2.2. Duomenų apsaugos sistema, kuria užtikrinamas geras atitikties lygis 27

3.2.3. Įgyvendinant duomenų apsaugos sistemą privaloma teikti paramą ir padėti duomenų subjektams pasinaudoti savo teisėmis ir atitinkamais teisių gynimo mechanizmais 27

4. JK VALDŽIOS INSTITUCIJŲ GALIMYBĖ SUSIPAŽINTI SU IŠ ES PERDUOTAIS ASMENS DUOMENIMIS IR JŲ NAUDOJIMAS 28

4.1. JK valdžios institucijų galimybė susipažinti su duomenimis ir jų naudojimas baudžiamosios teisėsaugos tikslais 28

4.1.1. Teisiniai pagrindai ir taikomi apribojimai / apsaugos priemonės 28

4.1.2. Tolimesnis teisėsaugos tikslais surinktos informacijos naudojimas (140–154 konstatuojamosios dalys) 30

4.1.3. Priežiūra 32

4.2. Bendroji duomenų apsaugos teisinė sistema nacionalinio saugumo srityje 32

4.2.1. Nacionalinio saugumo sertifikatai 32

4.2.2. Teisė taisyti ir trinti duomenis 33

4.2.3. Nacionalinio saugumo išimtys 33
4.3. JK valdžios institucijų galimybė susipažinti su duomenimis ir jų naudojimas nacionalinio saugumo tikslais 33
4.3.1. Teisiniai pagrindai, apribojimai ir apsaugos priemonės. Tyrimo įgaliojimai nacionalinio saugumo kontekste 34
4.3.2. Tolimesnis nacionalinio saugumo ir atskleidimo užjūrio valstybėms tikslais surinktos informacijos naudojimas 43
4.3.3. Priežiūra 47
4.3.4. Teisė kreiptis į teismą 48

Europos duomenų apsaugos valdyba,

atsižvelgdama į 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau – BDAR) 70 straipsnio 1 dalies s punktą,

atsižvelgdama į Europos ekonominės erdvės (toliau – EEE) susitarimą, visų pirma į jo XI priedą ir 37 protokolą su pakeitimais, padarytais 2018 m. liepos 6 d. EEE jungtinio komiteto sprendimu Nr. 154/2018[1],

atsižvelgdama į savo Darbo tvarkos taisyklių 12 ir 22 straipsnius,

PRIĖMĖ ŠIĄ NUOMONĘ:

1. SANTRAUKA

1. 2021 m. vasario 19 d. Europos Komisija patvirtino įgyvendinimo sprendimo dėl tinkamos asmens duomenų apsaugos Jungtinėje Karalystėje (toliau – JK) pagal BDAR projektą (toliau – sprendimo projektas)[2]. Po to Europos Komisija pradėjo jo oficialaus priėmimo procedūrą.

2. Tą pačią dieną Europos Komisija paprašė Europos duomenų apsaugos valdybos (toliau – EDAV) pateikti nuomonę[3]. EDAV Jungtinėje Karalystėje užtikrinamos apsaugos lygio tinkamumą įvertino išnagrinėjusi patį sprendimo projektą ir išanalizavusi Europos Komisijos pateiktus dokumentus.

3. EDAV daugiausia dėmesio skyrė tiek sprendimo projekto bendrųjų BDAR aspektų, tiek valdžios institucijų teisės susipažinti su asmens duomenimis, perduotais iš EEE, teisėsaugos ir nacionalinio saugumo tikslais, vertinimui, įskaitant teisių gynimo priemones, kuriomis gali pasinaudoti asmenys EEE. EDAV taip pat įvertino, ar pagal JK teisinę sistemą numatytos apsaugos priemonės yra įdiegtos ir veiksmingos.

4. Šiame vertinime EDAV daugiausia rėmėsi 2018 m. vasario mėn. priimtu BDAR tinkamumo kriterijų dokumentu[4] ir EDAV rekomendacijomis Nr. 02/2020 dėl Europos pagrindinių garantijų taikant stebėjimo priemones[5].

[1] Šioje nuomonėje daromos nuorodos į valstybes nares turėtų būti suprantamos kaip nuorodos į EEE valstybes nares.
[2] Žr. 2021 m. vasario 19 d. Europos Komisijos pranešimą spaudai „Duomenų apsauga. Europos Komisija pradeda procesą dėl asmens duomenų judėjimo į Jungtinę Karalystę“, https://ec.europa.eu/commission/presscorner/detail/lt/ip_21_661.
[3] Ten pat.
[4] Žr. 2017 m. lapkričio 28 d. 29 straipsnio darbo grupės priimtą dokumentą „Tinkamumo pavyzdžiai“, kuris buvo paskutinį kartą peržiūrėtas ir patvirtintas 2018 m. vasario 6 d., WP254 rev.01 (patvirtintą EDAV, žr. https://ec.europa.eu/newsroom/article29/items/614108); (toliau – *BDAR tinkamumo kriterijų dokumentas*).
[5] Žr. 2020 m. lapkričio 10 d. priimtas EDAV rekomendacijas Nr. 02/2020 dėl Europos pagrindinių garantijų taikant stebėjimo priemones, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_lt.

1.1. Konvergencijos sritys

5. Pagrindinis EDAV tikslas – pateikti Europos Komisijai nuomonę dėl Jungtinėje Karalystėje asmenims suteikiamos apsaugos lygio tinkamumo. Svarbu pažymėti, kad EDAV nesitiki, jog JK teisinė sistema visiškai atitiks Europos duomenų apsaugos teisę.

6. Tačiau EDAV primena, kad tam, kad būtų laikoma, kad užtikrinamas tinkamas apsaugos lygis, pagal BDAR 45 straipsnį ir Europos Sąjungos Teisingumo Teismo (toliau – ESTT) praktiką reikalaujama, kad trečiosios valstybės teisės aktai atitiktų BDAR įtvirtintų pagrindinių principų esmę. JK duomenų apsaugos sistema iš esmės grindžiama ES duomenų apsaugos sistema (visų pirma, BDAR ir Europos Parlamento ir Tarybos direktyva (ES) 2016/680 (toliau – ES teisėsaugos direktyva)), nes JK iki 2020 m. sausio 31 d. buvo ES valstybė narė. Be to, 2018 m. gegužės 23 d. įsigaliojusiame 2018 m. JK duomenų apsaugos įstatyme, kuriuo panaikintas 1998 m. JK duomenų apsaugos įstatymas, papildomai patikslintas BDAR taikymas JK teisėje, be to, juo į nacionalinę teisę perkelta ES teisėsaugos direktyva, taip pat suteikti įgaliojimai ir nustatytos pareigos nacionalinei duomenų apsaugos priežiūros institucijai – JK Informacijos komisaro biurui. Todėl EDAV pripažįsta, kad JK savo duomenų apsaugos sistemoje iš esmės atkartojo BDAR.

7. **Analizuojant trečiosios valstybės, kuri dar neseniai buvo ES valstybė narė, teisę ir praktiką, akivaizdu, kad EDAV nustatė, kad daugelis aspektų yra iš esmės lygiaverčiai.**

8. Duomenų apsaugos srityje EDAV pažymi, kad BDAR sistema ir JK teisinė sistema iš esmės sutampa dėl tam tikrų pagrindinių nuostatų, pavyzdžiui, sąvokų (pvz., asmens duomenys, asmens duomenų tvarkymas, duomenų valdytojas), teisiškai pagrįsto ir sąžiningo duomenų tvarkymo teisėtais tikslais pagrindų, tikslo apribojimo, duomenų kokybės ir proporcingumo, duomenų saugojimo, saugumo ir konfidencialumo, skaidrumo, specialiųjų kategorijų duomenų, tiesioginės rinkodaros, automatizuoto sprendimų priėmimo ir profiliavimo.

1.2. Sunkumai

9. Jungtinė Karalystė dar neseniai buvo ES valstybė narė. Todėl, analizuodama teisę ir praktiką EDAV nustatė, kad daugelis aspektų yra iš esmės lygiaverčiai. Kartu, atsižvelgdama į savo funkciją priimant išvadą dėl tinkamumo, taip pat į laiko apribojimus, EDAV nusprendė sutelkti dėmesį į tuos aspektus, į kuriuos, jos nuomone, reikia pažvelgti atidžiau ir atlikti išsamesnį patikrinimą.

10. Nepaisant to, vis dar yra neišspręstų problemų, todėl EDAV mano, kad siekiant užtikrinti iš esmės lygiavertį apsaugos lygį, reikėtų išsamiau įvertinti toliau nurodytus aspektus ir juos Jungtinėje Karalystėje turėtų atidžiai stebėti Europos Komisija.

1.2.1. Bendrieji klausimai

11. Pirmasis bendrojo pobūdžio sunkumas yra susijęs su JK visos duomenų apsaugos teisės sistemos raidos stebėsena. Iš tikrųjų JK Vyriausybė nurodė ketinanti kurti atskirą ir nepriklausomą duomenų apsaugos politiką ir galimai norinti nukrypti nuo ES duomenų apsaugos teisės. Lig šiol tokie politiniai pareiškimai JK teisinėje sistemoje dar nebuvo įgyvendinti. Tačiau dėl galimų **nukrypimų ateityje gali kilti pavojus, kad nebus išlaikytas iš ES perduodamų asmens duomenų apsaugos lygis. Todėl Europos Komisija raginama atidžiai stebėti tokius pokyčius nuo sprendimo dėl tinkamumo įsigaliojimo ir prireikus imtis reikiamų veiksmų, pavyzdžiui, pakeisti ir (arba) sustabdyti sprendimą.**

1.2.2. Bendrieji duomenų apsaugos aspektai

12. Pirma, vadinamosios „**imigracijos išimties**“, nustatytos **2018 m. Duomenų apsaugos įstatymo 2 priedo 1 dalies** 4 punkte, **formuluotė yra „plati“**. Visų pirma ji taikoma ir tuo atveju, kai duomenų valdytojas nerenka asmens duomenų imigracijos kontrolės tikslais, bet juos pateikia kitam duomenų valdytojui, kuris tokius asmens duomenis tvarko imigracijos kontrolės tikslais.

13. EDAV ragina Europos Komisiją patikrinti proceso eigą *Open Rights Group & Anor, R (On the Application Of) prieš Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin)* ir, kadangi sprendimas nėra galutinis (*res judicata*), patikrinti, ar jis patvirtintas, ar peržiūrėtas apeliacinio teismo sprendimu, atsižvelgiant į visus su tuo susijusius atnaujinimus ir nurodant juos sprendime. **EDAV taip pat ragina Europos Komisiją sprendime dėl tinkamumo pateikti daugiau informacijos apie imigracijos išimtį[6], visų pirma dėl tokio plataus pobūdžio išimties JK teisėje būtinumo ir proporcingumo, ypač atsižvelgiant į plačią taikymo sritį *ratione personae*.** Kartu EDAV ragina Europos Komisiją toliau nagrinėti, ar JK teisinėje sistemoje yra papildomų apsaugos priemonių arba ar jos galėtų būti numatytos, pavyzdžiui, teisiškai privalomomis priemonėmis, kuriomis būtų papildyta imigracijos išimtis, padidinant jos numatomumą ir duomenų subjektų apsaugos priemones, taip pat sudarant sąlygas geriau ir greičiau įvertinti ir stebėti būtinumo ir proporcingumo reikalavimus.

14. Antra, nors EDAV pripažįsta, kad JK duomenų apsaugos sistemoje iš esmės atkartojo BDAR V skyrių, EDAV nustatė tam tikrus JK teisinės sistemos aspektus, **susijusius su tolesniu duomenų perdavimu**, dėl kurių gali sumažėti iš EEE perduotų asmens duomenų apsaugos lygis.

15. Iš tiesų BDAR 44 straipsnyje[7] nustatyta, kad asmens duomenys perduodami ir toliau perduodami tik tuo atveju, jei nepakenkiama BDAR garantuojamam fizinių asmenų apsaugos lygiui. **Tai reiškia, kad pagal būsimą sprendimą dėl tinkamumo JK teisės aktai, susiję su asmens duomenų, perduodamų į JK, tvarkymu, turi būti ne tik „iš esmės lygiaverčiai“ ES teisės aktams, bet ir kad JK taikomomis taisyklėmis dėl tolesnio šių duomenų perdavimo į trečiąsias valstybes toliau būtų užtikrinamas iš esmės lygiavertis duomenų apsaugos lygis.**

16. Nors EDAV atkreipia dėmesį, kad JK turi pajėgumus pagal savo teisinę sistemą pripažinti teritorijas kaip užtikrinančias tinkamą apsaugos lygį pagal JK duomenų apsaugos sistemą, EDAV norėtų pabrėžti, kad šios teritorijos iki šiol negali pasinaudoti Europos Komisijos priimtu sprendimu dėl tinkamumo ir užtikrinti „iš esmės lygiavertį“ apsaugos lygį tam, kuris garantuojamas EEE. Dėl to gali kilti pavojus, kad nebus užtikrinta iš EEE perduodamų asmens duomenų apsauga, ypač jei ateityje JK duomenų apsaugos sistema skirsis nuo Sąjungos *acquis*. Be to, JK jau pripažino tinkamomis trečiąsias valstybes,

[6] Taip pat kai bus pateiktos šiuo metu vykdomos imigracijos išimties taikymo peržiūros išvados, kaip nurodyta 2020 m. kovo 13 d. JK Vyriausybės Aiškinamojo dokumento dėl sprendimų dėl tinkamumo E3 skirsnio „2 priedo apribojimai“ 5 p., https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf.

[7] *„Asmens duomenys, kurie yra tvarkomi arba kuriuos ketinama tvarkyti juos perdavus į trečiąją valstybę arba tarptautinei organizacijai, perduodami tik tuo atveju, jei duomenų valdytojas ir duomenų tvarkytojas, laikydamiesi kitų šio reglamento nuostatų, laikosi šiame skyriuje nustatytų sąlygų, be kita ko, susijusių su tolesniu asmens duomenų perdavimu iš tos trečiosios valstybės ar tarptautinės organizacijos į kitą trečiąją šalį ar kitai tarptautinei organizacijai. Visos šio skyriaus nuostatos taikomos siekiant užtikrinti, kad nebūtų pakenkta šiuo reglamentu garantuojamam fizinių asmenų apsaugos lygiui.*“

kurioms pagal Direktyvą 95/46/EB[8] Europos Komisija pateikė išvadą dėl tinkamumo, o Europos Komisija netrukus peržiūrės šias išvadas ir šios peržiūros išvados dar nežinomos.

17. **Pirmiau nurodytais atvejais Europos Komisija turėtų vykdyti savo stebėsenos funkciją, o jei neišlaikomas iš esmės lygiavertis iš EEE perduotų asmens duomenų apsaugos lygis, Europos Komisija turėtų apsvarstyti galimybę iš dalies pakeisti sprendimą dėl tinkamumo, kad būtų nustatytos konkrečios iš EEE perduotų duomenų apsaugos priemonės ir (arba) sustabdytas sprendimo dėl tinkamumo galiojimas.**

18. **Kalbant apie JK ir trečiųjų valstybių sudarytus tarptautinius susitarimus**, Europos Komisija raginama išnagrinėti JK duomenų apsaugos sistemos ir jos tarptautinių įsipareigojimų, ne vien JK ir Jungtinių Amerikos Valstijų (toliau – JAV) susitarimą dėl prieigos prie elektroninių duomenų siekiant kovoti su sunkiais nusikaltimais[9] (toliau – JK ir JAV susitarimas pagal CLOUD įstatymą), sąveiką, visų pirma siekiant užtikrinti apsaugos lygio tęstinumą, kai asmens duomenys perduodami iš ES į JK remiantis JK sprendimu dėl tinkamumo, o vėliau toliau perduodami į kitas trečiąsias valstybes, ir nuolat stebėti ir prireikus imtis veiksmų, jei dėl JK ir trečiųjų valstybių sudarytų tarptautinių susitarimų kyla pavojus, kad gali sumažėti ES nustatytas asmens duomenų apsaugos lygis.

19. Be to, Europos Komisijos prašoma stebėti, ar JK ir JAV susitarimu pagal CLOUD įstatymą užtikrinamos tinkamos papildomos apsaugos priemonės, atsižvelgiant į neskelbtiną atitinkamų kategorijų duomenų pobūdį ir vienintelius reikalavimus, susijusius su elektroninių įrodymų perdavimu, atliekamu tiesiogiai paslaugų teikėjų, o ne tarp institucijų, taip pat įvertinant, kokiomis aplinkybėmis apsaugos priemonės gali būti užtikrintos tinkamai įgyvendinant ES ir JAV bendrąjį susitarimą[10].

20. Be to, EDAV pažymi, kad tolesnis duomenų perdavimas iš JK į kitą trečiąją valstybę taip pat gali būti vykdomas remiantis **duomenų perdavimo priemonėmis pagal JK taikomus duomenų apsaugos teisės aktus**[11]. Atsižvelgdama į Sprendimą *Schrems II*[12], EDAV ragina Europos Komisiją sprendime dėl tinkamumo užtikrinti, kad būtinos apsaugos priemonės bus veiksmingai įgyvendintos atsižvelgiant ir į gaunančiosios trečiosios valstybės teisės aktus.

21. Atsižvelgiant į tai, kad JK teisės aktais nėra užtikrinama **apsauga pagal BDAR 48 straipsnį**, EDAV ragina Europos Komisiją pateikti papildomų garantijų ir konkrečių nuorodų į JK teisės aktus, kuriomis būtų užtikrinama, kad apsaugos lygis pagal JK teisinę sistemą iš esmės prilygsta EEE garantuojamam apsaugos lygiui.

22. Dėl **procedūrinių ir vykdymo užtikrinimo mechanizmų** EDAV pažymi, kad pagrindiniai elementai, kuriais turi pasižymėti Europos duomenų apsaugos sistemą atitinkanti duomenų apsaugos sistema, yra nepriklausoma priežiūros institucija ir veiksmingas jos veikimas, sistema, kuria užtikrinamas geras atitikties lygis, ir prieigos prie tinkamų teisių gynimo mechanizmų sistema, suteikianti asmenims EEE

[8] 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (OL L 281, 1995 11 23, p. 31).
[9] Žr. 2019 m. spalio 3 d. Jungtinės Didžiosios Britanijos ir Šiaurės Airijos Karalystės Vyriausybės ir Jungtinių Amerikos Valstijų Vyriausybės susitarimą dėl prieigos prie elektroninių duomenų siekiant kovoti su sunkiais nusikaltimais, Vašingtonas, JAV, https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019.
[10] Žr. 2016 m. gruodžio mėn. Jungtinių Amerikos Valstijų ir Europos Sąjungos susitarimą dėl su nusikalstamų veikų prevencija, tyrimu, atskleidimu ir baudžiamuoju persekiojimu susijusios asmeninio pobūdžio informacijos apsaugos (toliau – ES ir JAV bendrasis susitarimas), https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=LEGISSUM:3104_8&from=EN.
[11] Žr. JK BDAR 46 ir 47 straipsnius.
[12] Žr. Sprendimą *Schrems II*.

galimybę naudotis savo teisėmis ir reikalauti žalos atlyginimo be sudėtingų administracinių ir teisminių kliūčių.

23. EDAV pripažįsta, kad JK bendrajame duomenų apsaugos reglamente ir 2018 m. JK duomenų apsaugos įstatyme JK didžiąja dalimi atkartojo atitinkamas BDAR nuostatas, vis dėlto Europos Komisija raginama nuolat stebėti bet kokius JK teisinės sistemos ir praktikos pokyčius, dėl kurių šioms sritims gali būti padarytas neigiamas poveikis.

1.2.3. Dėl valdžios institucijų teisės susipažinti su duomenimis, perduotais į JK

24. EDAV atkreipia dėmesį į reikšmingus JK teisinės sistemos, taikomos saugumo ir žvalgybos agentūroms, pokyčius, visų pirma susijusius su ryšių duomenų perėmimu ir rinkimu. EDAV supranta, kad šie pakeitimai, *inter alia*, yra atsakas į ESTT ir Europos Žmogaus Teisių Teisme (toliau – EŽTT) pradėtus procesus ir jų naujausius sprendimus šiuo klausimu.

25. Visų pirma, EDAV palankiai vertina tai, kad JK įsteigė Tyrimo įgaliojimų teismą. Tyrimo įgaliojimų teismas yra kompetentingas nagrinėti bylas, susijusias ne tik su teisėsaugos institucijų, bet ir su žvalgybos tarnybų naudojimusi tyrimo įgaliojimais. Todėl, EDAV nuomone, Tyrimo įgaliojimų teismas veikia kaip tinkamas teismas, kaip apibrėžta Europos Sąjungos pagrindinių teisių chartijos (toliau – ES chartija) 47 straipsnyje.

26. Be to, EDAV teigiamai vertina tai, kad 2016 m. Tyrimo įgaliojimų įstatyme įtvirtinti „teismo komisarai“. Tai yra reikšmingas patobulinimas. Ji mano, kad svarbi teismo komisarų funkcija yra atskirais atvejais *ex ante* patvirtinti įvairias sekimo priemones, įskaitant tikslinį ryšio duomenų perėmimą ir masinį rinkimą (vadinamoji dvigubo patvirtinimo procedūra).

27. Tačiau, siekdama įvertinti šio papildomo priežiūros lygio veiksmingumą, EDAV mano, kad reikia išsamiau paaiškinti, kokiais atvejais galimas teisėtas duomenų perėmimas be Tyrimų įgaliojimų komisaro arba teismo komisarų patvirtinimo, ir ragina Europos Komisiją tai išsamiau įvertinti ir įrodyti, kad net ir tais atvejais, kai netaikoma dvigubo patvirtinimo procedūra, JK teisinėje sistemoje numatytos tinkamos apsaugos priemonės, įskaitant veiksmingą *ex post* priežiūrą ir asmenims suteikiamas teisių gynimo galimybes, taip užtikrinant iš esmės lygiavertį apsaugos lygį kaip ir ES.

28. Be to, EDAV ragina Europos Komisiją išsamiai įvertinti sąlygas, kuriomis gali būti taikoma skuba, ir pateikti paaiškinimus dėl galimų atitinkamų duomenų subjektų teisių įgyvendinimo būdų ir jiems siūlomų teisių gynimo būdų, susijusių su įrangos perėmimo operacijomis, visų pirma tuo atveju, kai nukrypstama nuo dvigubo patvirtinimo procedūros.

29. Be to, EDAV mano, kad reikia toliau patikslinti ir įvertinti masinio duomenų perėmimo atvejus, visų pirma selektorių atranką ir taikymą, siekiant išsiaiškinti, kokiu mastu prieiga prie asmens duomenų atitinka ESTT nustatytą ribą ir kokios apsaugos priemonės taikomos siekiant apsaugoti asmenų, kurių duomenys perimami šiomis aplinkybėmis, pagrindines teises, be kita ko, susijusias su duomenų saugojimo laikotarpiais. Nepriklausomas JK kompetentingų priežiūros institucijų vertinimas būtų ypač naudingas. EDAV taip pat pabrėžia, kad dar svarbiau atrodo tai, jog „su užjūrio valstybėmis susiję ryšiai“, kuriems taikoma masinio duomenų perėmimo praktika, reiškia, kad JK galėtų tiesiogiai perimti ir masiškai rinkti duomenis ES, įskaitant tranzitu tarp ES ir Jungtinės Karalystės perduodamus duomenis, kurie patektų į sprendimo projekto taikymo sritį. Atsižvelgdama į šio aspekto svarbą, EDAV ragina Europos Komisiją atidžiai stebėti pokyčius šioje srityje.

30. Kalbant apie masinį duomenų perėmimą, EDAV pabrėžia, kad EŽTT ir ESTT nuosekliai atlieka vertinimą, ir primena susirūpinimą keliančius klausimus, iškeltus dėl antrinių duomenų, kuriems dėl jų neskelbtino pobūdžio turėtų būti taikomos specialios apsaugos priemonės. Todėl EDAV ragina

Europos Komisiją atidžiai įvertinti, ar pagal JK teisę tokiai asmens duomenų kategorijai numatytos apsaugos priemonės užtikrina iš esmės lygiavertį apsaugos lygį tam, kuris garantuojamas EEE.

31. Šiomis aplinkybėmis EDAV žino, kad 2016 m. Žvalgybos ir saugumo komiteto vieša ataskaita dėl su masiniais duomenimis susijusių įgaliojimų naudojimo[13] yra susijusi su praktika, taikyta pagal ankstesnę teisinę sistemą, kurią vėliau pakeitė 2016 m. Tyrimo įgaliojimų įstatymas. Vis dėlto Valdyba mano, kad JK kompetentingos priežiūros institucijos turi toliau nepriklausomai vertinti ir prižiūrėti automatizuotų duomenų tvarkymo priemonių naudojimą, ir ragina Europos Komisiją toliau vertinti šį klausimą ir apsaugos priemones, kurios šiomis aplinkybėmis būtų ir (arba) galėtų būti suteiktos EEE duomenų subjektams.

32. EDAV pritaria Tyrimų įgaliojimų komisaro išsakytai nuomonei, kad būtina tolesnė peržiūra ir stebėsena siekiant užtikrinti, kad apsaugos priemonės, kurias praktikoje taiko kompetentingos institucijos nacionalinio saugumo ir žvalgybos srityje, siekdamos ištaisyti atitinkamų teisės aktų taikymo neatitikimus, būtų išlaikytos ir nuolat tobulinamos. EDAV taip pat palankiai vertina tai, kad dėl to 2019 m. Tyrimų įgaliojimų komisaras atliko savo požiūrio į masinio duomenų perėmimo tikrinimą peržiūrą, „*kuri apėmė kruopščią techniškai sudėtingų būdų, kuriais faktiškai įgyvendinamas masinis duomenų perėmimas, peržiūrą*“, ir įsipareigojo nuo 2020 m. į masinio duomenų perėmimo tikrinimus įtraukti „*išsamų selektorių ir paieškos kriterijų, apie kuriuos pirmiau užsiminė EŽTT, nagrinėjimą*“. Atsižvelgiant į šio aspekto svarbą, EDAV susirūpinimą kelia tai, kad Tyrimų įgaliojimų komisaras dar neatliko išsamaus selektorių ir paieškos kriterijų patikrinimo, ir ji ragina Europos Komisiją atidžiai stebėti pokyčius šioje srityje, visų pirma dėl to, kad konkreti tokios priežiūros forma dar turi būti patikslinta.

33. EDAV pabrėžia, kad, kai kalbama apie užjūrio valstybėse atskleidžiamą informaciją, taikant JK teisėje numatytą nacionalinio saugumo išimtį, gali trūkti apsaugos priemonių, kuriomis būtų užtikrinama, kad taip pat laikomasi tikslo apribojimo, būtinumo ir proporcingumo principų, arba kuriomis būtų numatoma, kad trečiojoje paskirties valstybėje būtų užtikrintos arba gerbiamos pakankamos asmenų teisės, priežiūra ir teisių gynimo priemonės. Todėl EDAV rekomenduoja Europos Komisijai toliau nagrinėti bendras apsaugos priemones, numatytas JK teisėje, kai kalbama apie informacijos atskleidimą užjūrio valstybėse, visų pirma atsižvelgiant į nacionalinio saugumo išimčių taikymą.

34. Galiausiai, EDAV nerimauja dėl kitų keitimosi informacija ir jos atskleidimo formų, remiantis kitais dokumentais, visų pirma įvairiais tarptautiniais susitarimais, kuriuos JK yra sudariusi su kitomis trečiosiomis valstybėmis, visų pirma tais atvejais, kai šie dokumentai neprieinami visuomenei, pavyzdžiui, Jungtinės Karalystės ir JAV susitarimu dėl ryšių žvalgybos. Dėl tokio susitarimo poveikio galėtų būti apeinamos apsaugos priemonės, nustatytos norint susipažinti su asmens duomenimis ir juos naudoti nacionalinio saugumo tikslais. EDAV mano, kad dvišalių ar daugiašalių susitarimų su trečiosiomis valstybėmis sudarymas žvalgybinio bendradarbiavimo tikslais, kuriais suteikiamas teisinis pagrindas tiesiogiai perimti ir rinkti asmens duomenis arba perduoti asmens duomenis į šias valstybes, taip pat gali turėti didelės įtakos tolesnio surinktos informacijos naudojimo sąlygoms, nes tikėtina, kad tokie susitarimai turės įtakos vertinamai JK duomenų apsaugos teisinei sistemai.

1.3. Išvada

[13] Žr. 2016 m. rugpjūčio mėn. nepriklausomo kovos su terorizmu teisės aktų vertintojo parengtą su masiniais duomenimis susijusių įgaliojimų peržiūros ataskaitą, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf.

35. EDAV mano, kad JK tinkamumo vertinimas yra unikalus, nes anksčiau JK turėjo ES valstybės narės statusą. Be to, tai taip pat būtų pirmasis sprendimas dėl tinkamumo, į kurį būtų įtraukta laikinojo galiojimo sąlyga.

36. Savo ruožtu EDAV pripažįsta daug JK ir ES duomenų apsaugos sistemų konvergencijos sričių. Tačiau tuo pat metu ir atlikusi kruopščią Europos Komisijos sprendimo projekto ir JK duomenų apsaugos teisės aktų analizę, EDAV nustatė keletą problemų, kurios išsamiai nagrinėjamos šioje nuomonėje. Šiomis aplinkybėmis EDAV norėtų pabrėžti svarbiausią Europos Komisijos įpareigojimą stebėti visus susijusius pokyčius JK.

37. Atsižvelgdama į tai, kas išdėstyta pirmiau, EDAV rekomenduoja Europos Komisijai spręsti šioje nuomonėje iškeltus uždavinius. EDAV taip pat ragina Europos Komisiją atidžiai stebėti visus atitinkamus pokyčius JK, kurie gali turėti įtakos esminiam asmens duomenų apsaugos lygio lygiavertiškumui, ir prireikus skubiai imtis atitinkamų veiksmų.

2. ĮVADAS

2.1. JK duomenų apsaugos sistema

38. JK duomenų apsaugos sistema iš esmės grindžiama ES duomenų apsaugos sistema (visų pirma BDAR ir ES teisėsaugos direktyva), nes JK iki 2020 m. sausio 31 d. buvo ES valstybė narė. Be to, 2018 m. gegužės 23 d. įsigaliojusiame 2018 m. JK duomenų apsaugos įstatyme, kuriuo panaikintas 1998 m. JK duomenų apsaugos įstatymas, papildomai patikslintas BDAR taikymas JK teisėje, be to, juo į nacionalinę teisę perkelta ES teisėsaugos direktyva, taip pat suteikti įgaliojimai ir nustatytos pareigos nacionalinei duomenų apsaugos priežiūros institucijai – JK Informacijos komisaro biurui.

39. Kaip minėta Europos Komisijos sprendimo projekto 12 konstatuojamojoje dalyje, JK Vyriausybė priėmė 2018 m. (išstojimo iš) Europos Sąjungos aktą, kuriuo tiesiogiai taikomi ES teisės aktai įtraukiami į Jungtinės Karalystės teisę. Pagal šį aktą JK ministrai turi įgaliojimus priimti antrinės teisės aktus, pasitelkdami įstatymų lydimuosius teisės aktus, kad po išstojimo iš ES Jungtinė Karalystė atliktų būtinus paliktos galioti ES teisės pakeitimus, kad ji atitiktų šalies vidaus aplinkybes.

40. Taigi pasibaigus pereinamajam laikotarpiui[14] JK taikomą atitinkamą teisinę sistemą sudaro:

- Jungtinės Karalystės bendrasis duomenų apsaugos reglamentas (toliau – JK BDAR), įtrauktas į JK teisę pagal 2018 m. (išstojimo iš) Europos Sąjungos aktą, iš dalies pakeistas 2019 m. Duomenų apsaugos, privatumo ir elektroninių ryšių (pakeitimai ir kt.) (išstojimo iš ES) taisyklėmis (toliau – DAPER taisyklės);
- 2018 m. Duomenų apsaugos įstatymas su pakeitimais, padarytais 2019 m. DAPER taisyklėmis ir 2020 m. Duomenų apsaugos, privatumo ir elektroninių ryšių (pakeitimai ir kt.) (išstojimo iš ES) taisyklėmis, ir
- 2016 m. Tyrimo įgaliojimų įstatymas

(toliau kartu – JK duomenų apsaugos sistema).

[14] Pereinamasis laikotarpis nustatytas iki 2020 m. gruodžio 31 d., po kurio JK nebetaikoma ES teisė. „Tarpinis laikotarpis“ nustatytas ne vėliau kaip iki 2021 m. birželio 30 d. ir reiškia papildomą laikotarpį, per kurį asmens duomenų perdavimas iš EEE į JK nelaikomas duomenų perdavimu.

2.2. EDAV vertinimo sritis

41. Europos Komisijos sprendimo projektas parengtas atlikus JK duomenų apsaugos sistemos vertinimą, po kurio surengtos diskusijos su JK Vyriausybe. Pagal BDAR 70 straipsnio 1 dalies s punktą tikimasi, kad EDAV pateiks nepriklausomą nuomonę dėl Europos Komisijos išvadų, nustatys tinkamumo sistemos trūkumus, jei tokių yra, ir stengsis pateikti pasiūlymų, kaip juos pašalinti.

42. Kaip minėta BDAR tinkamumo kriterijų dokumente: „*Europos Komisijos suteikta informacija turėtų būti išsami ir sudaryti sąlygas Europos duomenų apsaugos valdybai atlikti savo vertinimą, susijusį su duomenų apsaugos lygiu trečiojoje valstybėje.*“[15]

43. Šiuo klausimu reikia pažymėti, kad EDAV laiku gavo tik dalį dokumentų, reikšmingų norint ištirti JK teisinę sistemą. Didžiąją dalį sprendimo projekte nurodytų JK teisės aktų EDAV gavo iš nuorodų, kurios pateiktos sprendimo projekte. Europos Komisija negalėjo EDAV pateikti rašytinių paaiškinimų ir JK įsipareigojimų, susijusių su JK valdžios institucijų ir Europos Komisijos pasikeitimu informacija, susijusia su šia veikla[16].

44. Atsižvelgdama į tai, kas išdėstyta pirmiau, ir į ribotą laiką (2 mėnesius), kurį EDAV turėjo šiai nuomonei priimti, EDAV nusprendė sutelkti dėmesį į kai kuriuos konkrečius sprendimo projekte pateiktus punktus ir pateikti jų analizę bei nuomonę.

45. Analizuojant trečiosios valstybės, kuri dar neseniai buvo ES valstybė narė, teisę ir praktiką, akivaizdu, kad EDAV nustatė, kad daugelis aspektų yra iš esmės lygiaverčiai. Atsižvelgdama į savo vaidmenį priimant išvadą dėl tinkamumo ir į analizuotinų teisės aktų ir praktikos kiekį, EDAV nusprendė sutelkti dėmesį į tuos aspektus, kuriuos, jos manymu, reikia išnagrinėti atidžiau. Be to, vadovaujantis ESTT praktika, labai svarbi analizės dalis apima nacionalinio saugumo institucijų galimybės susipažinti su į JK perduodamų asmens duomenų teisiniu režimu ir JK nacionalinio saugumo sistemos praktiką. Tačiau reikia atsižvelgti į tai, kad nacionalinis saugumas akivaizdžiai yra teisės ir praktikos sritis, kurioje valstybių narių teisės aktai nėra suderinti ES lygmeniu, todėl gali skirtis.

46. EDAV atsižvelgė į taikomą Europos duomenų apsaugos sistemą, įskaitant ES chartijos 7, 8 ir 47 straipsnius, kuriais atitinkamai ginama teisė į privatų ir šeimos gyvenimą, teisė į asmens duomenų apsaugą, teisė į veiksmingą teisinę gynybą ir teisingą bylos nagrinėjimą, ir Europos žmogaus teisių

[15] Žr. WP254 rev.01, p. 3.

[16] Susijusia su: BDAR 48 straipsniu (sprendimo projekto 78 išnaša); sustiprintomis apsaugos priemonėmis ir saugumo priemonėmis, kurias duomenų valdytojai taiko tvarkydami duomenis nacionalinio saugumo kontekste (sprendimo projekto 64 išnaša); reikalavimu, kad duomenų valdytojas kiekvienu konkrečiu atveju apsvarstytų, ar reikia remtis išimtimi, net jei išduotas nacionalinio saugumo sertifikatas (sprendimo projekto 126 konstatuojamoji dalis ir 172 išnaša); tuo, kad ES ir JAV bendrojo susitarimo apsaugos priemonės bus taikomos visai pagal JK ir JAV susitarimą pagal CLOUD įstatymą parengtai ar saugomai asmens informacijai, neatsižvelgiant į prašymą pateikusios įstaigos pobūdį ar tipą, atsižvelgiant į konkretaus duomenų apsaugos priemonių įgyvendinimo duomenis, dėl kurių JK ir JAV vis dar diskutuoja, patvirtinimu, kad JK valdžios institucijos leis šiam susitarimui įsigalioti tik tada, kai įsitikins, kad jo įgyvendinimas atitinka jame numatytus teisinius įsipareigojimus, įskaitant aiškumą dėl bet kokių duomenų, kurių prašoma pagal šį susitarimą, atitikties duomenų apsaugos standartams (sprendimo projekto 153 konstatuojamoji dalis); situacijomis, kai duomenys perduodami iš ES į JK pagal šio sprendimo projekto taikymo sritį, ir tuo, kad visada bus „ryšys su Didžiosios Britanijos salomis", todėl bet kokiam įrangos perėmimui, kuris apima tokius duomenis, bus taikomas 2016 m. Tyrimo įgaliojimų įstatymo 13 skirsnio 1 dalyje nustatytas privalomo orderio reikalavimas (sprendimo projekto 206 konstatuojamoji dalis), ir pateiktais veiklos tikslų pavyzdžiais (sprendimo projekto 216 konstatuojamoji dalis ir 369 išnaša).

konvencijos (toliau – EŽTK) 8 straipsnį, kuriuo ginama teisė į privatų ir šeimos gyvenimą. Be to, EDAV atsižvelgė į BDAR reikalavimus ir atitinkamą teismų praktiką.

47. Šios veiklos tikslas – pateikti Europos Komisijai nuomonę dėl apsaugos lygio JK tinkamumo vertinimo. Sąvoką „tinkamo lygio apsauga“, kuri jau buvo apibrėžta Direktyvoje 95/46/EB, toliau išplėtojo Europos Sąjungos Teisingumo Teismas. Svarbu priminti Sprendime *Schrems I*, Europos Sąjungos Teisingumo Teismo nustatytą standartą, t. y. kad nors „apsaugos lygis“ trečiojoje valstybėje privalo būti „iš esmės lygiavertis“ tam, kuris garantuojamas ES, priemonės „*kurių ši trečioji valstybė šiuo klausimu imasi siekdama užtikrinti tokį apsaugos lygį, gali skirtis nuo priemonių, kurios [...] taikomos ES*“[17]. Todėl tikslas – ne atitikti kiekvieną Europos Sąjungos teisės akto punktą, o nustatyti pagrindinius, esmę perteikiančius to teisės akto reikalavimus. Tinkamumas gali būti pasiektas derinant duomenų subjektų teises ir prievoles, taikomas tiems, kas tvarko duomenis, arba tiems, kas kontroliuoja tokį nepriklausomų įstaigų vykdomą duomenų tvarkymą ir priežiūrą. Tačiau duomenų apsaugos taisyklės veiksmingos tik tada, jei galima užtikrinti jų vykdymą ir jomis vadovautis praktiškai. Todėl, siekiant užtikrinti tokių taisyklių veiksmingumą, svarbu apsvarstyti ne tik asmens duomenims, perduotiems trečiajai valstybei arba tarptautinei organizacijai, taikomų taisyklių turinį, bet ir veikiančią sistemą. Efektyvūs vykdymo užtikrinimo mechanizmai yra itin svarbūs siekiant, kad duomenų apsaugos taisyklės būtų veiksmingos[18].

2.3. Bendrosios pastabos ir susirūpinimą keliantys klausimai

2.3.1. JK prisiimti tarptautiniai įsipareigojimai

48. Pagal BDAR 45 straipsnio 2 dalies c punktą ir BDAR tinkamumo kriterijų dokumentą[19], vertindama trečiosios valstybės apsaugos lygio tinkamumą, Europos Komisija, be kita ko, atsižvelgia į trečiosios valstybės prisiimtus tarptautinius įsipareigojimus arba kitus įsipareigojimus, kylančius iš trečiosios valstybės dalyvavimo daugiašalėse ar regioninėse sistemose, visų pirma susijusius su asmens duomenų apsauga, taip pat į tokių įsipareigojimų įgyvendinimą. Be to, reikėtų atsižvelgti į trečiosios valstybės prisijungimą prie 1981 m. sausio 28 d. Europos Tarybos konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu[20] (toliau – Konvencija Nr. 108) ir jos papildomo protokolo[21].

49. **Šiuo atžvilgiu EDAV palankiai vertina tai, kad JK laikosi EŽTK nuostatų ir yra EŽTT jurisdikcijoje. Be to, JK taip pat prisijungė prie Konvencijos Nr. 108 ir jos papildomo protokolo, 2018 m. pasirašė Konvenciją Nr. 108+[22] ir šiuo metu rengiasi ją ratifikuoti.**

[17] Žr. 2015 m. spalio 6 d. ESTT sprendimo *Maximilian Schrems prieš Data Protection Commissioner*, C-362/14, ECLI:EU:C:2015:650 (toliau – Sprendimas *Schrems I*), 73–74 punktus.
[18] Žr. WP254 rev.01, p. 2.
[19] Žr. WP254 rev.01, p. 2.
[20] Žr. 1981 m. sausio 28 d. Konvenciją dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (Konvencija Nr. 108).
[21] Žr. Konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu Papildomą protokolą dėl priežiūros institucijų ir valstybės sienas kertančių duomenų srautų, kuris buvo pateiktas pasirašyti 2001 m. lapkričio 8 d.
[22] Žr. 2018 m. gegužės 18 d. Protokolą, kuriuo iš dalies keičiama Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (Konvencija Nr. 108+).

2.3.2. Galimi būsimi JK duomenų apsaugos sistemos skirtumai

50. Kaip minėta sprendimo projekto 281 konstatuojamojoje dalyje, Europos Komisija turi atsižvelgti į tai, kad pasibaigus Susitarime dėl išstojimo[23] numatytam pereinamajam laikotarpiui, JK administruoja, taiko ir įgyvendina savo duomenų apsaugos tvarką, o kai tik nustos galioti ES ir JK prekybos ir bendradarbiavimo susitarimo[24] FINPROV.10A straipsnyje numatyta tarpinė nuostata, tai visų pirma gali reikšti sprendimo projekte įvertintos duomenų apsaugos sistemos pakeitimus, taip pat kitus susijusius pokyčius.

51. Todėl Europos Komisija nusprendė į sprendimo projektą[25] įtraukti laikinojo galiojimo sąlygą, nustatydama, kad jis nustos galioti praėjus ketveriems metams nuo įsigaliojimo.

52. Svarbu pažymėti, kad dėl to, kad pasibaigus pereinamajam laikotarpiui JK ministrai ir JK valstybės sekretorius turi galimybę priimti antrinės teisės aktus, JK duomenų apsaugos sistema ateityje gali labai skirtis nuo ES duomenų apsaugos sistemos.

53. Iš tikrųjų JK Vyriausybė nurodė ketinanti kurti atskirą ir nepriklausomą duomenų apsaugos politiką, dėl kurios duomenų apsaugos teisė galimai skirsis nuo ES duomenų apsaugos teisės[26]. Šis ketinimas apima asmens duomenų aspektų įtraukimą į prekybos susitarimus[27], o tokia praktika kelia riziką, kad sumažės JK nustatytas asmens duomenų apsaugos lygis[28].

---

[23] Žr. Susitarimą dėl Jungtinės Didžiosios Britanijos ir Šiaurės Airijos Karalystės išstojimo iš Europos Sąjungos ir Europos atominės energijos bendrijos (OL L 029, 2020 1 31, p. 7).

[24] Žr. Europos Sąjungos bei Europos atominės bendrijos ir Jungtinės Didžiosios Britanijos ir Šiaurės Airijos Karalystės prekybos ir bendradarbiavimo susitarimą (OL L 444, 2020 12 31, p. 14).

[25] Žr. sprendimo projekto 4 straipsnį. Taip pat žr. sprendimo projekto 282 konstatuojamąją dalį.

[26] Viena iš JK Nacionalinėje duomenų strategijoje (paskutinį kartą atnaujinta 2020 m. gruodžio 9 d., https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy) nurodytų misijų yra tokia: *„Tarptautinio duomenų srauto skatinimas. Tarpvalstybinis informacijos srautas skatina pasaulines verslo operacijas, tiekimo grandines ir prekybą, o tai skatina augimą visame pasaulyje. Jis taip pat atlieka platesnį vaidmenį visuomenėje. Perduodant asmens duomenis užtikrinama, kad žmonėms būtų mokami atlyginimai, ir padedama jiems susisiekti su artimaisiais, gyvenančiais užsienyje. Kaip parodė koronaviruso pandemija, dalijimasis sveikatos duomenimis gali padėti atlikti gyvybiškai svarbius mokslinius ligų tyrimus ir suvienyti valstybes jų atsakui į pasaulines sveikatos krizes.* ***Išstojusi iš Europos Sąjungos, JK skatins naudotis duomenų teikiama nauda.*** *Skatinsime geriausią vidaus praktiką ir bendradarbiausime su tarptautiniais partneriais,* ***siekdami užtikrinti, kad duomenų netinkamai nevaržytų valstybių sienos ir fragmentiškos reguliavimo sistemos****, kad jie galėtų būti visapusiškai naudojami.“* (paryškinta autoriaus).

[27] Ten pat: *„Tarpvalstybinių duomenų srautų palengvinimas.* ***Dirbsime pasauliniu mastu, kad pašalintume nereikalingas kliūtis tarptautiniams duomenų srautams. Derybose dėl prekybos susitarsime dėl ambicingų nuostatų dėl duomenų*** *ir pasinaudosime savo nauja nepriklausoma vieta Pasaulio prekybos organizacijoje, kad darytume įtaką geresnių prekybos duomenimis taisyklių kūrimui.* ***Šalinsime kliūtis tarptautiniam duomenų perdavimui****, kuriuo skatinamas augimas ir inovacijos, be kita ko, plėtosime naujus JK pajėgumus, kurie užtikrins naujus ir novatoriškus tarptautinio duomenų perdavimo mechanizmus. Taip pat bendradarbiausime su G20 partneriais, kad sukurtume nacionalinių duomenų sistemų sąveiką ir sumažintume nesutarimus perduodant duomenis iš vienos valstybės į kitą.“* (paryškinta autoriaus).

[28] Žr. 2017 m. gruodžio 12 d. Europos Parlamento rezoliucijos *„Skaitmeninės prekybos strategijos kūrimas“* (2017/2065(INI)), V skirsnį, kuriame pabrėžiama, kad *„[ES] sudarant prekybos susitarimus negali būti jokių derybų dėl asmens duomenų apsaugos*“, nuoroda: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0488_LT.pdf. Taip pat žr. 2021 m. kovo 25 d. Europos Parlamento rezoliucijos dėl Komisijos vertinimo ataskaitos dėl Bendrojo duomenų apsaugos reglamento įgyvendinimo praėjus dvejiems metams nuo jo taikymo pradžios, 28 punktą, kuriame teigiama, kad *„[EP] remia Komisijos praktiką duomenų apsaugos ir asmens duomenų srautų klausimus spręsti atskirai nuo prekybos susitarimų“*, https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_LT.pdf.

54. Galiausiai, nuo pereinamojo laikotarpio pabaigos JK ne tik nebėra saistoma ESTT praktikos, bet ir jau priimti ESTT sprendimai, kurie laikomi JK teisinėje sistemoje palikta galioti teismų praktika, gali būti neprivalomi JK, nes pasibaigus tarpiniam laikotarpiui JK turi galimybę keisti išlaikytą ES teisę, o jos Aukščiausiasis Teismas nėra saistomas paliktos galioti ES teismų praktikos[29].

55. **Atsižvelgdama į riziką, susijusią su galimais JK duomenų apsaugos sistemos nukrypimais nuo ES *acquis* pasibaigus tarpiniam laikotarpiui, EDAV palankiai vertina Europos Komisijos sprendimą sprendimo projektui nustatyti ketverių metų laikinojo galiojimo sąlygą. Vis dėlto EDAV norėtų pabrėžti Europos Komisijos stebėsenos funkcijos svarbą[30]. Iš tiesų Europos Komisija turėtų nuolat stebėti visus atitinkamus pokyčius JK, kurie gali turėti įtakos esminiam asmens duomenų, perduodamų pagal JK sprendimą dėl tinkamumo, apsaugos lygio lygiavertiškumui nuo sprendimo įsigaliojimo. Be to, Europos Komisija turėtų imtis tinkamų veiksmų ir, atsižvelgdama į esamas aplinkybes, sustabdyti, iš dalies pakeisti arba panaikinti sprendimą dėl tinkamumo, jei po sprendimo dėl tinkamumo priėmimo Europos Komisija turi žinių, kad JK nebeužtikrinamas tinkamas duomenų apsaugos lygis.**

56. Savo ruožtu EDAV dės visas pastangas, kad informuotų Europos Komisiją apie visus atitinkamus veiksmus, kurių imasi valstybių narių duomenų apsaugos priežiūros institucijos (toliau – priežiūros institucijos) privačiajame arba viešajame sektoriuje, visų pirma susijusius su EEE duomenų subjektų skundais dėl asmens duomenų perdavimo iš EEE į JK.

3. BENDRIEJI DUOMENŲ APSAUGOS ASPEKTAI

3.1. Esminiai principai:

57. BDAR tinkamumo kriterijų dokumento 3 skyrius skirtas „esminiams principams“. Jie turi būti numatyti trečiosios valstybės sistemoje, kad jos duomenų apsaugos lygis būtų laikomas iš esmės lygiaverčiu tam, kuris garantuojamas ES. EDAV pripažįsta, kad JK neturi kodifikuotos konstitucijos, t. y. nėra vieno bendro dokumento, kuriame būtų išdėstytos pagrindinės valdymo srities taisyklės. Tačiau teisė į tai, kad būtų gerbiamas privatus ir šeimos gyvenimas, (ir teisė į duomenų apsaugą kaip šios teisės dalis) bei teisė į teisingą bylos nagrinėjimą[31] yra įtrauktos į 1998 m. Žmogaus teisių aktą, o JK teismai yra pripažinę šio įstatymo konstitucinę vertę. Iš tiesų 1998 m. Žmogaus teisių aktas apima EŽTK įtvirtintas teises[32]. Be to, 1998 m. Žmogaus teisių akte teigiama, kad labai svarbu, kad bet kokie valdžios institucijų veiksmai turi būti suderinami su EŽTK[33].

58. Be struktūrinių ir formalių JK ir ES teisės aktų skirtumų, EDAV pažymi, kad, kaip ir galima tikėtis, JK požiūris į duomenų apsaugą yra panašus į ES požiūrį, nes JK iki 2020 m. sausio 31 d. buvo ES valstybė narė. Dėl to daugelis esminių principų yra suderinti su BDAR principais ir todėl užtikrina iš esmės lygiavertį apsaugos lygį kaip ir ES. EDAV nusprendė tų esminių principų, kurie atitinka ES teisės aktus, toliau nenagrinėti ir palankiai vertina Europos Komisijos sprendimo projekte pateiktą analizę. Šie esminiai principai yra, pavyzdžiui: sąvokos (pvz., asmens duomenys, asmens duomenų tvarkymas, duomenų valdytojas), teisiškai pagrįsto ir sąžiningo duomenų tvarkymo teisėtais tikslais pagrindai, tikslo apribojimas, duomenų kokybė ir proporcingumas, duomenų saugojimas, saugumas ir

[29] Žr. 2018 m. (išstojimo iš) Europos Sąjungos akto 6 skirsnio 3–6 dalis.
[30] Žr. BDAR 45 straipsnio 4 dalį.
[31] Žr. EŽTK 6 ir 8 straipsnius (1998 m. Žmogaus teisių akto 1 priedas).
[32] Daugiau informacijos rasite sprendimo projekto 8–10 konstatuojamosiose dalyse.
[33] Žr. 1998 m. Žmogaus teisių akto 6 straipsnį.

konfidencialumas, skaidrumas, specialiųjų kategorijų duomenys, tiesioginė rinkodara, automatizuotas sprendimų priėmimas ir profiliavimas. EDAV taip pat pažymi, kad į JK BDAR ir 2018 m. Duomenų apsaugos įstatymą įtraukti esminiai principai, kurie yra platesni, nei reikalaujama pagal BDAR tinkamumo kriterijų dokumentą, ir atkartoja į BDAR įtrauktus principus, taigi JK užtikrinamas aukštesnis apsaugos lygis. Tokie esminiai principai, pavyzdžiui, yra susiję su pranešimais apie asmens duomenų saugumo pažeidimus, duomenų apsaugos pareigūnu, duomenų apsaugos poveikio vertinimu ir pritaikytąja ir standartizuotąja duomenų apsauga.

59. Tačiau, kaip minėta įžangoje, šioje nuomonėje EDAV norėtų konkrečiai aptarti tam tikrus klausimus, dėl kurių EDAV turi abejonių, ir norėtų paprašyti Europos Komisijos pateikti paaiškinimus.

3.1.1. Teisė susipažinti su duomenimis, reikalauti juos ištaisyti, ištrinti ir nesutikti

60. Vadinamoji imigracijos išimtis, nustatyta pagal **2018 m. Duomenų apsaugos įstatymo 2 priedo 1 dalies** 4 punktą, leidžia duomenų valdytojams, kurie vykdo „imigracijos kontrolę“, netaikyti tam tikrų 2018 m. Duomenų apsaugos įstatyme numatytų duomenų subjektų teisių, jei tai galėtų *„pakenkti veiksmingos imigracijos kontrolės užtikrinimui*“ arba *„veiklos, kuri pakenktų veiksmingos imigracijos kontrolės užtikrinimui, tyrimui ar nustatymui*“.

61. Kaip pripažįsta Europos Komisija savo sprendimo projekte[34] ir kaip nurodyta Europos Parlamento Piliečių laisvių, teisingumo ir vidaus reikalų (LIBE) komiteto nuomonėje dėl ES ir JK prekybos ir bendradarbiavimo susitarimo sudarymo Sąjungos vardu[35], ši išimtis yra **„plačiai“ suformuluota**. Ji taikoma šioms teisėms: teisei būti informuotam; teisei susipažinti su duomenimis; teisei reikalauti ištrinti duomenis; teisei riboti duomenų tvarkymą ir teisei nesutikti su duomenų tvarkymu.

62. Be to, svarbu pažymėti, kad išimtis taikoma ir tuo atveju, kai duomenų valdytojas (duomenų valdytojas Nr. 1) nerenka asmens duomenų imigracijos kontrolės tikslais, bet juos pateikia kitam duomenų valdytojui (duomenų valdytojas Nr. 2), kuris tokius asmens duomenis tvarko imigracijos kontrolės tikslais (pvz. JK Vidaus reikalų ministerija)[36].

---

[34] Žr. sprendimo projekto 62–65 konstatuojamąsias dalis.

[35] Šiuo klausimu dėl **plačios imigracijos išimties sąvokos formuluotės**, žr. 2021 m. vasario 5 d. Piliečių laisvių, teisingumo ir vidaus reikalų komiteto nuomonės dėl Europos Sąjungos bei Europos atominės energijos bendrijos ir Jungtinės Didžiosios Britanijos ir Šiaurės Airijos Karalystės prekybos ir bendradarbiavimo susitarimo ir Europos Sąjungos ir Jungtinės Didžiosios Britanijos ir Šiaurės Airijos Karalystės susitarimo dėl keitimosi įslaptinta informacija ir jos apsaugos saugumo procedūrų sudarymo Sąjungos vardu (2020/0382(NLE)), https://www.europarl.europa.eu/doceo/document/LIBE-AL-680848_LT.pdf, 10 punktą: *„primena, kad Parlamento 2020 m. vasario ir birželio mėn. rezoliucijose buvo atkreiptas dėmesys į JK duomenų apsaugos akte numatytas **bendras ir plataus masto išimtis** tvarkant asmens duomenis imigracijos tikslais“*, ir 11 punktą: *„mano, kad prieš priimant pagrįstą sprendimą dėl tinkamumo reikia pakeisti JK duomenų apsaugos įstatymo **bendrąją ir plataus masto** išimtį dėl asmens duomenų tvarkymo imigracijos tikslais;*(paryškinta autoriaus).

[36] Žr. Informacijos komisaro biuro pateiktą pavyzdį „Bendrojo duomenų apsaugos reglamento (BDAR) vadove“, 2021 m. sausio 1 d. redakcija, p. 307 (paryškinta autoriaus): *„Privati organizacija (duomenų valdytojas Nr. 1) įspėja Vidaus reikalų ministeriją (duomenų valdytoją Nr. 2) apie darbuotoją, kuris, manoma, pateikė suklastotus dokumentus savo tapatybei ir kvalifikacijai patvirtinti, kad gautų darbą. Darbdavys pateikia atitinkamą informaciją Vidaus reikalų ministerijai. Asmens teisė būti informuotam, kad jo asmens duomenys buvo perduoti Vidaus reikalų ministerijai, yra apribota tiek, kiek jos įgyvendinimas galėtų pakenkti tyrimui.*
***Todėl darbdavys neprivalo asmens informuoti, kad jo informacija buvo perduota Vidaus reikalų ministerijai**, o **Vidaus reikalų ministerija** savo ruožtu neprivalo pateikti asmeniui pareiškimo dėl privatumo, kuriuo jis būtų informuojamas, kad Vidaus reikalų ministerija dabar tvarko jo asmens duomenis. Išimtis abiem duomenų valdytojams taikoma vienodai.*

63. Byloje *Open Rights Group & Anor, R (On the Application Of) prieš Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin) (2019 m. spalio 3 d.)* pareiškėjai ginčijo imigracijos išimties teisėtumą remdamiesi tuo, kad ji prieštarauja BDAR 23 straipsniui ir yra nesuderinama su ES chartijos 7 ir 8 straipsniuose garantuojamomis teisėmis, susijusiomis su privatumu ir asmens duomenų apsauga. Anglijos ir Velso Aukštasis teismas (toliau – Aukštasis teismas) svarstė, ar 2018 m. Duomenų apsaugos įstatymo 2 priedo 1 dalies 4 punkte numatyta imigracijos išimtis yra teisėta, ir padarė išvadą, kad ji teisėta.

64. Aukštasis teismas visų pirma atsižvelgė į tai, kad:

- *„[...] Imigracijos išimtis yra akivaizdžiai „svarbaus viešojo intereso“ klausimas ir ja siekiama teisėto tikslo.[...]“*, 30 punktas;
- *„[...] Imigracijos išimtis atitinka reikalavimus, keliamus priemonei, kad ji „atitiktų įstatymą. […]“*, 38 punktas;
- *„Imigracijos išimtimi galima remtis tik tuo atveju ir tik tiek, kiek „išvardytų BDAR nuostatų“ laikymasis **galėtų pakenkti** veiksmingos imigracijos kontrolės užtikrinimui arba veiklos, kuri pakenktų veiksmingos imigracijos kontrolės užtikrinimui, tyrimui ar nustatymui. Formuluotė „galėtų pakenkti“ 1998 m. Duomenų apsaugos įstatymo (kuris buvo priimtas prieš 2018 m. Duomenų apsaugos įstatymą) kontekste buvo aiškinama kaip „labai reikšminga ir didelė tikimybė, kad bus pakenkta konkrečiam viešajam interesui. Rizikos laipsnis turi būti toks, kad „būtų labai tikėtina“, kad tiems interesams bus padaryta žala, net jei rizika toli gražu nėra labiau tikėtina nei netikėtina [...].“*, 39 punktas (paryškinta autoriaus).

65. Reikėtų pažymėti, kad, EDAV žiniomis, šis teismo sprendimas nėra galutinis ir buvo apskųstas.

66. Kaip nurodyta EDAV gairėse dėl apribojimų pagal BDAR 23 straipsnį (toliau – BDAR 23 straipsnio gairės), [37] *„[...] BDAR kontekste apribojimai turi būti **numatyti teisėkūros priemonėje**, susiję su **ribotu duomenų subjektų teisių ir (arba) duomenų valdytojo pareigų**, išvardytų BDAR 23 straipsnyje, skaičiumi, **jais turi būti paisoma** atitinkamų pagrindinių teisių ir laisvių esmės, jie turi būti **būtina ir proporcinga priemonė** demokratinėje visuomenėje ir jais turi būti apsaugotas vienas iš BDAR 23 straipsnio 1 dalyje nurodytų pagrindų [...].“*[38]

67. EDAV taip pat primena, kad BDAR 41 konstatuojamojoje dalyje teigiama, kad *„kai šiame reglamente nurodomas **teisinis pagrindas arba teisėkūros priemonė**, nebūtinai reiškia, kad parlamentas turi priimti teisėkūros procedūra priimamą aktą, nedarant poveikio reikalavimams, taikomiems pagal atitinkamos valstybės narės konstitucinę tvarką. Tačiau toks teisinis pagrindas arba teisėkūros priemonė turėtų būti **aiškūs ir tikslūs, o jų taikymas turėtų būti numatomas tiems asmenims,***

---

*Tačiau jei darbuotojas prašo Vidaus reikalų ministerijos, kuri dabar atlieka jo asmens duomenų tyrimą, pateikti savo asmens duomenų kopiją, **Vidaus reikalų ministerija gali remtis išimtimi** ir nesuteikti dalies asmens duomenų, jei jų atskleidimas galėtų pakenkti tyrimui. Jei darbuotojas panašų prašymą pateiktų **savo darbdaviui, šis taip pat galėtų taikyti tokią pačią išimtį**.“*
Kitaip tariant, kaip paaiškinta p. 300: *„Daugeliu atvejų Vidaus reikalų ministerija arba viena iš jos agentūrų ir rangovų yra duomenų valdytojas, kuris taiko šią išimtį. Tačiau svarbu pažymėti, kad šią išimtį gali taikyti ne tik Vidaus reikalų ministerija. Ją taip pat gali taikyti kiti duomenų valdytojai, pavyzdžiui, darbdaviai, universitetai ir policija, kurie su Vidaus reikalų ministerija bendradarbiauja imigracijos klausimais.“*

[37] Žr. EDAV gairių 10/2020 dėl BDAR 23 straipsnio apribojimų, 1.0 versiją, priimtą 2020 m. gruodžio 15 d., kurios šiuo metu baigiamos rengti po viešų konsultacijų, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-102020-restrictions-under-article-23_en.

[38] Žr. BDAR 23 straipsnio gairių, 9 punktą, p. 5.

***kuriems jie turi būti taikomi**, pagal Europos Sąjungos Teisingumo Teismo [...] ir Europos Žmogaus Teisių Teismo praktiką"* (paryškinta autoriaus).

68. Nors EŽTT patikslino, kad „dėl frazių *„pagal įstatymą" ir „nustatyta įstatymu", kurios vartojamos Konvencijos 8–11 straipsniuose, [EŽTT] pažymi, kad jis visada sąvoką „įstatymas" suprato „materialiąja", o ne „formaliąja" prasme; ji apima tiek „rašytinę teisę", įskaitant žemesnės nei įstatymo galios aktus ir reguliavimo priemones, patvirtintas profesinių asociacijų įgyvendinant savarankiškus normatyvinius įgaliojimus, suteiktus parlamento, tiek „nerašytinę teisę". „Įstatymas" turi būti suprantamas kaip apimantis tiek teisės aktus, tiek **teismų „kuriamą teisę"***[39], BDAR 23 straipsnio gairėse primenama, kad *„pagal ESTT praktiką bet kokia **teisėkūros priemonė**, priimta remiantis BDAR 23 straipsnio 1 dalimi, visų pirma **turi atitikti konkrečius BDAR 23 straipsnio 2 dalyje nustatytus reikalavimus**. BDAR 23 straipsnio 2 dalyje nustatyta, kad teisėkūros priemonėse, kuriomis nustatomi duomenų subjektų teisių ir duomenų valdytojų pareigų apribojimai, atitinkamais atvejais turi būti **konkrečios nuostatos dėl kelių toliau nurodytų kriterijų**. Paprastai **į teisėkūros priemonę**, kuria nustatomi apribojimai pagal BDAR 23 straipsnį, **turėtų būti įtraukti** visi toliau išsamiai išdėstyti reikalavimai*."[40]

69. Šiuo atžvilgiu galima pastebėti, kad pačioje **imigracijos išimtyje neįvardyti šie BDAR 23 straipsnio 2 dalyje nurodyti aspektai**:

- „apsaugos priemon[ės], kuriomis siekiama užkirsti kelią piktnaudžiavimui arba neteisėtam susipažinimui su duomenimis ar jų perdavimui" (d);
- „duomenų valdytojo arba duomenų valdytojų kategorij[os]" (e)[41];
- „ pavoja[i] duomenų subjektų teisėms ir laisvėms" (g);
- „ duomenų subjektų teis[ė] būti informuotiems apie apribojimą, nebent tai pakenktų apribojimo tikslui" (h).

---

[39] Žr. 2010 m. rugsėjo 14 d. EŽTT sprendimo *Sanoma Uitgevers B.V. / Nyderlandai*, EC:ECHR:2010:0914JUD003822403, 83 punktą (paryškinta autoriaus).

[40] Žr. BDAR 23 straipsnio gairių 45 ir 46 punktus, p. 11. Pagal ES chartijos 52 straipsnio 3 dalį *„[š]ioje Chartijoje nurodytų teisių, atitinkančių Žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos garantuojamas teises, esmė ir taikymo sritis yra tokia, kaip nustatyta toje Konvencijoje. Ši nuostata nekliudo Sąjungos teisėje numatyti didesnę apsaugą."* Dėl sąvokos „**numatytas įstatymo**", pagal ES chartijos 52 straipsnio 1 dalį, reikėtų vadovautis EŽTT parengtais kriterijais, kaip siūloma keliose ESTT generalinio advokato išvadose, žr., pavyzdžiui, išvadų sujungtose bylose C-203/15 ir C-698/15, *Tele2 Sverige AB*, ECLI:EU:C:2016:572, 137–154 punktus ir Sprendimo *Scarlet Extended*, C-70/10, ECLI:EU:C:2011:255, 88–114 punktus. Todėl, be kita ko, galima remtis EŽTT sprendimo *Weber ir Saravia prieš Vokietiją* 84 punktu: *„Teismas pakartoja, kad sąvoka „**pagal įstatymą**" [EŽTK] 8 straipsnio 2 dalies prasme pirmiausia reikalauja, kad ginčijama priemonė turėtų tam tikrą pagrindą **vidaus teisėje**; ji taip pat susijusi su atitinkamos **teisės kokybe**, reikalaujančia, kad ji būtų prieinama atitinkamam asmeniui, kuris, be to, turi galėti numatyti jos pasekmes sau, ir suderinama su teisinės valstybės principu."* (išskirta autoriaus).
Taip pat žr. BDAR 41 konstatuojamąją dalį: *„Toks [teisinis pagrindas ar] teisėkūros priemonė turėtų būti **aiškūs** ir **tikslūs, o jų taikymas turėtų būti numatomas tiems asmenims, kuriems jie turi būti taikomi**, pagal Europos Sąjungos Teisingumo Teismo [...] ir Europos Žmogaus Teisių Teismo praktiką"* (paryškinta autoriaus).

[41] Žr. pirmiau minėtos Aukštojo teismo bylos 54 punktą: *„Mano nuomone, nėra nieko neteisėto, kad imigracijos išimtis gali būti taikoma **visiems duomenų valdytojams**, tvarkantiems duomenis nurodytais tikslais Kaip nurodo atsakovai, be 4 straipsnio 3–4 dalių imigracijos išimtis taptų neveiksminga tais atvejais, kai duomenys gaunami iš trečiųjų šalių (pvz., vietos valdžios institucijos arba Jos Didenybės mokesčių ir muitų departamento) veiksmingos imigracijos kontrolės tikslais."* (paryškinta autoriaus), taigi patvirtinamas **apibendrintas** apribojimų taikymas.

70. Informacijos komisaro biuro „Bendrojo duomenų apsaugos reglamento (BDAR) vadove“[42], įskaitant skyrių apie „imigracijos išimtį“, pateikiami paaiškinimai apie imigracijos išimtį, tačiau jais **negali būti** *savaime* nustatytos privalomos ją papildančios taisyklės. Be to, „teisės kokybės“ klausimas yra ypač aktualus atsižvelgiant į apribotų teisių svarbą ir išimties išplėtimą[43].

71. *A fortiori*, „**išankstinio nusistatymo patikrinimu**“ nenustatomos apsaugos priemonės, kurios užkirstų kelią piktnaudžiavimui, neteisėtai prieigai ar perdavimui, ir kurias turi įgyvendinti, pavyzdžiui, Vidaus reikalų ministerija.

---

[42] Informacijos komisaro biuro „Bendrojo duomenų apsaugos reglamento (BDAR) vadovas“, 2021 m. sausio 1 d. redakcija, p. 299–307.

[43] Žr. minėtos Aukštojo teismo bylos 57 punktą: *„C. Knight mane informavo, kad komisaras netrukus parengs gaires dėl išimties, tačiau jos turės „teisės akto“ statusą tik ta prasme, kad bus priimtos remiantis komisaro įgaliojimais pagal BDAR 57 straipsnio 1 dalį. Jos neturės teisinio statuso pagal 2018 m. Duomenų apsaugos įstatymą.“*

Teisiškai privalomų gairių, kurias remia Informacijos komisaro biuras, parengimo pagrindimas visų pirma nurodomas teismo sprendimo 56–60 punktuose:

„56. Galiausiai, pereinu prie komisaro teiginio, kad be papildomų teisės aktais nustatytų gairių, kuriomis būtų užtikrintos apsaugos priemonės dėl imigracijos išimties reikšmės ir taikymo, išimtimi nebūtų proporcingai įgyvendinama BDAR 23 straipsnio 1 dalis. C. Knight teigimu, priėmus šias gaires, nuostata būtų proporcinga.

57. C. Knight mane informavo, kad komisaras netrukus parengs gaires dėl išimties, tačiau jos turės „teisės akto“ statusą tik ta prasme, kad bus priimtos remiantis komisaro įgaliojimais pagal BDAR 57 straipsnio 1 dalį. Jos neturės teisinio statuso pagal 2018 m. Duomenų apsaugos įstatymą. Taip pat suprantu, kad Vidaus reikalų ministerija parengė gairių darbuotojams dėl imigracijos išimties projektą (žr. [22] punktą). Praktikoje komisaro paskelbtos gairės turi įtakos, neatsižvelgiant į jų teisinį pagrindą. Tačiau komisaras neturi įgaliojimų skelbti „privalomų“ gairių, kokias Aukščiausiasis Teismas turėjo omenyje Krikščioniškojo instituto byloje (žr. [101] ir [107] punktus). Atrodo, kad reikėtų priimti pirminį teisės aktą, jei būtų manoma, kad reikia tokio paties statuso gairių dėl imigracijos išimties, kaip ir šiuo metu 2018 m. Duomenų apsaugos įstatymo 121–124 str. numatyti praktikos kodeksai.

58. Pasisakydamas už teisės aktais nustatytas gaires, C. Knight teigia, kad aplinkybės, kuriomis bus taikoma migracijos išimtis, neišvengiamai kelia susirūpinimą dėl jos buvimo ir taikymo būtinumo bei proporcingumo. Jis atkreipia dėmesį į du dalykus, ypač susijusius su teisiniu kontekstu. Pirma, asmens duomenys, kuriems taikoma imigracijos išimtis, iš esmės gali būti susiję su specialiosios kategorijos duomenimis, kaip apibrėžta BDAR 9 straipsnio 1 dalyje (t. y. duomenimis, „atskleidžiančiais rasinę ar etninę kilmę“). Tokie duomenys BDAR nurodyti todėl, kad jiems reikia didesnės apsaugos priemonių (Nuomonės 1/15 [2019] 3 C.M.L.R. 25 [141] punktas). Antra, pagrindinė duomenų apsaugos teisės nuostata yra ta, kad teisė susipažinti su duomenimis visų pirma yra labai svarbi, nes ja suteikiama galimybė naudotis kitomis duomenų subjektams suteiktomis teisėmis (žr. YS prieš Minister voor Immigratie, Integratie en Asiel (C-141/12) EU:C:2014:2081; [2015] 1 C.M.L.R. 18 [44] punktą).

59. C. Knight įvardija keturis praktinio pobūdžio klausimus. Pirma, kai duomenų valdytojai nepaaiškina duomenų subjektams, kad jie rėmėsi teisės aktuose nustatyta išimtimi, ir nepateikia išsamios priežasčių santraukos, duomenų subjektas nežinos, kad buvo pritaikyta išimtis, ir dėl to negalės jos veiksmingai užginčyti. Antra, duomenų subjektai turės visiškai pasikliauti duomenų valdytojais, kad šie išimtis taikys atsargiai ir tik tiek, kiek būtina. Nors bet kuris duomenų subjektas turi teisę pateikti skundą komisarui dėl išimties taikymo arba pareikšti ieškinį teisme, tikėtina, kad duomenų subjektas nežinos apie savo teises ir neturės lėšų imtis teisinių veiksmų, kai reikia greitai ir tiksliai laikytis teisės į duomenų apsaugą. Trečia, tikėtina, kad duomenų subjektas, kaip imigrantas, yra pažeidžiamoje padėtyje. Ketvirta, atsižvelgiant į atsakovų pateiktus įrodymus dėl imigracijos išimties taikymo, tai nėra abstraktus klausimas (žr. [4] punktą).

60. C. Knight teigia, kad tarp šio skundo dėl imigracijos išimties ir teismo argumentų Krikščioniškojo instituto [2016] UKSC 51 byloje yra glaudi paralelė. Jo teigimu, kaip ir Krikščioniškojo instituto byloje, imigracijos išimtis yra plati, joje vartojamos neapibrėžtos sąvokos, taikoma žema riba, pačioje nuostatoje nėra nustatyta aiški kontrolė ir ji taikoma labai plačiam kontekstų ir teisių spektrui. Kitaip nei Krikščioniškojo instituto bylos atveju, imigracijos išimties taikymui nėra jokių viešai prieinamų gairių, juo labiau turinčių teisės akto statusą, į kurias reikėtų atsižvelgti.“

72. Atsižvelgdama į visa tai, kas išdėstyta pirmiau, EDAV pastebi, kad reikia papildomų paaiškinimų dėl imigracijos išimties taikymo.

73. Be to, EDAV pažymi, kad nėra teisiškai privalomo dokumento, kuriame būtų paaiškinta imigracijos išimtis, atsižvelgiant į tai, ar ji iš esmės atitinka BDAR 23 straipsnį ir ES chartijos 7 ir 8 straipsnius. Kartu EDAV mano, kad Europos Komisija turi toliau remdamasi įrodymais pagrįsti plačios imigracijos išimties taikymo srities *ratione personae* būtinumą ir proporcingumą.

74. **Taigi EDAV ragina Europos Komisiją patikrinti minėto proceso *Open Rights Group & Anor, R (On the Application Of) prieš Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin)* eigą ir, kadangi sprendimas nėra galutinis (*res judicata*), patikrinti, ar jis patvirtintas, ar peržiūrėtas apeliacinio teismo sprendimu, atsižvelgti į visus su tuo susijusius atnaujinimus ir nurodyti juos sprendime dėl tinkamumo. EDAV taip pat ragina Europos Komisiją pateikti daugiau informacijos apie imigracijos išimties būtinumą ir proporcingumą, visų pirma atsižvelgiant į plačią taikymo sritį *ratione personae*.**

75. **Kartu EDAV ragina Europos Komisiją toliau nagrinėti, ar JK teisinėje sistemoje yra papildomų apsaugos priemonių arba ar jos galėtų būti numatytos, pavyzdžiui, teisiškai privalomomis priemonėmis, kuriomis būtų papildyta imigracijos išimtis, padidinant jos numatomumą ir duomenų subjektų apsaugos priemones, taip pat sudarant sąlygas geriau ir greičiau įvertinti ir stebėti būtinumo ir proporcingumo reikalavimus.**

3.1.2. Tolesnio duomenų perdavimo ribojimas

76. BDAR 44 straipsnyje nustatyta, kad asmens duomenys perduodami ir toliau perduodami tik tuo atveju, jei nepakenkiama BDAR garantuojamam fizinių asmenų apsaugos lygiui. Todėl asmens duomenims, kurie perduodami iš EEE į JK remiantis sprendimu dėl tinkamumo, užtikrinama iš esmės lygiavertė apsauga, kaip ir pagal ES duomenų apsaugos sistemą. **Tai reiškia, kad pagal sprendimo dėl tinkamumo projektą JK teisės aktai, susiję su asmens duomenų, perduodamų į JK, tvarkymu, turi būti ne tik „iš esmės lygiaverčiai“ ES teisės aktams, bet ir kad JK taikomomis taisyklėmis dėl tolesnio šių duomenų perdavimo į trečiąsias valstybes toliau būtų užtikrinamas iš esmės lygiavertis duomenų apsaugos lygis.**

77. Todėl svarbu, kad bet koks tolesnis EEE asmens duomenų perdavimas iš JK į kitą trečiąją valstybę būtų tinkamai apsaugotas arba vykdomas pagal taisykles dėl nuo apsaugos priemonių leidžiančių nukrypti nuostatų[44], kad būtų užtikrintas ES teisės aktais suteiktos apsaugos tęstinumas. **Iš tiesų, jei tokios apsaugos neįmanoma užtikrinti, tolesnis EEE asmens duomenų perdavimas neturėtų būti vykdomas.**

78. EDAV pripažįsta, kad JK BDAR (44–49 straipsniai) ir 2018 m. Duomenų apsaugos įstatymas[45] iš esmės atkartojo BDAR V skyrių. **Tačiau EDAV nustatė tam tikrus JK teisinės sistemos aspektus, susijusius su tolesniu duomenų perdavimu, kurie gali pakenkti iš EEE perduodamų asmens duomenų apsaugos lygiui.**

79. **Pirmoji EDAV nustatyta problema** yra susijusi su tuo, kad JK, laikydamasi 2018 m. Duomenų apsaugos įstatyme nustatytos tvarkos, pripažįsta trečiąsias valstybes, tarptautines organizacijas ar teritorijas[46] tinkamais duomenų gavėjais. Iš tiesų tolesnis EEE asmens duomenų perdavimas iš JK į

[44] Žr. JK BDAR 49 straipsnį.
[45] Žr. 2018 m. Duomenų apsaugos įstatymo 17A, 17B, 17C ir 18 skirsnius.
[46] Žr. 2018 m. Duomenų apsaugos įstatymo 17A skirsnį.

kitas trečiąsias valstybes galėtų vykti remiantis JK tinkamumo reglamentu[47], kuris galimai bus priimtas ateityje.

80. Konkrečiau, kaip paaiškinta sprendimo projekto 77 konstatuojamojoje dalyje, pasikonsultavęs su Informacijos komisaro biuru, JK valstybės sekretorius turi teisę pripažinti trečiąją valstybę (arba teritoriją ar sektorių trečiojoje valstybėje), tarptautinę organizaciją arba tokios valstybės, teritorijos, sektoriaus ar organizacijos aprašymą kaip užtikrinantį tinkamą asmens duomenų apsaugos lygį[48]. Vertindamas duomenų apsaugos lygio tinkamumą JK valstybės sekretorius turi atsižvelgti į tuos pačius aspektus, kuriuos Europos Komisija turi įvertinti pagal BDAR 45 straipsnio 2 dalies a–c punktus, aiškinamus kartu su BDAR 104 konstatuojamąja dalimi ir palikta galioti ES teismų praktika. Tai reiškia, kad vertinant trečiosios valstybės duomenų apsaugos lygio tinkamumą, nustatytas standartas bus tai, ar atitinkama trečioji valstybė užtikrina „iš esmės lygiavertį“ duomenų apsaugos lygį kaip tas, kuris garantuojamas JK. Nors EDAV atkreipia dėmesį, kad JK turi pajėgumus pagal JK BDAR pripažinti teritorijas kaip užtikrinančias tinkamą apsaugos lygį pagal JK duomenų apsaugos sistemą, EDAV norėtų pabrėžti, kad šios teritorijos iki šiol negali pasinaudoti Europos Komisijos priimtu sprendimu dėl tinkamumo, kuriuo apsaugos lygis pripažįstamas „iš esmės lygiaverčiu“ ES garantuojamam apsaugos lygiui. Dėl to gali kilti pavojus, kad nebus užtikrinta iš EEE perduodamų asmens duomenų apsauga, ypač jei ateityje JK duomenų apsaugos sistema skirtųsi nuo Sąjungos *acquis*. Reikia pažymėti, kad ESTT 2020 m. liepos mėn. priėmus precedentinį sprendimą Schrems II[49] buvo pripažintas negaliojančiu sprendimas dėl JAV privatumo skydo, nes, ESTT nuomone, JAV teisinė sistema negali būti laikoma užtikrinančia iš esmės lygiavertį apsaugos lygį, palyginti su ES teisine sistema. Tačiau jau priimti ESTT sprendimai, kurie JK teisinėje sistemoje laikomi palikta galioti teismų praktika, gali būti neprivalomi JK, nes pasibaigus tarpiniam laikotarpiui JK turi galimybę keisti paliktą galioti ES teisę, o jos Aukščiausiasis Teismas nėra saistomas paliktos galioti ES teismų praktikos[50].

81. **EDAV ragina Europos Komisiją atidžiai stebėti JK valdžios institucijų atliekamą tinkamumo vertinimo procesą ir kriterijus kitų trečiųjų valstybių atžvilgiu, visų pirma tų trečiųjų valstybių, kurių ES nepripažįsta tinkamomis pagal BDAR, atžvilgiu. Jei Europos Komisija nustato, kad trečioji valstybė, kurią JK pripažino tinkama, neužtikrina apsaugos lygio, iš esmės lygiaverčio tam, kuris garantuojamas ES, EDAV ragina Europos Komisiją imtis visų būtinų veiksmų, pavyzdžiui, iš dalies pakeisti JK sprendimą dėl tinkamumo, kad būtų įdiegtos konkrečios EEE kilmės asmens duomenų apsaugos priemonės, ir (arba) apsvarstyti galimybę sustabdyti JK sprendimo dėl tinkamumo galiojimą, jei asmens duomenys, perduodami iš EEE į JK, toliau perduodami į atitinkamą trečiąją valstybę remiantis JK tinkamumo reglamentu.**

82. **Antroji problema** – susijusi su būsima jau priimtų Europos Komisijos sprendimų dėl tinkamumo pagal Direktyvą 95/46/EB peržiūra. Po šios peržiūros Europos Komisija gali nuspręsti, kad tam tikros valstybės, kurioms iki šiol buvo taikomas sprendimas dėl tinkamumo, nebeužtikrina iš esmės lygiaverčio duomenų apsaugos lygio, atsižvelgiant į galiojančius ES teisės aktus ir naujausią teismų praktiką. Tačiau, kaip numatyta 2018 m. Duomenų apsaugos įstatymo 21 priedo 4 dalyje, JK jau pripažino, kad šios valstybės užtikrina tinkamą apsaugos lygį. Nors JK valstybės sekretorius per ketverius metus turi atlikti šių išvadų dėl tinkamumo peržiūrą, Europos Komisija savo sprendimo

[47] JK sprendimo dėl tinkamumo pagal BDAR atitikmuo.
[48] Žr. 2018 m. Duomenų apsaugos įstatymo 182 skirsnio 2 dalį. Taip pat žr. Susitarimo memorandumą dėl Informacijos komisaro biuro funkcijos, susijusios su naujais JK tinkamumo vertinimais, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/03/secretary-of-state-for-the-department-for-dcms-and-the-information-commissioner-sign-memorandum-of-understanding/.
[49] Žr. Sprendimą *Schrems II*.
[50] Žr. 2018 m. (išstojimo iš) Europos Sąjungos akto 6 skirsnio 3–6 dalis.

projekte pažymi, kad šios išvados dėl tinkamumo automatiškai nenustos galioti, jei JK valstybės sekretorius per nustatytą ketverių metų laikotarpį neatliks reikalaujamos peržiūros[51].

83. **EDAV ragina Europos Komisiją stebėti, ar, ES užbaigus jau priimtų sprendimų dėl tinkamumo peržiūrą, valstybę, kuri laikoma nebeužtikrinančia tinkamo duomenų apsaugos lygio, JK toliau laiko užtikrinančia tinkamą lygį. Jei taip yra, EDAV ragina Europos Komisiją, remiantis sprendimo projekto 277–280 konstatuojamosiomis dalimis, imtis visų tinkamų priemonių padėčiai ištaisyti, pavyzdžiui, iš dalies pakeičiant sprendimą dėl tinkamumo, kad būtų įtraukti specialūs reikalavimai asmens duomenims, kurių kilmės šalis yra EEE, ir (arba) sustabdyti sprendimo dėl tinkamumo galiojimą, jei iš EEE į JK perduodami asmens duomenys toliau perduodami į atitinkamą trečiąją valstybę. EDAV ragina Europos Komisiją tęsti šią stebėseną visą JK sprendimo dėl tinkamumo galiojimo laikotarpį.**

84. **Trečioji problema** – susijusi su tolesniu asmens duomenų perdavimu iš EEE į netinkamas valstybes, remiantis JK BDAR 46 ir 47 straipsniuose numatytomis duomenų perdavimo priemonėmis. Nors JK BDAR numatytos tos pačios duomenų perdavimo priemonės kaip ir BDAR, EDAV pabrėžia, kad reikia užtikrinti, kad jose numatytomis apsaugos priemonėmis būtų užtikrinta veiksminga duomenų apsauga trečiojoje valstybėje, visų pirma atsižvelgiant į Sprendimą *Schrems II*.

85. Po Sprendimo *Schrems II*, kuriame ESTT priminė, kad ES asmens duomenims suteikiama apsauga turi keliauti kartu su duomenimis, kad ir kur jie keliautų, EDAV jau priėmė pirmines rekomendacijas dėl papildomų priemonių[52], kurios prireikus padėtų eksportuotojams užtikrinti, kad duomenų subjektams būtų suteikta iš esmės tokio paties lygio apsauga, kokia užtikrinama ES.

86. Pasak ESTT, duomenų eksportuotojai kiekvienu konkrečiu atveju prireikus bendradarbiaudami su duomenų importuotoju trečiojoje valstybėje privalo patikrinti, ar trečiosios valstybės teisė ar praktika mažina BDAR 46 straipsnyje nurodytoms perdavimo priemonėms skirtų tinkamų apsaugos priemonių veiksmingumą[53]. Tais atvejais duomenų eksportuotojai turėtų įgyvendinti papildomas priemones, kurios užpildo šias apsaugos spragas ir padidina apsaugos lygį iki reikalaujamo ES teisės aktais.

87. **Siekiant užtikrinti apsaugos tęstinumą, EDAV ragina Europos Komisiją į sprendimo projektą įtraukti garantijas, kad tais atvejais, kai JK BDAR 46 ir 47 straipsniuose numatytomis duomenų perdavimo priemonėmis naudojasi duomenų eksportuotojai JK toliau perduodant EEE perduotus duomenis į kitas trečiąsias valstybes, šie duomenų eksportuotojai kiekvienu konkrečiu atveju įvertina trečiosios valstybės duomenų apsaugos sistemą ir, jei reikia, imasi atitinkamų priemonių, kad užtikrintų veiksmingą pasirinktoje perdavimo priemonėje numatytų apsaugos priemonių laikymąsi, kad būtų užtikrintas apsaugos lygis, iš esmės lygiavertis tam, kuris garantuojamas ES. EDAV pabrėžia, kad be šių garantijų kyla pavojus, kad apsauga, iš esmės lygiavertė tai, kuri garantuojama ES, sumažės toliau perduodant duomenis iš JK.**

88. **Ketvirtoji problema** – susijusi su tolesniu duomenų perdavimu ir su tarptautiniais susitarimais, kuriuos JK yra sudariusi arba kuriuos sudarys ateityje, ir galima tiesiogine trečiųjų valstybių, kurios

[51] Žr. sprendimo projekto 82 konstatuojamąją dalį.
[52] Žr. 2020 m. lapkričio 10 d. priimtas EDAV rekomendacijas 01/2020 dėl priemonių, papildančių duomenų perdavimo priemones, siekiant užtikrinti atitiktį ES asmens duomenų apsaugos lygiui, kurios šiuo metu baigiamos rengti po viešų konsultacijų, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.
[53] Žr. Sprendimo *Schrems II* 134 punktą.

yra tokių susitarimų šalys, institucijų prieiga prie EEE asmens duomenų. Iš tiesų EDAV išreiškė didelį susirūpinimą dėl jau sudaryto JK ir JAV susitarimo pagal CLOUD įstatymą, o Europos Komisija šią problemą pripažįsta ir pabrėžia, kad „*galimas susitarimo įsigaliojimas gali turėti įtakos šiame sprendime įvertintam apsaugos lygiui*“[54]. Iš tiesų, remiantis šiuo susitarimu, jam įsigaliojus, pagal sprendimo projektą iš EEE į JK perduodamiems asmens duomenims būtų taikomos šio susitarimo nuostatos, kuriomis nustatomos tiesioginės prieigos sąlygos JAV institucijoms, o tai turėtų įtakos JK duomenų apsaugos sistemai, visų pirma nuostatoms dėl tolesnio duomenų perdavimo. Todėl iš EEE perduodamiems duomenims teikiamos apsaugos lygį gali iš esmės paveikti su JAV sudaryto susitarimo nuostatos ir daryti poveikį tokių duomenų apsaugos lygiui. Šiuo klausimu EDAV pažymi, kad Europos Komisija savo sprendimo projekto 153 konstatuojamojoje dalyje remiasi JK valdžios institucijų paaiškinimais, tačiau necituoja ir nepateikia jokios konkrečios rašytinės garantijos ar įsipareigojimo ir nenurodo konkrečių teisinių nuostatų pagal JK teisę, kuriomis tokie paaiškinimai būtų įtvirtinti.

89. EDAV jau anksčiau išreiškė šį susirūpinimą 2020 m. birželio 15 d. Europos Parlamentui adresuotame laiške[55]. EDAV pabrėžė, kad, remdamasi „*ES acquis duomenų apsaugos srityje, visų pirma BDAR ir Teisėsaugos direktyva*“, EDAV abejoja, ar susitarime dėl prieigos prie asmens duomenų JK numatytos apsaugos priemonės bus taikomos tam tikromis aplinkybėmis, kai įpareigojama atskleisti duomenis JAV, taip pat ar šios apsaugos priemonės yra pakankamos, atsižvelgiant į ES standartus, kad nebūtų pakenkta ES teikiamos duomenų apsaugos lygiui.

90. Be to, JK ir JAV susitarimo pagal CLOUD įstatymą nuostatos gali turėti reikšmingos įtakos materialinėms ir procesinėms sąlygoms, kuriomis JK duomenų valdytojų arba duomenų tvarkytojų turimus asmens duomenis gali tiesiogiai gauti JAV valdžios institucijos, ir taip paveikti JK teisės garantuojamą duomenų apsaugos lygį. Siekiant užtikrinti iš esmės lygiavertį apsaugos lygį tam, kuris garantuojamas ES teisėje, pavyzdžiui „*labai svarbu, kad apsaugos priemonės pagal tokį susitarimą apimtų privalomą išankstinį teisminį leidimą, kaip esminę prieigos prie metaduomenų ir turinio duomenų garantiją. Remdamasi preliminariu vertinimu, EDAV pažymi, kad nors susitarime nurodomas vidaus teisės taikymas, tokios aiškios nuostatos JK ir JAV sudarytame susitarime ji negalėjo nustatyti.*“[56]

91. Nors Europos Komisija pabrėžia, kad pagal šį susitarimą gautiems duomenims būtų taikomos apsaugos priemonės, lygiavertės konkrečioms apsaugos priemonėms, numatytoms vadinamajame ES ir JAV bendrajame susitarime, EDAV abejoja, ar šių apsaugos priemonių įtraukimas į JK ir JAV susitarimą pagal CLOUD įstatymą vien tik kaip nuorodos, taikomos *mutatis mutandis*, atitiktų aiškių, tikslių ir prieinamų taisyklių, susijusių su prieiga prie asmens duomenų, kriterijus, ar jomis būtų pakankamai įtvirtintos tokios apsaugos priemonės, kad jos būtų veiksmingos ir taikytinos pagal JK teisę.

92. **Todėl EDAV rekomenduoja Europos Komisijai paaiškinti, kaip ir remiantis kokiu teisiniu dokumentu įsigaliotų apsaugos priemonės, lygiavertės konkrečioms apsaugos priemonėms, numatytoms pagal ES ir JAV bendrąjį susitarimą, kurios būtų privalomos pagal JK teisę.**

[54] Žr. sprendimo projekto 153 konstatuojamąją dalį.
[55] Žr. 2020 m. birželio 15 d. priimtą EDAV atsakymą Europos Parlamento nariams Sophie in’t Veld ir Moritzui Körneriui dėl JAV ir JK susitarimo pagal JAV CLOUD įstatymą, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0054-uk-usagreement.pdf.
[56] Žr. nurodytą EDAV laišką.

93. EDAV taip pat pažymi, kad JK ir JAV susitarimo pagal CLOUD įstatymą nuostatos, skaitomos kartu su JAV CLOUD įstatymo[57] 3 skirsniu, kelia klausimų dėl faktinio susitarime numatytų apsaugos priemonių taikymo, kai JAV teisėsaugos institucijos gali susipažinti su asmens duomenimis JK, kuriuos tvarko JAV jurisdikcijai priklausantys elektroninių ryšių paslaugų teikėjai arba nuotolinės kompiuterijos paslaugų teikėjai (toliau – ryšių paslaugų teikėjai). Iš tiesų, jei JK esančiam ryšių paslaugų teikėjui būtų taikoma JAV teisė (pvz., dėl to, kad jis yra JAV bendrovės dukterinė įmonė), dar reikia išsiaiškinti, ar JAV institucijos, norėdamos gauti tuos duomenis, privalėtų remtis JK ir JAV susitarimu pagal CLOUD įstatymą. Kadangi Europos Komisija nurodo, kad *„ypatingas dėmesys bus skiriamas Bendrojo susitarimo apsaugos priemonių taikymui ir pritaikymui konkrečioms duomenų perdavimo rūšims, kurioms taikomas JK ir JAV susitarimas“*, EDAV pabrėžia, kad remiantis preliminariu vertinimu nėra aišku, ar JK ir JAV susitarime pagal CLOUD įstatymą įtvirtintos apsaugos priemonės, taigi ir tos, kurios numatytos ES ir JAV bendrajame susitarime, būtų taikomos visiems JAV institucijų prašymams susipažinti su duomenimis JK pagal JAV CLOUD įstatymą, jei tokių būtų.

94. Ateityje JK gali sudaryti kitus tarptautinius susitarimus ar priimti įsipareigojimus su trečiosiomis valstybėmis, kurie būtų taikomi asmens duomenims, perduodamiems iš EEE į JK pagal sprendimo projektą[58]. Priklausomai nuo šių susitarimų nuostatų ir konkrečių duomenų apsaugos sąlygų taikymo, kadangi šie tarptautiniai susitarimai darys poveikį JK duomenų apsaugos sistemai, jie taip pat gali turėti didelį poveikį materialinėms ir procedūrinėms sąlygoms, susijusioms su trečiųjų valstybių institucijų prieiga prie asmens duomenų JK. Visų pirma tai taikoma Europos Tarybos konvencijos dėl elektroninių nusikaltimų (toliau – Budapešto konvencija) antrojo papildomo protokolo projektui, dėl kurio šiuo metu derasi šios konvencijos šalys, tarp kurių yra kelios ES nepriklausančios šalys. Iš tiesų į protokolo projektą įtrauktos nuostatos, kurias šalys gali taikyti savo nuožiūra, pavyzdžiui, dėl leidimo suteikti prieigą prie turinio duomenų arba jos nesuteikti. Nors visos ES valstybės narės šias išlygas aktyvuotų laikydamosi ES duomenų apsaugos taisyklių, nepateikta jokių garantijų dėl JK, kuri galėtų gerokai nukrypti nuo apsaugos lygio, kuris tokiu atveju būtų užtikrinamas ES. Kitas pirmiau pateiktų klausimų pavyzdys – JK ir Japonijos susitarimas dėl visapusiškos ekonominės partnerystės[59], pirmasis JK prekybos susitarimas po „Brexit'o“, įsigaliojęs 2021 m. sausio 1 d.,[60] į kurį įtrauktos nuostatos dėl asmens duomenų[61]. Be to, EDAV pažymi, kad 2021 m. vasario 1 d. JK taip pat oficialiai paskelbė apie savo prašymą prisijungti prie Visapusiško ir pažangaus Ramiojo vandenyno šalių partnerystės susitarimo (angl. CPTPP), kuris apima Partnerystės abipus Ramiojo vandenyno (angl. TPP) susitarimą [62].

[57] Žr. JAV CLOUD įstatymą, https://www.congress.gov/bill/115th-congress/senate-bill/2383/text.

[58] Žr. 2.3.3 skirsnį.

[59] Žr. JK / Japonija: Visapusiškos ekonominės partnerystės susitarimas [CS Japonija Nr. 1/2020], https://www.gov.uk/government/publications/ukjapan-agreement-for-a-comprehensive-economic-partnership-cs-japan-no12020.

[60] Žr. JK vyriausybės gaires dėl JK prekybos susitarimų su ES nepriklausančiomis valstybėms, https://www.gov.uk/guidance/uk-trade-agreements-with-non-eu-countries.

[61] Pagal JK ir Japonijos susitarimo dėl visapusiškos ekonominės partnerystės 8.80 straipsnio 5 dalį šalys įsipareigoja raginti kurti mechanizmus, kuriais būtų skatinamas jų skirtingų teisinių požiūrių į (asmens) duomenų apsaugą suderinamumas. Pagal 8.84 straipsnį šalys įsipareigoja nedrausti ir neriboti tarpvalstybinio informacijos perdavimo elektroninėmis priemonėmis, įskaitant asmeninę informaciją, kai ši veikla yra susijusi su atitinkamo asmens verslo vykdymu, kaip apibrėžta JK ir Japonijos susitarime dėl visapusiškos ekonominės partnerystės.

[62] Pagal Partnerystės abipus Ramiojo vandenyno susitarimo 14.11 straipsnio 2 dalį šalys įsipareigoja leisti tarpvalstybinį informacijos perdavimą elektroninėmis priemonėmis, įskaitant asmeninę informaciją, kai ši veikla yra susijusi su atitinkamo asmens verslo vykdymu.

95. EDAV pažymi, kad, be JK ir JAV susitarimo pagal CLOUD įstatymą, pirmiau minėti tarptautiniai susitarimai sprendimo projekte nenagrinėjami.

96. **EDAV ragina Europos Komisiją:**

- **išnagrinėti JK duomenų apsaugos sistemos ir jos tarptautinių įsipareigojimų, ne vien JK ir JAV susitarimo pagal CLOUD įstatymą, sąveiką, visų pirma siekiant užtikrinti duomenų apsaugos lygio tęstinumą tuo atveju, kai iš EEE į JK perduodami asmens duomenys toliau perduodami į kitas trečiąsias valstybes remiantis JK sprendimu dėl tinkamumo, ir nuolat stebėti ir prireikus imtis veiksmų, jei dėl JK ir trečiųjų valstybių sudarytų kitų tarptautinių susitarimų kyla pavojus, kad gali sumažėti ES nustatytas asmens duomenų apsaugos lygis;**

- **pateikti EDAV rašytinius JK valdžios institucijų įsipareigojimus ir nurodyti konkrečias JK teisės nuostatas, susijusias su paaiškinimais dėl galimo JK ir JAV susitarimo pagal CLOUD įstatymą taikymo ir įgyvendinimo, kaip nurodyta sprendimo projekto 153 konstatuojamojoje dalyje;**

- **šiomis aplinkybėmis stebėti, ar be apsaugos priemonių, kurios galėtų būti užtikrintos tinkamai įgyvendinant ES ir JAV bendrojo susitarimo pritaikymą, JK ir JAV susitarimu pagal CLOUD įstatymą užtikrinamos tinkamos papildomos apsaugos priemonės, siekiant atsižvelgti į neskelbtiną atitinkamų kategorijų duomenų pobūdį ir specifinius reikalavimus, susijusius su elektroninių įrodymų perdavimu, kai juos tiesiogiai vienas kitam perduoda ryšių paslaugų teikėjai, o ne institucijos;**
- **įvertinti neseniai JK pasirašytuose tarptautiniuose susitarimuose, pavyzdžiui, JK ir Japonijos susitarime dėl visapusiškos ekonominės partnerystės, įtvirtintų nuostatų dėl asmens duomenų poveikį ir galimą riziką.**

97. **Penktoji problema** – susijusi su nukrypti leidžiančių nuostatų taikymu perduodant asmens duomenis į trečiąją valstybę. Nors pagal JK BDAR galimos nukrypti leidžiančios nuostatos yra tokios pačios kaip ir numatytos BDAR, svarbu, kad Informacijos komisaro biuras toliau taikytų su šių nukrypti leidžiančių nuostatų taikymu susijusį aiškinimą, suderintą su EDAV aiškinimu. Priešingu atveju arba jei JK ateityje nukryptų nuo šio aiškinimo, kiltų pavojus, kad iš EEE į trečiąsias valstybes per JK perduodamų duomenų apsaugos lygis gali sumažėti.

98. **EDAV ragina Europos Komisiją, vykdant stebėsenos užduotį, konkrečiai patikrinti, ar JK aiškinimas dėl nukrypti leidžiančių nuostatų taikymo ir toliau atitinka ES aiškinimą. Jei vis dėlto JK skirtingai aiškintų nukrypti leidžiančias nuostatas ir taip sumažintų duomenų apsaugos lygį, labai svarbu, kad Europos Komisija imtųsi būtinų veiksmų iš dalies pakeisdama sprendimą dėl tinkamumo, kad užtikrintų, jog EEE asmens duomenims, perduotiems į JK, suteikiamas apsaugos lygis vėliau nebūtų sumažintas, kai šie duomenys toliau perduodami iš JK į trečiąsias valstybes remiantis kitokiu nukrypti leidžiančių nuostatų aiškinimu.**

99. **Šeštoji problema** (paskutinė šiame skirsnyje) susijusi su tuo, kad JK duomenų apsaugos sistemoje nėra apsaugos priemonių, numatytų BDAR 48 straipsnyje.

100. Europos Komisija savo sprendimo projekte iš tiesų paaiškina, kad jeigu nėra tinkamumo taisyklių arba tinkamų apsaugos priemonių, duomenų perdavimas gali būti vykdomas tik remiantis JK BDAR 49 straipsnyje nustatytomis nukrypti leidžiančiomis nuostatomis, *„išskyrus Reglamento (ES) 2016/679 48 straipsnį, kurio JK nusprendė neįtraukti į JK BDAR.“*[63] Dėl to, kad JK duomenų apsaugos sistemoje nėra iš esmės lygiavertės BDAR 48 straipsniui nuostatos, įtvirtintos dėl duomenų perdavimo ar atskleidimo po kitos trečiosios valstybės teismo arba administracinės institucijos sprendimo, gali kilti

[63] Žr. sprendimo projekto 78 išnašą.

teisinis netikrumas dėl to, ar pagal sprendimo projektą iš EEE į JK perduodamų asmens duomenų apsaugos lygis bus iš esmės paveiktas.

101. BDAR tinkamumo kriterijų dokumente EDAV nurodo, kad, kalbant apie tolesnį duomenų perdavimą, *„tolesnis asmens duomenų perdavimas, kurį vykdo pirminis duomenų perdavimo gavėjas, turėtų būti leidžiamas tik tuo atveju, jei tolesniam gavėjui taip pat taikomos tinkamo lygio apsaugą užtikrinančios taisyklės ir jis laikosi atitinkamų nurodymų tvarkydamas duomenis duomenų valdytojo vardu.“*[64] Be to, EDAV pabrėžia, kad *„pirminis iš ES perduotų duomenų gavėjas privalo užtikrinti, kad tolesniam duomenų perdavimui, kai nėra sprendimo dėl tinkamumo, būtų numatytos tinkamos apsaugos priemonės. Toks tolesnis duomenų perdavimas turėtų būti vykdomas tik ribotais ir konkrečiais tikslais ir tik jeigu yra teisinis pagrindas tokiam duomenų tvarkymui.“*[65] Vertinant, ar JK teisine sistema šiuo atžvilgiu užtikrinamas iš esmės lygiavertis duomenų apsaugos lygis, reikia visapusiškai atsižvelgti į 48 straipsnį, kuris yra BDAR V skyriaus dalis[66].

102. Šiame kontekste EDAV pabrėžia ESTT praktiką, susijusią su piktnaudžiavimo arba neteisėtos prieigos prie duomenų ir jų naudojimo rizika, visų pirma teigdamas, kad *„kalbant apie Europos Sąjungoje garantuojamą pagrindinių teisių ir laisvių apsaugos lygį, ES teisės aktais, susijusiais su kišimusi į Chartijos 7 ir 8 straipsniuose garantuojamas pagrindines teises, pagal nusistovėjusią Teismo praktiką turi būti nustatomos aiškios ir tikslios taisyklės, reglamentuojančios priemonės taikymo sritį ir taikymą bei nustatančios minimalias apsaugos priemones, kad susijusių asmenų asmens duomenims būtų suteiktos pakankamos garantijos, leidžiančios veiksmingai apsaugoti jų duomenis nuo piktnaudžiavimo pavojaus ir nuo bet kokios neteisėtos prieigos prie tų duomenų ir jų naudojimo. Tokių apsaugos priemonių poreikis yra dar didesnis, kai asmens duomenys tvarkomi automatiniu būdu ir kai yra didelis neteisėtos prieigos prie tų duomenų pavojus“*[67].

103. Šiuo atžvilgiu EDAV pažymi, kad, remiantis sprendimo projekte pateikta informacija, JK duomenų apsaugos sistemoje nėra aiškiai numatyta, kad bet koks trečiosios valstybės teismo sprendimas ir bet koks trečiosios valstybės administracinės institucijos sprendimas, kuriuo reikalaujama, kad duomenų valdytojas arba duomenų tvarkytojas perduotų ar atskleistų asmens duomenis, gali būti pripažįstamas arba bet kokiu būdu vykdomas tik tuo atveju, jei jis grindžiamas galiojančiu tarptautiniu susitarimu tarp prašančiosios trečiosios valstybės ir JK. BDAR 48 straipsnis yra esminė BDAR V skyriaus nuostata, nes juo reikalaujama, kad asmens duomenų perdavimas arba atskleidimas priėmus trečiosios valstybės teismo ar administracinės institucijos sprendimą ar nutartį gali būti pripažintas arba vykdytinas tik tuo atveju, jei jis grindžiamas galiojančiu prašančiosios trečiosios valstybės ir Europos Sąjungos arba valstybės narės tarptautiniu susitarimu, nepažeidžiant kitų duomenų perdavimo pagrindų pagal BDAR V skyrių. Iš tiesų EDAV primena, kad *„užsienio institucijos prašymas pats savaime nėra teisinis perdavimo pagrindas. Nurodymas gali būti pripažintas tik tuo atveju, jei jis grindžiamas tarptautiniu susitarimu, pavyzdžiui, galiojančia prašančiosios trečiosios valstybės ir Europos Sąjungos arba valstybės narės savitarpio teisinės pagalbos sutartimi“*[68]. Todėl labai svarbu, kad pagal JK teisę būtų galima nustatyti iš esmės lygiavertes nuostatas.

---

[64] Žr. WP254 rev.01, p. 6.
[65] Žr. WP254 rev.01, p. 6.
[66] Žr. BDAR 44 straipsnio paskutinį sakinį, visų pirma: *„Visos šio skyriaus nuostatos taikomos siekiant užtikrinti, kad nebūtų pakenkta šiuo reglamentu garantuojamam fizinių asmenų apsaugos lygiui.“*
[67] Žr. sprendimo *Schrems I* 91 punktą.
[68] Žr. 2019 m. liepos 10 d. priimto EDAV ir EDAPP bendro atsakymo Piliečių laisvių, teisingumo ir vidaus reikalų (LIBE) komitetui dėl JAV CLOUD įstatymo poveikio Europos asmens duomenų apsaugos teisinei sistemai priedą, https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_lt.

104. Sprendimo projekte Europos Komisija pateikia JK valdžios institucijų paaiškinimus, pagal kuriuos pagal bendrąją teisę arba įstatymus užsienio teismo sprendimas, kuriuo prašoma pateikti duomenis, be tarptautinio susitarimo JK nevykdomas, o bet kokiam duomenų perdavimui užsienio teismo ar administracinės institucijos prašymu reikalinga perdavimo priemonė, pavyzdžiui, tinkamumo taisyklės arba atitinkamos apsaugos priemonės, išskyrus atvejus, kai pagal JK BDAR 49 straipsnį taikoma nukrypti leidžianti nuostata. Tačiau EDAV nebuvo pateikti Europos Komisijos ir JK valdžios institucijų[69] pasikeitimai informacija šiuo klausimu, todėl ji negali analizuoti ir nepriklausomai įvertinti, ar JK valdžios institucijų pateiktų garantijų pakanka iš esmės lygiaverčiam apsaugos lygiui užtikrinti, palyginti su BDAR 48 straipsnyje nustatytomis apsaugos priemonėmis.

105. **EDAV ragina Europos Komisiją pateikti papildomų garantijų ir konkrečių nuorodų į JK teisės aktus, kuriais būtų užtikrinama, kad apsaugos lygis pagal JK teisinę sistemą iš esmės prilygsta EEE garantuojamam apsaugos lygiui. Todėl EDAV ragina Europos Komisiją pateikti raštiškus paaiškinimus ir Jungtinės Karalystės valdžios institucijų įsipareigojimus, susijusius su iš esmės lygiavertės apsaugos tai apsaugai, kuri numatyta BDAR 48 straipsnyje, įgyvendinimu.**

106. **EDAV mano, kad yra dar svarbiau įvardyti JK teisės nuostatas, kuriomis užtikrinamas iš esmės lygiavertis duomenų apsaugos lygis, palyginti su BDAR 48 straipsnyje nustatytomis apsaugos priemonėmis, atsižvelgiant į anksčiau išsakytas abejones dėl JAV ar kitų trečiųjų valstybių institucijų pateiktų prašymų susipažinti su duomenimis JK ir į tai, kad pagal sprendimą dėl tinkamumo asmens duomenys galėtų būti perduodami iš EEE į JK be jokių papildomų garantijų ar privalomų gavėjo įsipareigojimų, susijusių su kitų trečiųjų valstybių institucijų prašymais susipažinti su duomenimis.**

3.2. Procedūriniai ir vykdymo užtikrinimo mechanizmai

107. Remdamasi BDAR tinkamumo kriterijų dokumente nustatytais kriterijais, EDAV išanalizavo šiuos sprendimo projekte įvardytus JK duomenų apsaugos sistemos aspektus: nepriklausomos priežiūros instituciją ir jos veiksmingą veikimą; sistema, kuria užtikrinamas geras atitikties lygis, ir prieigos prie tinkamų teisių gynimo mechanizmų sistemą, suteikianti asmenims ES galimybę naudotis savo teisėmis ir reikalauti žalos atlyginimo be sudėtingų administracinių ir teisminių kliūčių.

3.2.1 Kompetentinga nepriklausoma priežiūros institucija

108. EDAV palankiai vertina Europos Komisijos pastangas išsamiai išnagrinėti JK priežiūros institucijos įsteigimą, veikimą ir įgaliojimus sprendimo projekto 2.6 skyriuje. Jungtinėje Karalystėje informacijos komisarui pavesta prižiūrėti ir užtikrinti, kad būtų laikomasi JK BDAR ir 2018 m. Duomenų apsaugos įstatymo. Pagal 2018 m. Duomenų apsaugos įstatymo 12 priedą informacijos komisaras yra „Corporation Sole“, t. y. atskiras juridinis asmuo, sudarytas iš vieno asmens, kuriam padeda Informacijos komisaro biuras.

109. Dėl informacijos komisaro nepriklausomumo EDAV pabrėžia, kad JK BDAR 51 straipsnyje nėra aiškaus paaiškinimo, kad informacijos komisaras yra nepriklausoma valdžios institucija, kaip tai nurodyta BDAR 51 straipsnyje dėl priežiūros institucijų. Vis dėlto EDAV pripažįsta, kad JK BDAR 52 straipsnis panašiai atkartoja atitinkamas taisykles dėl nepriklausomumo, kaip nustatyta BDAR 52 straipsnio 1–3 dalyse.

110. Be to, EDAV pažymi, kad JK BDAR 52 straipsnyje nenustatytos pareigos, atitinkančios BDAR 52 straipsnio 4–6 dalis, kuriomis aiškiai užtikrinama, kad atitinkama priežiūros institucija būtų aprūpinta

[69] Žr. sprendimo projekto 78 išnašą.

ištekliais, reikalingais veiksmingam jos užduočių atlikimui ir įgaliojimų vykdymui. Tačiau EDAV pripažįsta, kad 2018 m. Duomenų apsaugos įstatyme yra nuostatų, kuriomis siekiama užtikrinti tinkamą Informacijos komisaro biuro[70] finansavimą, taip pat ir tas aplinkybes, kad Informacijos komisaro biuras šiuo metu yra viena didžiausių priežiūros institucijų, palyginti su priežiūros institucijomis ES / EEE. Kadangi nuolatinis tinkamų išteklių, visų pirma personalo ir biudžeto[71], skyrimas yra būtinas siekiant užtikrinti tinkamą priežiūros institucijos veikimą, kad ji galėtų vykdyti visas jai pavestas užduotis, ir kadangi Europos Parlamentas neseniai pažymėjo, kad tai yra labai svarbu[72], EDAV mano, kad būtina skirti ypatingą dėmesį būsimiems pokyčiams šioje srityje.

111. **Todėl EDAV ragina Europos Komisiją stebėti bet kokius pokyčius, susijusius su išteklių skyrimu Informacijos komisaro biurui, kurie galėtų pakenkti tinkamam Informacijos komisaro biuro užduočių vykdymui.**

3.2.2. Duomenų apsaugos sistema, kuria užtikrinamas geras atitikties lygis

112. Sprendimo projekte išsamiai nagrinėjami Informacijos komisaro biuro įgaliojimai pagal JK BDAR 58 straipsnį ir 2018 m. Duomenų apsaugos įstatymo, siekiant užtikrinti teisės aktų stebėseną ir vykdymą. EDAV pripažįsta, kad JK BDAR 58 straipsnis artimai atkartoja atitinkamas taisykles dėl priežiūros institucijos įgaliojimų, kaip nustatyta BDAR 58 straipsnyje. Kalbant apie įgaliojimus skirti administracines baudas, atsižvelgiant į kiekvieno konkretaus atvejo aplinkybes, JK BDAR 83 straipsnyje pateikiamos panašios nuostatos ir didžiausios sumos, kaip ir BDAR 83 straipsnyje Taigi EDAV mano, kad šiuo metu JK teisinė sistema šioje srityje atitinka atitinkamuose ES teisės aktuose nustatytus standartus. Šiuo atžvilgiu EDAV vis dėlto pabrėžia, kad *veiksmingų* sankcijų buvimas atlieka svarbų vaidmenį užtikrinant, kad būtų laikomasi taisyklių.[73]

113. **Atsižvelgdama į tai, kas išdėstyta pirmiau, EDAV ragina Europos Komisiją stebėti JK duomenų apsaugos sistemoje numatytų sankcijų ir atitinkamų teisių gynimo priemonių veiksmingumą.**

3.2.3. Įgyvendinant duomenų apsaugos sistemą privaloma teikti paramą ir padėti duomenų subjektams pasinaudoti savo teisėmis ir atitinkamais teisių gynimo mechanizmais

114. Veiksmingas priežiūros mechanizmas, leidžiantis nepriklausomai tirti skundus, kad būtų galima praktikoje nustatyti duomenų subjekto teisių pažeidimus ir už juos bausti, taip pat veiksminga administracinė ir teisminė teisių gynimo priemonė (įskaitant žalos, patirtos dėl neteisėto duomenų subjekto asmens duomenų tvarkymo, atlyginimą) yra svarbiausi aspektai vertinant, ar duomenų apsaugos sistema užtikrina tinkamo lygio apsaugą.

115. EDAV palankiai vertina tai, kad Informacijos komisaro biuras savo interneto svetainėje pateikia išsamią informaciją ir gaires, kuriomis siekiama didinti duomenų valdytojų ir duomenų tvarkytojų informuotumą apie jų prievoles ir pareigas, taip pat padėti duomenų subjektams, kad jie būtų informuoti apie savo asmens duomenų teises ir galėtų ginti savo individualias teises pagal JK BDAR ir 2018 m. Duomenų apsaugos įstatymą.

116. **Nepaisant dabartinės padėties, EDAV ragina Europos Komisiją nuolat stebėti, kokią konkrečią paramą Informacijos komisaro biuras teikia asmenims, kurių asmens duomenys pagal sprendimą**

[70] Žr. 2018 m. Duomenų apsaugos įstatymo 137, 138, 182 skirsnius ir 12 priedo 9 punktą.
[71] Žr. WP 254 rev.01, p. 7.
[72] 2021 m. kovo 25 d. Europos Parlamento rezoliucijos dėl Komisijos vertinimo ataskaitos dėl Bendrojo duomenų apsaugos reglamento įgyvendinimo praėjus dvejiems metams nuo jo taikymo pradžios, 15 punktas, https://www.europarl.europa.eu/doceo/document/B-9-2021-0211_LT.html.
[73] Žr. WP 254 rev.01, p. 7.

dėl tinkamumo buvo perduoti JK, kad padėtų jiems naudotis savo teisėmis pagal JK duomenų apsaugos tvarką.

4. JK VALDŽIOS INSTITUCIJŲ GALIMYBĖ SUSIPAŽINTI SU IŠ ES PERDUOTAIS ASMENS DUOMENIMIS IR JŲ NAUDOJIMAS

4.1. JK valdžios institucijų galimybė susipažinti su duomenimis ir jų naudojimas baudžiamosios teisėsaugos tikslais

4.1.1. Teisiniai pagrindai ir taikomi apribojimai / apsaugos priemonės

117. Kalbant apie Europos Komisijos atliktą ir sprendimo projekto 132 ir paskesnėse konstatuojamosiose dalyse pateiktą vertinimą **dėl prieigos teisėsaugos tikslais**, Europos Komisija pateikia išsamią informaciją su niuansais ir iš esmės daro suprantamas išvadas. Todėl EDAV šioje nuomonėje nekartoja daugumos nustatytų faktų ir vertinimų. Tačiau kai kuriais atvejais faktų aprašymo ar išvadų paaiškinimo nepakanka, kad EDAV jas palaikytų.

4.1.1.1. Sutikimo naudojimas

118. EDAV atkreipia dėmesį į tai, kad sprendimo projekto 184 išnašoje Europos Komisija teigia, [74] jog **sutikimo naudojimas** nėra svarbus pagal tinkamumo scenarijų, nes duomenų perdavimo atvejais JK teisėsaugos institucija tiesiogiai nerenka duomenų iš duomenų subjekto sutikimo pagrindu. Todėl Europos Komisija nevertina sutikimo kaip teisinio pagrindo, kuris naudojamas policijos veikloje.

119. Šiuo atžvilgiu EDAV primena, kad pagal BDAR 45 straipsnio 2 dalies a punktą reikalaujama įvertinti daugybę aspektų, neapsiribojant vien perdavimo situacija, įskaitant *„teisinės valstybės principą, pagarbą žmogaus teisėms ir pagrindinėms laisvėms, atitinkamus bendruosius ir atskiriems sektoriams skirtus teisės aktus, įskaitant [...] baudžiamą[ją[teis[ę[“*.

120. EDAV, remdamasi ir Europos Komisijos informacija , pateikta jos įgyvendinimo sprendimo pagal Europos Parlamento ir Tarybos direktyvą (ES) 2016/680 dėl tinkamos asmens duomenų apsaugos JK projekto 38 konstatuojamojoje dalyje (toliau – sprendimo dėl ES teisėsaugos direktyvos projekto), pažymi, kad sutikimo, kaip jis suformuluotas JK sistemoje, naudojimui teisėsaugos kontekste visada reikėtų teisinio pagrindo, kuriuo būtų galima remtis. Tai reiškia, kad net jei policija turi teisės aktais nustatytus įgaliojimus tvarkyti duomenis tyrimo tikslais, tam tikromis konkrečiomis aplinkybėmis (pavyzdžiui, DNR mėginiui paimti) policija gali manyti, kad tikslinga prašyti duomenų subjekto sutikimo.

121. **EDAV ragina Europos Komisiją į sprendimą dėl tinkamumo įtraukti savo analizę dėl galimo sutikimo naudojimo teisėsaugos kontekste, kaip numatyta sprendimo dėl ES teisėsaugos direktyvos projekte**.

4.1.1.2. Kratos orderiai ir įrodymų pateikimo orderiai

122. Nors EDAV neturi pastabų dėl policijos atliekamos įrodymų paieškos pasinaudojant kratos orderiais ir įrodymų pateikimo orderiais apskritai, iš sprendimo projekto 136 konstatuojamosios dalies matyti, kad Europos Komisija savo argumentuose, susijusiuose su teisėsaugos institucijų prieiga prie

[74] Žr. sprendimo projekto 37 išnašą.

duomenų, daugiausia dėmesio skyrė policijai, o kitų teisėsaugos institucijų atliekamas asmens duomenų tvarkymas buvo mažiau nagrinėjamas.

123. Pavyzdžiui, JK Aiškinamojo dokumento dėl sprendimų dėl tinkamumo F skirsnio „Teisėsauga“[75], p. 11 siūloma, kad **Nacionalinė kovos su nusikalstamumu agentūra** (angl. NCA) galėtų būti ypač svarbi teisėsaugos agentūra, kuri, be kita ko, atlieka platesnę kriminalinės žvalgybos funkciją. Nacionalinė kovos su nusikalstamumu agentūra savo misiją apibūdina kaip žvalgybinės informacijos, gaunamos iš įvairių šaltinių, telkimą, siekiant kuo labiau padidinti analizę, vertinimą ir taktines galimybes, įskaitant techninį pranešimų perėmimą, teisėsaugos partnerius JK ir užjūrio valstybėse, saugumo ir žvalgybos agentūrų informaciją[76]. Nacionalinė kovos su nusikalstamumu agentūra taip pat yra viena iš pagrindinių tarptautinių teisėsaugos dialogo partnerių ir atlieka svarbų vaidmenį keičiantis kriminalinės žvalgybos informacija[77].

124. EDAV taip pat atkreipia dėmesį į tai, kad Vyriausybės ryšių valdyba (angl. GCHQ), kurios veikla paprastai patenka į 2018 m. Duomenų apsaugos įstatymo 4 dalies, t. y. nacionalinio saugumo, taikymo sritį, taip pat atlieka aktyvų vaidmenį mažinant žalą visuomenei ir finansinę žalą, kurią JK kelia sunkių formų organizuoti nusikaltimai, glaudžiai bendradarbiaudama su Vidaus reikalų ministerija, Nacionaline kovos su nusikalstamumu agentūra, Pajamų mokesčių ir muitų departamentu (angl. HMRC) ir kitais vyriausybės departamentais[78]. Jos veikla susijusi su kova su seksualine prievarta prieš vaikus, sukčiavimu, kitais ekonominiais nusikaltimais, įskaitant pinigų plovimą, technologijų naudojimu nusikalstamiems tikslams, kibernetiniais nusikaltimais, organizuotu imigracijos nusikalstamumu, įskaitant prekybą žmonėmis, ir narkotikais, šaunamaisiais ginklais ir kita neteisėta kontrabandos veikla.

125. **EDAV ragina Europos Komisiją savo analizę papildyti ir išanalizuoti teisėsaugos srityje veikiančias agentūras, kurios, vykdydamos savo kasdienę veiklą, tikėtina, renka ir analizuoja duomenis, įskaitant asmens duomenis, visų pirma Nacionalinę kovos su nusikalstamumu agentūrą. Be to, EDAV ragina Europos Komisiją atidžiau išnagrinėti tokias agentūras kaip antai Vyriausybės ryšių**

[75] Žr. 2020 m. kovo 13 d. JK vyriausybės Aiškinamojo dokumento dėl sprendimų dėl tinkamumo F skirsnį „Teisėsauga“, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.

[76] Žr. Nacionalinės nusikaltimų tyrimo agentūros svetainę: Žvalgyba. JK poveikį darančių sunkių formų organizuotų nusikaltimų apžvalgos gerinimas, https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work/intelligence-enhancing-the-picture-of-serious-organised-crime-affecting-the-uk.

[77] Nors ne visa Nacionalinės kovos su nusikalstamumu agentūros tvarkoma žvalgybos informacija yra asmens duomenys, didelė jos dalis gali būti asmens informacija, o čia aprašyta veikla skiriasi nuo klasikinės policijos veiklos, todėl teisėsaugos institucijų prieigos prie asmens duomenų JK vertinimas būtų neišsamus, jei nebūtų išsamiai įvertinta Nacionalinės kovos su nusikalstamumu agentūros veikla. Atrodo tikslinga įsitikinti, kad duomenų apsaugos principams suteikiama vienoda reikšmė visose atitinkamose teisėsaugos institucijose, taip atkreipiant dėmesį į daug duomenų turinčią agentūrą, kaip antai Nacionalinė kovos su nusikalstamumu agentūra. Be to, „žvelgiant į ateitį“, paaiškinime toliau teigiama, kad *„[mes] nuolat ieškome naujų galimybių rinkti, plėtoti ir tobulinti tradicinius pajėgumus, kad padidintume žvalgybinės informacijos, kurią galima panaudoti tiek JK, tiek užsienyje, kiekį ir kokybę.“ „Todėl, pasinaudodami Nusikaltimų ir teismų įstatymu agentūrai suteiktais įgaliojimais, kuriame naujus nacionalinius duomenų panaudojimo pajėgumus, kad būtų galima susieti, pasiekti ir panaudoti visos vyriausybės turimus duomenis.“* [...] *„ Visa tai padidins mūsų operatyvumą ir lankstumą, kad galėtume reaguoti į naujas grėsmes ir veikti aktyviai, rinkti ir analizuoti informaciją ir žvalgybos duomenis apie kylančias grėsmes, kad galėtume imtis veiksmų, kol grėsmės dar nepasireiškė.“*

[78] Žr. Vyriausybės ryšių valdybos svetainėje: Misija, rimtų formų organizuoti nusikaltimai, https://www.gchq.gov.uk/section/mission/serious-crime.

valdyba, kurių veikla patenka į teisėsaugos ir nacionalinio saugumo sritį, ir joms taikomą asmens duomenų tvarkymo teisinę sistemą.

4.1.1.3. Tyrimo įgaliojimai teisėsaugos tikslais

126. Pagal BDAR tinkamumo kriterijų dokumento 4 skyrių „Esminės trečiųjų valstybių garantijos, suteikiamos prieigai teisėsaugos ir nacionalinio saugumo tikslais, siekiant apriboti pagrindinių teisių pažeidimus“, EDAV primena, kad „*[a]tsižvelgdamas į tai, teismas taip pat kritiškai pažymėjo, kad ankstesniame Saugaus uosto sprendime nenustatyta, kad Jungtinėse Amerikos Valstijose yra valstybinio pobūdžio taisyklių, skirtų nustatyti asmenų, kurių asmens duomenys perduoti iš Sąjungos į Jungtines Amerikos Valstijas, galimoms pagrindinių teisių apribojimų riboms, t. y.* ***apribojimų, kuriuos šios šalies valstybiniai subjektai gali nustatyti siekdami teisėtų tikslų****, pavyzdžiui, nacionalinio saugumo.*“[79] Šiame tinkamumo kriterijų dokumente EDAV nurodo, kad **norint, kad prieiga prie duomenų**[80] nacionalinio saugumo arba **teisėsaugos tikslais būtų laikoma tinkama, visos trečiosios valstybės turi laikytis keturių Europos pagrindinių garantijų,** visų pirma **turi būti įrodytas būtinumas ir proporcingumas siekiamų teisėtų tikslų atžvilgiu.**

127. Šiame sprendimo projekto skirsnyje Europos Komisija daro išvadą (139 konstatuojamoji dalis): „*kadangi 2016 m. Tyrimo įgaliojimų įstatyme numatyti tyrimo įgaliojimai yra tokie patys, kokius turi nacionalinio saugumo agentūros, tokiems įgaliojimams taikomos sąlygos, apribojimai ir apsaugos priemonės išsamiai aptariamos skirsnyje dėl JK valdžios institucijų prieigos prie asmens duomenų ir jų naudojimo nacionalinio saugumo tikslais*“. Tačiau pagal ESTT praktiką taikant būtinumo ir proporcingumo principą valstybių narių teisės aktams, kuriais valdžios institucijoms leidžiama saugoti asmens duomenis ir su jais susipažinti, teisėti tikslai, pavyzdžiui, nacionalinis saugumas ar kova su sunkiais nusikaltimais, yra nevienodi, todėl vienu iš jų galima pateisinti tam tikros rūšies perėmimą, o kitu – ne[81].

128. **Todėl EDAV norėtų, kad sprendime būtų konkrečiai įvertintas 174 ir paskesnėse konstatuojamosiose dalyse (tai yra skirsnis, skirtas priemonėms, kuriomis siekiama nacionalinio saugumo tikslų) aprašytų sąlygų, apribojimų ir apsaugos priemonių būtinumas ir proporcingumas, kai šios sąlygos, apribojimai ir apsaugos priemonės taikomos teisėsaugos tikslais. Todėl Valdyba ragina Europos Komisiją toliau aiškintis, ar aprašytas asmens duomenų saugojimas ir prieiga prie jų teisėsaugos tikslais yra pakankamai apriboti, kad būtų užtikrintas apsaugos lygis, iš esmės lygiavertis tam, kuris garantuojamas ES.**

4.1.2. Tolimesnis teisėsaugos tikslais surinktos informacijos naudojimas (140–154 konstatuojamosios dalys)

129. EDAV pažymi, kad JK duomenų apsaugos sistemoje numatytos panašios apsaugos priemonės ir apribojimai, susiję su tolesniu surinktos informacijos naudojimu teisėsaugos tikslais, kaip ir ES teisėje.

4.1.2.1. Tolimesnis naudojimas kitais teisėsaugos tikslais

130. 2018 m. Duomenų apsaugos įstatyme iš tiesų numatyta, kad kompetentingos institucijos teisėsaugos tikslais surinkti asmens duomenys gali būti toliau tvarkomi (pirminio duomenų valdytojo arba kito duomenų valdytojo) bet kuriuo kitu teisėsaugos tikslu, jei duomenų valdytojas pagal įstatymą yra įgaliotas tvarkyti duomenis tuo kitu tikslu ir jei toks tvarkymas yra būtinas ir proporcingas tam tikslui.

[79] Žr. WP254 rev.01, p. 9.
[80] Žr. EDAV rekomendacijas Nr. 02/2020 dėl Europos pagrindinių garantijų taikant stebėjimo priemones.
[81] Žr. 2020 m. spalio 6 d. ESTT sprendimą *La Quadrature du Net ir kiti*, sujungtos bylos C-511/18, C-512/18 ir C-520/18, , ECLI:EU:C:2020:791.

Europos Komisija pažymi, kad gaunančiosios institucijos atliekamam duomenų tvarkymui taikomos visos 2018 m. Duomenų apsaugos įstatymo 3 dalyje numatytos apsaugos priemonės. Tačiau EDAV pabrėžia, kad pagal 2018 m. Duomenų apsaugos įstatymo 3 dalies 44 skirsnio 4 dalį, 45 skirsnio 4 dalį, 48 skirsnio 3 dalį ir 68 skirsnio 7 dalį numatyta galimybė apriboti duomenų subjekto teises, o 79 skirsnyje numatyta galimybė išduoti sertifikatus, patvirtinančius, kad apribojimas yra būtina ir proporcinga priemonė nacionaliniam saugumui apsaugoti. **Todėl EDAV rekomenduoja Europos Komisijai toliau vertinti galimą tokių apribojimų poveikį asmens duomenų apsaugos lygiui, susijusį su tolesniu surinktos informacijos naudojimu. Taip pat reikėtų pateikti daugiau paaiškinimų dėl JK teisinės sistemos, pagal kurią leidžiamas toks tolesnis dalijimasis duomenimis, visų pirma 2017 m. Skaitmeninės ekonomikos įstatymu, taip pat 2013 m. Nusikaltimų ir teismų įstatymu, pagal kuriuos leidžiama dalytis informacija su Nacionaline kovos su nusikalstamumu agentūra.**

4.1.2.2. Tolesnis naudojimas kitais nei teisėsaugos tikslais Jungtinėje Karalystėje

131. 2018 m. Duomenų apsaugos įstatyme taip pat nustatyta, kad bet kuriuo teisėsaugos tikslu surinkti asmens duomenys gali būti tvarkomi kitu nei teisėsaugos tikslu, kai tvarkyti duomenis leidžiama pagal įstatymą. Šiuo atveju teisinis pagrindas, leidžiantis tokį dalijimąsi duomenimis, yra 2008 m. Kovos su terorizmu įstatymo 19 skirsnis. Šiuo atžvilgiu EDAV pažymi, kad Kovos su terorizmu įstatymo 19 skirsnio taikymo sritis ir nuostatos Europos Komisijos vertinime nėra išsamiai aptartos ir gali reikšti tolesnį platesnio pobūdžio naudojimą, visų pirma kiek tai susiję su 19 skirsnio 2 dalimi, kurioje nustatyta, kad „[*i]nformaciją, kurią bet kuri žvalgybos tarnyba gavo vykdydama bet kurią iš savo funkcijų, ta tarnyba gali naudoti vykdydama bet kurią kitą savo funkciją*.“

132. EDAV taip pat pažymi, kad Europos Komisijos nuoroda į tai, kad kompetentingos institucijos yra valdžios institucijos, kurios privalo veikti laikydamosi EŽTK, įskaitant jos 8 straipsnį, taip užtikrindamos, kad visas teisėsaugos institucijų ir žvalgybos tarnybų dalijimasis duomenimis atitiktų duomenų apsaugos teisės aktus ir EŽTK, galėtų būti dar labiau pagrįsta nurodant atitinkamus JK teisinės sistemos teisės aktus ir įstatymus, kuriuose aiškiai ir tiksliai nustatytos tokios ribos.

4.1.2.3. Tolesnis naudojimas tolesnio duomenų perdavimo už JK ribų kontekste

133. Nors Europos Komisija nurodė, kad JK ir JAV susitarimas pagal CLOUD įstatymą gali turėti įtakos tolesniam duomenų perdavimui iš JK esančių ryšių paslaugų teikėjų į JAV, EDAV taip pat pabrėžia, kad šio susitarimo įsigaliojimas taip pat gali turėti įtakos tolesniam informacijos, surinktos perdavus informaciją iš JK teisėsaugos institucijų, naudojimui, visų pirma susijusiam su įsakymų išdavimu ir perdavimu pagal JK ir JAV susitarimo pagal CLOUD įstatymą 5 straipsnį.

134. Žvelgiant plačiau, EDAV mano, kad dvišalių susitarimų su trečiosiomis valstybėmis sudarymas ateityje teisėsaugos institucijų bendradarbiavimo tikslais, kuriais suteikiamas teisinis pagrindas šioms valstybėms perduoti asmens duomenis, taip pat gali turėti didelės įtakos tolesnio surinktos informacijos naudojimo sąlygoms, nes tokie susitarimai turės įtakos vertinamai JK duomenų apsaugos teisinei sistemai. Todėl EDAV rekomenduoja Europos Komisijai toliau vertinti šį klausimą, nustatyti, ar yra sudaryta tarptautinių susitarimų, ir paaiškinti, ar šių susitarimų nuostatos gali turėti įtakos JK duomenų apsaugos teisės taikymui, ir numatyti papildomus apribojimus ar išimtis, susijusias su tolesniu teisėsaugos tikslais surinktos informacijos naudojimu ir atskleidimu užjūrio valstybėse. EDAV mano, kad tokia informacija ir vertinimas yra būtini, kad būtų galima visapusiškai įvertinti JK teisinės sistemos ir praktikos, susijusios su duomenų atskleidimu ir tolesniu naudojimu užjūrio valstybėse, teikiamos apsaugos lygį.

4.1.3. Priežiūra

135. EDAV pažymi, kad baudžiamosios teisėsaugos institucijų priežiūrą užtikrina ne tik Informacijos komisaro biuras, bet ir įvairūs komisarai. Tinkamumo išvadų projekte minimi Tyrimų įgaliojimų komisaras, Biometrinės informacijos saugojimo ir naudojimo komisaras, taip pat Stebėjimo kamerų komisaras. Šiame kontekste pažymėtina, kad ESTT ne kartą pabrėžė nepriklausomos priežiūros būtinybę. Prieigos prie į JK perduotų asmens duomenų klausimais itin svarbus yra Tyrimų įgaliojimų komisaras. EDAV supranta, kad Tyrimų įgaliojimų komisaras yra vadinamasis teismo komisaras, kaip ir kiti nacionalinio saugumo skyriaus kontekste nurodyti teismo komisarai, ir kad šie teismo komisarai naudojasi teisėjų nepriklausomumu ir tada, kai eina komisarų pareigas. Kalbant apie Tyrimų įgaliojimų komisarą, Europos Komisija sprendimo projekto 245 konstatuojamojoje dalyje paaiškina, kad jis veikia nepriklausomai kaip laikantis vadinamojo ištiestosios rankos principo veikianti institucija, nors jį finansuoja Vidaus reikalų ministerija.

136. Sprendimo projekte EDAV nerado daugiau paaiškinimų, kurie leistų įvertinti Tyrimų įgaliojimų komisaro, Biometrinės informacijos saugojimo ir naudojimo komisaro, taip pat Stebėjimo kamerų komisaro nepriklausomumo.

137. **Europos Komisija raginama toliau vertinti teismo komisarų nepriklausomumą taip pat ir tais atvejais, kai komisaras (jau) nebedirba teisėju, taip pat įvertinti Biometrinės informacijos saugojimo ir naudojimo komisaro ir Stebėjimo kamerų komisaro nepriklausomumą.**

4.2. Bendroji duomenų apsaugos teisinė sistema nacionalinio saugumo srityje

4.2.1. Nacionalinio saugumo sertifikatai

138. Pagal 2018 m. Duomenų apsaugos įstatymo 111 skirsnį duomenų valdytojai gali prašyti ministro, vyriausybės nario, generalinio prokuroro arba Škotijos generalinio advokato išduoti nacionalinio saugumo sertifikatus, kuriais patvirtinama, kad 2018 m. Duomenų apsaugos įstatymo 4–6 dalyse įtvirtintos pareigų ir teisių išimtys yra būtina ir proporcinga nacionalinio saugumo apsaugos priemonė. Šiais sertifikatais siekiama duomenų valdytojams suteikti daugiau teisinio tikrumo ir jie bus įtikinamas įrodymas, kad asmens duomenys tvarkomi pagal nacionalinio saugumo reikalavimus. Vis dėlto reikėtų paminėti, kad šie sertifikatai nereikalingi norint vadovautis nacionalinio saugumo išimtimis, jie yra skaidrumo priemonė[82].

139. Iš 2018 m. Duomenų apsaugos įstatymo 20 priedo 17 ir 18 skirsnių EDAV supranta, kad nacionalinio saugumo sertifikato, išduoto pagal 1998 m. Duomenų apsaugos įstatymą (toliau – senasis sertifikatas), galiojimas asmens duomenų tvarkymui pagal 2018 m. Duomenų apsaugos įstatymą buvo pratęstas iki 2019 m. gegužės 25 d. Jei senieji sertifikatai nebuvo pakeisti arba atšaukti, iki šios datos jie buvo laikomi išduotais pagal 2018 m. Duomenų apsaugos įstatymą.

140. Tačiau, jei pagal 1998 m. Duomenų apsaugos įstatymą išduotame nacionalinio saugumo sertifikate nėra aiškios galiojimo pabaigos datos, EDAV supranta, kad toks sertifikatas toliau galios duomenų tvarkymui pagal 1998 m. Duomenų apsaugos įstatymą, nebent sertifikatas būtų atšauktas arba

[82] Žr. 2020 m. rugpjūčio mėn. Vidaus reikalų ministerijos 2018 m. Duomenų apsaugos įstatymo, Nacionalinio saugumo sertifikatų gairių 4 punktą, p. 3., https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf.

panaikintas[83]. Nors šių senų sertifikatų teikiama apsauga apsiriboja asmens duomenų tvarkymu pagal 1998 m. Duomenų apsaugos įstatymą, EDAV atkreipia dėmesį į tai, kad nauji nacionalinio saugumo sertifikatai gali būti išduoti pagal 1998 m. Duomenų apsaugos įstatymą asmens duomenims, kurie buvo tvarkomi pagal 1998 m. Duomenų apsaugos įstatymą[84].

141. **Siekiant išsamumo, EDAV ragina Europos Komisiją sprendimo projekte paaiškinti, kad nacionalinio saugumo sertifikatai vis dar gali būti išduodami pagal 1998 m. Duomenų apsaugos įstatymą. Be to, EDAV ragina Europos Komisiją savo sprendimo projekte aprašyti žalos atlyginimo ir priežiūros mechanizmus, susijusius su sertifikatais, išduotais pagal 1998 m. Duomenų apsaugos įstatymą. Galiausiai, EDAV ragina Europos Komisiją į sprendimo projektą įtraukti esamų sertifikatų, išduotų pagal 1998 m. Duomenų apsaugos įstatymą, skaičių ir šį aspektą atidžiai stebėti.**

4.2.2. Teisė taisyti ir trinti duomenis

142. Dėl teisės ištaisyti ir ištrinti duomenis EDAV atkreipia dėmesį, kad pagal 2018 m. Duomenų apsaugos įstatymo 100 ir 149 straipsnius duomenų subjektai turi galimybę kreiptis į Aukštąjį Teismą (Škotijoje – į Sesijų teismą), kad šis įpareigotų duomenų valdytoją nedelsiant ištaisyti arba ištrinti jų duomenis.

143. **EDAV pabrėžia, kad reikia veiksmingai užtikrinti naudojimąsi duomenų subjektų teisėmis, todėl ragina Europos Komisiją sprendimo projekte aprašyti, kaip 2018 m. Duomenų apsaugos įstatymo 100 skirsnis veikia praktikoje, ir atidžiai stebėti šio skirsnio taikymą.**

4.2.3. Nacionalinio saugumo išimtys

144. EDAV nori atkreipti dėmesį į 2018 m. Duomenų apsaugos įstatymo 110 skirsnį, visų pirma į 11 priedą, kuriame nustatyti konkretūs tikslai, kuriais žvalgybos tarnybos gali nukrypti nuo tam tikrų duomenų apsaugos principų, be kita ko, susijusių su duomenų subjektų teisėmis, ir neprivalo Informacijos komisaro biurui pranešti apie asmens duomenų saugumo pažeidimus[85].

145. **EDAV ragina Europos Komisiją išsamiau paaiškinti išimčių taikymo sritį, nes jai kyla klausimas, ar visos 2018 m. Duomenų apsaugos įstatymo 11 priede numatytos išimtys yra svarbios žvalgybos tarnybų darbui ir ar jomis užtikrinamas lygiavertiškumas su būtinumo ir proporcingumo principais**. Visų pirma **EDAV prašo Europos Komisijos pateikti daugiau paaiškinimų, kokiomis aplinkybėmis žvalgybos tarnyba galėtų remtis 2018 m. Duomenų apsaugos įstatymo 11 priedo 10 skirsniu, kuriame nustatyta, kad *„[i]švardytos nuostatos netaikomos asmens duomenims, kuriuos sudaro įrašai apie duomenų valdytojo ketinimus, susijusius su bet kokiomis derybomis su duomenų subjektu, tiek, kiek išvardytų nuostatų taikymas galėtų pakenkti deryboms.“***

4.3. JK valdžios institucijų galimybė susipažinti su duomenimis ir jų naudojimas nacionalinio saugumo tikslais

[83] Žr. 2020 m. rugpjūčio mėn. Vidaus reikalų ministerijos 2018 m. Duomenų apsaugos įstatymo, Nacionalinio saugumo sertifikatų gaires, p. 5.
[84] Žr. 2020 m. rugpjūčio mėn. Vidaus reikalų ministerijos 2018 m. Duomenų apsaugos įstatymo, Nacionalinio saugumo sertifikatų gairių 8 punktą, p. 5.
[85] Tikslai yra tokie: „nusikaltimų“ prevencija ir atskleidimas, „informacija, kurią reikia atskleisti pagal įstatymus ir kt., arba susijusi su teisminiais procesais“, „parlamentinis imunitetas“, „teisminiai procesai“, „Karūnos garbė ir orumas“, „ginkluotosios pajėgos“, „ekonominė gerovė“, „teisininko profesinės paslapties apsauga“, „derybos“, „duomenų valdytojo pateiktos konfidencialios rekomendacijos“, „egzaminų scenarijai ir pažymiai“, „moksliniai tyrimai ir statistika“ ir „archyvavimas viešojo intereso labui“.

146. Bendrai kalbant EDAV pripažįsta, kad valstybėms suteikiama plati veiksmų laisvė nacionalinio saugumo klausimais, ką pripažįsta ir EŽTT. EDAV taip pat primena, kad, kaip pabrėžta atnaujintose Rekomendacijose dėl Europos pagrindinių garantijų taikant stebėjimo priemones[86], Europos Sąjungos sutarties 6 straipsnio 3 dalyje nustatyta, kad EŽTK įtvirtintos pagrindinės teisės yra bendrieji ES teisės principai. Tačiau, kaip savo praktikoje primena ESTT, kol ES nėra prisijungusi prie EŽTK, tai nėra teisinis dokumentas, oficialiai įtrauktas į ES teisę[87]. Taigi pagal BDAR 45 straipsnį reikalaujamas pagrindinių teisių apsaugos lygis turi būti nustatomas remiantis to reglamento nuostatomis, atsižvelgiant į ES chartijoje įtvirtintas pagrindines teises. Atsižvelgiant į tai, pagal ES chartijos 52 straipsnio 3 dalį joje įtvirtintos teisės, atitinkančios EŽTK garantuojamas teises, turi turėti tokią pačią reikšmę ir taikymo sritį kaip ir EŽTK nustatytos teisės. Todėl, kaip priminė ESTT, reikia atsižvelgti į EŽTT praktiką, susijusią su teisėmis, kurios taip pat numatytos ES chartijoje, kaip į minimalią apsaugos ribą aiškinant atitinkamas ES chartijoje numatytas teises[88]. Tačiau pagal ES chartijos 52 straipsnio 3 dalies paskutinį sakinį *„ši nuostata netrukdo Sąjungos teisės aktais nustatyti platesnę apsaugą*.“

147. Todėl šiame vertinime EDAV atsižvelgė į EŽTT praktiką tiek, kiek ES chartija, kaip ją aiškina ESTT, nenumato aukštesnio apsaugos lygio, kuriame būtų nustatyti kitokie reikalavimai nei EŽTT praktikoje.

4.3.1. Teisiniai pagrindai, apribojimai ir apsaugos priemonės. Tyrimo įgaliojimai nacionalinio saugumo kontekste

4.3.1.1. Bendrosios pastabos

148. EDAV primena, kad 2016 m. Tyrimo įgaliojimų įstatyme yra neseniai priimtas įstatymas, kuriuo iš dalies pakeistos kelios 1994 m. Žvalgybos tarnybų įstatymo nuostatos. Jame nustatyta, kokiu mastu gali būti naudojami tam tikri tyrimo įgaliojimai, kuriais kišamasi į privatumą[89]. Nepaisant to, kad buvo parengtos dvi Tyrimų įgaliojimų komisarų ataskaitos, kuriose pateikiama naudingos informacijos apie šios naujos teisinės sistemos taikymą, vis dar neatlikta tam tikrų aspektų, visų pirma susijusių su selektoriais ir taikomais paieškos kriterijais, peržiūra.

149. Be to, bendrai kalbant apie 2016 m Tyrimo įgaliojimų įstatymą ir jos taikymo sritį, EDAV pabrėžia šiuos keturis dėmesio vertus aspektus:

150. Dėl **pirmojo klausimo**, susijusio su įstatymo ypatybėmis, EDAV norėtų pabrėžti du aspektus:

151. Pirma, EDAV pažymi, kad teisės aktuose nurodomi platūs 2016 m Tyrimo įgaliojimų įstatyme numatytų procedūrų naudojimo tikslai, o ne asmenų, kurių duomenys gali būti renkami pagal 2016 m Tyrimo įgaliojimų įstatymo 2–7 dalis, kategorijos. Šiuo atžvilgiu EDAV primena, kad turėtų būti ryšys tarp asmenų, kuriems gali būti taikomos stebėjimo priemonės, kategorijų ir tikslų, kurių siekiama teisės aktuose apibrėžiant subjektinę teisės taikymo sritį.

152. Be to, EDAV taip pat pabrėžia, kad „telekomunikacijų operatorių“, „telekomunikacijų paslaugos“ ir „telekomunikacijų sistemos“ apibrėžtys, kuriomis apibrėžiama įstatymo taikymo sritis, taip pat yra labai plačios ir iš dalies neaiškios. Iš tiesų EDAV pabrėžia, kad šios sąvokos 2016 m Tyrimo įgaliojimų įstatymo taikymo srityje turi būti suprantamos daug plačiau nei pagal telekomunikacijų teisės aktus,

[86] Žr. EDAV rekomendacijas Nr. 02/2020 dėl Europos pagrindinių garantijų taikant stebėjimo priemones.
[87] Žr. Sprendimo *Schrems II* 98 punktą.
[88] Žr. 2020 m. spalio 6 d. ESTT sprendimo *La Quadrature du Net ir kiti*, sujungtos bylos C-511/18, C-512/18 ir C-520/18, , ECLI:EU:C:2020: 791, 124 punktą.
[89] Žr. 2016 m Tyrimo įgaliojimų įstatymo 1 skirsnį.

kaip apibrėžta, pavyzdžiui, Europos elektroninių ryšių kodekse[90]. EDAV pažymi, kad įstatyme pateiktos „telekomunikacijų paslaugos“ ir „telekomunikacijų sistemos“ apibrėžtys, kaip teigiama, yra sąmoningai plačios, kad jos išliktų aktualios naujoms technologijoms. Telekomunikacijų operatoriaus apibrėžtis taip pat yra labai plati ir galėtų apimti, pavyzdžiui, internetinius vaizdo žaidimus su pokalbių funkcija arba kitas interneto svetaines, kuriose yra tik tokie pokalbių langai[91].

153. Be to, nors procedūros ir priežiūra, susijusios su duomenų rinkimo ir prieigos prie jų būtinumo ir proporcingumo vertinimu, iš esmės yra numatytos, pačiame įstatyme nėra apibrėžti kriterijai, kuriais remiantis toks vertinimas atliekamas. Papildomų elementų galima rasti kituose dokumentuose, pavyzdžiui, praktikos kodeksuose.

154. Tačiau, kaip priminta EDAV rekomendacijose Nr. 02/2020 dėl Europos pagrindinių garantijų, taikomų stebėjimo priemonėms, ESTT nurodė, kad „*reikalavimas, kad bet koks pagrindinių teisių įgyvendinimo apribojimas būtų numatytas įstatyme, reiškia, kad pačiame teisiniame pagrinde, kuriuo leidžiamas šių teisių suvaržymas, būtų apibrėžta atitinkamos teisės įgyvendinimo apribojimo apimtis*“[92]. Tiksliau tariant, ESTT išaiškino, kad „*[t]am, kad atitiktų proporcingumo reikalavimą, teisės aktuose turi būti numatytos aiškios ir tikslios taisyklės, reglamentuojančios nagrinėjamos priemonės apimtį ir taikymą bei nustatančios minimalius reikalavimus, kad asmenys, kurių asmens duomenys tvarkomi, turėtų pakankamai garantijų, leidžiančių veiksmingai apsaugoti šiuos duomenis nuo piktnaudžiavimo pavojų. Tokie teisės aktai turi būti teisiškai privalomi pagal nacionalinę teisę ir juose turi būti nurodyta, kokiomis aplinkybėmis ir sąlygomis gali būti imtasi tokios duomenų tvarkymą numatančios priemonės, taip užtikrinant, kad teisių suvaržymas neviršytų to, kas griežtai būtina*.“[93]

155. EŽTT taip pat pabrėžė, kad svarbu, jog įstatymas būtų aiškus, kad asmenims „*būtų tinkamai nurodyta, kokiomis aplinkybėmis ir kokiomis sąlygomis valdžios institucijos yra įgaliotos taikyti bet kokias tokias priemones.*“[94]

156. **Todėl EDAV ragina Europos Komisiją toliau vertinti šiuos aspektus, susijusius su atitinkamo įstatymo tikslumu, aiškumu ir išsamumu, ir pateikti papildomų duomenų, įrodančių, kad įstatymas užtikrintas apsaugos lygis, iš esmės lygiavertis tam, kuris garantuojamas ES. EDAV taip pat pabrėžia, kad plačios apibrėžtys taip pat turėtų būti vertinamos atsižvelgiant į perėmimo priemonių proporcingumą.**

157. Be to, nors keliuose kompetentingų žvalgybos bendruomenės institucijų vidaus kodeksuose iš dalies plėtojami kai kurie iš šių aspektų, pavyzdžiui, dėl duomenų rinkimo būtinumo ir proporcingumo vertinimo, EDAV pabrėžia, kad ESTT reikalavimai, susiję su teisės pobūdžiu, reiškia, kad pagrindiniai elementai, be kita ko, tai, kad asmenys galėtų jais remtis kreipdamiesi dėl žalos atlyginimo, turi būti

[90] Žr. Europos elektroninių ryšių kodekso 2 straipsnio 5 dalį, kurioje, pavyzdžiui, „asmenų tarpusavio ryšio paslauga“ apibrėžiama kaip *„paprastai už atlygį teikiama paslauga, leidžianti tiesiogiai ir interaktyviai keistis informacija elektroninių ryšių tinklais tarp riboto skaičiaus asmenų, kai ryšį pradedantys ar jame dalyvaujantys asmenys nustato informacijos gavėją (-us), ir neapimanti paslaugų, kurias teikiant galimas asmenų tarpusavio ir interaktyvus ryšys vien tik kaip neesminė pagalbinė funkcija, kuri iš esmės susijusi su kita paslauga.*“

[91] Žr. 2018 m. kovo mėn. Vidaus reikalų ministerija, Ryšių perėmimo praktikos kodekso 2.5 ir paskesnius punktus, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

[92] Žr. Sprendimo *Schrems II* 175 punktą ir cituotą teismų praktiką, taip pat 2020 m. spalio 6 d. ESTT sprendimo *Privacy International / Secretary of State for Foreign ir kiti,* C-623/17, ECLI:EU:C:2020:790 (toliau – Privacy International), 65 punktą, ECLI:EU:C:2020:790 (toliau – Sprendimas *Privacy International*), 65 punktą.

[93] Žr. Sprendimo *Privacy International* 68 punktą.

[94] Žr. 2015 m. gruodžio 4 d. EŽTT sprendimo *Zakharov / Russia*, CE:ECHR:2015:1204JUD004714306, 229 punktą.

numatyti teisės aktuose, kuriuose numatytos teisės pareikšti ieškinį[95]. Iš tiesų 2016 m Tyrimo įgaliojimų įstatymo 7 priedo 6 dalyje minima, kad teismai (ir priežiūros institucijos) „*spręsdami klausimą bet kurioje tokioje byloje atsižvelgia į tai, kad asmuo neatsižvelgė į kodeksą*“, tačiau nepaaiškinama, ar asmenys gali pareikšti ieškinį dėl kodeksų pažeidimo teismuose (ar priežiūros institucijose). Be to, kol kas sprendimo projekte pateikti aspektai yra susiję su EŽTT pripažinimu, kad šiuose kodeksuose numatytos taisyklės[96] yra numatomos, o ne su tuo, kad jomis numatoma „galimybė pareikšti ieškinį“ teisme, kaip reikalauja ESTT, arba su tuo, kad JK teismai kai kuriose bylose rėmėsi kodeksais, tačiau nė vienoje iš paminėtų bylų neparodyta, kad asmenys gali pareikšti ieškinį dėl teisių, kylančių iš kodeksų. **Jeigu būtų padaryta išvada, kad JK teisėje nepakankamai nurodomos aplinkybės ir sąlygos, kuriomis gali būti priimta priemonė, ir kad šie aspektai iš tikrųjų yra numatyti Bendrijos žvalgybos institucijų vidaus kodeksuose**, **EDAV ragintų Europos Komisiją toliau vertinti, ar skirtinguose Bendrijos žvalgybos institucijų vidaus kodeksuose numatytus apribojimus ir apsaugos priemones asmenys gali ginčyti teisme ir užtikrinti jų vykdymą.**

158. **Antrasis klausimas** susijęs su tuo, kad nuostatos, susijusios, viena vertus, su tikslingu ryšių duomenų rinkimu ir saugojimu ir, kita vertus, su masiniu rinkimu, numatytos 2016 m Tyrimo įgaliojimų įstatyme arba kituose teisės aktuose, pavyzdžiui, 1994 m. Žvalgybos tarnybų įstatyme arba 2000 m. Tyrimo įgaliojimų įstatymo reglamente, bus taikomos ir duomenims, perduodamiems iš ES į Jungtinę Karalystę. Kalbant apie masinį duomenų rinkimą, EDAV pabrėžia, kad atitinkamomis JK teisės aktų nuostatomis leidžiama rinkti duomenis už JK ribų; taigi tai galėtų apimti ir tranzitu iš EEE į Jungtinę Karalystę perduodamus duomenis, remiantis sprendimu dėl tinkamumo[97]. Be to, EDAV pastebi, kad Europos Komisija nurodo, kad „*[r]eikia pažymėti, kad ryšių duomenų saugojimas ir rinkimas paprastai nėra susijęs su ES duomenų subjektų asmens duomenimis, pagal šį sprendimą perduotais į Jungtinę Karalystę. Prievolė saugoti arba atskleisti ryšių duomenis pagal 2016 m Tyrimo įgaliojimų įstatymo 3 ir 4 dalis taikoma duomenims, kuriuos telekomunikacijų operatoriai Jungtinėje Karalystėje renka tiesiogiai iš telekomunikacijų paslaugos naudotojų.*“[98] Vis dėlto EDAV pabrėžia, kad trūksta aiškumo dėl to, kad tik JK esančios šių operatorių įstaigos gali gauti JK kompetentingų institucijų prašymus, nes pagal 2016 m Tyrimo įgaliojimų įstatymo 261 skirsnio 10 dalyje pateiktą telekomunikacijų operatoriaus apibrėžtį numatyta, kad „telekomunikacijų operatorius – tai asmuo, kuris siūlo arba teikia telekomunikacijų paslaugą JK esantiems asmenims *arba kuris kontroliuoja arba teikia telekomunikacijų sistemą, kuri (visiškai arba iš dalies) yra JK arba yra kontroliuojama iš JK.*“ Todėl tai iš tikrųjų gali būti atitinkami EEE duomenų subjektų asmens duomenys, pavyzdžiui, duomenys, kuriuos surinko arba sukūrė EEE esantis JK telekomunikacijų operatoriaus padalinys, ir kurie, remiantis sprendimu dėl tinkamumo, (komerciniais tikslais) buvo perduoti to paties operatoriaus padaliniui, esančiam Jungtinėje Karalystėje, ir kuriuos po to JK rinko kompetentingos valdžios institucijos.

---

[95] Šiuo atžvilgiu ESTT mano, kad, pavyzdžiui, JAV Prezidento politinė direktyva Nr. 28 neatitinka reikalavimų, nors joje taip pat numatyti tam tikri apribojimai, susiję su masiniu duomenų rinkimu, žr. Sprendimo *Schrems II* 181 punktą.

[96] Žr. 2018 m. rugsėjo 13 d. EŽTT sprendimo *Big Brother Watch ir kiti / Jungtinė Karalystė*, ECLI:CE:ECHR:2018:0913JUD005817013 (toliau – Sprendimas *Big Brother Watch*), 325 punktą: „*Kadangi Informacijos komisaro kodeksas yra viešas dokumentas, kuris turi būti patvirtintas abiejuose parlamento rūmuose ir į kurį turi atsižvelgti asmenys, vykdantys perėmimo pareigas, ir teismai, Teismas aiškiai pripažino, kad į jo nuostatas galima atsižvelgti vertinant Tyrimo įgaliojimų reglamentavimo akto (angl. RIPA) tvarkos numatomumą*.“

[97] Žr. Sprendimo *Schrems II* 183 ir paskesnius punktus dėl teisės akto, kuriuo suteikiama prieiga prie duomenų, perduodamų tarp ES ir trečiosios valstybės, vertinimo priimant sprendimą dėl tinkamumo.

[98] Žr. sprendimo projekto 196 konstatuojamąją dalį.

159. **Todėl EDAV laikosi nuomonės, kad šių nuostatų vertinimas taip pat yra svarbus vertinant JK teisinės sistemos tinkamumo lygį, ir ragina Europos Komisiją paaiškinti šį aspektą ir toliau vertinti, kiek tai yra aktualu. Visų pirma EDAV ragina Europos Komisiją paaiškinti, kaip ji supranta šio teisės akto taikymo sritį, be kita ko, ką apima sąvoka „telekomunikacijų paslaugų vartotojai“, ir ar, atsižvelgiant į labai plačią telekomunikacijų operatorių apibrėžtį, būtų galima prašyti duomenų iš telekomunikacijų operatorių padalinių, esančių už JK ribų, tiek, kiek tai susiję su EEE duomenų subjektų duomenimis.**

160. **Trečiasis klausimas** susijęs su „dvigubo patvirtinimo“ procedūra. EDAV pažymi, kad 2016 m. Tyrimo įgaliojimų įstatyme nustatyta nauja „dvigubo patvirtinimo“ procedūra. Vis dėlto EDAV taip pat supranta, kad nors iš esmės rinkti duomenis ar susipažinti su jais nacionalinio saugumo ar žvalgybos tikslais galima tik turint teismo komisaro patvirtintą orderį, 2016 m. Tyrimo įgaliojimų įstatyme numatyta, kad „*tam tikrais konkrečiais atvejais teisėtas duomenų perėmimas galimas be orderio ir reikalingas tik išankstinis pačių kompetentingų informacijos komisarų institucijų leidimas[[žr. tolesnį skirsnį apie priežiūrą]], įskaitant perėmimą pagal užjūrio valstybių prašymus (2016 m. Tyrimo įgaliojimų įstatymo 52 skirsnis).*“ Kaip pabrėžiama toliau, tai taip pat sutampa su EDAV susirūpinimą keliančiais klausimais, visų pirma dėl užjūrio valstybėse atskleidžiamų duomenų. Be to, EDAV taip pat pažymi, kad įrangos perėmimo atveju, nepriklausomai nuo to, ar tai būtų tikslinis, ar masinis perėmimas, taip pat galima nukrypti nuo dvigubo patvirtinimo procedūros ir kad teismo komisaras turi teisę patvirtinti tik masinių orderių atnaujinimą, praėjus ne ilgesniam kaip 6 mėnesių pradiniam laikotarpiui. **EDAV ragina Europos Komisiją toliau vertinti ir įrodyti, kad net ir tais atvejais, kai dvigubo patvirtinimo procedūra netaikoma, JK teisinėje sistemoje numatytos tinkamos apsaugos priemonės, įskaitant veiksmingą *ex post* priežiūrą ir asmenims suteikiamas žalos atlyginimo galimybes, siekiant užtikrinti, kad užtikrintas apsaugos lygis, iš esmės lygiavertis tam, kuris garantuojamas ES (taip pat žr. paskesnį 4.3.3 skirsnį dėl priežiūros).**

161. Be to, nors 2016 m. Tyrimo įgaliojimų įstatyme iš tiesų nustatyta „dvigubo patvirtinimo“ procedūra, EDAV tebėra susirūpinusi dėl tam tikrų naujojo teisės akto ypatybių. Pateikus atitinkamus sprendimo projekto skirsnius, EDAV išnagrinėjo šias duomenų rinkimo ir prieigos prie jų rūšis ta pačia tvarka, kaip jas pateikė Europos Komisija. Todėl toliau vertinamų aspektų eiliškumas nėra pateiktas EDAV klausimų svarbos tvarka.

4.3.1.2. Tikslingas ryšių duomenų rinkimas ir saugojimas

162. EDAV pažymi, kad yra dviejų tipų pareigūnai, galintys išduoti tikslinius leidimus ryšių duomenims gauti: Leidimus Ryšių duomenų leidimų biure leidimus suteikiantis pareigūnas (toliau – Tyrimų įgaliojimų komisaras), paskirtas aukštas pareigūnas (atitinkamoje valstybės institucijoje nustatytas pareigas ar poziciją užimantis asmuo), be to, tam tikrais atvejais leidimą išduoda teismo komisarai. Tačiau pagal įstatymą ir atitinkamą kodeksą EDAV lieka neaišku, kuris tiksliai pareigūnas suteikia leidimą kokios rūšies tiksliniam ryšių duomenų rinkimui ir ar paskirtas pareigūnas yra pakankamai nepriklausomas[99].

163. **Todėl EDAV ragina Europos Komisiją toliau vertinti šį aspektą ir pateikti aiškesnius paaiškinimus dėl šių aspektų.**

164. Dėl pranešimo, kuriuo reikalaujama saugoti ryšių duomenis, EDAV taip pat pažymi, kad tokie pranešimai gali būti skirti „operatorius apibūdinti“. Atrodo, kad ši sąvoka reiškia, jog vienu metu galima reikalauti, kad keli operatoriai saugotų duomenis. Iš tikrųjų tikslinis duomenų rinkimo pobūdis susijęs ne su operatorių skaičiumi, o su asmenų, organizacijų, vietovės ar asmenų grupės, kurie

[99] Taip pat žr. toliau dėl dvigubo patvirtinimo procedūros vertinimo ir teismo komisaro nepriklausomumo.

sudaro „tikslinę grupę“, pavadinimu ar aprašymu, tyrimo pobūdžio aprašymu ir veiklos, kuriai naudojama įranga, aprašymu. Todėl EDAV pabrėžia, kad priklausomai nuo su tokiu „operatorių apibūdinimu“ susijusių operatorių skaičiaus, pranešimas gali būti platesnio pobūdžio nei gali atrodyti pagal tikslinio saugojimo procedūrą. **EDAV kviečia Europos Komisiją toliau vertinti šį aspektą ir pateikti papildomų garantijų, kad net ir tais atvejais, kai pranešimai skirti keliems operatoriams, jie apsiribos tik tuo, kas yra griežtai būtina ir proporcinga.**

4.3.1.3. Įrangos perėmimas

165. EDAV pažymi, kad skubiais atvejais „įrangos perėmimas“ gali nukrypti nuo dvigubo patvirtinimo procedūros[100]. Todėl EDAV reiškia susirūpinimą, kad tikslai, dėl kurių gali būti reikalaujama tokio įrangos perėmimo, yra plataus pobūdžio, o skubos kriterijai (kai teismo komisaras, įvertinęs įrangos perėmimo būtinumą ir proporcingumą, neprivalo pateikti *ex ante* leidimo) lieka neaiškūs. Kadangi tuo atveju, kai teismo komisaras nepatvirtina įrangos perėmimo *ex post*, „orderis nustoja galioti ir negali būti atnaujintas“, EDAV supranta, kad surinkti duomenys tuo tarpu ir toliau laikomi teisėtai surinktais. Kad šie duomenys būtų ištrinti, gali būti priimtas specialus teismo komisaro įsakymas[101].

166. **EDAV ragina Europos Komisiją išsamiai įvertinti sąlygas, kuriomis gali būti taikoma skuba, ir pateikti paaiškinimus dėl galimų atitinkamų duomenų subjektų teisių įgyvendinimo būdų ir jiems siūlomų teisių gynimo būdų, susijusių su įrangos perėmimo operacijomis, visų pirma tuo atveju, kai jie perimami skubos tvarka ir nukrypstama nuo dvigubo patvirtinimo procedūros.**

4.3.1.4. Masinis duomenų perėmimas iš duomenų nešiklių

167. Kaip aprašyta su masiniais duomenimis susijusių įgaliojimų peržiūros ataskaitoje[102], *„[m]asinis duomenų perėmimas paprastai apima ryšių rinkimą, kai jie keliauja per tam tikrus nešiklius (ryšių kanalus)*.“ Oficialioje 2016 m. Tyrimo įgaliojimų įstatymo informacijos suvestinėje „masinis duomenų perėmimas“ apibūdinamas kaip „*didelio kiekio ryšių duomenų rinkimo procesas, po kurio atrenkami konkretūs pranešimai, kurie skaitomi, peržiūrimi ar klausomi, jei tai būtina ir proporcinga*.“ EDAV pažymi, kad „masinis duomenų perėmimas“ iš tikrųjų reiškia duomenų rinkimą dar prieš tai, kai atliekamas bet koks duomenų filtravimas pagal selektorius (paprastus, kai stebimi asmenys, kurie jau žinoma, kad kelia grėsmę, arba sudėtingus, kai nustatomos naujos grėsmės ir anksčiau nežinomi įtariami asmenys).

168. Masinis ryšių duomenų rinkimas taip pat buvo vienas iš klausimų, kuriuos ESTT nagrinėjo byloje *Privacy International*, kurioje 2020 m. spalio 6 d. didžioji kolegija priėmė sprendimą (taip pat ir klausimas, ar toks duomenų rinkimas buvo vykdomas ES teisės kontekste, net ir nacionalinio saugumo tikslais). 2016 m. Tyrimo įgaliojimų įstatymas pakeitė teisės aktus, dėl kurių buvo priimtas šis sprendimas.

169. EDAV pažymi, kad, 2016 m. JK teisėje priėmus 2016 m. Tyrimo įgaliojimų įstatymą, dabar orderis reikalingas ir masiniam duomenų perėmimui. Šio orderio išdavimo procesas priklauso nuo nustatytų „veiklos tikslų“. Šių veiklos tikslų sąrašą sudaro žvalgybos tarnybų vadovai, o vėliau jį tvirtina valstybės sekretorius. Patį sprendimą tvirtina nepriklausomas teismo komisaras, kuris turi patikrinti, ar orderis yra būtinas ir proporcingas veiklos tikslams pasiekti. EDAV supranta, kad teismo komisaras turi įgaliojimus vertinti ne pačius veiklos tikslus, o tai, ar orderis yra būtinas ir proporcingas orderyje išvardytiems veiklos tikslams pasiekti. Parlamentinės žvalgybos ir saugumo komitetui kas tris

[100] Žr. 2016 m Tyrimo įgaliojimų įstatymo 109 skirsnį.
[101] Žr. 2016 m. Tyrimo įgaliojimų įstatymo 110 skirsnio 3 poskirsnio b punktą.
[102] Žr. 2016 m. rugpjūčio mėn. nepriklausomo kovos su terorizmu teisės aktų vertintojo parengtą su masiniais duomenimis susijusių įgaliojimų peržiūros ataskaitą.

mėnesius pateikiama sąrašo kopija, o Ministras Pirmininkas bent kartą per metus peržiūri šių veiklos tikslų sąrašą.

170. Tačiau, remiantis Europos Komisijos sprendimo projekte pateiktais aspektais, sunku įvertinti šių sąraše nurodytų veiklos tikslų apimtį ir tai, ar pagal juos leidžiamas duomenų rinkimas atitinka ESTT nustatytą ribą (pavyzdžiui, tam tikros geografinės teritorijos duomenų rinkimo ribos gali būti siauros – apimti tik kelias gatves, taip pat gali būti renkami duomenys iš visos EEE).

171. Be to, EDAV pabrėžia, kad masiškai surinkti duomenys gali būti saugomi ilgą laiką (kad su jais būtų galima toliau susipažinti tyrimui). Iš tiesų EDAV pažymi, kad 2016 m. Tyrimo įgaliojimų įstatymo 150 skirsnio 5–6 dalyse numatyta, kad surinktų duomenų kopijos sunaikinamos tik tuo atveju, jei jų saugojimas nėra būtinas arba mažai tikėtina, kad taps būtinas, atsižvelgiant į nacionalinio saugumo interesus arba bet kokius kitus pagrindus, patenkančius į 2016 m. Tyrimo įgaliojimų įstatymo 138 skirsnio 2 dalies taikymo sritį, arba jei saugojimas nėra būtinas keliais kitais tikslais[103]. EDAV pabrėžia, kad šie pagrindai atrodo labai platūs ir bet kuriuo atveju minimos tik gautų duomenų kopijos.

172. Be to, EDAV taip pat pažymi, kad skubiais atvejais 2016 m. Tyrimo įgaliojimų įstatymu taip pat leidžiama keisti orderius be išankstinio teismo komisaro patvirtinimo ir kad tokiu atveju, jei teismo komisaras, su kuriuo buvo konsultuojamasi *ex post*, per tris darbo dienas po orderio pakeitimo, atsisako pakeitimą patvirtinti, orderis turėtų galioti taip, tarsi pakeitimas nebūtų buvęs padarytas, tačiau laikoma, kad tuo tarpu surinkti duomenys surinkti teisėtai[104]. Kad šie duomenys būtų ištrinti, gali būti priimtas specialus teismo komisaro įsakymas[105].

173. **Be EDAV ragina Europos Komisiją toliau patikslinti ir įvertinti masinio duomenų perėmimo atvejus, visų pirma selektorių atranką ir taikymą masinio duomenų perėmimo aplinkybėmis, siekiant išsiaiškinti, kokiu mastu prieiga prie asmens duomenų atitinka ESTT nustatytą ribą (taip pat žr. 4.3.1.7 skirsnį, visų pirma apie selektorių priežiūrą) ir kokios apsaugos priemonės taikomos siekiant apsaugoti asmenų, kurių duomenys perimami šiomis aplinkybėmis, pagrindines teises, be kita ko, susijusias su duomenų saugojimo laikotarpiais. Nepriklausomas JK kompetentingų priežiūros institucijų vertinimas būtų ypač naudingas.**

174. **EDAV taip pat pabrėžia, kad dar svarbiau atrodo tai, jog „su užjūrio valstybėmis susiję ryšiai“, kuriems taikoma masinio duomenų perėmimo praktika, reiškia, kad JK galėtų tiesiogiai perimti ir masiškai rinkti duomenis ES, įskaitant tranzitu tarp ES ir Jungtinės Karalystės perduodamus duomenis, kurie patektų į sprendimo projekto taikymo sritį (žr. 4.3.2. skirsnį dėl tolimesnio nacionalinio saugumo ir atskleidimo užjūrio valstybėms tikslais surinktos informacijos naudojimo).**

4.3.1.5. Antrinių duomenų apsauga ir apsaugos priemonės

175. Be to, EDAV reiškia susirūpinimą, kad atitinkamais JK teisės aktais, susijusiais su masiniu duomenų perėmimu, neužtikrinama vienodo lygio visų ryšių duomenų apsauga. Pagal 2016 m. Tyrimo įgaliojimų įstatymo 137 skirsnį „antriniai duomenys“, kuriuos galima gauti gavus masinio duomenų perėmimo orderį, yra tiek „sistemų duomenys“, *„kurie yra įtraukti į (siuntėjo ar kitų subjektų) pranešimą, yra jo dalis, pridėti prie jo ar logiškai su juo susiję“*, tiek „identifikavimo duomenys“, *„kurie yra įtraukti į (siuntėjo ar kitų subjektų) pranešimą, yra jo dalis, pridėti prie jo ar logiškai su juo susiję, kuriuos galima logiškai atskirti nuo likusios pranešimo dalies, ir jeigu jie būtų taip atskirti, neatskleistų nieko, kas pagrįstai galėtų būti laikoma pranešimo prasme (jeigu tokia yra), neatsižvelgiant į bet*

[103] Žr. 2016 m. Tyrimo įgaliojimų įstatymo 150 skirsnio 3 ir 6 poskirsnius.
[104] Žr. 2016 m. Tyrimo įgaliojimų įstatymo 147 skirsnį (6 dalies I skyrius).
[105] Žr. 2016 m. Tyrimo įgaliojimų įstatymo 181 skirsnio 3 poskirsnio b punktą.

kokią prasmę, kylančią iš pranešimo fakto arba iš bet kokių duomenų, susijusių su pranešimo perdavimu“[106].

176. EDAV pažymi, kad šiems „antriniams duomenims“, dar vadinamiems metaduomenimis[107], gautiems surinkus didelį kiekį duomenų, atrodo, netaikomos tokios pat apsaugos priemonės taip pat kaip masiškai gautiems turinio duomenims, surinktiems pagal tikslinį orderį. Iš tiesų EDAV pastebi, kad bet kokio perimto turinio atrankai taikomos didesnės apsaugos priemonės[108] nei antrinių duomenų atrankai[109].

177. Be to, EDAV pabrėžia, kad EŽTT[110] ir ESTT[111] suabejojo tuo, kad tokie duomenys yra mažiau jautrūs nei kiti, visų pirma nei turinio duomenys. Iš tiesų Praktikos kodekse dėl perėmimo kaip „antrinių duomenų“ pavyzdžiai pateikiami („sistemų duomenys“, pavyzdžiui, maršruto parinktuvo konfigūracijos, e. pašto adresai arba naudotojų ID, taip pat alternatyvūs paskyros identifikatoriai, taip pat „identifikaciniai duomenys“, pavyzdžiui, susitikimo vieta kalendoriaus žymoje, informacija apie nuotraukas, pavyzdžiui, laikas, data ir vieta, kada jos buvo padarytos). **Todėl pabrėžia, kad EŽTT ir ESTT nuosekliai atlieka vertinimą, ir primena susirūpinimą keliančius klausimus, iškeltus dėl antrinių duomenų, kuriems dėl jų neskelbtino pobūdžio turėtų būti taikomos specialios apsaugos priemonės. Todėl EDAV ragina Europos Komisiją atidžiai įvertinti, ar pagal JK teisę tokiai asmens duomenų kategorijai numatytos apsaugos priemonės užtikrina iš esmės lygiavertį apsaugos lygį tam, kuris garantuojamas EEE.**

4.3.1.6. Automatizuotas ryšių duomenų tvarkymas

178. EDAV pažymi, kad Bendrijos žvalgybos institucijos naudoja ne tik paprastus ar sudėtingus selektorius masiškai gaunamiems duomenims filtruoti, bet ir gali remtis kitomis automatinio apdorojimo priemonėmis, kad išanalizuotų „*didelius informacijos kiekius, kurie agentūroms taip pat leidžia rasti sąsajas, modelius, asociacijas ar elgesį, kurie gali rodyti rimtą grėsmę, kurią reikėtų tirti*“, kaip

---

[106] „Sistemų duomenys“ ir „identifikavimo duomenys“ apibrėžti 2016 m. Tyrimo įgaliojimų įstatymo 263 skirsnyje.

[107] Žr. 2016 m. rugpjūčio mėn. nepriklausomo kovos su terorizmu teisės aktų vertintojo parengtą su masiniais duomenimis susijusių įgaliojimų peržiūros ataskaitą.

[108] Žr. 2016 m. Tyrimo įgaliojimų įstatymo 152 skirsnio 1 poskirsnio c punktą, 3 ir paskesnius poskirsnius.

[108] Žr. 2016 m. Tyrimo įgaliojimų įstatymo 152 skirsnio 1 poskirsnio c punktą, 3 ir paskesnius poskirsnius.

[109] Žr. 2016 m. Tyrimo įgaliojimų įstatymo 152 skirsnio 1 poskirsnio a ir b punktą.

[110] Žr. EŽTT bylos *Big Brother Watch* 357 punktą, perduodant didžiajai kolegijai: „*Todėl, nors Teismas neabejoja, kad susiję ryšių duomenys yra svarbi žvalgybos tarnybų priemonė kovojant su terorizmu ir sunkios formos nusikaltimais, jis nemano, kad valdžios institucijos užtikrino teisingą pusiausvyrą tarp konkuruojančių viešųjų ir privačių interesų, visiškai juos atleisdamos nuo apsaugos priemonių, taikomų turinio paieškai ir tyrimui. Nors Teismas nesiūlo, kad su susijusiais ryšių duomenimis turėtų būti galima susipažinti tik siekiant nustatyti, ar asmuo yra Britanijos salose, ar nėra, nes tai reikštų, kad susijusiems ryšių duomenims reikėtų taikyti griežtesnius standartus nei turiniui, vis dėlto turėtų būti nustatytos pakankamos apsaugos priemonės, užtikrinančios, kad susijusių ryšių duomenų atleidimas nuo Tyrimo įgaliojimų reglamentavimo akto 16 skirsnio reikalavimų apsiribotų tokia apimtimi, kuri būtina siekiant nustatyti, ar asmuo šiuo metu yra Britanijos salose.*“

[111] Žr. ESTT sprendimo *Privacy International* 71 punktą: „*Chartijos 7 straipsnyje įtvirtintos teisės suvaržymas, kurį lemia srauto ir vietos nustatymo duomenų perdavimas saugumo ir žvalgybos tarnyboms, turi būti laikomas ypač dideliu, atsižvelgiant, be kita ko, į informacijos, kurią gali atskleisti šie duomenys, jautrumą ir, be kita ko, į galimybę remiantis šiais duomenimis nustatyti duomenų subjektų profilį, nes tokia informacija yra tokia pat jautri kaip ir pats pranešimų turinys. Be to, toks suvaržymas duomenų subjektams gali sudaryti įspūdį, kad jų privatus gyvenimas yra nuolat stebimas (pagal analogiją žr. 2014 m. balandžio 8 d. Sprendimo Digital Rights Ireland ir kt., C-293/12 ir C-594/12, EU:C:2014:238, 27 ir 37 punktus ir 2016 m. gruodžio 21 d. Sprendimo Tele2, C-203/15 ir C-698/15, EU:C:2016:970, 99 ir 100 punktus)*.“

teigiama Žvalgybos ir saugumo komiteto 2015 m. ataskaitoje[112]. **EDAV žino, kad ši vieša ataskaita yra susijusi su praktika, taikyta pagal ankstesnę teisinę sistemą, kurią vėliau pakeitė 2016 m. Tyrimo įgaliojimų įstatymas. Vis dėlto Valdyba mano, kad JK kompetentingos priežiūros institucijos turi toliau nepriklausomai vertinti ir prižiūrėti automatizuotų duomenų tvarkymo priemonių naudojimą, ir ragina Europos Komisiją toliau vertinti šį klausimą ir apsaugos priemones, kurios šiomis aplinkybėmis būtų ir (arba) galėtų būti suteiktos EEE duomenų subjektams**.

4.3.1.7. Bendrijos kompetentingų žvalgybos institucijų atitikties rizika ir nesuderinama praktika

179. EDAV atkreipia dėmesį į tai, kad yra parengtos išsamios priežiūros ataskaitos. Jose pateikiama vertingų duomenų apie tai, kas vertinama kaip teigiama atitikties praktika, taip pat apie nustatytus atitikties rizikos veiksnius ir nesuderinamą praktiką.

180. Šiuo atžvilgiu, kaip teigiama 2019 m. Tyrimų įgaliojimų komisaro ataskaitoje, keli aspektai, susiję su įvairių kompetentingų institucijų teisinės sistemos taikymu, atskleidė tam tikrą kompetentingų institucijų neatitikties (riziką).

181. Pirma, EDAV pastebėjo, kad, atrodo, kad duomenų rinkinio priskyrimo masiniams asmens duomenims arba tiksliniams duomenims kriterijai ne visada yra aiškūs pačioms MI5 ir Slaptajai žvalgybos tarnybai (angl. SIS), visų pirma MI5, o tai gali lemti, kad duomenims netaikomos tinkamos apsaugos priemonės[113]. 2019 m. ataskaitoje Tyrimų įgaliojimų komisaras pasiūlė, kad *„šis klausimas turėtų būti išspręstas prioriteto tvarka“*[114]. Be to, kalbant apie didelius asmens duomenų rinkinius, EDAV pažymi, kad Vyriausybės ryšių centrinės tarnybos (angl. GCHQ) atveju, nors atrodo, kad didelių asmens duomenų rinkinių klasifikavimas yra patenkinamas (tačiau Tyrimų įgaliojimų komisaras dar turi atlikti auditą), 2019 m. kovo mėn. specialiosios grupės atlikta orderių vidaus atitikties peržiūra sukėlė rimtų abejonių: 50 proc. Vyriausybės ryšių centrinės tarnybos atitikties grupės peržiūrėtų didelių duomenų rinkinių rinkimo orderių pagrindimų neatitiko reikalaujamo standarto. Tyrimų įgaliojimų komisaro teigimu, atitikties užtikrinimo grupė pradėjo tirti šią problemą ir perkvalifikuoti darbuotojus, kad šis standartas būtų pagerintas. Atnaujinti mokymai apie 2016 m. Tyrimo įgaliojimų įstatymo nuostatas ir papildomi mokymai, kuriuos organizavo politikos ir atitikties tinklai, pagerino Vyriausybės ryšių centrinės tarnybos atitiktį šioje srityje. Tyrimų įgaliojimų komisaras nemano, kad per būsimus patikrinimus šis standartas bus pažeistas, tačiau ir toliau atidžiai peržiūrės šią sritį[115]. **Todėl EDAV pritaria nuomonei, kad Europos Komisija, vertindama apsaugos lygį, turi toliau peržiūrėti ir stebėti minėtus aspektus, kad būtų užtikrintas šio standarto gerinimas, kaip pabrėžiama Tyrimų įgaliojimų komisaro ataskaitoje, ir primena, kad vertinant trečiosios valstybės**

---

[112] Žr. Parlamentinės žvalgybos ir saugumo komiteto Saugumo komiteto 2015 m. privatumo ir saugumo ataskaitos „Šiuolaikiška ir skaidri teisinė sistema“, 18 punktą, p. 13, https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf.

[113] Žr. 2020 m. gruodžio 15 d. Tyrimų įgaliojimų komisaro 2019 m. metinės ataskaitos 8.39 punktą, https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPC-Annual-Report-2019_Web-Accessible-version_final.pdf: *„Stebime teigiamą [Masiškai surinktų duomenų priežiūros grupės] raidą ir pastebime jos poveikį vidaus atitikties valdymui. Toliau siekiame daugiau aiškumo dėl proceso, kurį MI5 taiko atlikdama pirminius naujų duomenų rinkinių tyrimus, kad geriau suprastume, kada nusprendžiama masinius duomenų rinkinius klasifikuoti, pavyzdžiui, kaip tikslinius duomenis. Mums susirūpinimą sukėlė vienas neišspręstas Duomenų rinkinių priežiūros grupės protokole nurodytas veiksmas, susijęs su MI5 ir Slaptosios žvalgybos tarnybos duomenų rinkinio paskirstymo neatitikimais. Dėl skirtingo duomenų naudojimo ir skirtingo turimų duomenų suskirstymo gali būti, kad abi agentūros turi tą patį duomenų rinkinį arba jo versijas ir kad viena agentūra jį teisėtai gali priskirti prie masinių duomenų, o kita – prie tikslinių duomenų. Kyla rizika, kad jei viena iš agentūrų neteisingai klasifikuotų turimus duomenis kaip tikslinius, tada tie duomenys būtų laikomi be atitinkamo leidimo ir jiems nebūtų taikomos tinkamos apsaugos priemonės*.“

[114] Žr. Tyrimų įgaliojimų komisaro 2019 m. metinės ataskaitos 8.39 punktą.

[115] Žr. Tyrimų įgaliojimų komisaro 2019 m. metinės ataskaitos 10.48 punktą.

esminį lygiavertiškumą taip pat atsižvelgiama į teisinės sistemos įgyvendinimą ir konkretų taikymą, kaip numatyta BDAR 45 straipsnyje.

182. Žvelgiant plačiau, EDAV pabrėžia tuos pačius Tyrimų įgaliojimų komisaro klausimus, susijusius su MI5 pareigūnų atliekamomis „paieškomis pagal užduotis“, kurios leidžia tyrėjui atlikti daugiau nei vieną jam prieinamų didelių asmens duomenų rinkinių paiešką, ir „*rimta atitikties rizika, susijusia su tam tikromis MI5 naudojamomis technologinėmis aplinkomis*“, susijusią su tuo, kur duomenys buvo saugomi aplinkoje, kas turėjo prieigą prie jų, kokiu mastu jie buvo kopijuojami ar dalijamasi jais, kokie buvo jiems taikomi ištrynimo procesai, taip pat jų saugojimo laikotarpius. Nors Tyrimų įgaliojimų komisaras nurodo, kad buvo imtasi priemonių ir įdiegtos apsaugos priemonės, tačiau kai kurios iš jų tebėra taikomos rankiniu būdu ir vykdomos individualiai, pasitelkiant žmogiškuosius išteklius, joje pabrėžiama, kad labai svarbu, jog „*MI5 ir toliau palaikytų šiuos naujus procesus ir skirtų pakankamai išteklių, kad jie veiktų veiksmingai. Jei MI5 nustatys, kad padaugėjo reikalavimų neatitinkančio elgesio atvejų*“[116]. Tyrimų įgaliojimų komisaras tikisi, kad į juos kuo greičiau bus atkreiptas tarnybos dėmesys. **Todėl EDAV ragina Europos Komisiją ateityje atidžiai stebėti šiuos aspektus**.

183. Dėl Vyriausybės ryšių centrinės tarnybos EDAV iš Tyrimų įgaliojimų komisaro ataskaitos taip pat supranta, kad operacijų, vykdomų pagal masinius orderius, atveju „*paraiškų dėl vidaus patvirtinimo kokybė buvo nevienoda, ir pastebėjome, kad galima tobulinti tokių paraiškų rengimą*“[117], o tikslinio įrangos perėmimo atveju paaiškinimai dėl bendrųjų aprašų naudojimo kartais buvo pernelyg bendri ir netikslūs[118]. EDAV taip pat pastebėjo, kad, kalbant apie įrangos perėmimą, Tyrimų įgaliojimų komisaras rekomenduoja, kad „*paraiškose turėtų būti nuosekliai ir aiškiai užfiksuotas ryšys tarp tikslo ir teisės aktais nustatyto tikslo bei žvalgybos reikalavimų*“[119], kad „*vertinant proporcingumą visose paraiškose turėtų būti aiškiai aptartas galimas šalutinis kišimosi poveikis ir atitinkamos švelninančios priemonės*“[120] ir kad Tyrimų įgaliojimų komisaras pabrėžė, jog, nepaisant pažangos, „*vis dar yra kur tobulėti*“[121] ir ateityje taip pat reikės tam skirti daugiau dėmesio.

184. Dėl masinio duomenų perėmimo tvarką pagal 2000 m. Tyrimo įgaliojimų reglamentavimo aktą, kuris vėliau buvo pakeistas 2016 m. Tyrimo įgaliojimų įstatymo nuostatomis, EDAV primena, kad nepakankama interneto duomenų paslaugų perėmimui atrankos, filtravimo, paieškos ir perimtų pranešimų atrankos tyrimui priežiūra, buvo vienas iš pagrindinių aspektų, kuriuos EŽTT pripažino neatitinkančiais EŽTK 8 straipsnio, kiek tai susiję su ankstesniais teisės aktais dėl JK valdžios institucijų tyrimo įgaliojimų nacionalinio saugumo kontekste byloje *Big Brother Watch*, dabar perduotoje didžiajai kolegijai. **EDAV ragina Europos Komisiją patikrinti bylos nagrinėjimo eigą, , atsižvelgti į šiuos aspektus ir nurodyti juos sprendime dėl tinkamumo, jei Europos Komisija jį priimtų.**

185. Šioje byloje EŽTT „*nebuvo įsitikinęs, kad apsaugos priemonės, reglamentuojančios duomenų paslaugų atranką perėmimui ir perimtos medžiagos atranką tyrimui, yra pakankamai griežtos, kad suteiktų pakankamas garantijas, apsaugančias nuo piktnaudžiavimo. Tačiau didžiausią susirūpinimą kelia tai, kad nėra patikimos nepriklausomos selektorių ir paieškos kriterijų, naudojamų perimtiems pranešimams filtruoti, priežiūros*.“[122] Kaip pabrėžė Tyrimų įgaliojimų komisaras, „*ši išvada atkartojo panašią rekomendaciją, pateiktą 2015 m. kovo mėn. Žvalgybos ir saugumo komiteto dokumente:*

[116] Žr. Tyrimų įgaliojimų komisaro 2019 m. metinės ataskaitos 8.52 punktą.
[117] Žr. Tyrimų įgaliojimų komisaro 2019 m. metinės ataskaitos 10.2 punktą.
[118] Žr. Tyrimų įgaliojimų komisaro 2019 m. metinės ataskaitos 10.16 ir 10.17 punktus.
[119] Žr. Tyrimų įgaliojimų komisaro 2019 m. metinės ataskaitos 10.23 punktą.
[120] Žr. Tyrimų įgaliojimų komisaro 2019 m. metinės ataskaitos 10.23 punktą.
[121] Žr. Tyrimų įgaliojimų komisaro 2019 m. metinės ataskaitos 10.23 punktą.
[122] Žr. EŽTT bylos *Big Brother Watch* 347 punktą.

„Šiuolaikiška ir skaidri teisinė sistema“[123]. **EDAV palankiai vertina tai, kad dėl to 2019 m. Tyrimų įgaliojimų komisaras atliko savo požiūrio į masinio duomenų perėmimo tikrinimo peržiūrą, *„kuri apėmė kruopščią techniškai sudėtingų būdų, kuriais faktiškai įgyvendinamas masinis duomenų perėmimas, peržiūrą“*[124], ir įsipareigojo nuo 2020 m. į masinio duomenų perėmimo tikrinimus įtraukti *„išsamų selektorių ir paieškos kriterijų, apie kuriuos pirmiau užsiminė EŽTT, nagrinėjimą“*[125]. Atsižvelgiant į šio aspekto svarbą, EDAV susirūpinimą kelia tai, kad Tyrimų įgaliojimų komisaras dar neatliko išsamaus selektorių ir paieškos kriterijų patikrinimo, ir ji ragina Europos Komisiją atidžiai stebėti pokyčius šioje srityje, visų pirma dėl to, kad konkreti tokios priežiūros forma dar turi būti patikslinta[126].**

4.3.2. Tolimesnis nacionalinio saugumo ir atskleidimo užjūrio valstybėms tikslais surinktos informacijos naudojimas

186. Kalbant apie tolesnį surinktos informacijos naudojimą nacionalinio saugumo tikslais, Europos Komisija savo vertinime remiasi 2018 m. Duomenų apsaugos įstatymo 87 straipsnio 1 dalimi, kurioje iš tiesų numatyta, kad *„tokiu būdu surinkti asmens duomenys neturi būti tvarkomi būdu, nesuderinamu su tikslu, kuriuo jie surinkti*“. Tačiau EDAV nurodo, kad šiai nuostatai gali būti taikomos nacionalinio saugumo išimtys pagal 2018 m. Duomenų apsaugos įstatymo 110 skirsnį. Be to, EDAV pažymi, kad tikslinio duomenų perėmimo ir tyrimo, tikslinio ryšių duomenų rinkimo ir saugojimo, tikslinio įrangos perėmimo, masinio duomenų perėmimo ir masinio įrangos perėmimo atvejais teisės aktuose numatyta galimybė „atskleisti duomenis užjūrio valstybėms“.

4.3.2.1. Tolesnis naudojimas, atskleidimas užjūrio valstybėms ir Jungtinėje Karalystėje taikoma teisinė sistema

187. Europos Komisija nurodė, kad 2018 m. Duomenų apsaugos įstatymo 4 dalis, visų pirma jos 109 skirsnis, yra svarbios nuostatos, kuriose nustatomi konkretūs tolesnio surinktos informacijos naudojimo reikalavimai, be kita ko, žvalgybos tarnybų vykdomam tarptautiniam asmens duomenų perdavimui trečiosioms valstybėms ar tarptautinėms organizacijoms. Tačiau EDAV pažymi, kad 2018 m. Duomenų apsaugos įstatymo 110 skirsnyje numatyta nacionalinio saugumo išimtis, kurioje nurodoma, kad tam tikros 2018 m. Duomenų apsaugos įstatymo nuostatos netaikomos, jei šių nuostatų išimtis reikalinga siekiant užtikrinti nacionalinį saugumą. Atitinkamos nuostatos, kurios gali būti netaikomos, apima 2018 m. Duomenų apsaugos įstatymo 4 dalies 2 skyrių, susijusį su duomenų apsaugos principais, visų pirma tikslo apribojimą, taip pat 2018 m. Duomenų apsaugos įstatymo 4 dalies 3 skyrių, susijusį su duomenų subjekto teisėmis. Dėl 2018 m. Duomenų apsaugos įstatymo 109 skirsnio, skaitomo kartu su 2018 m. Duomenų apsaugos įstatymo 110 skirsniu, ir sąlygų, kuriomis jis taikomas, gali pasitaikyti atvejų, kai žvalgybos tarnybų vykdomas tarptautinis asmens duomenų perdavimas į trečiąsias valstybes vyksta netaikant nuostatų, susijusių su duomenų apsaugos principais ir duomenų subjekto teisėmis.

188. Kaip nurodė Europos Komisija, tokia išimtis turi būti vertinama kiekvienu konkrečiu atveju ir gali būti taikoma tik tuo atveju, jei konkrečios nuostatos taikymas turėtų neigiamų pasekmių nacionaliniam saugumui. Iš tiesų išduodant nacionalinį sertifikatą JK žvalgybos tarnyboms, siekiama patvirtinti, kad išimtis reikalinga konkrečių asmens duomenų, kurie tvarkomi nacionalinio saugumo užtikrinimo tikslais, atžvilgiu. Vis dėlto EDAV pažymi, kad JK Vidaus reikalų ministerija savo nacionalinio saugumo

[123] Žr. Tyrimų įgaliojimų komisaro 2019 m. metinės ataskaitos 10.28 punktą.
[124] Žr. Tyrimų įgaliojimų komisaro 2019 m. metinės ataskaitos 10.28 punktą.
[125] Žr. Tyrimų įgaliojimų komisaro 2019 m. metinės ataskaitos 10.28 punktą.
[126] Žr. Tyrimų įgaliojimų komisaro 2019 m. metinės ataskaitos 10.28 punktą. „dėl tikslios šio patikrinimo formos dar reikia susitarti“.

sertifikato gairėse pagal 2018 m. Duomenų apsaugos įstatymą paaiškina, kad „*[i]š pat pradžių svarbu pažymėti, kad norint remtis nacionalinio saugumo išimtimi, sertifikatas nėra būtinas; iš tiesų daugeliu atvejų duomenų valdytojai patys nustato, ar taikytina nacionalinio saugumo išimtis*.“ [127] Be to, JK Vidaus reikalų ministerijos gairėse pažymima, kad „*nacionalinio saugumo sertifikatai gali būti taikomi asmens duomenims, kuriuos galima konkrečiai identifikuoti, arba apimti platesnę asmens duomenų kategoriją. Jie gali būti tiek prevencinio, tiek retrospektyvinio pobūdžio*.“ [128] Todėl nacionalinio saugumo išimtis gali būti taikoma žvalgybos tarnyboms tarptautiniu mastu perduodant asmens duomenis trečiosioms valstybėms, kai nėra nacionalinio saugumo sertifikato.

189. Be to, EDAV pažymi, kad, pavyzdžiui, nacionalinio saugumo sertifikate DPA/S27/Saugumo tarnyba[129] numatyta, kad iki 2024 m. liepos 24 d. asmens duomenims, tvarkomiems „*Saugumo tarnybos vardu, jos prašymu ar jai padedant*“ ir „*kai toks tvarkymas yra būtinas siekiant palengvinti tinkamą Saugumo tarnybos funkcijų, aprašytų 1989 m. Saugumo tarnybos įstatymo 1 skirsnyje, vykdymą*“, netaikomos atitinkamos JK teisės nuostatos, susijusios su asmens duomenų perdavimu į trečiąsias valstybes ar tarptautinėms organizacijoms, kaip numatyta BDAR V skyriuje. Nors kituose viešai skelbiamuose nacionalinio saugumo sertifikatuose nenumatyta 2018 m. Duomenų apsaugos įstatymo 109 skirsnio nuostatų taikymo išimtis, reikia priminti, kad dalis arba visas nacionalinio saugumo sertifikato tekstas gali būti neskelbiamas, jei jo paskelbimas prieštarautų nacionalinio saugumo interesams, viešajam interesui arba galėtų kelti pavojų kurio nors asmens saugumui.

190. Apskritai, vertindama sprendimo projektą šių nuostatų atžvilgiu, EDAV pastebi, kad šių duomenų atskleidimo apsaugos priemonės apima tik reikalavimą, kad duomenų gavėjas laikytųsi duomenų saugumo reikalavimo, atskleistų tik būtinosios apimties duomenis, duomenų saugojimo ir prieigos prie duomenų suteikimo tik ribotam asmenų skaičiui reikalavimo. Taigi **EDAV pabrėžia, kad, kai kalbama apie užjūrio valstybėms atskleidžiamą informaciją, taikant JK teisėje numatytą nacionalinio saugumo išimtį, gali susidaryti situacijos, kai trečiojoje paskirties valstybėje nebūtų visiškai užtikrintos ar laikomasi apsaugos priemonių, užtikrinančių tikslo apribojimo, būtinumo ir proporcingumo principų, taip pat asmenų teisių, priežiūros ir žalos atlyginimo. Todėl EDAV rekomenduoja Europos Komisijai toliau nagrinėti bendras apsaugos priemones, numatytas JK teisėje, kai kalbama apie informacijos atskleidimą užjūrio valstybėse, visų pirma atsižvelgiant į nacionalinio saugumo išimčių taikymą.**

4.3.2.2. Informacijos atskleidimas užjūrio valstybėms ir dalijimasis žvalgybos informacija tarptautinio bendradarbiavimo kontekste

191. EDAV taip pat pažymi, kad Europos Komisija, atlikdama tinkamumo vertinimą, neatsižvelgė į galiojančius tarptautinius susitarimus, sudarytus tarp JK ir trečiųjų valstybių ar tarptautinių organizacijų, kuriuose gali būti numatytos konkrečios nuostatos dėl žvalgybos tarnybų vykdomo tarptautinio asmens duomenų perdavimo trečiosioms valstybėms.

192. EDAV taip pat pabrėžia, kad Europos Komisija savo vertinime daugiausia remiasi 2018 m. Duomenų apsaugos įstatymo 4 dalies vertinimu, ir yra itin susirūpinusi, kad 2016 m. Duomenų apsaugos įstatyme daugiausia dėmesio skiriama „prašymams“ keistis žvalgybos informacija su užsienio

[127] Žr. 2020 m. rugpjūčio mėn. Vidaus reikalų ministerijos 2018 m. Duomenų apsaugos įstatymo, Nacionalinio saugumo sertifikatų gairių 3 punktą, p. 3.
[128] Žr. 2020 m. rugpjūčio mėn. Vidaus reikalų ministerijos 2018 m. Duomenų apsaugos įstatymo, Nacionalinio saugumo sertifikatų gairių 5 punktą, p. 4.
[129] Žr. 2019 m. liepos 24 d. DPA/S27/Saugumo tarnyba, 2018 m. Duomenų apsaugos įstatymo 27 skirsnis, Valstybės sekretoriaus sertifikatas, https://ico.org.uk/media/about-the-ico/documents/nscs/2615660/nsc-part-2-mi5-201908.pdf.

partneriais, tačiau nenagrinėjamos kitos dalijimosi žvalgybos informacija formos. Šiuo atžvilgiu EDAV atkreipia dėmesį į tai, kad Europos Komisijos sprendimo projekte nenurodoma ir nevertinama JK teisinės sistemos sąsaja su Jungtinės Karalystės ir JAV susitarimu dėl ryšių žvalgybos. Neseniai paskelbtame pareiškime, skirtame šio susitarimo 75-osioms metinėms paminėti, JAV nacionalinio saugumo agentūra (toliau – NSA) paminėjo, kad ši partnerystė leidžia „*abiem agentūroms keistis informacija kiek įmanoma daugiau ir su minimaliais apribojimais*“ ir kad „*šiuo novatorišku dokumentu buvo sukurta JK ir JAV žvalgybos specialistų politika ir procedūros, skirtos dalytis ryšių, vertimo, analizės ir kodų laužymo informacija*.“[130] Šis susitarimas taip pat tapo kitų žvalgybos partneryščių su Australija, Kanada ir Naująja Zelandija pagrindu.

193. Šio susitarimo konfidencialumas ir konkrečios jo nuostatos kelia rimtų sunkumų, susijusių su teisės aiškumu ir numatomumu dėl tolesnio JK valdžios institucijų nacionalinio saugumo tikslais surinktos informacijos naudojimo ir atskleidimo užjūrio valstybėse. Šiomis aplinkybėmis EDAV primena, kad kalbant apie ES garantuojamą apsaugos lygį, ESTT pabrėžė, kad teisės aktuose, susijusiuose su kišimusi į pagrindinę teisę į asmens duomenų apsaugą, turi būti „*nustatytos aiškios ir tikslios taisyklės, reglamentuojančios priemonės taikymo sritį ir įgyvendinimą bei nustatančios minimalias apsaugos priemones, kad susijusių asmenų duomenims būtų suteikiamos pakankamos garantijos, leidžiančias veiksmingai apsaugoti jų duomenis nuo piktnaudžiavimo pavojaus ir nuo bet kokios neteisėtos prieigos prie tų duomenų ir jų naudojimo. Tokių apsaugos priemonių poreikis yra dar didesnis, kai asmens duomenys tvarkomi automatiniu būdu ir kai yra didelis neteisėtos prieigos prie tų duomenų pavojus*“[131]. Todėl EDAV mano, kad Europos Komisija, atlikdama tinkamumo vertinimą, turėtų apsvarstyti JK ir JAV susitarimo dėl ryšių žvalgybos poveikį.

194. EŽTT 2018 m. rugsėjo 13 d. pirmosios dalies Sprendime *Big Brother Watch* įvertino JK dalijimosi žvalgybos informacija tvarką, visų pirma JK ir JAV CŽV susitarimą. EŽTT iš tiesų nurodė, kad „*[į]statyminė sistema, pagal kurią JK žvalgybos tarnybos gali prašyti perimtos medžiagos iš užsienio žvalgybos agentūrų, nėra numatyta 2000 m. Tyrimo įgaliojimų reglamentavimo akte. 1946 m. kovo 5 d. JK ir JAV susitarimas dėl ryšių žvalgybos konkrečiai leidžia keistis medžiaga tarp Jungtinių Valstijų ir Jungtinės Karalystės*“[132] ir laikoma, kad yra „*teisinis pagrindas prašyti žvalgybinės informacijos iš užsienio žvalgybos agentūrų ir kad tas įstatymas yra pakankamai prieinamas*.“[133] Nors EŽTT padarė išvadą, kad dalijimosi žvalgybos informacija tvarka nepažeidė EŽTK 8 straipsnio[134], EDAV pažymi, kad šis sprendimas dabar perduotas didžiajai kolegijai, kurios sprendimas dar nepriimtas. EDAV taip pat pažymi, kad prie šio sprendimo pridėtoje bendroje ir atskiroje nuomonėje teisėja P. Koskelo, prie kurios prisijungė teisėja K. Turković[135], padarė išvadą, kad EŽTK 8 straipsnis dėl dalijimosi žvalgybos informacija tvarkos buvo pažeistas, nurodydama, kad „*[n]esunku sutikti su principu, kad bet kokiu susitarimu, pagal kurį žvalgybos informacija iš perimtų pranešimų gaunama per užsienio žvalgybos tarnybas, remiantis prašymais vykdyti tokį perėmimą arba perduoti jo rezultatus, neturėtų būti leidžiama apeiti apsaugos priemonių, kurios turi būti taikomos bet kokiam vidaus institucijų vykdomam sekimui (žr. 216, 423 ir 447 punktus). Iš tiesų, bet koks kitas požiūris būtų neįtikėtinas.*“

---

[130] Žr. 2021 m. vasario 5 d. NSA pranešimą spaudai *GCHQ and NSA Celebrate 75 Years of Partnership* („Vyriausybės ryšių centrinė tarnyba ir NSA švenčia 75 partnerystės metus“), https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2494453/gchq-and-nsa-celebrate-75-years-of-partnership/.

[131] Žr. Sprendimo *Schrems I* 91 punktą.

[132] Žr. EŽTT bylos *Big Brother Watch* 425 punktą.

[133] Žr. EŽTT bylos *Big Brother Watch* 427 punktą.

[134] Žr. EŽTT bylos *Big Brother Watch* 448 punktą.

[135] Žr. EŽTT byloje *Big Brother Watch*, pridėtoje bendroje ir atskiroje teisėjos P. Koskelo ir teisėjos K. Turković nuomonėje.

195. Kaip pabrėžiama keliuose žiniasklaidos ir nevyriausybinių organizacijų pranešimuose[136][137], naujausia viešai paskelbta JK ir JAV susitarimo dėl ryšių žvalgybos versija yra 1956 m., o nuo to laiko ryšių technologijos ir signalų žvalgybos pobūdis labai pasikeitė. Žiniasklaidos pranešimuose, pavyzdžiui, atskleista, kad duomenis, perduodamus povandeniniais kabeliais, kurie pasiekia Jungtinę Karalystę, perima Vyriausybės ryšių centrinė tarnyba ir pateikia juos NSA[138].

196. EDAV svarbiausias su dalijimusi žvalgybos informacija susijęs klausimas: ar 2018 m. Duomenų apsaugos įstatymo 109 skirsnis ir 2016 m. Duomenų apsaugos įstatymo nuostatos ir toliau taikomos, kai JK žvalgybos tarnybos veikia pagal JK ir JAV susitarimą dėl ryšių žvalgybos. Kitas svarbus aspektas, kurį reikia įvertinti, yra tai, ar šio susitarimo nuostatos arba veiksmingas taikymas daro poveikį asmens duomenų, perduodamų iš EEE į Jungtinę Karalystę, apsaugos lygiui, ar leidžia kitų trečiųjų valstybių žvalgybos tarnyboms tiesiogiai susipažinti su asmens duomenimis ir juos gauti.

197. Todėl, be išlygų, pareikštų dėl „užjūrio valstybėms atskleidžiamos informacijos“ remiantis 2018 m. Duomenų apsaugos įstatymo 4 dalimi ir su ja susijusia nacionalinio saugumo išimtimi, taip pat dėl prašymų pagal 2016 m. Duomenų apsaugos įstatymą, **EDAV nerimauja dėl kitų keitimosi informacija ir jos atskleidimo formų remiantis kitomis priemonėmis, visų pirma įvairiais tarptautiniais susitarimais, kuriuos JK sudarė su kitomis trečiosiomis valstybėmis, visų pirma tais atvejais, kai šios priemonės lieka viešai neprieinamos, pavyzdžiui, JK ir JAV susitarimas dėl ryšių žvalgybos. Dėl tokio susitarimo poveikio galėtų būti apeinamos apsaugos priemonės, nustatytos norint susipažinti su asmens duomenimis ir juos naudoti nacionalinio saugumo tikslais.**

198. Iš tiesų EDAV pritaria Jungtinių Tautų specialiojo pranešėjo Joe Cannatacci išsakytai nuomonei, kad *„dalijimasis žvalgybos informacija neturi tapti nelegaliu būdu, kuriuo pasinaudojus būtų galima gauti ar palengvinti kitiems gauti žvalgybos informaciją, netaikant vidaus apsaugos priemonių, taip pat neturi atsirasti spragų užsienio vyriausybėms, kuriose taikomi žemesni privatumo (ar kitų žmogaus teisių) apsaugos standartai, gauti žvalgybos informaciją iš JK žvalgybos, dėl kurios galėtų būti pažeistos žmogaus teisės*“[139].

199. Be to, **EDAV mano, kad dvišalių ar daugiašalių susitarimų su trečiosiomis valstybėmis sudarymas žvalgybinio bendradarbiavimo tikslais, kuriais suteikiamas teisinis pagrindas tiesiogiai perimti ir rinkti asmens duomenis arba į šias valstybes perduoti asmens duomenis, taip pat gali turėti didelės įtakos tolesnio surinktos informacijos naudojimo sąlygoms, nes tikėtina, kad tokie susitarimai turės įtakos vertinamai JK duomenų apsaugos teisinei sistemai.**

---

[136] Žr. BBC, *Diary reveals birth of secret UK-US spy pact that grew into Five Eyes* („Dienoraštis atskleidžia slaptą JK ir JAV šnipinėjimo susitarimą, kuris tapo „Penkių akių“ susitarimu“), 2021 m. kovo 5 d., https://www.bbc.com/news/uk-56284453.

[137] Žr. *Privacy International*, *Policy Briefing - UK Intelligence Sharing Arrangements* („Politikos santrauka. Jungtinės Karalystės susitarimai dėl dalijimosi žvalgybos informacija“), 2018 m. balandžio mėn., https://privacyinternational.org/sites/default/files/2018-04/Privacy%20International%20Briefing%20-%20Intelligence%20Sharing%20%28UK%29%20FINAL.pdf.

[138] Žr. *The Guardian*, *GCHQ taps fibre-optic cables for secret access to world's communications* („Vyriausybės ryšių centrinė tarnyba jungiasi prie šviesolaidinių kabelių, norėdama gauti slaptą prieigą prie pasaulio ryšių“), 2013 m. birželio 21 d., https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

[139] Žr. 2018 m. birželio 29 d. Specialiojo pranešėjo ataskaita teisės į privatumą klausimais misijos į Jungtinę Didžiosios Britanijos ir Šiaurės Airijos Karalystę pabaigoje, Londonas, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E#:~:text=Intelligence%20sharing%20must%20not%20result,UK%20intelligence%20that%20could%20give.

4.3.3. Priežiūra

200. EDAV pabrėžia nepriklausomų priežiūros institucijų vykdomos visapusiškos priežiūros svarbą siekiant užtikrinti tinkamą duomenų apsaugos lygį. Priežiūros institucijų nepriklausomumo garantija, kaip apibrėžta ES chartijos 8 straipsnio 3 dalyje, siekiama užtikrinti veiksmingą ir patikimą fizinių asmenų apsaugos tvarkant asmens duomenis taisyklių laikymosi stebėseną.

201. Kai asmens duomenys gaunami ir naudojami nacionalinio saugumo tikslais, priežiūros funkciją daugiausia atlieka Tyrimų įgaliojimų komisaras ir teismo komisarai (toliau – teismo komisarai).

202. **EDAV iš esmės pripažįsta, kad 2016 m. Tyrimo įgaliojimų įstatyme įtvirtinti teismo komisarai yra reikšmingas patobulinimas.** Atsižvelgiant į pirmiau pateiktą prašymą, Europos Komisijos prašoma išsamiau įvertinti **teismo komisarų nepriklausomumą, visų pirma tai, kokiu mastu teisiškai užtikrintas Tyrimų įgaliojimų komisaro ir Tyrimų įgaliojimų komisaro biuro nepriklausomumas, nes 2016 m. Tyrimo įgaliojimų įstatyme tai nenustatyta.** Tai dar svarbiau, nes Tyrimų įgaliojimų komisaras priima sprendimus dėl vyriausybės apeliacinių skundų, jei teismo komisaras atmetė prašymą taikyti priežiūros **priemonę**.

203. Tyrimų įgaliojimų komisaras atlieka *ex ante*, taip pat *ex post* priežiūros funkcijas. Kalbant apie *ex ante* priežiūrą, EDAV supranta, kad teismo komisarų funkcija yra atskirais atvejais patvirtinti įvairias sekimo priemones, be kita ko, tikslinį perėmimą ir masinį ryšių duomenų rinkimą. Be to, EDAV pažymi, kad išankstinis priežiūros priemonių patvirtinimas negali būti kildinamas iš ESTT praktikos kaip absoliutus priežiūros priemonių proporcingumo reikalavimas.[140]

204. Vis dėlto, siekdama įvertinti šio lygio priežiūros veiksmingumą, EDAV mano, kad reikia toliau aiškinti, kokiais atvejais galimas teisėtas perėmimas be išankstinio teismo komisarų patvirtinimo.

205. Savo sprendimo projekto 201 ir 266 išnašose Europos Komisija mini „tam tikrus konkrečius atvejus“, numatytus 2016 m. Tyrimo įgaliojimų įstatymo 44–52 skirsniuose, susijusius su tiksliniu perėmimu. EDAV pažymi, kad 2016 m. Tyrimo įgaliojimų įstatymo 45–51 skirsniai yra išimtys, kuriomis, kaip teigiama, žvalgybos tarnybos reguliariai nesinaudoja. Be to, **EDAV supranta** kad **tais atvejais, kai išimtys taikomos**, (pvz., telekomunikacijų ir pašto paslaugų teikėjams), teismo komisarų atliekamas išankstinis patvirtinimas turi būti atliekamas tuo atveju, jei teisėsaugos institucijos ar žvalgybos tarnybos **prašo** prieigos prie šių duomenų**, ir prašo Europos Komisijos savo sprendime patvirtinti, kad tai yra teisinga**.

206. EDAV pripažįsta, kad pagal 2016 m. Tyrimo įgaliojimų įstatymo 44 straipsnio 2 dalį leidžiama perimti pranešimus, jei viena iš šalių (siuntėjas arba gavėjas) sutiko ir yra suteiktas leidimas pagal 2000 m. Tyrimo įgaliojimų reglamentavimo aktą arba 2000 m. (Škotijos) Tyrimo įgaliojimų reguliavimo aktą (2000 m. Škotijos Parlamento įstatymas Nr. 11), t. y. ankstesnę teisinę padėtį iki teismo komisarų įsteigimo. EDAV **ragina** Europos Komisiją paaiškinti, ar tai reiškia, kad tais atvejais, kai egzistuoja vienašalis sutikimas, išankstinio patvirtinimo procedūra apskritai nebūtų taikoma.

207. Kalbant apie *ex post* priežiūrą, taip pat svarbu patikrinti, ar užtikrinama veiksminga nepriklausoma priežiūra ir nėra spragų, visų pirma tais atvejais, kai ji nenumatyta *ex ante*.

[140] Tačiau ji taip pat pažymi, kad ESTT, pripažindamas privatumo skydą negaliojančiu Sprendime *Schrems II*, atkreipė dėmesį į tai, kad pagal JAV teisę vadinamasis FISA teismas „*neleidžia taikyti atskirų sekimo priemonių, bet leidžia vykdyti sekimo programas (pavyzdžiui, PRISM, UPSTREAM) remdamasis metiniais sertifikatais*.“ (179 punktas).

208. EDAV atkreipia dėmesį į tai, kad dėl 2016 m. Tyrimo įgaliojimų įstatymo 48–52 skirsnių teismo komisarai atlieka *ex post* peržiūrą, ir **ragina Europos Komisiją paaiškinti, pagal kokius reikalavimus ir kieno iniciatyva turi būti atliekama tokia *ex post* peržiūra**.

209. Pagal 2016 m. Tyrimo įgaliojimų įstatymo 229 skirsnio 4 dalį Tyrimų įgaliojimų komisaro tikslas nėra peržiūrėti, kaip vykdomos tam tikros funkcijos. Šiuo atžvilgiu EDAV ragina Europos Komisiją paaiškinti 2016 m. Tyrimo įgaliojimų įstatymo 229 skirsnio 4 dalies d ir e punktų nuostatas dėl jų praktinio poveikio Tyrimų įgaliojimų komisaro peržiūros kompetencijai. **EDAV supranta, kad Informacijos komisaro biuras yra kompetentinga priežiūros institucija tais atvejais, kai taikomos 2016 m. Tyrimo įgaliojimų įstatymo 229 skirsnio 4 dalies išimtys, ir EDAV prašo Europos Komisijos savo sprendime patvirtinti, kad tai yra teisinga.**

210. **Atrodo, kad atliekant** *ex post* priežiūrą, **Tyrimų įgaliojimų komisaro** funkcija **apsiriboja** rekomendacijų teikimu neatitikties atvejais ir pranešimu duomenų subjektui, jei klaida yra rimta ir asmens informavimas atitinka viešąjį interesą. **EDAV ragina Europos Komisiją paaiškinti, kaip Tyrimų įgaliojimų komisaro biuras gali veiksmingai užtikrinti teisės aktų laikymąsi.**

211. **Galiausiai EDAV supranta, kad nukentėję asmenys negali tiesiogiai kreiptis į Tyrimų įgaliojimų komisaro biurą, bet turi pateikti skundą Tyrimų įgaliojimų komisarui, kuris vis dėlto turi ribotą kompetenciją nacionalinio saugumo srityje. Todėl EDAV ragina Europos Komisiją išsamiau paaiškinti, kaip teisiškai užtikrinama, kad tokiais atvejais Tyrimų įgaliojimų komisaro biuras nagrinėtų skundus.**

4.3.4. Teisė kreiptis į teismą

212. Atsižvelgiant į ESTT sprendimus *Schrems I* ir *Schrems II*, akivaizdu, kad veiksminga teisminė apsauga, kaip apibrėžta ES chartijos 47 straipsnyje, yra labai svarbi trečiosios valstybės teisės tinkamumo prielaidai. Iš sprendimų taip pat matyti, kad šiuo atžvilgiu ypatingas dėmesys turi būti skiriamas veiksmingai teisminei apsaugai nacionalinio saugumo prieigos prie asmens duomenų srityje.

213. **EDAV pripažįsta, kad JK įsteigė Tyrimo įgaliojimų teismą. Tyrimo įgaliojimų teismas yra kompetentingas nagrinėti bylas, susijusias ne tik su teisėsaugos institucijų, bet ir su žvalgybos tarnybų naudojimusi tyrimo įgaliojimais. EDAV nuomone, Tyrimo įgaliojimų teismas veikia kaip tinkamas teismas, kaip apibrėžta ES chartijos 47 straipsnyje. Kalbant apie jo įgaliojimus, Europos Komisijos prašoma patvirtinti, kad Tyrimo įgaliojimų teismas turi visus sprendimo projekto 262 konstatuojamojoje dalyje nurodytus įgaliojimus, nepriklausomai nuo teisinio pagrindo, kuriuo remiantis pateiktas skundas.**

214. Žvalgybos agentūrų vykdomas slaptas sekimas dažnai reiškia, kad sekimo objektas, t. y. duomenų subjektas, nežino ir nesužinos apie sekimą. Šiomis aplinkybėmis, kai teko analizuoti JAV teisę, EDAV ne kartą išreiškė susirūpinimą dėl, kaip aiškinama JAV teisėje, *locus standi* reikalavimo stebėjimo bylose. Atsižvelgdama į tai, EDAV pažymi, kad Tyrimo įgaliojimų teisme pateiktam skundui reikalingas tik „įsitikinimo“ patikrinimas, pagal kurį skundo pateikėjas turi įrodyti, kad jam gali grėsti pavojus, jog jam bus taikoma priemonė.

215. Analizuodama Tyrimo įgaliojimų teismą, EDAV taip pat skiria ypatingą dėmesį tam, kad ne kartą buvo nustatyta, jog Tyrimo įgaliojimų teismo veikla atitinka EŽTK, kaip ją aiškina EŽTT.