



18/LT

WP 254, 1-oji peržiūrėta  
versija

### 29 straipsnio darbo grupė

#### Tinkamumo pavyzdžiai

Priimta 2017 m. lapkričio 28 d.

Paskutinį kartą peržiūrėta ir priimta 2018 m. vasario 6 d.

Ši darbo grupė sudaryta pagal Direktyvos 95/46/EB 29 straipsnį. Tai nepriklausomas Europos patariamasis organas duomenų apsaugos ir privatumo klausimais. Jo užduotys aprašytos Direktyvos 95/46/EB 30 straipsnyje ir Direktyvos 2002/58/EB 15 straipsnyje.

Sekretoriato funkcijas atlieka Europos Komisijos Teisingumo generalinio direktorato C direktoratas (Pagrindinės teisės ir Europos Sąjungos pilietybė), B-1049 Briuselis, Belgija, kabineto Nr. MO-59 02/013.

Svetainė [http://ec.europa.eu/newsroom/article29/news.cfm?item\\_type=1358&tpa\\_id=6936](http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936)

## **Ivadas**

ES duomenų apsaugos institucijų darbo grupė<sup>1</sup> (WP29) anksčiau buvo paskelbusi darbinį dokumentą dėl asmens duomenų perdavimo trečiosioms valstybėms (WP12)<sup>2</sup>. Pakeitus direktyvą ES Bendrojo duomenų apsaugos reglamentu (BDAR)<sup>3</sup>, WP29 iš naujo peržiūri savo ankstesnes gaires – WP12, siekdama atnaujinti jas pagal naują teisės aktą ir naujausią Europos Sąjungos Teisingumo Teismo praktiką<sup>4</sup>.

Šiuo darbinio dokumentu siekiama atnaujinti WP12 1 skyrių, susijusį su pagrindiniu klausimu – kaip užtikrinti tinkamą duomenų apsaugos lygį trečiojoje valstybėje, teritorijoje arba viename ar daugiau nurodytų sektorių toje trečiojoje valstybėje, arba tarptautinėje organizacijoje (toliau – trečiosios valstybės arba tarptautinės organizacijos). Artimiausiais metais šis dokumentas bus ir toliau peržiūrimas ir prireikus atnaujinamas, remiantis taikant BDAR įgyta praktine patirtimi. WP12 dokumento 2 skyrius (*Požiūrio taikymas šalims, ratifikavusioms 108-ąją konvenciją*) ir 3 skyrius (*Požiūrio taikymas pramonės savikontrolėi*) turėtų būti atnaujinami vėliau.

Šiame darbiniame dokumente dėmesys sutelkiamas vien į sprendimus dėl tinkamumo, kurie pagal BDAR 45 straipsnį laikomi Europos Komisijos įgyvendinimo aktais<sup>5</sup>. Kiti asmens duomenų perdavimo trečiosioms valstybėms ir tarptautinėms organizacijoms aspektai bus nagrinėjami rengiant vėlesnius darbinius dokumentus, kurie bus skelbiami atskirai (įmonėms privalomos taisyklės, nukrypti leidžiančios nuostatos).

Šiuo dokumentu siekiama pagal BDAR teikti rekomendacijas Europos Komisijai ir WP29 dėl duomenų apsaugos lygio trečiosiose valstybėse ir tarptautinėse organizacijose vertinimo, nustatant pagrindinius duomenų apsaugos principus, kurie turi būti įtraukti į trečiosios valstybės teisinę sistemą arba tarptautinės organizacijos nuostatus, kad būtų užtikrinta ES sistemai iš esmės lygiavertė sistema. Be to, šiuo dokumentu gali būti teikiamos rekomendacijos sprendimą dėl tinkamumo norinčioms gauti trečiosioms valstybėms ir tarptautinėms organizacijoms. Vis dėlto šiame darbiniame dokumente nustatyti principai nėra tiesiogiai taikomi duomenų valdytojams arba duomenų tvarkytojams.

Šį dokumentą sudaro keturi skyriai:

**1 skyrius.** Šiek tiek bendrosios informacijos apie tinkamumo sąvoką

**2 skyrius.** Procedūriniai išvadų dėl tinkamumo aspektai pagal BDAR

**3 skyrius.** Bendrieji duomenų apsaugos principai. Šiame skyriuje pateikiami pagrindiniai bendrieji duomenų apsaugos principai, kuriais siekiama užtikrinti, kad duomenų apsaugos lygis trečiojoje valstybėje arba tarptautinėje organizacijoje būtų iš esmės lygiavertis ES teisės aktais nustatytam lygiui.

**4 skyrius.** Esminės garantijos, suteikiamos prieigai teisėsaugos ir nacionalinio saugumo tikslais, siekiant apriboti pagrindinių teisių pažeidimus. Šiame skyriuje nurodomos esminės garantijos, suteikiamos prieigai teisėsaugos ir nacionalinio saugumo tikslais, atsižvelgiant į Europos Sąjungos Teisingumo Teismo 2015 m. Sprendimą *Schrems* ir remiantis 2016 m. priimtu WP29 darbinio dokumentu dėl esminių garantijų.

---

<sup>1</sup>Kaip nustatyta pagal ES Duomenų apsaugos direktyvos 95/46/EB 29 straipsnį.

<sup>2</sup>WP12, darbinis dokumentas „Asmens duomenų perdavimas trečiosioms valstybėms. ES Duomenų apsaugos direktyvos 25 ir 26 straipsnių taikymas“ (angl. *Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*), kurį 1998 m. liepos 24 d. priėmė darbo grupė.

<sup>3</sup>2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (Tekstas svarbus EEE).

<sup>4</sup>Jskaitant 2015 m. spalio 6 d. Sprendimą *Maximilian Schrems / Data Protection Commissioner*, C-362/14.

<sup>5</sup>Daugiau informacijos apie įgyvendinimo aktus galima rasti susijusioje BDAR 45 straipsnio 3 dalyje ir 93 straipsnio 2 dalyje.

## 1 skyrius. Šiek tiek bendrosios informacijos apie tinkamumo sąvoką

BDAR 45 straipsnio 1 dalyje nustatytas principas, pagal kurį asmens duomenys į trečiąją valstybę arba tarptautinei organizacijai perduodami tik jeigu atitinkama trečioji valstybė, teritorija arba vienas ar daugiau nurodytų sektorių toje trečiojoje valstybėje, arba atitinkama tarptautinė organizacija užtikrina tinkamo lygio apsaugą.

Sąvoką „tinkamo lygio apsauga“, kuri jau buvo apibrėžta Direktyvoje 95/46/EB, toliau išplėtojo Europos Sąjungos Teisingumo Teismas. Čia svarbu priminti Sprendime *Schrems* Europos Sąjungos Teisingumo Teismo 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]*<sup>6</sup>. Todėl tikslas – ne atitikti kiekvieną Europos Sąjungos teisės akto punktą, o nustatyti pagrindinius, esmę perteikiančius to teisės akto reikalavimus.

Valstybėms narėms privalomų<sup>7</sup> 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<sup>8</sup>. 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 apsvastyti 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.

BDAR 45 straipsnio 2 dalyje nustatyti aspektai, į kuriuos Europos Komisija atsižvelgia vertindama trečiosios valstybės ar tarptautinės organizacijos apsaugos lygio tinkamumą.

Pavyzdžiui, Komisija atsižvelgia į teisinės valstybės principą, pagarbą žmogaus teisėms ir pagrindinėms laisvėms, atitinkamus teisės aktus, į tai, ar yra ir ar veiksmingai veikia viena ar kelios nepriklausomos priežiūros institucijos, taip pat į atitinkamos trečiosios valstybės arba tarptautinės organizacijos priimtus tarptautinius įsipareigojimus.

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

Esminiai duomenų apsaugos turinio principai ir procedūriniai ir (arba) vykdymo užtikrinimo reikalavimai, kuriuos galima laikyti būtinaisiais reikalavimais, kad apsaugos lygis būtų tinkamas, kildinami iš ES pagrindinių teisių chartijos ir BDAR. Be to, reikėtų atsižvelgti ir į kitus tarptautinius susitarimus dėl duomenų apsaugos, pvz., Europos Tarybos 108-ąją konvenciją<sup>9</sup>.

Taip pat privalu atkreipti dėmesį į valdžios institucijų prieigai prie asmens duomenų taikomą teisinę sistemą. Daugiau rekomendacijų šia tema pateikta 237-ajame darbiniam dokumente (t. y. Esminių garantijų dokumente)<sup>10</sup> dėl apsaugos priemonių vykdant su priežiūra susijusią veiklą.

Bendrųjų nuostatų dėl duomenų apsaugos ir privatumo trečiojoje valstybėje nepakanka. Priešingai – į trečiosios valstybės arba tarptautinės organizacijos teisinę sistemą privaloma įtraukti konkrečias nuostatas, kuriomis atsižvelgiama į konkrečius poreikius, susijusius su praktiškai svarbiais teisės į duomenų apsaugą aspektais. Šios nuostatos turi būti vykdytinos.

<sup>6</sup> 2015 m. spalio 6 d. Sprendimas *Maximillian Schrems / Data Protection Commissioner*, C-362/14 (73, 74 punktai).

<sup>7</sup> SESV 288 straipsnio 2 dalis.

<sup>8</sup> 2015 m. spalio 6 d. Sprendimas *Maximillian Schrems / Data Protection Commissioner*, C-362/14 (52 punktas).

<sup>9</sup> BDAR 105 konstatuojamoji dalis.

<sup>10</sup> Darbinis dokumentas Nr. 01/2016 dėl pagrindinių teisių į privatumą ir duomenų apsaugą pažeidimų pagrindimo, asmens duomenų perdavimui pasitelkiant priežiūros priemones (Europos esminės garantijos) (angl. *Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees)*, 16/EN WP 237, 2016 m. balandžio 13 d.

## 2 skyrius. Procedūriniai tinkamumo išvadų aspektai pagal BDAR

Kad Europos duomenų apsaugos valdyba galėtų atlikti savo užduotis, t. y. konsultuoti Europos Komisiją, kaip numatyta BDAR 70 straipsnio 1 dalies s punkte, Europos duomenų apsaugos valdybai turėtų būti pateikti atitinkami dokumentai, įskaitant atitinkamus Europos Komisijos susirašinėjimus ir priimtas išvadas. 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 savo vertinimą, susijusį su duomenų apsaugos lygiu trečiojoje valstybėje. Europos duomenų apsaugos valdyba laiku pateiks nuomonę dėl Europos Komisijos išvadų ir nurodys tinkamumo sistemos trūkumus, jei jų bus. Europos duomenų apsaugos valdyba taip pat sieks pasiūlyti patobulinimų ir pakeitimų, kaip šalinti galimus trūkumus.

Remiantis BDAR 45 straipsnio 4 dalimi, būtent Europos Komisija turi nuolat stebėti pokyčius, kurie galėtų daryti poveikį sprendimo dėl tinkamumo veikimui.

BDAR 45 straipsnio 3 dalyje numatyta, kad periodinės peržiūros turi būti atliekamos bent 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.

Atsižvelgiant į įgaliojimą 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, Europos duomenų apsaugos valdyba 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 pageidautų būti pakviesta dalyvauti tokiuose peržiūros procesuose ir vizituose.

Taip pat reikėtų pažymėti, kad pagal BDAR 45 straipsnio 5 dalį Europos Komisija turi teisę panaikinti, iš dalies pakeisti priimtus sprendimus dėl tinkamumo arba sustabdyti jų galiojimą. Todėl Europos duomenų apsaugos valdyba turėtų būti įtraukiama į panaikinimo, dalinio pakeitimo ar galiojimo sustabdymo procedūrą, pagal 70 straipsnio 1 dalies s punktą prašant jos pateikti nuomonę.

Be to, kaip dabar pripažįstama BDAR 58 straipsnio 5 dalyje ir pagal Europos Sąjungos Teisingumo Teismo sprendimą *Schrems*, duomenų apsaugos institucijoms turi būti sudarytos sąlygos dalyvauti teismo procese, jei jos mano, kad asmens pateiktas ieškinys dėl sprendimo dėl tinkamumo yra tinkamai pagrįstas: *[Š]iuo 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 priežiūros institucija, turėtų abejonių dėl šio sprendimo galiojimo.*<sup>11</sup>

<sup>11</sup> 2015 m. spalio 6 d. Sprendimas *Maximillian Schrems / Data Protection Commissioner*, C-362/14 (65 punktas).

**3 skyrius. Bendrieji duomenų apsaugos principai, kuriais siekiama užtikrinti, kad duomenų apsaugos lygis trečiojoje valstybėje, teritorijoje arba viename ar daugiau nurodytų sektorių toje trečiojoje valstybėje, arba tarptautinėje organizacijoje būtų iš esmės lygiavertis ES teisės aktais nustatytam lygiui**

Trečiosios valstybės arba tarptautinės organizacijos sistemoje turi būti numatyti toliau aprašyti pagrindiniai turinio ir procedūriniai ir (arba) vykdymo užtikrinimo duomenų apsaugos principai ir mechanizmai

#### **A. Turinio principai**

##### **1) Sąvokos**

Reikėtų nustatyti pagrindines duomenų apsaugos sąvokas ir (arba) principus. Jie neturi visiškai sutapti su BDAR terminologija, tačiau turėtų perteikti Europos duomenų apsaugos teisėje įtvirtintas sąvokas ir su jomis derėti. Pavyzdžiui, BDAR pateikiamos šios svarbios sąvokos: „asmens duomenys“, „asmens duomenų tvarkymas“, „duomenų valdytojas“, „duomenų tvarkytojas“, „duomenų gavėjas“ ir „neskelbtini duomenys“.

##### **2) Teisiškai pagrįsto ir sąžiningo duomenų tvarkymo teisėtais tikslais pagrindai**

Duomenys privalo būti tvarkomi teisiškai pagrįstai, sąžiningai ir teisėtai.

Reikėtų pakankamai aiškiai išdėstyti teisėtus pagrindus, kuriais remiantis galima teisiškai pagrįstai, sąžiningai ir teisėtai tvarkyti asmens duomenis. Europos sistemoje pripažįstami keli tokie teisėti pagrindai, įskaitant, pvz., nacionalinės teisės nuostatas, duomenų subjekto sutikimą, sutarties vykdymą arba teisėtą duomenų valdytojo arba trečiosios šalies interesą, tačiau jis nėra viršesnis už asmens interesus.

##### **3) Tikslų ribojimo principas**

Duomenys turėtų būti tvarkomi konkrečiu tikslu ir vėliau naudojami tik tuo atveju, jei tai nėra nesuderinama su jų tvarkymo tikslu.

##### **4) Duomenų kokybės ir proporcingumo principas**

Duomenys turėtų būti tikslūs ir, jei reikia, atnaujinami. Duomenys turėtų būti adekvatūs, tinkami ir neviršijantys to, ko reikia siekiant tikslų, kuriais jie tvarkomi.

##### **5) Duomenų saugojimo principas**

Paprastai duomenys turėtų būti saugomi ne ilgiau nei reikia tikslams, dėl kurių tvarkomi asmens duomenys, pasiekti.

##### **6) Saugumo ir konfidencialumo principas**

Bet koks asmens duomenis tvarkantis subjektas turėtų užtikrinti, kad, taikant atitinkamas technines ar organizacines priemones, duomenys būtų tvarkomi užtikrinant asmens duomenų saugumą, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo, taip pat nuo netyčinio praradimo, sunaikinimo ar sugadinimo. Užtikrinant duomenų saugumą reikėtų atsižvelgti į techninių galimybių išsivystymo lygį ir su tuo susijusias sąnaudas.

## **7) Skaidrumo principas**

Kiekvienas asmuo turėtų būti informuojamas apie visus pagrindinius jo asmens duomenų tvarkymo elementus ir ta informacija turėtų būti aiški, lengvai prieinama, glausta, skaidri ir suprantama. Kartu su šia informacija turėtų būti nurodomas duomenų tvarkymo tikslas, duomenų valdytojo tapatybė, jam suteiktos teisės ir kita informacija, kurios reikia siekiant užtikrinti sąžiningumą. Esant tam tikroms aplinkybėms, gali būti taikomos kelios šios teisės į informaciją išimties, pvz., siekiant užtikrinti baudžiamosios veikos tyrimų apsaugą, nacionalinį saugumą, teismų nepriklausomumą ir teismo procesų apsaugą ar kitus svarbius tikslus, susijusius su bendrais viešaisiais interesais, kaip nurodyta BDAR 23 straipsnyje.

## **8) Teisė susipažinti su duomenimis, reikalauti juos ištaisyti, ištrinti ir nesutikti**

Duomenų subjektui turėtų būti suteikta teisė gauti patvirtinimą, ar su juo susiję duomenys yra tvarkomi, ar ne, taip pat teisė susipažinti su savo duomenimis, be kita ko, suteikiant teisę gauti visų su juo susijusių tvarkomų duomenų kopiją.

Duomenų subjektui, nurodžius priežastis, turėtų būti suteikta teisė reikalauti ištaisyti savo duomenis kaip tinkama, pavyzdžiui, kai duomenys yra netikslūs arba neišsamūs, ir teisė ištrinti savo asmens duomenis, kai, pavyzdžiui, jų nebereikia tvarkyti arba kai tai būtų neteisėta.

Duomenų subjektui taip pat turėtų būti suteikta teisė dėl su jo konkrečiu atveju susijusių teisėtų priešasčių bet kuriuo metu nesutikti, kad su juo susiję asmens duomenys būtų tvarkomi pagal konkrečias trečiosios valstybės teisinėje sistemoje nustatytas sąlygas. Pavyzdžiui, kelios iš BDAR numatytų tokių sąlygų – kai duomenis tvarkyti yra būtina siekiant atlikti užduotį, vykdomą viešojo intereso labui, vykdant duomenų valdytojui pavestas viešosios valdžios funkcijas arba kai juos tvarkyti būtina siekiant teisėtų duomenų valdytojo arba trečiosios šalies interesų.

Duomenų subjektui neturėtų būti pernelyg sunku šiomis teisėmis pasinaudoti. Gali būti taikomi šių teisių apribojimai, pvz., siekiant užtikrinti baudžiamosios veikos tyrimų apsaugą, nacionalinį saugumą, teismų nepriklausomumą ir teismo procesų apsaugą ar kitus svarbius tikslus, susijusius su bendrais viešaisiais interesais, kaip nurodyta BDAR 23 straipsnyje.

## **9) Tolesnio duomenų perdavimo ribojimas**

Pradiniam pirmą kartą perduodamų duomenų gavėjui toliau perduoti asmens duomenis turėtų būti leidžiama tik tais atvejais, kai paskesniam gavėjui (t. y. toliau perduodamų duomenų gavėjui) taip pat taikomos taisyklės (įskaitant sutartimi numatytas taisykles), kuriomis užtikrinamas tinkamas apsaugos lygis ir kuriomis laikomasi atitinkamų nurodymų, kai duomenys tvarkomi duomenų valdytojo vardu. Vykdamas tolesnį duomenų perdavimą negali būti daromas neigiamas poveikis fizinių asmenų, kurių duomenys perduodami, apsaugos lygiui. Jei nepriimtas sprendimas dėl tinkamumo, pradinis iš ES perduodamų duomenų gavėjas privalo užtikrinti, kad tolesniam duomenų perdavimui būtų taikomos atitinkamos apsaugos priemonės. Toks tolesnis duomenų perdavimas gali būti vykdomas tik ribotais ir konkrečiais tikslais, jei tokiam duomenų tvarkymui yra teisinis pagrindas.

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

### **1) Specialių kategorijų duomenys**

Tais atvejais, kai tvarkomi „specialių kategorijų duomenys“<sup>12</sup>, turėtų būti taikomos konkrečios apsaugos priemonės. Šios kategorijos turėtų atspindėti BDAR 9 ir 10 straipsniuose įtvirtintas kategorijas. Tokias apsaugos priemones įgyvendinti reikėtų taikant griežtesnius duomenų tvarkymo reikalavimus, pavyzdžiui, kad duomenų subjektas duotų aiškų sutikimą tvarkyti duomenis, arba taikant papildomas apsaugos priemones.

## **2) Tiesioginė rinkodara**

Tais atvejais, kai duomenys tvarkomi tiesioginės rinkodaros tikslais, duomenų subjektui turėtų būti suteikta teisė be jokio mokesčio prieštarauti, kad jo duomenys bet kuriuo metu būtų tvarkomi tokiais tikslais.

## **3) Automatizuotas sprendimų priėmimas ir profiliavimas**

Sprendimai, grindžiami tik automatizuotu duomenų tvarkymu (automatizuotas atskirų sprendimų priėmimas), įskaitant profiliavimą, ir kuriais daromas teisinis poveikis ar didelis poveikis duomenų subjektui, gali būti priimami tik laikantis tam tikrų sąlygų, nustatytų trečiosios valstybės teisinėje sistemoje. Kelios iš tokių sąlygų, numatytų Europoje taikomoje sistemoje, – pavyzdžiui, būtinybė gauti aiškų duomenų subjekto sutikimą arba priimti tokį sprendimą, kad būtų galima sudaryti sutartį. Jei sprendimu nesilaikoma tokių sąlygų, kaip nustatyta trečiosios valstybės teisinėje sistemoje, duomenų subjektas turėtų turėti teisę, kad jam jis nebūtų taikomas. Trečiosios valstybės teisėje bet kuriuo atveju turėtų būti numatytos reikiamos apsaugos priemonės, įskaitant teisę būti informuotam apie konkrečius šį sprendimą pagrindžiančius motyvus ir susijusias logines priežastis, teisę ištaisyti netikslią ar neišsamią informaciją ir teisę užginčyti sprendimą, jei jis buvo priimtas remiantis neteisingu faktiniu pagrindu.

## **C. Procedūriniai ir vykdymo užtikrinimo mechanizmai**

**Nors priemonės, kuriomis naudojasi trečiosios valstybės, siekdamos užtikrinti tinkamą apsaugos lygį, gali skirtis nuo tų, kurios taikomos Europos Sąjungoje<sup>13</sup>, į su Europos sistema suderintą sistemą turi būti įtraukti toliau išvardyti elementai.**

### **1) Kompetentinga nepriklausoma priežiūros institucija**

Turėtų veikti viena ar kelios nepriklausomos priežiūros institucijos, kurioms pavesta stebėti, kaip trečiojoje valstybėje laikomasi duomenų apsaugos ir privatumo nuostatų, užtikrinti, kad jų būtų laikomasi 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 reikiami ir įmanomi įgaliojimai ir funkcijos, kuriuos pasitelkiant būtų galima 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.

### **2) Įgyvendinant duomenų apsaugos sistemą privaloma užtikrinti, kad būtų tinkamai laikomasi nuostatų**

---

<sup>12</sup> Tokie specialių kategorijų duomenys BDAR 10 konstatuojamojoje dalyje dar vadinami neskelbtiniais duomenimis.

<sup>13</sup> 2015 m. spalio 6 d. Sprendimas *Maximilian Schrems / Data Protection Commissioner*, C-362/14 (74 punktas).

Igyvendinant trečiosios valstybės sistemą turėtų būti užtikrinamas aukštas duomenų valdytojų ir tų, kurie jų vardu tvarko asmens duomenis, atskaitomybės ir informuotumo, susijusių 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, žinoma, valdžios institucijų, auditorių ar nepriklausomų duomenų apsaugos pareigūnų atliekamų tiesioginių patikrinimų sistemos.

### **3) Atskaitomybė**

Pagal trečiosios valstybės duomenų apsaugos sistemą duomenų valdytojai ir (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. Kelios iš tokių priemonių galėtų būti, pavyzdžiui, poveikio duomenų apsaugai vertinimai, su duomenų tvarkymo veikla susijusių dokumentų ir įrašų saugojimas tam tikrą laiką, duomenų apsaugos pareigūno skyrimas arba pritaikytoji ir standartizuotoji duomenų apsauga.

### **4) Igyvendinant duomenų apsaugos sistemą privaloma teikti paramą ir padėti pavieniams duomenų subjektams pasinaudoti savo teisėmis ir atitinkamais teisių gynimo mechanizmais**

Asmenims turėtų būti sudarytos sąlygos pasinaudoti teisių gynimo priemonėmis, kuriomis nedelsiant ir veiksmingai, be pernelyg didelių išlaidų būtų užtikrintos jų teisės ir atitiktis. To siekiant turėtų veikti priežiūros mechanizmai, kuriais sudaromos sąlygos atlikti nepriklausomus skundų tyrimus, taip pat nustatyti visus teisės į duomenų apsaugą bei teisės į privatą gyvenimą pažeidimus ir skirti už juos realias bausmes.

Jei taisyklių nesilaikoma, duomenų subjektui 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.



#### **4 skyrius. Esminės trečiųjų valstybių garantijos, suteikiamos prieigai teisėsaugos ir nacionalinio saugumo tikslais, siekiant apriboti pagrindinių teisių pažeidimus**

Vertinant apsaugos lygio tinkamumą, pagal 45 straipsnio 2 dalies a punktą Komisijos reikalaujama atsižvelgti į *atitinkamus bendruosius ir atskiriems sektoriams skirtus teisės aktus, įskaitant susijusius su visuomenės saugumu, gynyba, nacionaliniu saugumu, baudžiamąja teise ir valdžios institucijų prieiga prie asmens duomenų, taip pat tokių teisės aktų įgyvendinimą.*

Europos Sąjungos Teisingumo Teismas Sprendime *Schrems* pažymėjo, kad žodžių junginys „adekvatus apsaugos lygis“ turi būti suprantamas kaip reikalaujantis, kad ši trečioji šalis savo įstatymais arba tarptautiniais įsipareigojimais iš tikrųjų užtikrintų iš esmės tokį patį pagrindinių laisvių ir teisių apsaugos lygį, koks garantuojamas Sąjungoje pagal Direktyvą 95/46, siejamą su Chartija. Nors priemonės, kurių ši trečioji valstybė šiuo klausimu imasi, gali skirtis nuo priemonių, kurios taikomos Sąjungoje, vis dėlto praktiškai šios priemonės turi būti veiksmingos<sup>14</sup>.

Atsižvelgdamas į tai, teismas taip pat kritiškai pažymėjo, kad ankstesniame Saugaus uosto sprendime *nenustatyta, kad Jungtinėse Amerikos Valstijose yra valstybinio pobūdžio taisyklių, skirtų nustatyti asmenų, kurių asmens duomenys perduoti iš Sąjungos į Jungtines Amerikos Valstijas, galimoms pagrindinių teisių apribojimų riboms, t. y. apribojimų, kuriuos šios šalies valstybiniai subjektai gali nustatyti siekdami teisėtų tikslų, pavyzdžiui, nacionalinio saugumo.*

2016 m. balandžio 13 d. priimtoje WP237 nuomonėje WP29 nustatė esmines garantijas, kuriomis atsižvelgiama į su priežiūros sritimi susijusią Europos Sąjungos Teisingumo Teismo ir EŽTT praktiką. Nors WP237 nuomonėje išdėstytos rekomendacijos tebegalioja ir į jas reikėtų atsižvelgti vertinant trečiosios valstybės tinkamumą priežiūros srityje, šių garantijų taikymas galimybės susipažinti su duomenimis teisėsaugos ir nacionalinio saugumo tikslais srityje gali skirtis. Vis dėlto, norėdamos gauti galimybę susipažinti su duomenimis – tiek nacionalinio saugumo, tiek teisėsaugos tikslais, – kad būtų laikomos tinkamomis, visos trečiosios valstybės turi paisyti šių keturių garantijų:

- 1) duomenų tvarkymas turėtų būti grindžiamas aiškiomis, tikslėmis ir viešai skelbiamomis taisyklėmis (teisiniu pagrindu);**
- 2) turi būti įrodytas reikalingumas ir proporcingumas, palyginti su teisėtais siekiamais tikslais;**
- 3) duomenų tvarkymui turi būti taikoma nepriklausoma priežiūra;**
- 4) asmenims turi būti suteikiamos veiksmingos teisių gynimo priemonės.**

---

<sup>14</sup> 2015 m. spalio 6 d. Sprendimo *Maximillian Schrems / Data Protection Commissioner*, C-362/14, 74 punktas.