Rekomendacijos

Rekomendacijos 01/2021 dėl tinkamumo pavydžių pagal Teisėsaugos direktyvą

Priimtos 2021 m. vasario 2 d.

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

Informacija apie versijas

1.1 versija	2021 m. liepos 6 d.	Formatavimo pakeitimai
1.0 versija	2021 m. vasario 2 d.	Rekomendacijų priėmimas

Turinys

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 kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR[1], 51 straipsnio 1 dalies b punktą,

atsižvelgdama į savo Darbo taisyklių 12 ir 22 straipsnius,

PRIĖMĖ TOLIAU PATEIKTAS REKOMENDACIJAS

1. ĮVADAS

1. 29 straipsnio darbo grupė (WP29) paskelbė darbinį dokumentą[2] dėl tinkamumo pavyzdžių pagal Bendrąjį duomenų apsaugos reglamentą (BDAR)[3]. Šį darbinį dokumentą Europos duomenų apsaugos valdyba patvirtino per pirmąjį plenarinį posėdį.

2. Kaip nurodyta prie Lisabonos sutarties pridėtoje Deklaracijoje Nr. 21, dėl teisminio bendradarbiavimo baudžiamosiose bylose ir policijos bendradarbiavimo sričių ypatingo pobūdžio šiose srityse gali reikėti konkrečių taisyklių dėl asmens duomenų apsaugos ir laisvo šių duomenų judėjimo, pagrįstų Sutarties dėl Europos Sąjungos veikimo (SESV) 16 straipsniu.

3. Atsižvelgdamas į tai, ES teisės aktų leidėjas priėmė Direktyvą (ES) 2016/680 (Teisėsaugos direktyva, toliau – TD), kurioje nustatomos konkrečios taisyklės dėl kompetentingų institucijų atliekamo asmens duomenų tvarkymo **nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais, įskaitant grėsmių visuomenės saugumui prevencijos užtikrinimą**.

4. TD nustatyti pagrindai, kuriais remiantis asmens duomenis leidžiama šiais tikslais perduoti trečiajai valstybei ar tarptautinei organizacijai. Vienas iš tokio duomenų perdavimo pagrindų yra Europos Komisijos sprendimas, kad atitinkama trečioji valstybė ar tarptautinė organizacija užtikrina tinkamo lygio apsaugą.

5. Darbiniu dokumentu WP254 (1-oji peržiūrėta versija) dėl tinkamumo pavyzdžių siekiama teikti rekomendacijas Europos Komisijai dėl duomenų apsaugos lygio trečiosiose valstybėse ir tarptautinėse organizacijose pagal BDAR, o šiuo dokumentu siekiama teikti panašias rekomendacijas pagal TD. Atsižvelgiant į tai, jame nustatomi pagrindiniai duomenų apsaugos

[1] OL L 119, 2016 5 4, p. 89.
[2] 2017 m. lapkričio 28 d. WP29 priimtas WP 254, 1-oji peržiūrėta versija, paskutinį kartą peržiūrėta ir priimta 2018 m. vasario 6 d. Juo atnaujinamas 1998 m. liepos 24 d. WP29 priimto darbinio dokumento WP12 „Asmens duomenų perdavimas trečiosioms valstybėms. ES duomenų apsaugos direktyvos 25 ir 26 straipsnių taikymas“ 1 skyrius.
[3] 2016 m. balandžio 26 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL L 119, 2016 5 4, p. 1).

principai, kurie turi būti įtraukti į trečiosios valstybės teisinę sistemą arba tarptautinės organizacijos nuostatus, kad būtų užtikrinta ES sistemai TD taikymo srityje (t. y. dėl kompetentingų institucijų atliekamo asmens duomenų tvarkymo nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais) iš esmės lygiavertė sistema. Be to, šiame dokumente pateiktos rekomendacijos gali būti naudingos sprendimą dėl tinkamumo norinčioms gauti trečiosioms valstybėms ir tarptautinėms organizacijoms.

6. Šiame dokumente dėmesys sutelkiamas tik į sprendimus dėl tinkamumo. Pagal TD 36 straipsnio 3 dalį šie sprendimai yra Europos Komisijos įgyvendinimo aktai.

2. TINKAMUMO SĄVOKA

7. TD nustatytos taisyklės dėl asmens duomenų perdavimo trečiosioms valstybėms ir tarptautinėms organizacijoms, jei toks duomenų perdavimas patenka į šios direktyvos taikymo sritį. Taisyklės dėl tarptautinio asmens duomenų perdavimo nustatytos TD V skyriuje, visų pirma 35–39 straipsniuose.

8. Pagal TD 36 straipsnį perduoti duomenis trečiajai valstybei arba tarptautinei organizacijai galima tuo atveju, jeigu trečioji valstybė, teritorija arba vienas ar daugiau nurodytų sektorių trečiojoje valstybėje, arba atitinkama tarptautinė organizacija užtikrina tinkamo lygio apsaugą. Iš Europos Sąjungos Teisingumo Teismo (ESTT) jurisprudencijos[4] matyti, kad ši nuostata turi būti aiškinama atsižvelgiant į TD 35 straipsnį „Bendrieji asmens duomenų perdavimo principai“, kuriame nurodyta, kad „[v]isos [TD V skyriaus] nuostatos taikomos siekiant užtikrinti, kad nesumažėtų šia direktyva fiziniams asmenims užtikrinamos apsaugos lygis“.

9. Jei Europos Komisija nusprendžia, kad užtikrinamas toks apsaugos lygio tinkamumas, asmens duomenys gali būti perduodami į tą trečiąją valstybę, teritoriją, sektorių ar tarptautinę organizaciją nereikalaujant jokio specialaus leidimo, išskyrus atvejus, kai kita valstybė narė, iš kurios duomenys buvo gauti, turi duoti leidimą dėl duomenų perdavimo, kaip numatyta TD 35 ir 36 straipsniuose bei 66 konstatuojamojoje dalyje. Tai nedaro poveikio reikalavimui, kad atitinkamos valstybės narės institucijos duomenis tvarkytų laikydamosi nacionalinių nuostatų, priimtų pagal Direktyvos (ES) 2016/680 nuostatas.

10. Ši sąvoka „tinkamas apsaugos lygis“, kuri jau buvo numatyta Direktyvoje 95/46[5] ir Tarybos pamatiniame sprendime 2008/977/TVR[6], buvo toliau išplėtota ESTT šiomis aplinkybėmis, o neseniai – ir BDAR sistemoje.

11. Kaip nurodė ESTT, nors trečiojoje valstybėje turi būti užtikrintas iš esmės toks pats apsaugos lygis, koks garantuojamas Sąjungoje, „priemonės, kurių ši trečioji šalis šiuo klausimu imasi siekdama užtikrinti tokį apsaugos lygį, gali skirtis nuo priemonių, kurios Sąjungoje taikomos“, tačiau „praktiškai šios priemonės turi būti veiksmingos“[7]. Taigi, pagal tinkamumo standartą reikalaujama

[4] Byla C-311/18, *Data Protection Commissioner / Facebook Ireland Ltd ir Maximillian Schrems*, 2020 m. liepos 16 d., ECLI:EU:C:2020:559, 92 punktas (toliau – Sprendimas *Schrems II*).
[5] 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).
[6] 2008 m. lapkričio 27 d. Tarybos pamatinis sprendimas 2008/977/TVR dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos (OL L 350, 2008 12 30, p. 60).
[7] Byla C−362/14, *Maximillian Schrems / Data Protection Commissioner*, 2015 m. spalio 6 d., ECLI:EU:C:2015:650, 73 ir 74 punktai (toliau – Sprendimas *Schrems I*).

ne atkartoti kiekvieną Europos Sąjungos teisės akto punktą, o nustatyti pagrindinius – esmę perteikiančius to teisės akto reikalavimus.

12. Atsižvelgdamas į tai, teismas taip pat pažymėjo, kad Komisijos sprendime dėl tinkamumo turėtų būti nustatyta, kad trečiojoje valstybėje yra valstybinio pobūdžio taisyklių, skirtų nustatyti asmenų, kurių asmens duomenys perduoti iš Sąjungos į tą trečiąją valstybę, galimoms pagrindinių teisių apribojimų riboms, t. y. apribojimų, kuriuos šios šalies valstybiniai subjektai *gali nustatyti* siekdami teisėtų tikslų, pavyzdžiui, nacionalinio saugumo[8].

13. Valstybėms narėms[9], įskaitant jų kompetentingas duomenų apsaugos institucijas[10], privalomų Europos Komisijos sprendimų dėl tinkamumo paskirtis – oficialiai patvirtinti, kad duomenų apsaugos lygis trečiojoje valstybėje ar tarptautinėje organizacijoje yra iš esmės lygiavertis Europos Sąjungoje užtikrintam duomenų apsaugos lygiui. Trečioji valstybė turėtų suteikti garantijų, kuriomis būtų užtikrinta atitinkamo lygio apsauga, iš esmės lygiavertė Sąjungoje užtikrinamai apsaugai, visų pirma tada, kai duomenys tvarkomi viename ar keliuose konkrečiuose sektoriuose[11].

14. 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[12].

3. PROCEDŪRINIAI IŠVADŲ DĖL TINKAMUMO ASPEKTAI PAGAL TD

15. Kad Europos duomenų apsaugos valdyba galėtų atlikti savo užduotis, t. y. konsultuoti Europos Komisiją, kaip numatyta TD 51 straipsnio 1 dalies g punkte, jai turėtų būti pateikti visi reikšmingi dokumentai, įskaitant atitinkamus Europos Komisijos susirašinėjimus ir priimtas išvadas. Visi reikšmingi dokumentai Europos duomenų apsaugos valdybai privalo būti pateikiami pakankamai iš anksto ir turi būti išversti į anglų kalbą, kad prieš galutinai priimant sprendimus dėl tinkamumo galėtų vykti argumentuotos ir naudingos diskusijos. Jei teisinė sistema yra sudėtinga, prie tų dokumentų reikėtų pridėti visus trečiosios valstybės arba tarptautinės organizacijos parengtus pranešimus apie duomenų apsaugos lygį. Bet kuriuo atveju Europos Komisijos suteikta informacija turėtų būti išsami ir sudaryti sąlygas Europos duomenų apsaugos valdybai atlikti Komisijos atliktos analizės dėl duomenų apsaugos lygio trečiojoje valstybėje ar tarptautinėje organizacijoje vertinimą.

[8] Sprendimas *Schrems I*, 88 punktas.
[9] SESV 288 straipsnis;
[10] Sprendimas *Schrems I*, 52 punktas.
[11] TD 67 konstatuojamoji dalis.
[12] Sprendimas *Schrems I*, 72–74 punktai, ir 2017 m. liepos 26 d. ESTT išvados 1/15 dėl Kanados ir Europos Sąjungos susitarimo projekto, ECLI:EU:C:2017:592 (toliau – Išvada 1/15), 134 punktas: „Šia teise į asmens duomenų apsaugą, be kita ko, reikalaujama užtikrinti aukšto Sąjungos teisės suteikiamo pagrindinių teisių ir laisvių apsaugos lygio tęstinumą, kai asmens duomenys iš Sąjungos yra perduodami į trečiąją šalį. Nors tokiam apsaugos lygiui užtikrinti skirtos priemonės gali skirtis nuo priemonių, kurios Sąjungoje taikomos siekiant garantuoti Sąjungos teisėje nustatytų reikalavimų laikymąsi, vis dėlto praktiškai šios priemonės turi būti veiksmingos, kad būtų užtikrinta iš esmės tokia pati apsauga, kokia garantuojama Sąjungoje“.

16. Europos duomenų apsaugos valdyba laiku pateiks nuomonę dėl Europos Komisijos išvadų, nurodys tinkamumo sistemos trūkumus, jei jų bus, ir jei, reikia, pateiks galimas rekomendacijas.

17. Remiantis TD 36 straipsnio 4 dalimi, Europos Komisija turi nuolat stebėti įvykius trečiosiose valstybėse ir tarptautinėse organizacijose, kurie galėtų padaryti poveikio sprendimų dėl tinkamumo veikimui.

18. TD 36 straipsnio 3 dalyje numatyta, kad periodinė peržiūra turi būti atliekama ne rečiau kaip kas ketverius metus. Tačiau tai tik bendro pobūdžio terminas, kurį reikia koreguoti kiekvienos trečiosios valstybės ar tarptautinės organizacijos, kurios atžvilgiu priimtas sprendimas dėl tinkamumo, atveju. Atsižvelgiant į tam tikras susiklosčiusias aplinkybes, gali būti reikalaujama, kad peržiūros ciklas būtų trumpesnis. Be to, dėl incidentų ar kitos informacijos apie atitinkamos trečiosios valstybės ar tarptautinės organizacijos teisinę sistemą arba pokyčių joje gali prireikti peržiūrą atlikti anksčiau, nei numatyta. Taip pat atrodo tinkama pirmąją visiškai naujo sprendimo dėl tinkamumo peržiūrą atlikti kuo greičiau ir tuomet palaipsniui koreguoti peržiūros ciklą, atsižvelgiant į rezultatus.

19. Europos duomenų apsaugos valdyba, atsižvelgdama į savo funkciją pateikti Europos Komisijai nuomonę apie tai, ar trečioji valstybė, teritorija arba vienas ar daugiau nurodytų sektorių toje trečiojoje valstybėje, arba tarptautinė organizacija nebeužtikrina tinkamo apsaugos lygio, turi laiku gauti reikšmingos informacijos apie ES Komisijos vykdomą atitinkamų pokyčių stebėjimą toje trečiojoje valstybėje ar tarptautinėje organizacijoje. Taigi, Europos duomenų apsaugos valdyba turėtų būti nuolat informuojama apie visus peržiūros procesus ir peržiūros vizitus trečiojoje valstybėje ar tarptautinėje organizacijoje. Europos duomenų apsaugos valdyba rekomenduoja kviesti ją dalyvauti tuose peržiūros procesuose ir vizituose, kaip buvo numatyta sprendime dėl „privatumo skydo“ ir numatyta sprendime dėl tinkamumo, priimtame dėl Japonijos.

20. Taip pat reikėtų pažymėti, kad pagal TD 36 straipsnio 5 dalį Europos Komisija turi įgaliojimus panaikinti, iš dalies pakeisti priimtus sprendimus dėl tinkamumo arba sustabdyti jų galiojimą, jei trečioji valstybė arba tarptautinė organizacija nebeužtikrina tinkamo lygio apsaugos. Sprendimo panaikinimo, keitimo iš dalies ar galiojimo sustabdymo procedūros metu Europos duomenų apsaugos valdybos prašoma pateikti nuomonę pagal TD 51 straipsnio 1 dalies g punktą.

21. Be to, nedarant poveikio baudžiamojo persekiojimo institucijų įgaliojimams, priežiūros institucijoms taip pat turėtų būti suteikti įgaliojimai atkreipti teisminių institucijų dėmesį į šios direktyvos pažeidimus arba būti teisminio proceso šalimi[13]. Visų pirma iš ESTT sprendimo *Schrems I* matyti, kad duomenų apsaugos institucijos, nustačiusios, kad asmens prieštaravimas dėl sprendimo dėl tinkamumo yra pagrįstas, turi turėti galimybę kreiptis į nacionalinius teismus[14]. Šis vertinimas patvirtintas Sprendime *Schrems II*[15].

[13] Žr. TD 47 straipsnio 5 dalį ir 82 konstatuojamąją dalį.

[14] Žr. Sprendimo *Schrems I* 65 punktą: „Šiuo atžvilgiu nacionalinis teisės aktų leidėjas turi numatyti teisių gynimo priemones, leidžiančias atitinkamai nacionalinei priežiūros institucijai remtis nacionaliniuose teismuose kaltinimais, kurie, jos nuomone, yra pagrįsti, tam, kad šie teismai, vertindami Komisijos sprendimo galiojimą, pateiktų prašymą priimti prejudicinį sprendimą, jei, kaip ir ši institucija, turėtų abejonių dėl šio sprendimo galiojimo.“

[15] Žr. Sprendimo *Schrems II* 120 punktą: „Taigi, net jei Komisija yra priėmusi sprendimą dėl tinkamumo, kompetentinga nacionalinė priežiūros institucija, gavusi asmens skundą dėl jo teisių ir laisvių apsaugos tvarkant jo asmens duomenis, turi turėti galimybę visiškai nepriklausomai išnagrinėti, ar perduodant šiuos duomenis laikytasi BDAR nustatytų reikalavimų, ir prireikus kreiptis į nacionalinius teismus, kad jie pateiktų prašymą priimti prejudicinį sprendimą, kad būtų išnagrinėtas šio sprendimo galiojimas, jei, kaip ir ši institucija, turėtų abejonių dėl šio galiojimo“.

4. ES TINKAMUMO STANDARTAI VYKDANT POLICIJOS IR TEISMINĮ BENDRADARBIAVIMĄ BAUDŽIAMOSIOSE BYLOSE

22. Iš esmės sprendimuose dėl tinkamumo daugiausia dėmesio turi būti skiriama teoriniam ir praktiniam visų esamų atitinkamos trečiosios valstybės teisės aktų vertinimui atsižvelgiant į TD 36 straipsnyje nustatytus vertinimo kriterijus. Trečiosios valstybės arba tarptautinės organizacijos sistemoje turi būti numatyti toliau aprašyti pagrindiniai bendrieji, procedūriniai ir vykdymo užtikrinimo duomenų apsaugos principai ir mechanizmai.

23. TD 36 straipsnio 2 dalyje nustatyti aspektai, į kuriuos Europos Komisija atsižvelgia vertindama trečiosios valstybės ar tarptautinės organizacijos apsaugos lygio tinkamumą.

24. Visų pirma Komisija atsižvelgia į teisinės valstybės principą, pagarbą žmogaus teisėms ir pagrindinėms laisvėms[16], atitinkamus teisės aktus, taip pat tų teisės aktų įgyvendinimą, veiksmingas ir vykdytinas duomenų subjektų teises ir veiksmingas administracines bei teismines duomenų subjektų, kurių asmens duomenys yra perduodami, teisių gynimo priemones, į tai, ar yra ir ar veiksmingai veikia viena ar kelios nepriklausomos priežiūros institucijos, ir į trečiosios valstybės arba tarptautinės organizacijos prisiimtus tarptautinius įsipareigojimus.

25. Todėl aišku, kad bet koks prasmingas tinkamos apsaugos vertinimas privalo apimti du pagrindinius aspektus – taikomų taisyklių turinį ir veiksmingo jų įgyvendinimo praktikoje užtikrinimo priemones. Būtent Europos Komisija turi reguliariai tikrinti, ar galiojančios taisyklės yra praktiškai veiksmingos.

26. Esminiai duomenų apsaugos bendrieji principai ir procedūriniai ir vykdymo užtikrinimo reikalavimai, kuriuos galima laikyti būtinaisiais reikalavimais, kad apsaugos lygis būtų tinkamas, kildinami iš ES pagrindinių teisių chartijos (toliau – Chartija) ir TD. Bendrųjų nuostatų dėl duomenų apsaugos ir privatumo trečiojoje valstybėje nepakanka. Priešingai – į trečiosios valstybės arba tarptautinės organizacijos teisinę sistemą privaloma įtraukti konkrečias nuostatas dėl teisės į duomenų apsaugą teisėsaugos srityje. Trečioji valstybė turėtų suteikti garantijų, kuriomis būtų užtikrinta tinkamo lygio apsauga, iš esmės lygiavertė Sąjungoje užtikrinamai apsaugai. Šios nuostatos turi būti vykdytinos.

27. Be to, dėl proporcingumo principo[17] ESTT pažymėjo, kad, kalbant apie valstybių narių įstatymus, klausimas, ar galima pateisinti teisių į privatumą ir duomenų apsaugą apribojimą, turi būti

[16] Vertinant trečiosios valstybės teisinę sistemą taip pat reikia atsižvelgti į galimybę, kad remiantis iš ES perduotais duomenimis asmeniui gali būti skirta mirties bausmė arba kita žiauraus ir nežmoniško elgesio bausmė. Iš tiesų, jei trečiosios valstybės teisėje numatyta tokia bausmė, tos valstybės teisinėje sistemoje turėtų būti numatytos papildomos apsaugos priemonės, skirtos užtikrinti, kad iš Sąjungos perduoti duomenys nebus naudojami siekiant prašyti skirti, skirti ar vykdyti mirties bausmę arba kitą žiauraus ir nežmoniško elgesio bausmę (pvz., tarptautinis susitarimas, kuriame nustatomos duomenų perdavimo sąlygos, trečiosios valstybės įsipareigojimas neskirti mirties bausmės arba kitos žiauraus ir nežmoniško elgesio bausmės remiantis iš Sąjungos perduotais duomenimis ar mirties bausmės moratoriumas).

[17] Chartijos 52 straipsnio 1 dalis.

vertinamas atsižvelgiant į **suvaržymo**, kurį lemia toks apribojimas, **dydį**[18] ir tikrinant, ar šiuo apribojimu siekiamo **bendrojo intereso tikslo svarba** jį atitinka[19].

28. Pagal ESTT jurisprudenciją tam, kad būtų įvykdytas proporcingumo principas, pačiame teisiniame pagrinde, kuriuo leidžiami pagrindinių teisių suvaržymai, turi būti apibrėžta atitinkamos teisės įgyvendinimo ribojimo apimtis[20]. Nukrypti nuo asmens duomenų apsaugos leidžiančios nuostatos ir šios apsaugos apribojimai privalo neviršyti to, kas yra griežtai būtina[21]. Siekiant įvykdyti šį reikalavimą atitinkamame teisės akte ne tik turi būti numatytos aiškios ir tikslios taisyklės, kuriomis būtų reglamentuojama atitinkamos priemonės apimtis ir taikymas, bet ir nustatomi minimalūs reikalavimai, kad asmenims, kurių duomenys perduodami, būtų suteikta pakankamai garantijų, leidžiančių veiksmingai apsaugoti jų asmens duomenis nuo piktnaudžiavimo pavojų. „Konkrečiai jame turi būti nurodyta, kokiomis aplinkybėmis ir sąlygomis tokių duomenų tvarkymą numatančios priemonės gali būti imamasi, taip užtikrinant, kad suvaržymas neviršytų to, kas griežtai būtina. Būtinybė turėti tokias garantijas yra dar svarbesnė tais atvejais, kai asmens duomenys tvarkomi automatiniu būdu“[22].

29. Europos duomenų apsaugos valdyba priėmė rekomendacijas, kuriose nurodytos pagrindinės garantijos, kuriomis atsižvelgiama į ESTT ir Europos Žmogaus Teisių Teismo jurisprudenciją, susijusią su priežiūros sritimi, kurios turi būti nustatytos trečiosios valstybės teisėje vertinant duomenų subjektų teisių apribojimus pagal tokioje trečiojoje valstybėje taikomas priežiūros priemones tuo atveju, kai duomenys į tą trečiąją valstybę perduodami pagal BDAR[23]. Kalbant apie vertinimą, ar įvykdytos TD 36 straipsnio 2 dalies a punkte nustatytos sąlygos, Europos duomenų apsaugos valdyba mano, kad į tose rekomendacijose nurodytas garantijas turi būti atsižvelgiama pagal TD vertinant trečiosios valstybės tinkamumą priežiūros srityje, atsižvelgiant į papildomas konkrečias sąlygas priežiūros srityje.

30. Kalbant apie 36 straipsnio 2 dalies b punkte nustatytą reikalavimą, trečioji valstybė turėtų ne tik užtikrinti veiksmingą nepriklausomą duomenų apsaugos priežiūrą, bet ir nustatyti bendradarbiavimo su valstybių narių duomenų apsaugos institucijomis mechanizmus[24].

31. Kalbant apie 36 straipsnio 2 dalies c punkte nustatytą reikalavimą, reikėtų atsižvelgti ne tik į trečiosios valstybės arba tarptautinės organizacijos prisiimtus tarptautinius įsipareigojimus, bet ir į įsipareigojimus, kylančius dėl trečiosios valstybės arba tarptautinės organizacijos dalyvavimo daugiašalėse ar regioninėse sistemose, visų pirma susijusio su asmens duomenų apsauga, ir į tokių įsipareigojimų įgyvendinimą, visų pirma, į trečiosios valstybės narės prisijungimą prie kitų tarptautinių susitarimų dėl duomenų apsaugos, pvz., reikėtų atsižvelgti į 1981 m. sausio 28 d. Europos tarybos konvenciją dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu ir jos papildomą protokolą (Konvencija Nr. 108[25] ir jos atnaujinta versija Konvencija Nr. 108+). Taip pat gali būti atsižvelgiama į tai, kaip trečioji valstybė laikosi tarptautiniuose

[18]Pavyzdžiui, Teisingumo Teismas pažymėjo, kad „suvaržymas, susijęs su duomenų, leidžiančių nustatyti galinio įrenginio vietą, rinkimu realiuoju laiku, yra ypač didelis, nes šie duomenys kompetentingoms nacionalinėms institucijoms suteikia galimybę tiksliai ir nuolat stebėti mobiliųjų telefonų naudotojų judėjimą <...>“ (sujungtos bylos C-511/18, C-512/18 ir C-520/18, *La Quadrature du Net ir kt.*, 2020 m. spalio 6 d., ECLI:EU:C:2020:791, 187 punktas, įskaitant nurodytą jurisprudenciją).
[19] Sprendimas *La Quadrature du Net ir kt.*, 131 punktas.
[20] Sprendimas *Schrems II*, 180 punktas.
[21] Sprendimas *Schrems II*, 176 punktas, įskaitant jame nurodytą jurisprudenciją.
[22] Sprendimas *Schrems II*, 176 punktas, įskaitant jame nurodytą jurisprudenciją.
[23] 2020 m. lapkričio 10 d. Europos duomenų apsaugos valdybos rekomendacijos Nr. 02/2020 dėl Europos pagrindinių garantijų taikant stebėjimo priemones.
[24] TD 67 konstatuojamoji dalis.
[25] TD 68 konstatuojamoji dalis.

dokumentuose, pavyzdžiui, Europos Tarybos praktiniame vadove dėl asmens duomenų naudojimo policijos sektoriuje, kuriame aptariama, kaip apsaugoti asmens duomenis kovojant su nusikalstamumu, įtvirtintų principų.

32. Sprendimu dėl tinkamumo turėtų būti užtikrinama, kad visoje užsienio sistemoje užtikrinamas reikiamas duomenų, įskaitant į tą užsienio valstybę perduodamus duomenis, apsaugos lygis – teisių į privatumą esmė, veiksmingas jų įgyvendinimas, priežiūra ir įgyvendinimo užtikrinimas. Kaip ESTT pažymėjo Sprendime *Schrems II*, aukšto lygio apsauga taip pat turi būti užtikrinta, kai duomenys perduodami į trečiąją valstybę[26].

33. Galiausiai Komisija, priimdama tik su teritorija arba nurodytu sektoriumi trečiojoje valstybėje susijusį sprendimą dėl tinkamumo, turėtų atsižvelgti į aiškius ir objektyvius kriterijus, pavyzdžiui, kriterijus, susijusius su konkrečia duomenų tvarkymo veikla ar trečiojoje valstybėje taikytinų teisinių standartų bei galiojančių teisės aktų taikymo sritimi[27].

A. Bendrieji principai ir apsaugos priemonės

a) Sąvokos

34. Reikėtų nustatyti pagrindines duomenų apsaugos sąvokas. Jos neturi visiškai sutapti su TD terminologija, tačiau turėtų perteikti Europos duomenų apsaugos teisėje įtvirtintas sąvokas ir su jomis derėti. Pavyzdžiui, TD pateikiamos šios svarbios sąvokos: „asmens duomenys“, „asmens duomenų tvarkymas“, „kompetentingos institucijos“, „duomenų valdytojas“, „duomenų tvarkytojas“, „duomenų gavėjas“, „neskelbtini duomenys“, „tikslumas“, „profiliavimas“, „Pritaikytoji duomenų apsauga ir standartizuotoji duomenų apsauga“, „priežiūros institucija“ ir „pseudonimų suteikimas“.

b) Teisėtas ir sąžiningas asmens duomenų tvarkymas (4 straipsnis – 26 konstatuojamoji dalis)

35. Pagal Chartijos 8 straipsnio 2 dalį asmens duomenys turėtų, be kita ko, būti tvarkomi „tik konkretiems tikslams ir tik atitinkamam asmeniui sutikus ar kitais įstatymo nustatytais teisėtais pagrindais“[28]. Tačiau teisėsaugos srityje reikia pažymėti, kad nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas užduočių vykdymas, instituciniu požiūriu teisės aktais priskirtas kompetentingoms institucijoms, suteikia joms galimybę prašyti ar reikalauti, kad fiziniai asmenys vykdytų pateiktus prašymus. Tokiu atveju duomenų subjekto sutikimas neturėtų suteikti teisinio pagrindo kompetentingų institucijų vykdomam asmens duomenų tvarkymui[29].

36. Šiame teisiniame pagrinde turi būti numatytos aiškios ir tikslios taisyklės, kuriomis būtų reglamentuojama atitinkamos duomenų tvarkymo veiklos apimtis ir taikymas ir nustatomi

[26] Žr. 93 punktą.
[27] TD 67 konstatuojamoji dalis.
[28] Žr. Sprendimo *Schrems II* 173 punktą.
[29] TD 35 konstatuojamojoje dalyje taip pat nurodyta, kad „[t]uo atveju, kai iš duomenų subjekto reikalaujama įvykdyti teisinę prievolę, duomenų subjektas faktiškai neturi laisvo pasirinkimo, taigi duomenų subjekto reakcija negalėtų būti laikoma laisvai išreikštais jo pageidavimais. Tuo valstybėms narėms neturėtų būti trukdoma teisės aktais nustatyti, kad duomenų subjektas gali sutikti su jo asmens duomenų tvarkymu šios direktyvos tikslais, pavyzdžiui, DNR tyrimų vykdant nusikalstamų veikų tyrimus tikslu arba duomenų subjekto buvimo vietos stebėsenos naudojant elektroninius žymenis, siekiant vykdyti baudžiamąsias sankcijas, tikslu“.

minimalūs reikalavimai[30]. Be to, ESTT priminė, kad „teisės aktai turi būti teisiškai privalomi pagal nacionalinę teisę“[31].

37. Kad duomenų tvarkymas[32] būtų teisėtas, jis turi būti būtinas kompetentingai institucijai siekiant atlikti užduotį, vykdomą nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo, įskaitant grėsmių visuomenės saugumui prevencijos užtikrinimą, tikslais[33]. Šie tikslai turi būti numatyti nacionalinėje teisėje.

38. Asmens duomenys turi būti tvarkomi sąžiningai. Vienas iš duomenų apsaugos principų – sąžiningo duomenų tvarkymo principas – yra sąvoka, kuri skiriasi nuo teisės į teisingą bylos nagrinėjimą, kaip apibrėžta Chartijos 47 straipsnyje ir Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos (toliau – EŽTK) 6 straipsnyje[34].

c) Tikslų ribojimo principas (4 straipsnis)

39. Konkretūs tikslai, kuriais tvarkomi asmens duomenys, turėtų būti aiškūs, teisėti ir nustatyti asmens duomenų rinkimo metu[35].

40. Duomenys turi būti tvarkomi konkrečiu, aiškiu ir teisėtu tikslu, susijusiu su nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo, įskaitant grėsmių visuomenės saugumui prevencijos užtikrinimo trečiojoje valstybėje, tikslais ir vėliau naudojami bet kuriuo iš šių tikslų tik tuo atveju, jei tai nėra nesuderinama su pradiniu duomenų tvarkymo tikslu (pvz., susijusiame vykdymo užtikrinimo procese arba archyvavimo dėl viešojo intereso, panaudojimo moksliniais, statistiniais ar istorinių tyrimų tikslais), ir taikant tinkamas duomenų subjektų teisių ir laisvių apsaugos priemones[36]. Jei tas pats ar kitas duomenų valdytojas (kompetentinga institucija[37]) asmens duomenis tvarko kitu su nusikalstamų veikų prevencija, tyrimu, atskleidimo ar baudžiamuoju persekiojimu už jas arba bausmių vykdymu susijusiu tikslu nei tas, kuriuo tie duomenys buvo surinkti, duomenis tvarkyti galima, jei toks duomenų tvarkymas leidžiamas pagal taikomas teisės nuostatas ir yra būtinas ir proporcingas tam kitam tikslui[38]. Taip pat reikėtų atsižvelgti į tai, ar yra mechanizmas, pagal kurį atitinkamos valstybės narės kompetentingos institucijos būtų informuojamos apie tokį tolesnį duomenų

[30] Žr. Sprendimo *Schrems II* 175 ir 180 punktus, Nuomonės 1/15 139 punktą ir juose nurodytą jurisprudenciją.
[31] Žr. 2020 m. spalio 6 d. Sprendimo *Privacy International v Secretary of State for Foreign and Commonwealth Affairs ir kt.*, C-623/17, ECLI:EU:C:2020:790, 68 punktą – iš sprendimo versijos prancūzų kalba matyti, kad ESTT vartoja žodį „*réglementation*“, kuris apima ne tik parlamento aktus.
[32] Asmens duomenų tvarkymas visiškai arba iš dalies automatizuotomis priemonėmis ir asmens duomenų tvarkymas ne automatizuotomis priemonėmis, kai šie duomenys laikomi arba juos ketinama laikyti susistemintame rinkinyje.
[33] Kompetentinga institucija – tai bet kuri šiais tikslais kompetentinga valdžios institucijos ar bet kuri kita įstaiga ar kitas subjektas, kuriems teisės aktais pavesta vykdyti viešosios valdžios funkcijas ir naudotis viešaisiais įgaliojimais.
[34] TD 26 konstatuojamoji dalis.
[35] TD 26 konstatuojamoji dalis.
[36] Prie jų priskiriama policijos veikla iš anksto nežinant, ar tam tikras incidentas yra nusikalstama veika, ar ne. Tokia veikla taip pat gali apimti valdžios funkcijų vykdymą imantis prievartos priemonių, pavyzdžiui, policijos veiklą demonstracijose, svarbiuose sporto renginiuose ir riaušėse. Tai taip pat apima viešosios tvarkos palaikymą kaip policijai ar kitoms teisėsaugos institucijoms priskirtą užduotį prireikus užtikrinti apsaugą nuo grėsmių visuomenės saugumui ir teisės aktais saugomiems pagrindiniams visuomenės interesams, dėl kurių gali atsirasti sąlygos nusikalstamai veikai įvykdyti, ir užkirsti joms kelią“ (TD 12 konstatuojamoji dalis). Ji turi būti atskiriama nuo nacionalinio saugumo tikslo ar veiklos, kuriai taikomas Europos Sąjungos sutarties (toliau – ES sutartis) V antraštinės dalies 2 skyrius (TD 14 konstatuojamoji dalis).
[37] Žr. 33 išnašą.
[38] TD 29 konstatuojamoji dalis.

tvarkymą[39]. Be to, bet kuriuo atveju neturėtų būti daromas neigiamas poveikis TD Sąjungoje nustatytam fizinių asmenų apsaugos lygiui, taip pat ir tais atvejais, kai asmens duomenys iš trečiosios valstybės perduodami duomenų valdytojams ar tvarkytojams toje pačioje trečiojoje valstybėje[40].

d) Konkrečios tolesnio duomenų tvarkymo kitais tikslais sąlygos (9 straipsnis)

41. Iš Sąjungos 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. Taip pat reikėtų atsižvelgti į tai, ar yra mechanizmas, pagal kurį atitinkamos valstybės narės kompetentingos institucijos būtų informuojamos apie tokį tolesnį duomenų tvarkymą[41]. Šiuo atveju toliau tvarkomiems ar atskleistiems duomenims taip pat turėtų būti taikoma tokio paties lygio apsauga, kaip tuo atveju, kai tie duomenys buvo iš pradžių tvarkomi gaunančiosios kompetentingos institucijos.

e) Duomenų kiekio mažinimo principas

42. Duomenys turėtų būti adekvatūs, tinkami ir neviršijantys to, ko reikia siekiant tikslų, kuriais jie tvarkomi. Visų pirma reikėtų atsižvelgti į pritaikytosios ir standartizuotosios duomenų apsaugos reikalavimų, pavyzdžiui, ribotų įvedimo laukų (struktūrizuotų ryšių) ar automatizuotų ir neautomatizuotų kokybės patikrų, taikymą.

f) Duomenų tikslumo principas

43. Duomenys turėtų būti tikslūs ir, jei reikia, atnaujinami. Vis dėlto duomenų tikslumo principas turėtų būti taikomas atsižvelgiant į atitinkamo duomenų tvarkymo pobūdį ir tikslą. Visų pirma vykstant teismo procesui daromi pareiškimai, kuriuose yra asmens duomenų, yra pagrįsti subjektyviu fizinių asmenų suvokimu ir jų neįmanoma visada patikrinti. Todėl tikslumo reikalavimas neturėtų būti siejamas su pareiškimo tikslumu, o tik su faktu, kad padarytas konkretus pareiškimas[42].

44. Reikėtų užtikrinti, kad asmens duomenys, kurie yra netikslūs, neišsamūs arba pasenę, nebūtų persiunčiami arba nebūtų suteikiama galimybė jais naudotis[43], ir kad būtų numatytos netikslių duomenų ištaisymo ar panaikinimo procedūros. Visų pirma reikėtų atsižvelgti į bet kokią tvarkomos informacijos klasifikavimo sistemą atsižvelgiant į šaltinio patikimumą ir faktinių aplinkybių tikrinimo lygį[44].

g) Duomenų saugojimo principas

45. Duomenys turėtų būti saugomi ne ilgiau nei reikia tikslams, dėl kurių jie tvarkomi, pasiekti. Turėtų būti nustatyti tinkami asmens duomenų ištrynimo mechanizmai; tai gali būti nustatytas laikotarpis arba duomenų saugojimo poreikio periodinė peržiūra (arba šių dviejų elementų derinys:

[39] Toks mechanizmas gali būti, pavyzdžiui, duomenų tvarkymo kodeksai, dėl kurių susitarta tarpusavyje, tarptautinėje teisinėje priemonėje numatytas įpareigojimas pranešti, įskaitant galimus automatinius pranešimus, ar kitos panašios skaidrumo priemonės.
[40] TD 64 konstatuojamoji dalis.
[41] Žr. 39 išnašą.
[42] TD 30 konstatuojamoji dalis.
[43] TD 32 konstatuojamoji dalis.
[44] Pvz., tinkamumo vertinimų ir duomenų tvarkymo kodeksų „4 x 4 lentelės“.

nustatytas ilgiausias laikotarpis ir periodinė peržiūra tam tikrais intervalais)[45]. Asmens duomenims, saugomiems ilgesniais laikotarpiais archyvavimo dėl viešojo intereso, panaudojimo moksliniais, statistiniais ar istorinių tyrimų tikslais, turėtų būti taikomos tinkamos apsaugos priemonės (pvz., dėl susipažinimo)[46].

h) Saugumo ir konfidencialumo principas (29 straipsnis, 28 ir 71 konstatuojamosios dalys)

46. Bet kuris subjektas, tvarkantis asmens duomenis, turėtų užtikrinti, kad duomenys būtų tvarkomi taip, kad būtų užtikrintas asmens duomenų saugumas, be kita ko, užkertant kelią neteisėtai prieigai prie asmens duomenų ir jų tvarkymui skirtos įrangos ar neteisėtam jų naudojimui. Tai apima apsaugą nuo neteisėto duomenų tvarkymo, taip pat nuo netyčinio praradimo, sunaikinimo ar sugadinimo ir tam spręsti skirtas tinkamas priemones naudojant tinkamas technines ir organizacines priemones. Nustatant duomenų tvarkymo saugumo lygį, taip pat reikėtų atsižvelgti į techninių galimybių išsivystymo lygį, įgyvendinimo išlaidas ir duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat į įvairios tikimybės ir dydžio pavojų fizinių asmenų teisėms ir laisvėms.

47. Turėtų būti užtikrinti saugūs valstybių narių institucijų, perduodančių asmens duomenis, ir trečiųjų valstybių gaunančiųjų institucijų ryšių kanalai.

i) Skaidrumo principas (13 straipsnis, 26, 39, 42, 43, 44, 46 konstatuojamosios dalys)

48. Fiziniai asmenys turėtų būti informuoti apie su jų asmens duomenų tvarkymu susijusius pavojus, taisykles, apsaugos priemones bei teises ir apie tai, kaip naudotis savo teisėmis duomenų tvarkymo atžvilgiu[47].

49. Asmenims turėtų būti pateikiama informacija apie visus pagrindinius jų asmens duomenų tvarkymo aspektus. Ši informacija turėtų būti lengvai prieinama ir suprantama, pateikiama aiškia ir suprantama kalba. Kartu su šia informacija turėtų būti nurodomas duomenų tvarkymo tikslas, duomenų valdytojo tapatybė, jam suteiktos teisės[48] ir kita informacija, kurios reikia siekiant užtikrinti sąžiningumą.

50. Gali būti taikomos kelios šios teisės į informaciją išimtys. Tačiau toks apribojimas turėtų būti leidžiamas teisinėje priemonėje ir turėtų būti būtinas ir proporcingas siekiant netrukdyti atlikti oficialius arba teisinius nagrinėjimus, tyrimus ar procedūras, nepakenkti nusikalstamų veikų prevencijai, tyrimui, atskleidimui ar baudžiamajam persekiojimui už jas arba bausmių vykdymui, užtikrinti visuomenės saugumą arba nacionalinį saugumą arba apsaugoti kitų asmenų teises ir laisves, jei toks dalinis arba visiškas apribojimas, tinkamai paisant atitinkamo fizinio asmens pagrindinių teisių ir teisėtų interesų, yra būtina ir proporcinga demokratinės visuomenės priemonė. Tokie apribojimai taip pat turėtų būti nagrinėjami ir vertinami atsižvelgiant į galimybę pateikti skundą priežiūros institucijai arba siekti teisių gynimo priemonės. Bet kokie galimi apribojimai bet kuriuo atveju turėtų būti laikini, ne bendro pobūdžio ir apimti panašias sąlygas, apsaugos priemones ir apribojimus kaip tie, kurių reikalaujama pagal Chartiją ir EŽTK, kaip išaiškinta atitinkamai ESTT ir EŽTT jurisprudencijoje, ir šiais apribojimais visų pirma turi būti paisoma tų teisių ir laisvių esmės.

[45] TD 5 straipsnis;
[46] TD 26 konstatuojamoji dalis.
[47] TD 26 konstatuojamoji dalis.
[48] Ir materialinės teisės (teisė susipažinti su duomenimis, reikalauti juos ištaisyti ir kt.), ir teisė į teisių gynimą.

j) Teisė susipažinti su duomenimis, reikalauti juos ištaisyti ir ištrinti (14 ir 16 straipsniai)

51. Duomenų subjektui turėtų būti suteikta teisė gauti patvirtinimą, ar su juo susiję duomenys yra tvarkomi, ar ne, ir, jei tokie duomenys tvarkomi – teisė susipažinti su savo duomenimis. Ši teisė turėtų bent apimti tam tikrą informaciją apie duomenų tvarkymą, pavyzdžiui, duomenų tvarkymo tikslus ir teisinį pagrindą, teisę pateikti skundą priežiūros institucijai arba atitinkamų asmens duomenų kategorijas[49]. Tai ypač svarbu tuo atveju, kai skaidrumas užtikrinamas paskelbiant bendrą pranešimą (pvz., pateikiant informaciją institucijos interneto svetainėje).

52. Duomenų subjektui turėtų būti suteikta teisė reikalauti ištaisyti jo duomenis dėl nurodytų priežasčių, pavyzdžiui, kai duomenys yra netikslūs arba neišsamūs. Duomenų subjektui taip pat turėtų būti suteikta teisė reikalauti jo duomenis ištrinti, kai, pavyzdžiui, jų nebereikia tvarkyti arba kai tai būtų neteisėta.

53. Duomenų subjektui neturėtų būti pernelyg sunku šiomis teisėmis pasinaudoti.

k) Duomenų subjektų teisių apribojimai

54. Galimi šių teisių apribojimai gali būti numatyti siekiant netrukdyti atlikti oficialius arba teisinius nagrinėjimus, tyrimus ar procedūras, nepakenkti nusikalstamų veikų prevencijai, tyrimui, atskleidimui ar baudžiamajam persekiojimui už jas arba bausmių vykdymui, užtikrinti visuomenės saugumą arba nacionalinį saugumą arba apsaugoti kitų asmenų teises ir laisves, jei toks dalinis arba visiškas apribojimas, tinkamai paisant atitinkamo fizinio asmens pagrindinių teisių ir teisėtų interesų, yra būtina ir proporcinga demokratinės visuomenės priemonė. Tokie apribojimai taip pat turėtų būti nagrinėjami ir vertinami atsižvelgiant į galimybę pateikti skundą priežiūros institucijai arba siekti teisminės teisių gynimo priemonės.

l) Tolesnio duomenų perdavimo ribojimas (35 straipsnis, 64–65 konstatuojamosios dalys)

55. Pradiniam gavėjui asmens duomenis toliau perduodant į kitą trečiąją valstybę ar tarptautinę organizaciją negali sumažėti Sąjungoje numatytas fizinių asmenų, kurių duomenys perduodami, apsaugos lygis. Taigi, toks tolesnis duomenų perdavimas turėtų būti leidžiamas tik tuo atveju, jei užtikrinamas pagal Sąjungos teisę suteikto apsaugos lygio tęstinumas[50]. Visų pirma tolesnis gavėjas (t. y. toliau perduodamų duomenų gavėjas) turėtų būti teisėsaugos tikslais kompetentinga institucija[51], o toks tolesnis duomenų perdavimas gali būti vykdomas tik ribotais ir konkrečiais tikslais, jei tokiam duomenų tvarkymui yra teisinis pagrindas.

56. Taip pat reikėtų 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 Sąjungos perduotų duomenų pradinis gavėjas turėtų įrodyti, kad atitinkama valstybės narės kompetentinga institucija leido toliau perduoti duomenis[52] ir kad yra numatytos tinkamos apsaugos priemonės, taikomos tolesniam duomenų perdavimui[53].

[49] TD 14 straipsnis.
[50] Taip pat žr. Nuomonę 1/15.
[51] Žr. 33 išnašą.
[52] Atsižvelgiant į tai, turėtų būti atsižvelgiama į tai, ar yra pareiga ar įsipareigojimas įgyvendinti atitinkamus perduodančiosios valstybės narės institucijų nustatytus duomenų tvarkymo kodeksus.
[53] Pirmiau nurodyti reikalavimai nedaro poveikio konkrečioms tolesnio duomenų perdavimo į tinkamą apsaugą užtikrinančią valstybę sąlygoms, nustatytoms TD (35 straipsnio 1 dalies c ir e punktai).

m) Atskaitomybės principas (4 straipsnio 4 dalis)

57. Duomenų valdytojas yra atsakingas už tai, kad būtų laikomasi TD 4 straipsnyje nustatytų duomenų apsaugos principų, ir turi sugebėti tai įrodyti.

B. Papildomų principų, kurie turi būti taikomi konkrečių rūšių duomenų tvarkymui, pavyzdžiai

a) Specialių kategorijų duomenys (10 straipsnis ir 37 konstatuojamoji dalis)

58. Tais atvejais, kai tvarkomi „specialių kategorijų duomenys“[54], turėtų būti taikomos konkrečios apsaugos priemonės, kuriomis atsižvelgiama į konkretų susijusį pavojų[55]. Šios kategorijos turėtų atspindėti TD 10 straipsnyje įtvirtintas kategorijas. Todėl tvarkant specialių kategorijų duomenis turėtų būti taikomos konkrečios apsaugos priemonės, o toks duomenų tvarkymas turėtų būti leidžiamas tik tuo atveju, kai tai yra griežtai būtina tam tikromis sąlygomis, pavyzdžiui, siekiant apsaugoti gyvybiškai svarbius asmens interesus.

b) Automatizuotas sprendimų priėmimas ir profiliavimas (11 straipsnis ir 38 konstatuojamoji dalis)

59. Sprendimai, grindžiami tik automatizuotu duomenų tvarkymu (automatizuotas atskirų sprendimų priėmimas), įskaitant profiliavimą, ir kuriais daromas teisinis poveikis ar didelis poveikis duomenų subjektui, turėtų būti priimami tik laikantis tam tikrų sąlygų, nustatytų trečiosios valstybės teisinėje sistemoje[56].

60. Europos Sąjungos sistemoje tokios sąlygos apima, pavyzdžiui, konkrečios informacijos duomenų subjektui suteikimą ir teisę iš duomenų valdytojo reikalauti žmogaus įsikišimo, visų pirma pareikšti savo požiūrį, gauti sprendimo, priimto atlikus tokį vertinimą, paaiškinimą, arba ginčyti tą sprendimą.

61. Trečiosios 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.

c) Pritaikytoji ir standartizuotoji duomenų apsauga (20 straipsnis)

62. Vertinant tinkamumą taip pat reikėtų atsižvelgti į tai, ar duomenų valdytojams yra numatytas įpareigojimas priimti vidaus politiką ir įgyvendinti priemones, kuriomis būtų paisoma pritaikytosios duomenų apsaugos ir standartizuotosios duomenų apsaugos principų atsižvelgiant į techninių galimybių išsivystymo lygį, įgyvendinimo išlaidas ir duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat į įvairios tikimybės ir dydžio pavojų fizinių asmenų teisėms ir laisvėms, kylantį dėl duomenų tvarkymo, ir tuo metu, kai nustatomos duomenų tvarkymo priemonės, ir paties duomenų tvarkymo metu, priimti tinkamas technines ir organizacines priemones, pavyzdžiui, pseudonimų suteikimą, kuriomis siekiama veiksmingai įgyvendinti duomenų apsaugos principus, pavyzdžiui, duomenų kiekio mažinimą, ir į duomenų tvarkymo procesą įtraukti reikiamas apsaugos priemones.

[54] Tokie specialių kategorijų duomenys TD 37 konstatuojamojoje dalyje dar vadinami neskelbtinais duomenimis.
[55] Tokios papildomos apsaugos priemonės gali būti, pavyzdžiui, konkrečios apsaugos priemonės, ribota darbuotojų teisė susipažinti su duomenimis, tolesnio duomenų tvarkymo, automatizuoto sprendimų priėmimo, tolesnio atskleidimo ar perdavimo apribojimai.
[56] Nuomonės 1/15 173 punktas.

C. Procedūriniai ir vykdymo užtikrinimo mechanizmai

63. Nors priemonės, kuriomis naudojasi trečiosios valstybės, siekdamos užtikrinti tinkamą apsaugos lygį, gali skirtis nuo tų, kurios taikomos Europos Sąjungoje[57], į su Europos sistema suderintą sistemą turi būti įtraukti toliau išvardyti elementai.

a) Kompetentinga nepriklausoma priežiūros institucija (36 straipsnio 2 dalies b punktas, 36 straipsnio 3 dalis ir 67 konstatuojamoji dalis)

64. Turėtų veikti viena ar kelios nepriklausomos priežiūros institucijos, kurioms pavesta užtikrinti, kad trečiojoje valstybėje būtų laikomasi duomenų apsaugos ir privatumo nuostatų ir kad jos būtų vykdomos. Ši priežiūros institucija, vykdydama savo pareigas ir įgaliojimus, veikia visiškai nepriklausomai ir nešališkai, taigi, nesiekia gauti bei nepriima nurodymų. Todėl priežiūros institucijai turėtų būti suteikti visi tinkami vykdymo užtikrinimo įgaliojimai, kuriuos pasitelkiant būtų galima veiksmingai užtikrinti, kad būtų paisoma duomenų apsaugos teisių ir skatinamas informuotumas. Taip pat reikėtų atsižvelgti į priežiūros institucijos darbuotojus ir biudžetą. Priežiūros institucijai taip pat turėtų būti sudarytos sąlygos savo iniciatyva atlikti tyrimus. Jai taip pat turėtų būti pavesta padėti duomenų subjektams naudotis savo teisėmis ir patarti, kaip tai daryti (taip pat žr. c punktą). Sprendimuose dėl tinkamumo turėtų būti nurodyta (jei taikoma) ta priežiūros institucija ar institucijos ir bendradarbiavimo su valstybių narių priežiūros institucijomis mechanizmai siekiant užtikrinti duomenų apsaugos taisyklių vykdymą.

b) Veiksmingas duomenų apsaugos taisyklių įgyvendinimas

65. Įgyvendinant trečiosios valstybės sistemą turėtų būti užtikrinamas aukštas duomenų valdytojų ir tų, kurie jų vardu tvarko asmens duomenis, informuotumo, susijusio su jų prievolėmis, užduotimis ir pareigomis, lygis ir aukštas duomenų subjektų informuotumo apie jų teises ir priemones tomis teisėmis pasinaudoti lygis. Svarbų vaidmenį užtikrinant, kad būtų laikomasi taisyklių, gali atlikti veiksmingos ir atgrasomos sankcijos ir valdžios institucijų, auditorių ar nepriklausomų duomenų apsaugos pareigūnų atliekamų tiesioginių patikrinimų sistemos.

66. Pagal trečiosios valstybės duomenų apsaugos sistemą duomenų valdytojai arba tie, kurie jų vardu tvarko asmens duomenis, turėtų būti įpareigoti laikytis šia sistema nustatytų taisyklių ir įrodyti kompetentingai priežiūros institucijai, kad jie jų laikosi. Tokios priemonės turėtų apimti su duomenų tvarkymo veikla susijusių dokumentų ir įrašų saugojimą tam tikrą laiką Jos taip pat gali būti, pavyzdžiui, poveikio duomenų apsaugai vertinimai, duomenų apsaugos pareigūno skyrimas arba pritaikytoji ir standartizuotoji duomenų apsauga.

c) Duomenų apsaugos sistemoje turi būti sudarytos palankesnės sąlygos duomenų subjektams naudotis savo teisėmis (TD 12, 17 ir 46 straipsniai)

67. Pagal trečiosios valstybės duomenų apsaugos sistemą duomenų valdytojai turėtų būti įpareigoti sudaryti palankesnes sąlygas duomenų subjektams naudotis savo teisėmis, nurodytomis šio dokumento A skyriaus j dalyje, ir turėtų būti numatyta, kad tos trečiosios valstybės priežiūros institucija bet kurio duomenų subjekto prašymu suteiktų jam informaciją apie naudojimąsi savo teisėmis[58].

[57] Sprendimas *Schrems I*, 74 punktas.
[58] Duomenų subjektas savo teisėmis gali naudotis tiesiogiai arba netiesiogiai.

d) Duomenų apsaugos sistemoje turi būti numatyti tinkami teisių gynimo mechanizmai

68. Nors šiuo metu nėra jurisprudencijos, susijusios su trečiosios valstybės teisinės sistemos tinkamumu pagal TD, ESTT yra išaiškinęs Chartijos 47 straipsnyje įtvirtintą pagrindinę teisę į veiksmingą teisminę gynybą. Pagal Chartijos 47 straipsnio 1 pastraipą kiekvienas asmuo, kurio teisės ir laisvės, garantuojamos Europos Sąjungos teise, yra pažeistos, turi turėti teisę į veiksmingą jų gynybą teisme[59] tame straipsnyje nustatytomis sąlygomis.

69. Pagal ESTT suformuotą jurisprudenciją pats veiksmingos teisminės kontrolės, skirtos Sąjungos teisės nuostatų laikymuisi užtikrinti, egzistavimas neatsiejamas nuo teisinės valstybės egzistavimo. Taigi reglamentavimu, kuriuo asmeniui nenumatoma jokios galimybės pasinaudoti teisių gynimo priemonėmis tam, kad gautų prieigą prie su juo susijusių asmens duomenų arba galėtų juos taisyti ar ištrinti, nepaisoma Europos Sąjungos pagrindinių teisių chartijos 47 straipsnyje įtvirtintos pagrindinės teisės į veiksmingą teisminę gynybą esmės[60].

70. Asmenims turėtų būti sudarytos sąlygos pasinaudoti teisių gynimo priemonėmis, kuriomis nedelsiant ir veiksmingai, be pernelyg didelių išlaidų būtų užtikrintos jų teisės ir atitiktis.

71. To siekiant turėtų veikti priežiūros mechanizmai, kuriais sudaromos sąlygos atlikti nepriklausomus skundų tyrimus, taip pat nustatyti visus teisės į duomenų apsaugą bei teisės į privatų gyvenimą pažeidimus ir skirti už juos realias bausmes.

72. Jei taisyklių nesilaikoma, duomenų subjektui, kurio duomenys perduodami į trečiąją valstybę, trečiojoje valstybėje taip pat turėtų būti suteikiamos veiksmingos administracinės ir teisminės teisių gynimo priemonės, įskaitant kompensaciją už žalą, patirtą dėl neteisėto jo asmens duomenų tvarkymo. Tai viena svarbiausių sąlygų, kuri turi būti užtikrinama įdiegus nepriklausomo sprendimų priėmimo arba arbitražo sistemą, pagal kurią atitinkamais atvejais būtų galima išmokėti kompensaciją ir skirti sankcijas.

[59] ESTT mano, kad veiksmingą teisminę apsaugą gali užtikrinti ne tik teismas, bet ir įstaiga, kurioje suteikiamos garantijos, iš esmės lygiavertės toms, kurių reikalaujama Chartijos 47 straipsnyje (žr. Sprendimo *Schrems II* 197 punktą). Tai gali būti reikšminga visų pirma tarptautinėms organizacijoms.
[60] Sprendimas *Schrems II*, 187 ir 194 punktai, įskaitant juose nurodytą jurisprudenciją.