

**Nuomonė 15/2021 dėl Europos Komisijos įgyvendinimo
sprendimo pagal Direktyvą (ES) 2016/680 dėl tinkamos
duomenų apsaugos Jungtinėje Karalystėje**

projekto

Priimta 2021 m. balandžio 13 d.

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

Informacija apie versijas

Versija 1.1	2021 m. liepos 6 d.	Formatavimo pakeitimai
Versija 1.0	2021 m. balandžio 13 d.	Nuomonės priėmimas

TURINYS

1. SANTRAUKA.....	4
2. ĮVADAS	5
2.1. JK duomenų apsaugos sistema	5
2.2. EDAV vertinimo apimtis.....	6
2.3. Bendrosios pastabos ir abejonės	7
2.3.1. JK prisiimti tarptautiniai įsipareigojimai.....	7
2.3.2. Galimi JK duomenų apsaugos sistemos skirtumai ateityje.....	8
3. TAISYKLĖS, TAIKOMOS KOMPETENTINGOMS INSTITUCIJOMS TVARKANT ASMENS DUOMENIS BAUDŽIAMOSIOS TEISĖSAUGOS TIKSLAIS	9
3.1. Materialinė taikymo sritis.....	9
3.2. Apsaugos priemonės, teisės ir prievolės.....	10
3.2.1. Duomenų tvarkymas remiantis duomenų subjekto sutikimu	10
3.2.2. Asmens teisės	10
3.2.2.1. <i>Nacionalinio saugumo pažymėjimai</i>	10
3.2.2.2. <i>Automatizuotas sprendimų priėmimas pagal TD</i>	11
3.2.3. Tolesnis perdavimas	12
3.2.4. Tolesnis duomenų tvarkymas, įskaitant tolesnį atskleidimą nacionalinio saugumo tikslais.....	14
3.3. Priežiūra ir vykdymo užtikrinimas.....	14

Europos duomenų apsaugos valdyba,

atsižvelgdama į 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyvos (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuria panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR¹ (toliau – TD) 51 straipsnio 1 dalies g punktą,

atsižvelgdama į savo Darbo tvarkos taisyklių 12 ir 22 straipsnius,

PRIĖMĖ ŠIĄ NUOMONĘ:

1. SANTRAUKA

1. 2021 m. vasario 19 d. Europos Komisija patvirtino savo įgyvendinimo sprendimo pagal TD dėl tinkamos asmens duomenų apsaugos Jungtinėje Karalystėje (toliau – JK) projektą (toliau – sprendimo projektas)². Po to Europos Komisija pradėjo oficialaus jo priėmimo procedūrą.
2. Tą pačią dieną Europos Komisija paprašė Europos duomenų apsaugos valdybos (toliau – EDAV) pateikti nuomonę³. EDAV JK suteikiamos apsaugos lygio tinkamumo vertinimas buvo atliktas išnagrinėjus patį sprendimo projektą, taip pat išanalizavus Europos Komisijos pateiktus dokumentus.
3. EDAV šiame darbe daugiausia rėmėsi savo Rekomendacijomis dėl tinkamumo pavyzdžių pagal TD⁴, priimtomis 2021 m. vasario 2 d., taip pat atitinkama jurisprudencija, nurodyta EDAV rekomendacijoje 02/2020 dėl Europos pagrindinių garantijų taikant stebėjimo priemones⁵.
4. Pagrindinis EDAV tikslas yra pateikti Europos Komisijai nuomonę dėl JK asmenims suteikiamos apsaugos lygio tinkamumo. Svarbu pažymėti, kad EDAV nesitiki, jog JK teisinė sistema visiškai atitiks Europos duomenų apsaugos teisę.
5. Tačiau EDAV primena, jog tam, kad trečioji valstybė būtų laikoma užtikrinančia tinkamo lygio apsaugą, pagal TD 36 straipsnį ir Europos Sąjungos Teisingumo Teismo (toliau – ESTT) jurisprudenciją reikalaujama, kad jos teisės aktai atitiktų TD įtvirtintų pagrindinių principų esmę. Duomenų apsaugos srityje EDAV pažymi, kad TD sistema ir JK teisinė sistema yra tinkamai suderintos 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; automatizuoto sprendimų priėmimo ir profiliavimo.

¹ OL L 119, 2016 5 4, p. 89.

² Žr. Europos Komisijos pranešimą spaudai „Duomenų apsauga. Europos Komisija pradeda procesą dėl asmens duomenų judėjimo į Jungtinę Karalystę, 2021 m. vasario 19 d. https://ec.europa.eu/commission/presscorner/detail/lt/ip_21_661.

³ Ten pat.

⁴ Žr. EDAV rekomendacijas 01/2021 dėl tinkamumo pavydžių pagal Teisės saugos direktyvą, priimtas 2021 m. vasario 2 d., https://edpb.europa.eu/system/files/2021-05/recommendations012021onart.36led.pdf_lt.pdf.

⁵ Žr. EDAV rekomendacijas Nr. 02/2020 dėl Europos pagrindinių garantijų taikant stebėjimo priemones, priimtas 2020 m. lapkričio 10 d., https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_lt.pdf.

6. EDAV rekomenduoja Europos Komisijai papildyti savo analizę informacija apie tai, ar yra mechanizmas, pagal kurį atitinkamos valstybės narės kompetentingos institucijos būtų informuojamos apie JK institucijų, kurioms jos perdavė asmens duomenis, vykdomą tolesnį duomenų tvarkymą ar atskleidimą, ir nustatyti jo veiksmingumą pagal JK teisinę sistemą.
7. EDAV mano, kad dėl JK teisėsaugos institucijos vykdomo asmens duomenų perdavimo trečiajai valstybei 2018 m. Duomenų apsaugos akto (toliau – 2018 m. DAA) 3 dalies 5 skyriaus nuostatose iš principo numatytas apsaugos lygis, kuris yra iš esmės lygiavertis pagal ES teisę užtikrintam apsaugos lygiui.
8. Nors EDAV pažymi, kad JK pagal savo teisinę sistemą gali pripažinti teritorijas užtikrinančiomis tinkamą duomenų apsaugos lygį atsižvelgiant į JK duomenų apsaugos sistemą, EDAV atkreipia dėmesį, kad dėl to gali kilti pavojus iš ES perduotų asmens duomenų apsaugai, ypač tuo atveju, jei ateityje JK duomenų apsaugos sistema nukryptų nuo Sąjungos *acquis*. **Todėl pirmiau nurodytais atvejais Europos Komisija turėtų vykdyti savo stebėsenos funkciją ir, jeigu neužtikrinamas iš esmės lygiavertis iš ES perduotų asmens duomenų apsaugos lygis, Europos Komisija turėtų apsvarstyti galimybę keisti sprendimą dėl tinkamumo, numatydama konkrečias iš ES perduotų duomenų apsaugos priemones, ir (arba) sustabdyti sprendimo dėl tinkamumo galiojimą.**
9. **Galiausiai, dėl JK ir trečiųjų valstybių sudarytų tarptautinių susitarimų** Europos Komisija raginama išnagrinėti JK duomenų apsaugos sistemos ir jos tarptautinių įsipareigojimų sąveiką, visų pirma siekiant užtikrinti apsaugos lygio tęstinumą, kai asmens duomenys iš ES perduodami į JK pagal JK sprendimą dėl tinkamumo, o tada toliau perduodami į kitas trečiąsias valstybes, bei nuolat stebėti ir prireikus imtis veiksmų, jeigu JK sudarius tarptautinius susitarimus su trečiosiomis valstybėmis kyla pavojus, kad gali sumažėti ES numatytas asmens duomenų apsaugos lygis.
10. Šiuo klausimu EDAV pažymi, kad JK ir JAV susitarimo dėl prieigos prie elektroninių duomenų siekiant kovoti su sunkiais nusikaltimais (toliau – JK ir JAV susitarimas pagal CLOUD aktą)⁶ įsigaliojimas gali turėti poveikio JK teisėsaugos institucijų vykdomam tolesniam duomenų perdavimui, visų pirma dėl orderių išdavimo ir perdavimo pagal JK ir JAV susitarimo pagal CLOUD aktą 5 straipsnį.
11. EDAV taip pat rekomenduoja Europos Komisijai nuolat stebėti, ar būsimų susitarimų su trečiosiomis valstybėmis sudarymas teisėsaugos bendradarbiavimo tikslu, numatant asmens duomenų perdavimo į tas trečiąsias valstybes teisinį pagrindą, gali turėti poveikio tolesnio surinktos informacijos atskleidimo sąlygoms, visų pirma, kai tų tarptautinių susitarimų nuostatos gali turėti poveikio JK duomenų apsaugos teisės taikymui ir kai jose numatyti papildomi apribojimai ar išimtys dėl teisėsaugos tikslais surinktos informacijos tolesnio naudojimo ar atskleidimo užsienyje. EDAV mano, kad tokia informacija ir vertinimas yra būtini, kad būtų galima atlikti išsamią JK teisės aktų sistemos ir praktikos dėl duomenų atskleidimo užsienyje suteikiamo apsaugos lygio peržiūrą.

2. ĮVADAS

2.1. JK duomenų apsaugos sistema

12. JK duomenų apsaugos sistema daugiausia grindžiama ES duomenų apsaugos sistema (visų pirma TD ir 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų

⁶ Žr. 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, 2019 m. spalio 3 d.

apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (toliau – BDAR)), o taip yra todėl, kad iki 2020 m. sausio 31 d. JK buvo ES valstybė narė. Be to, 2018 m. gegužės 23 d. įsigaliojusio 2018 m. DAA, kuriuo buvo panaikintas 1998 m. JK duomenų apsaugos aktas, 3 dalimi į nacionalinę teisę perkelta TD, be to, tame akte išsamiau nustatytas BDAR taikymas JK teisėje, taip pat suteikti įgaliojimai nacionalinei duomenų apsaugos priežiūros institucijai – JK informacijos komisaro biurui (toliau – IKB) ir nustatytos jos pareigos.

13. Kaip nurodyta sprendimo projekto 12 konstatuojamojoje dalyje, JK vyriausybė priėmė 2018 m. (išstojimo iš) Europos Sąjungos aktą, kuriuo tiesiogiai taikomi ES teisės aktai perkelti į JK teisę. Pagal šį aktą JK ministrai yra įgalioti priimti antrinės teisės aktus naudodami įstatymų lydimuosius teisės aktus, kad JK išstojus iš ES galėtų atlikti reikiamus paliktų galioti ES teisės aktų pakeitimus, kad jie atitiktų šalies vidaus aplinkybes.
14. Todėl atitinkamą JK taikomą teisinę sistemą pasibaigus pereinamajam laikotarpiui⁷ sudaro:
 - Jungtinės Karalystės bendrasis duomenų apsaugos reglamentas (toliau – JK BDAR), perkeltas į JK teisę pagal 2018 m. (išstojimo iš) Europos Sąjungos aktą, su pakeitimais, padarytais 2019 m. DPPEC (Duomenų apsaugos, privatumo ir elektroninių ryšių (pakeitimai ir kt.) (dėl išstojimo iš ES)) taisyklėmis;
 - 2018 m. DAA, su pakeitimais, padarytais 2019 m. DPPEC taisyklėmis ir 2020 m. Duomenų apsaugos, privatumo ir elektroninių ryšių (pakeitimai ir kt.) (dėl išstojimo iš ES) taisyklėmis, ir
 - 2016 m. Tyrimo įgaliojimų aktas (toliau – 2016 m. IPA).

(toliau kartu – JK duomenų apsaugos sistema).

2.2. EDAV vertinimo apimtis

15. Europos Komisijos sprendimo projektas buvo priimtas atlikus JK duomenų apsaugos sistemos vertinimą, po jo vyko diskusijos su JK vyriausybe. Pagal TD 51 straipsnio 1 dalies g punktą EDAV turėtų pateikti nepriklausomą nuomonę dėl Europos Komisijos nustatytų faktų, nustatyti tinkamumo sistemos trūkumus, jei jų yra, ir stengtis teikti pasiūlymus jiems pašalinti.
16. Kaip nurodyta Rekomendacijose dėl tinkamumo pavyzdžių pagal TD, „*Europos Komisijos suteikta informacija turėtų būti išsami ir sudaryti sąlygas Europos duomenų apsaugos valdybai atlikti savo vertinimą, susijusį su duomenų apsaugos lygiu trečiojoje valstybėje*⁸“.
17. Šiuo klausimu reikia pažymėti, kad EDAV laiku gavo tik dalį dokumentų, reikšmingų norint ištirti JK teisinę sistemą. Daugumą sprendimo projekte nurodytų JK teisės aktų EDAV gavo naudodama jame pateiktus saitus. Europos Komisija negalėjo EDAV pateikti JK rašytinių paaiškinimų ir įsipareigojimų, susijusių su JK institucijų ir Europos Komisijos keitimusi duomenimis, reikšmingais šiai užduočiai⁹.

⁷ Pereinamasis laikotarpis nustatytas iki 2020 m. gruodžio 31 d. Po šios datos ES teisė JK nebetaikoma. Tarpinis laikotarpis nustatytas vėliausiai iki 2021 m. birželio 30 d. Tai yra papildomas laikotarpis, kuriuo asmens duomenų perdavimas iš ES į JK nėra laikomas duomenų perdavimu.

⁸ Žr. Rekomendacijų 01/2021 dėl tinkamumo pavyzdžių pagal Teisėsapgautos direktyvą 15 punktą, p. 5.

⁹ Toliau nurodyti elementai, dėl kurių Europos Komisija savo sprendimo projekte remiasi JK institucijų paaiškinimais, nepateikdama tuos paaiškinimus pagrindžiančių JK institucijų rašytinių dokumentų, pavyzdžiui: pereinamojo laikotarpio nuostatų poveikis ir laikino galiojimo nuostatos nebuvimas (87 konstatuojamoji dalis); sutikimo, kaip tinkamo duomenų tvarkymo pagrindo, pavyzdžiai (68 išnaša); sąvoka „netikslūs“, reiškianti „neteisingus ar klaidinančius“ asmens duomenis (79 išnaša); ISC įgaliojimai (245 išnaša); žema skundo pateikimo

18. Atsižvelgdama į tai, kas išdėstyta pirmiau, ir į ribotą laikotarpį (2 mėnesiai), skirtą EDAV šiai nuomonei priimti, EDAV nusprendė daugiausia dėmesio skirti keliems konkrečioms sprendimo projekte nurodytiems klausimams ir dėl jų pateikti savo analizę ir nuomonę. Matyti, kad EDAV, analizuodama trečiosios valstybės, kuri dar visai neseniai buvo ES valstybė narė, teisę ir praktiką, nustatė, kad daug aspektų yra iš esmės lygiaverčiai. Atsižvelgdama į savo vaidmenį sprendimo dėl tinkamumo priėmimo procese ir tai, kiek teisės ir praktikos reikia išanalizuoti, EDAV nusprendė daugiausia dėmesio skirti tiems aspektams, kuriuos, jos nuomone, labiausiai reikia įvertinti atidžiau.
19. EDAV atsižvelgė į taikomą Europos duomenų apsaugos sistemą, įskaitant Europos Sąjungos pagrindinių teisių chartijos (toliau – ES chartija) 7, 8 ir 47 straipsnius, kuriais atitinkamai saugoma teisė į privatų ir šeimos gyvenimą, teisė į asmens duomenų apsaugą bei teisė į veiksmingą teisinę gynybą ir teisingą bylos nagrinėjimą, ir Europos žmogaus teisių konvencijos (toliau – EŽTK) 8 straipsnį, kuriuo saugoma teisė į privatų ir šeimos gyvenimą. Be to, EDAV atsižvelgė į TD numatytus reikalavimus, taip pat į atitinkamą jurisprudenciją.
20. Šio darbo 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 ESTT. Svarbu priminti Sprendime *Schrems I* ESTT nustatytą standartą, t. y. kad nors „apsaugos lygis“ trečiojoje valstybėje privalo būti „iš esmės lygiavertis“ ES užtikrintam apsaugos lygiui, „priemonės, kurių ši trečioji šalis šiuo klausimu imasi siekdama užtikrinti tokį apsaugos lygį, gali skirtis nuo priemonių, kurios taikomos ES“¹⁰. Todėl tikslas – ne atitikti kiekvieną Europos Sąjungos teisės akto punktą, o nustatyti pagrindinius, esmę perteikiančius nagrinėjamo 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 veiksmingos¹¹.

2.3. Bendrosios pastabos ir abejonės

2.3.1. JK priiimti tarptautiniai įsipareigojimai

21. Pagal TD 36 straipsnio 2 dalies c punktą ir Rekomendacijas dėl tinkamumo pavyzdžių pagal TD¹², vertindama apsaugos lygio trečiojoje valstybėje tinkamumą, Komisija visų pirma atsižvelgia, be kita ko, į trečiosios valstybės priiimtus tarptautinius įsipareigojimus ar kitus įsipareigojimus, atsirandančius dėl jos dalyvavimo daugiašalėse ar regioninėse sistemose, visų pirma, kiek tai susiję su asmens duomenų apsauga, taip pat į tokių įsipareigojimų vykdymą. Be to, reikėtų atsižvelgti į trečiosios valstybės prisijungimą prie 1981 m. sausio 28 d. Europos Tarybos konvencijos dėl asmenų apsaugos

IPT riba ir tai, kad IPT neretai nusprendžia, kad dėl skundo pateikėjo valdžios institucija iš tiesų niekada neatliko tyrimo (263 išnaša); teisės aktuose ir bendrojoje teisėje numatytų įgaliojimų derinys (52 išnaša); vyriausybės įgyvendinami prerogatyviniai įgaliojimai (62 išnaša); tai, kad kitos organizacijos gali laisvai laikytis MOPI praktikos kodekso principų, jeigu to pageidauja (86 išnaša).

¹⁰ Žr. ESTT, C-362/14, *Maximilian Schrems / Data Protection Commissioner*, 2015 m. spalio 6 d., ECLI:EU:C:2015:650 (toliau – Sprendimas *Schrems I*), 73–74 punktus.

¹¹ Žr. EDAV rekomendacijų 01/2021 dėl tinkamumo pavyzdžių pagal Teisėsaugos direktyvą 14 punktą, p. 5.

¹² Žr. EDAV rekomendacijų 01/2021 dėl tinkamumo pavyzdžių pagal Teisėsaugos direktyvą 24 punktą, p. 7.

ryšium su asmens duomenų automatizuotu tvarkymu (toliau – Konvencija 108)¹³ ir jos papildomo protokolo¹⁴.

22. Šiuo klausimu EDAV teigiamai vertina tai, kad JK prisijungė prie EŽTK ir kad jai taikoma Europos Žmogaus Teisių Teismo (toliau – EŽTT) jurisdikcija. Be to, JK prisijungė prie Konvencijos 108 ir jos papildomo protokolo, 2018 m. pasirašė Konvenciją 108+¹⁵ ir šiuo metu rengiasi ją ratifikuoti.

2.3.2. Galimi JK duomenų apsaugos sistemos skirtumai ateityje

23. Kaip nurodyta sprendimo projekto 171 konstatuojamojoje dalyje, Europos Komisija turi atsižvelgti į tai, kad pasibaigus Susitarime dėl išstojimo¹⁶ numatytam pereinamajam laikotarpiui JK administruoja, taiko ir vykdo savo duomenų apsaugos sistemą, o nustojus galioti ES ir JK prekybos ir bendradarbiavimo susitarimo¹⁷ FINPROV.10A straipsnyje numatytai tarpinei nuostatai¹⁸, sprendimo projekte įvertinta duomenų apsaugos sistema gali būti iš dalies keičiama arba keičiama, taip pat gali būti kitų reikšmingų pokyčių.
24. Todėl Europos Komisija nusprendė į sprendimo projektą įtraukti laikino galiojimo sąlygą¹⁹, kurioje nustatyta galiojimo pabaigos data – ketveri metai nuo jos įsigaliojimo.
25. Svarbu pažymėti, kad dėl JK ministrų ir JK valstybės sekretoriaus galimybės priimti antrinės teisės aktus pasibaigus tarpiniam laikotarpiui ateityje gali atsirasti didelių JK ir ES duomenų apsaugos sistemų skirtumų.
26. Galiausiai, pasibaigus pereinamajam laikotarpiui JK ne tik nebeprivaloma ESTT jurisprudencija, tačiau jai gali būti nebeprivalomi ir jau priimti ESTT sprendimai, kurie JK teisinėje sistemoje laikomi palikta galioti jurisprudencija, visų pirma atsižvelgiant į tai, kad pasibaigus tarpiniam laikotarpiui JK turi galimybę keisti paliktą galioti ES teisę, o jos Aukščiausiajam Teismui jokia palikta galioti ES jurisprudencija neprivaloma²⁰.
27. **Atsižvelgdama į pavojų, susijusį su galimu JK duomenų apsaugos sistemos nukrypimu nuo Sąjungos *acquis* pasibaigus tarpiniam laikotarpiui, EDAV teigiamai vertina Europos Komisijos sprendimą į sprendimo projektą įtraukti ketverių metų laikino galiojimo sąlygą. Tačiau čia EDAV norėtų atkreipti dėmesį į Europos Komisijos stebėsenos funkcijos²¹ svarbą. Iš tiesų Europos Komisija turėtų stebėti visus susijusius įvykius JK, kurie gali turėti poveikio pagal JK sprendimą dėl tinkamumo nuo pat jo įsigaliojimo nuolat perduodamų asmens duomenų iš esmės lygiaverčiui apsaugos lygiui. Be to, jeigu**

¹³ Žr. Konvenciją dėl asmenų apsaugos ryšium su asmens duomenų tvarkymu, Konvencija 108, 1981 m. sausio 28 d.

¹⁴ Žr. Konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu Papildomą protokolą dėl priežiūros institucijų ir valstybės sienas kertančių duomenų srautų, pateiktą pasirašyti 2001 m. lapkričio 8 d.

¹⁵ Žr. Protokolą, kuriuo iš dalies keičiama Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (toliau – Konvencija 108+), 2018 m. gegužės 18 d.

¹⁶ 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).

¹⁷ 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).

¹⁸ Pereinamasis laikotarpis nustatytas iki 2020 m. gruodžio 31 d. Po šios datos ES teisė JK nebetaikoma. Tarpinis laikotarpis nustatytas vėliausiai iki 2021 m. birželio 30 d. Tai yra papildomas laikotarpis, kuriuo asmens duomenų perdavimas iš ES į JK nėra laikomas duomenų perdavimu.

¹⁹ Žr. sprendimo projekto 4 straipsnį. Taip pat žr. sprendimo projekto 172 konstatuojamąją dalį.

²⁰ Žr. 2018 m. (išstojimo iš) Europos Sąjungos akto 6 straipsnio 3–6 dalis.

²¹ Žr. TD 36 straipsnio 4 dalį.

Europos Komisija, priėmusi sprendimą dėl tinkamumo, nustato, kad JK nebeužtikrinama tinkamo lygio apsauga, ji turėtų imtis atitinkamų veiksmų ir, atsižvelgdama į esamas aplinkybes, sustabdyti sprendimo dėl tinkamumo galiojimą, tą sprendimą iš dalies pakeisti arba panaikinti.

28. Savo ruožtu EDAV dė visas pastangas, kad informuotų Europos Komisiją apie bet kokius reikšmingus valstybės narės duomenų apsaugos priežiūros institucijų (toliau – PI) veiksmus, visų pirma dėl ES duomenų subjektų pateiktų skundų, susijusių su asmens duomenų perdavimu iš ES į JK.

3. TAISYKLĖS, TAIKOMOS KOMPETENTINGOMS INSTITUCIJOMS TVARKANT ASMENS DUOMENIS BAUDŽIAMOSIOS TEISĖSAUGOS TIKSLAIS

3.1. Materialinė taikymo sritis

29. Dėl sprendimo projekto 24 ir paskesnių konstatuojamųjų dalių EDAV pažymi, kad sprendimo dėl tinkamumo projekte pateikta nedaug informacijos apie kitų teisėsaugos pareigų turinčių institucijų, išskyrus policiją, veiklą ir joms taikomą teisinę sistemą.
30. Pavyzdžiui, iš JK aiškinamojo dokumento dėl sprendimų dėl tinkamumo F skyriaus „Teisėsauga“²² 11 puslapio matyti, kad **Nacionalinė nusikaltimų tyrimo agentūra** (toliau – NCA) gali būti itin svarbi teisėsaugos institucija, kuri, be kita ko, vykdo platesnę kriminalinės žvalgybos funkciją. NCA nurodo, kad jos misija yra sutelkti žvalgybos informaciją iš įvairių šaltinių siekiant kuo geriau išnaudoti analizės, vertinimo ir taktines galimybes, be kita ko, techninėmis priemonėmis perimant ryšius, gaunant informaciją iš teisėsaugos partnerių JK ir užsienyje, saugumo ir žvalgybos institucijų²³. NCA taip pat yra viena iš pagrindinių institucijų, palaikanti ryšį su tarptautiniais teisėsaugos partneriais, ir atlieka svarbų vaidmenį keičiantis kriminalinės žvalgybos informacija²⁴.
31. EDAV taip pat pažymi, kad Vyriausybės ryšių centrinis biuras (toliau – GCHQ), kurio veikla paprastai patenka į 2018 m. DPA 4 dalies, t. y. dėl nacionalinio saugumo, taikymo sritį, taip pat atlieka aktyvų vaidmenį siekdamas sumažinti sunkių ir organizuotų nusikaltimų visuomeninę ir finansinę žalą JK,

²² Žr. JK vyriausybė, Aiškinamasis dokumentas dėl sprendimų dėl tinkamumo, F skyrius „Teisėsauga“, 2020 m. kovo 13 d. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F-Law-Enforcement.pdf.

²³ Žr. Nacionalinės nusikaltimų tyrimo agentūros svetainę, „Intelligence: enhancing the picture of serious organised crime affecting the UK“, <https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work/intelligence-enhancing-the-picture-of-serious-organised-crime-affecting-the-uk>.

²⁴ Nors ne visa NCA tvarkoma žvalgybos informacija yra asmens duomenys, didelė jos dalis gali būti asmeninė informacija, o čia aprašyta veikla skiriasi nuo įprastos policijos veiklos, todėl visapusiškai neįvertinus NCA veiklos vertinimas dėl JK teisėsaugos institucijų prieigos prie asmens duomenų būtų nebaigtas. Atrodo pagrįsta patikrinti, ar visose susijusiose teisėsaugos institucijose duomenų apsaugos principai suprantami vienodai, taip geriau suprantant institucijos, kuri ypač grindžiama duomenimis, kaip antai NCA, veiklą. Be to, paaiškinimo dalyje dėl ateities tikslų nurodyta: „nuolat ieškome naujų galimybių rinkti, plėtoti ir tobulinti įprastus pajėgumus siekdami padidinti žvalgybos informacijos, kurią galima naudoti ir JK, ir užsienyje, kiekį ir pagerinti jos kokybę.“ „Tai darydami kuriame naują nacionalinių duomenų naudojimo pajėgumą, naudodamiesi pagal Nusikaltimų ir teismų įstatymą institucijai suteiktais įgaliojimais, kad susietumėme, pasiektumėme ir naudotumėme vyriausybės turimus duomenis.“ <...> „Visa tai pagerins mūsų dinamiškumą ir lankstumą siekiant reaguoti į naujas grėsmes ir veikti aktyviai, surinkti ir analizuoti informaciją ir žvalgybos informaciją apie kylančias grėsmes, kad galėtume imtis veiksmų prieš joms atsirandant.“

bendradarbiaudamas su Vidaus reikalų ministerija, NCA, Jos Didenybės mokesčių ir muitų departamentu (toliau – HMRC) ir kitais vyriausybės departamentais²⁵. Jo veikla susijusi su kova su seksualine prievarta prieš vaikus, sukčiavimu, kitų rūšių ekonominiais nusikaltimais, įskaitant pinigų plovimą, nusikalstamą naudojimąsi technologijomis, kibernetinius nusikaltimus, organizuotą nusikalstamumą imigracijos srityje, įskaitant prekybą žmonėmis bei narkotikų, šaunamųjų ginklų ir kitų daiktų neteisėtą gabenimą.

32. **EDAV ragina Europos Komisiją papildyti savo analizę teisėsaugos srityje veikiančių institucijų (visų pirma – NCA), kurių kasdienėje veikloje daugiausia dėmesio skiriama duomenų, įskaitant asmens duomenis, rinkimui ir analizei, analize. Be to, EDAV ragina Komisiją atidžiau įvertinti institucijas, kaip antai GCHQ, kurių veikla patenka ir į teisėsaugos, ir į nacionalinio saugumo sritį, bei joms taikomą teisinę sistemą tvarkant asmens duomenis.**

3.2. Apsaugos priemonės, teisės ir prievolės

3.2.1. Duomenų tvarkymas remiantis duomenų subjekto sutikimu

33. EDAV pažymi, kad Europos Komisija sprendimo projekto 37 ir 38 konstatuojamosiose dalyse teigia, kad **rėmimasis sutikimu** tinkamumo situacijose nelaikomas reikšmingu, nes duomenų perdavimo atvejais JK teisėsaugos institucija iš duomenų subjekto tiesiogiai nerenka duomenų remdamasi sutikimu.
34. Šiuo klausimu EDAV primena, kad pagal TD 36 straipsnio 2 dalies a punktą reikalaujama įvertinti įvairius elementus neapsiribojant duomenų perdavimo atveju, „įskaitant teisinės valstybės principą, pagarbą žmogaus teisėms ir pagrindinėms laisvėms, atitinkamus bendruosius ir atskiriems sektoriams skirtus teisės aktus, įskaitant <...> dėl <...> baudžiamosios teisės“.
35. Teisėsaugos srityje sutikimas gali būti reikšmingas kaip duomenų tvarkymo teisinis pagrindas, kaip papildoma apsaugos priemonė arba bendresne prasme – kaip tyrimo įgaliojimų, kuriais naudojantis gaunami asmens duomenys, vykdymo pagrindas, pavyzdžiui, trečiosios šalies sutikimas dėl jos patalpų apieškojimo arba duomenų saugyklos konfiskavimo.
36. EDAV, be kita ko, remdamasi Europos Komisijos sprendimo projekto 38 konstatuojamojoje dalyje pateikta informacija, pažymi, kad norint naudoti sutikimą, kaip numatyta JK sistemoje, visada turėtų būti remiamasi teisiniu pagrindu. Tai reiškia, kad, net jeigu policija turi teisės aktuose numatytus įgaliojimus tvarkyti duomenis tyrimo tikslais, tam tikromis konkrečiomis aplinkybėmis (pavyzdžiui, norint paimti DNR mėginį), policijai gali atrodyti tinkama paprašyti duomenų subjekto sutikimo.
37. **EDAV ragina Europos Komisiją, kad ši, vertindama trečiosios valstybės tinkamumą pagal LED, paprastai išanalizuotų galimą sutikimo naudojimą teisėsaugos srityje.**

3.2.2. Asmens teisės

3.2.2.1. Nacionalinio saugumo pažymėjimai

38. Pagal 2018 m. DPA 79 straipsnį duomenų valdytojai gali prašyti ministro, kabineto nario, generalinio prokuroro arba Škotijos generalinio advokato išduoti nacionalinį saugumo pažymėjimą, kuriuo patvirtinama, kad 2018 m. DPA 3 dalies 3 ir 4 skyriuose numatytų teisių ir pareigų apribojimai yra būtina ir proporcinga priemonė nacionaliniam saugumui užtikrinti.

²⁵ Žr. GCHQ svetainę – „Misija, sunkus ir organizuotas nusikalstamumas“, <https://www.gchq.gov.uk/section/mission/serious-crime>.

39. Šie pažymėjimai skirti suteikti duomenų valdytojams daugiau teisinio tikrumo ir jie laikomi įtikinamais įrodymais, kad tvarkant asmens duomenis taikomas nacionalinis saugumas. Tačiau reikia pažymėti, kad šie pažymėjimai yra neprivalomi norint remtis nacionalinio saugumo apribojimais, tačiau jie yra skaidrumo priemone²⁶.
40. Iš 2018 m. DPA 20 priedo 17 ir 18 straipsnių EDAV supranta, kad pagal 1998 m. Duomenų apsaugos aktą išduoti nacionalinio saugumo pažymėjimai (toliau – senas pažymėjimas) iki 2019 m. gegužės 25 d. toliau buvo taikomi asmens duomenų tvarkymui pagal 2018 m. DPA. Iki šios datos seni pažymėjimai, kurie nebuvo pakeisti ar panaikinti, buvo vertinami taip, tarsi jie būtų išduoti pagal 2018 m. DPA. Tačiau, kai pagal 1998 m. Duomenų apsaugos aktą išduotame nacionalinio saugumo pažymėjime aiškiai nenurodyta galiojimo pabaigos data, EDAV mano, kad toks pažymėjimas (išskyrus atvejus, kai jis atšaukiamas arba panaikinamas) bus toliau taikomas duomenų tvarkymui pagal 1998 m. duomenų apsaugos aktą²⁷. Nors pagal šiuos senus pažymėjimus suteikiama apsauga taikoma tik tvarkant asmens duomenis pagal 1998 m. Duomenų apsaugos aktą, EDAV pažymi, kad dėl asmens duomenų, kurie buvo tvarkomi pagal 1998 m. Duomenų apsaugos aktą, pagal šį aktą gali būti išduoti nauji nacionalinio saugumo pažymėjimai²⁸.
41. **Siekdama didesnio aiškumo EDAV ragina Europos Komisiją savo sprendimo dėl tinkamumo projekte patikslinti, kad pagal 1998 m. Duomenų apsaugos aktą vis dar gali būti išduodami nacionaliniai saugumo pažymėjimai. Be to, EDAV ragina Europos Komisiją savo sprendimo dėl tinkamumo projekte aprašyti teisių gynimo ir priežiūros mechanizmus dėl pažymėjimų, išduotų pagal 1998 m. Duomenų apsaugos aktą. Galiausiai EDAV ragina Europos Komisiją savo sprendimo dėl tinkamumo projekte nurodyti esamų pažymėjimų, išduotų pagal 1998 m. Duomenų apsaugos aktą, skaičių ir atidžiai stebėti šį aspektą.**

3.2.2.2. *Automatizuotas sprendimų priėmimas pagal TD*

42. EDAV pažymi, kad pagal TD 11 straipsnio 3 dalį draudžiamas profiliavimas, sukeliantis fizinių asmenų diskriminaciją remiantis specialių kategorijų asmens duomenimis. Tačiau EDAV pažymi, kad 2018 m. DPA 50 straipsnyje, kuriame nustatytos konkrečios automatizuoto sprendimų priėmimo taisyklės, toks draudimas nenumatytas.
43. **Todėl EDAV ragina Europos Komisiją patikrinti šį aspektą ir aiškiai nurodyti nustatytus faktus savo sprendime dėl tinkamumo. Be to, EDAV ragina Europos Komisiją atidžiai stebėti atvejus, susijusius su automatizuotu sprendimų priėmimu ir profiliavimu.**
44. Rekomendacijose dėl tinkamumo pavyzdžių pagal TD nurodyta, kad „[t]rečiosios valstybės teisėje bet kuriuo atveju turėtų būti numatytos reikiamos duomenų subjekto teisių ir laisvių apsaugos priemonės. Atsižvelgiant į tai, taip pat turėtų būti atsižvelgiama į tai, ar yra mechanizmas, pagal kurį atitinkamos valstybės narės kompetentingos institucijos būtų informuojamos apie bet kokį tolesnį duomenų tvarkymą, pavyzdžiui, perduotų duomenų naudojimą plataus masto profiliavimui“²⁹.

²⁶ Žr. JK vidaus reikalų ministerija, 2018 m. Duomenų apsaugos aktas, Gairės dėl nacionalinio saugumo pažymėjimų, 2020 m. rugpjūčio mėn. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf, p. 4.

²⁷ Žr. JK vidaus reikalų ministerija, 2018 m. Duomenų apsaugos aktas, Gairės dėl nacionalinio saugumo pažymėjimų, 2020 m. rugpjūčio mėn., p. 5.

²⁸ Žr. JK vidaus reikalų ministerija, 2018 m. Duomenų apsaugos aktas, Gairės dėl nacionalinio saugumo pažymėjimų, 2020 m. rugpjūčio mėn., p. 5.

²⁹ Žr. EDAV rekomendacijų 01/2021 dėl tinkamumo pavydžių pagal Teisės saugos direktyvą 59–61 punktus.

45. **EDAV ragina Komisiją įvertinti šį elementą atsižvelgiant į EDAV rekomendacijose dėl tinkamumo pavydžių pateiktas gaires.**

3.2.3. Tolesnis perdavimas

46. Pagal Rekomendacijas dėl tinkamumo pavyzdžių pagal TD pradiniam gavėjui asmens duomenis toliau perduodant į kitą trečiąją valstybę ar tarptautinei organizacijai negali sumažėti ES numatytas fizinių asmenų, kurių duomenys perduodami, apsaugos lygis. Taigi, toks tolesnis duomenų perdavimas turėtų būti leidžiamas tik tuo atveju, jei užtikrinamas pagal ES teisę suteikto apsaugos lygio tęstinumas. EDAV mano, kad, kaip savo vertinime pažymėjo Europos Komisija, dėl JK teisėsaugos institucijos vykdomo asmens duomenų perdavimo trečiajai valstybei 2018 m. DPA 3 dalies 5 skyriaus nuostatose, o ypač 73 straipsnyje, iš principo numatytas apsaugos lygis, kuris yra iš esmės lygiavertis pagal ES teisę užtikrintam apsaugos lygiui.
47. Pirma, 2018 m. DPA 73 straipsnio 1 dalies b punkte numatyta, kad duomenų valdytojas asmens duomenų negali perduoti į trečiąją valstybę ar tarptautinei organizacijai, išskyrus atvejus, „*kai asmens duomenis duomenų valdytojui ar kitai kompetentingai institucijai iš pradžių perdavė ar kitaip pateikė valstybė narė, kuri nėra Jungtinė Karalystė, ir ta valstybė narė ar bet kuris toje valstybėje narėje veikiantis subjektas, kuris yra kompetentinga institucija pagal Teisėsaugos direktyvą, leido perduoti duomenis pagal valstybės narės įstatymus*“. Tokios nuostatos atitinka Rekomendacijas dėl tinkamumo pavyzdžių pagal TD, kuriose numatyta, kad taip pat reiktų atsižvelgti į tai, ar yra mechanizmas, pagal kurį atitinkamos valstybės narės kompetentingos institucijos būtų informuojamos apie tokį tolesnį duomenų perdavimą ir galėtų duoti leidimą jį vykdyti. Jei dėl trečiosios valstybės, į kurią būtų toliau perduodami duomenys, nepriimtas sprendimas dėl tinkamumo, iš ES perduotų duomenų pradinis gavėjas turėtų įrodyti, kad atitinkama valstybės narės kompetentinga institucija leido toliau perduoti duomenis ir kad yra numatytos tinkamos apsaugos priemonės, taikomos tolesniam duomenų perdavimui. „*Atsižvelgiant į tai, turėtų būti atsižvelgiama į tai, ar yra pareiga ar įsipareigojimas įgyvendinti atitinkamus perduodančiosios valstybės narės institucijų nustatytus duomenų tvarkymo kodeksus.*“³⁰.
48. **EDAV ragina Komisiją įvertinti šį elementą atsižvelgiant į EDAV rekomendacijose dėl tinkamumo pavydžių pagal TD pateiktas gaires.**
49. Antra, kaip paaiškinta sprendimo projekto 81 konstatuojamojoje dalyje, JK valstybės sekretorius, pasitaręs su ICO, turi įgaliojimus pripažinti, kad trečioji valstybė (arba tos trečiosios valstybės teritorija ar sektorius) ar tarptautinė organizacija užtikrina tinkamą asmens duomenų apsaugos lygį, arba pripažinti, kad tokios valstybės, teritorijos, sektoriaus ar organizacijos apibūdinimu užtikrinamas tinkamas asmens duomenų apsaugos lygis³¹. Vertindamas apsaugos lygio tinkamumą JK valstybės sekretorius turi atsižvelgti į tuos pačius elementus, kuriuos Europos Komisija privalo įvertinti pagal TD 36 straipsnio 2 dalies a–c punktus, aiškinamus kartu su TD 67 konstatuojamąja dalimi ir palikta galioti ES jurisprudencija. Tai reiškia, kad vertinant apsaugos lygio trečiojoje valstybėje tinkamumą reikšmingas standartas yra tai, ar atitinkama trečioji valstybė užtikrina apsaugos lygį, kuris yra „iš esmės lygiavertis“ JK garantuojamam apsaugos lygiui. Nors EDAV pažymi, kad pagal 2018 m. DPA JK gali pripažinti teritorijas kaip užtikrinančias tinkamą apsaugos lygį pagal JK duomenų apsaugos sistemą, EDAV atkreipia dėmesį į tai, kad šiuo metu pastarosioms teritorijoms gali nebūti taikomas Europos

³⁰ Žr. EDAV rekomendacijų 01/2021 dėl tinkamumo pavydžių pagal Teisėsaugos direktyvą 55 ir 56 punktus.

³¹ Žr. 2018 m. DPA 182 straipsnio 2 dalį. Taip pat žr. Susitarimo memorandumą dėl ICO vaidmens dėl naujų JK tinkamumo vertinimų, <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/>.

Komisijos priimtas sprendimas dėl tinkamumo, kuriuo apsaugos lygis pripažįstamas „iš esmės lygiaverčiu“ ES garantuojamam apsaugos lygiui. Tai gali kelti pavojų iš ES perduotiems asmens duomenims teikiamai apsaugai, ypač tuo atveju, jei ateityje JK duomenų apsaugos sistema nukryptų nuo Sąjungos *acquis*. Reikia pažymėti, kad ESTT 2020 m. liepos mėn. priėmus precedentinį sprendimą *Schrems II*³² buvo panaikintas JAV privatumo skydo sprendimas, nes, ESTT nuomone, JAV sistema negali būti laikoma suteikiančia apsaugos lygį, iš esmės lygiavertį ES garantuojamam apsaugos lygiui. Tačiau jau priimti ESTT sprendimai, kurie JK teisinėje sistemoje laikomi palikta galioti jurisprudencija, JK gali būti nebeprivalomi, visų pirma atsižvelgiant į tai, kad pasibaigus tarpiniam laikotarpiui JK turi galimybę keisti paliktą galioti ES teisę, o jos Aukščiausiajam Teismui jokia palikta galioti ES jurisprudencija neprivaloma³³.

50. **Todėl EDAV ragina Europos Komisiją atidžiai stebėti JK institucijų vykdomą tinkamumo vertinimo procesą ir taikomus kriterijus dėl trečiųjų valstybių, ypač dėl tų trečiųjų valstybių, kurių ES nėra pripažinusi tinkamomis pagal TD.**
51. Jeigu Europos Komisija nustatytų, kad trečioji valstybė, kurią JK pripažino tinkama, neužtikrina apsaugos lygio, kuris būtų iš esmės lygiavertis ES garantuojamam apsaugos lygiui, kaip nustatyta TD 36 straipsnyje, **EDAV ragina Europos Komisiją imtis visų bet kokių būtinų veiksmų, pavyzdžiui, iš dalies keisti sprendimą dėl JK tinkamumo numatant konkrečias asmens duomenų, perduotų iš ES, apsaugos priemones ir (arba) apsvaistyti galimybę sustabdyti sprendimo dėl JK tinkamumo galiojimą, kai iš ES į JK perduoti asmens duomenys toliau perduodami minėtai trečiajai valstybei pagal JK taisyklės dėl tinkamumo.**
52. **Galiausiai, dėl JK sudarytų tarptautinių susitarimų arba tarptautinių susitarimų, kuriuos ji sudarys ateityje, ir trečiosios (-ių) valstybės (-ių), kuri (-ios) yra tokių susitarimų šalis (-ys), institucijų galimos priegios prie asmens duomenų iš ES, EDAV rekomenduoja Europos Komisijai išnagrinėti JK duomenų apsaugos sistemos ir jos tarptautinių įsipareigojimų sąveiką, visų pirma siekiant užtikrinti apsaugos lygio tęstinumą, kai iš ES į JK perduoti duomenys pagal JK sprendimą dėl tinkamumo toliau perduodami į kitas trečiąsias valstybes, bei nuolat stebėti ir prireikus imtis veiksmų dėl JK ir trečiųjų valstybių sudarytų tarptautinių susitarimų, dėl kurių kyla pavojus, kad gali sumažėti ES numatytas asmens duomenų apsaugos lygis.** Pavyzdžiui, nors Europos Komisija nurodė, kad JK ir JAV susitarimas pagal CLOUD aktą³⁴ gali turėti poveikio JK paslaugų teikėjų vykdomam tolesniam duomenų perdavimui JAV, **EDAV pažymi, kad šio susitarimo įgaliojimas taip pat gali turėti poveikio JK teisėsaugos institucijų vykdomam tolesniam duomenų perdavimui, visų pirma dėl orderių išdavimo ir perdavimo pagal JK ir JAV susitarimo pagal CLOUD aktą 5 straipsnį.**
53. EDAV taip pat mano, kad būsimų susitarimų su trečiosiomis valstybėmis sudarymas teisėsaugos bendradarbiavimo tikslais, numatant asmens duomenų perdavimą į tas valstybes teisinį pagrindą, gali turėti poveikio tolesnio surinktos informacijos atskleidimo sąlygoms, nes tokie susitarimai gali turėti poveikio įvertintai JK duomenų apsaugos teisei sistemai.
54. **Todėl EDAV rekomenduoja Europos Komisijai nuolat stebėti, ar būsimų JK susitarimų su trečiosiomis valstybėmis sudarymas gali turėti poveikio JK duomenų apsaugos teisės taikymui, ir numatyti papildomus apribojimus ar išimtis dėl teisėsaugos tikslais surinktos informacijos tolesnio naudojimo**

³² Žr. ESTT, C-311/18, *Data Protection Commissioner / Facebook Ireland Ltd ir Maximilian Schrems*, 2020 m. liepos 16 d., ECLI:EU:C:2020:559 (toliau – Sprendimas *Schrems II*).

³³ Žr. 2018 m. (išstojimo iš) Europos Sąjungos akto 6 straipsnio 3–6 dalis.

³⁴ Žr. Jungtinės Didžiosios Britanijos ir Šiaurės Airijos Karalystės vyriausybės ir Jungtinių Amerikos Valstijų vyriausybės susitarimą dėl priegios prie elektroninių duomenų siekiant kovoti su sunkiais nusikaltimais, Vašingtonas, JAV, 2019 m. spalio 3 d, <https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-counteracting-serious-crime-cs-usa-no62019>.

ar atskleidimo užsienyje. EDAV mano, kad tokia informacija ir vertinimas yra būtini, kad būtų galima atlikti išsamią JK teisės aktų sistemos ir praktikos dėl duomenų atskleidimo užsienyje suteikiamo apsaugos lygio peržiūrą.

55. Galiausiai, EDAV pažymi, kad pagal 2018 m. DPA 76 straipsnio („Duomenų perdavimas remiantis ypatingomis aplinkybėmis“) 4 dalies b punktą JK teisėsaugos institucijos gali asmens duomenis perduoti trečiajai valstybei ar tarptautinei organizacijai, kai perduoti duomenis „*būtina siekiant gauti teisinę konsultaciją, susijusią su bet kuriuo iš teisėsaugos tikslų*“. **EDAV pažymi, kad TD 38 straipsnyje atitinkamos nuostatos nėra, todėl ji ragina Europos Komisiją išsiaiškinti, ką reiškia sąvoka „teisinė konsultacija“, ir kokiais duomenimis keičiamasi tokiais atvejais.**

3.2.4. Tolesnis duomenų tvarkymas, įskaitant tolesnį atskleidimą nacionalinio saugumo tikslais

56. EDAV savo Rekomendacijose dėl tinkamumo pavyzdžių pagal TD pažymėjo, kad iš ES perduotų duomenų tolesnis tvarkymas ar atskleidimas ne teisėsaugos tikslais, pavyzdžiui, nacionalinio saugumo tikslais, taip pat turėtų būti numatytas įstatyme ir turėtų būti būtinas ir proporcingas. Kaip Europos Komisija įvertino savo sprendimo projekte, 2018 m. DPA 36 straipsnio 3 dalyje, 2017 m. Skaitmeninės ekonomikos akte, 2013 m. Nusikaltimų ir teismų akte ir 2017 m. Sunkių nusikaltimų akte numatytas aiškus teisinis pagrindas, pagal kurį leidžiamas tolesnis duomenų atskleidimas, su sąlyga, kad toks tolesnis atskleidimas atitinka 2018 m. DPA nustatytas taisykles.
57. EDAV pažymi, kad dėl iš ES perduotų asmens duomenų tolesnio tvarkymo kitais tikslais Europos Komisija neįvertino, ar yra mechanizmų, pagal kuriuos JK teisėsaugos institucijos praneštų atitinkamų valstybių narių kompetentingoms institucijoms apie galimą tolesnį duomenų tvarkymą. Tačiau Rekomendacijose dėl tinkamumo pavyzdžių pagal TD tai laikoma elementu, į kurį reikia atsižvelgti³⁵. Be to, pagal Rekomendacijas dėl tinkamumo pavyzdžių tai, ar yra mechanizmas, pagal kurį atitinkamos valstybės narės kompetentingos institucijos būtų informuojamos apie tolesnį duomenų tvarkymą teisėsaugos tikslais, taip pat laikoma elementu, į kurį reikia atsižvelgti³⁶.
58. **Todėl EDAV ragina Europos Komisiją papildyti savo analizę informacija apie tai, ar yra mechanizmų, pagal kuriuos JK teisėsaugos institucijos praneštų atitinkamų valstybių narių kompetentingoms institucijoms apie galimą tolesnį iš ES perduotų duomenų tvarkymą.**
59. Be to, dėl teisėsaugos institucijos surinktų duomenų atskleidimo žvalgybos institucijai nacionalinio saugumo tikslais, tokio tolesnio atskleidimo teisinis pagrindas yra 2008 m. Kovos su terorizmu aktas. Šiuo klausimu EDAV pažymi, kad Europos Komisijos vertinime nėra visapusiškai išnagrinėta 2008 m. Kovos su terorizmu akto 19 straipsnio taikymo sritis ir nuostatos, kurios gali reikšti tolesnį platesnio pobūdžio naudojimą, ypač atsižvelgiant į 2008 m. Kovos su terorizmu akto 19 straipsnio 2 dalį, kurioje numatyta, kad *informaciją, kurią bet kuri žvalgybos institucija gavo atlikdama kurią nors iš savo funkcijų, ji gali naudoti atlikdama visas kitas savo funkcijas.*“ Šiuo klausimu EDAV pažymi, kad duomenis toliau tvarkant arba atskleidžiant jiems turėtų būti taikoma tokio paties lygio apsauga, kaip tada, kai juos iš pradžių tvarkė gaunančioji kompetentinga institucija.

3.3. Priežiūra ir vykdymo užtikrinimas

60. EDAV pažymi, kad teisėsaugos institucijų priežiūrą užtikrina skirtingi komisarai bei ICO. Išvadų dėl tinkamumo projekte nurodytas tyrimų įgaliojimų komisaras (toliau – IPC), biometrinės medžiagos

³⁵ Žr. EDAV rekomendacijų 01/2021 dėl tinkamumo pavydžių pagal Teisėsaugos direktyvą 41 punktą ir 39 išnašą.

³⁶ Žr. EDAV rekomendacijų 01/2021 dėl tinkamumo pavydžių pagal Teisėsaugos direktyvą 40 punktą.

saugojimo ir naudojimo komisaras, taip pat vaizdo stebėjimo kamerų komisaras. Šiomis aplinkybėmis reikia pažymėti, kad ESTT ne kartą atkreipė dėmesį į nepriklausomos priežiūros būtinybę. Dėl klausimų dėl prieigos prie asmens duomenų, perduotų į JK, itin svarbus IPC. EDAV mano, kad IPC yra vadinamasis teismo komisaras, kaip ir kiti teismo komisarai, į kuriuos galima kreiptis nacionalinio saugumo klausimais, ir kad tiems teismo komisarams taikomas teisėjų nepriklausomumas, taip pat ir tada, kai jie eina komisaro pareigas. Dėl IPC pareigų Europos Komisija sprendimo projekto 245 konstatuojamojoje dalyje paaiškino, kad jis veikia nepriklausomai kaip vadinamoji „nekontroliuojama institucija“, nors jį finansuoja vidaus reikalų ministerija.

61. Be to, IPC taip pat kompetentingas atlikti priežiūros priemonių *ex-post* priežiūrą. Tačiau atrodo, kad atliekant šią funkciją IPC vaidmuo yra teikti rekomendacijas reikalavimų nesilaikymo atvejais ir informuoti duomenų subjektą, jei klaida yra rimta, o asmens informavimas atitinka viešąjį interesą.
62. EDAV sprendimo projekte daugiau nerado jokių duomenų, kad galėtų įvertinti biometrinės medžiagos saugojimo ir naudojimo komisaro ir vaizdo stebėjimo kamerų komisaro nepriklausomumą.
63. **Europos Komisija raginama išsamiau įvertinti teismų komisarų nepriklausomumą, taip pat ir tais atvejais, kai komisaras neina (nebeina) teisėjo pareigų, taip pat įvertinti biometrinės medžiagos saugojimo ir naudojimo komisaro ir vaizdo stebėjimo kamerų komisaro nepriklausomumą.**