Dažnai užduodami klausimai dėl Europos Sąjungos Teisingumo Teismo sprendimo *Data Protection Commissioner / Facebook Ireland Ltd ir Maximillian Schrems*, C–311/18

Priimta 2020 m. liepos 23 d.

Šio dokumento tikslas – pateikti atsakymus į kai kuriuos dažnai užduodamus klausimus, kurių gauna priežiūros institucijos (toliau – PI); jis bus keičiamas ir papildomas atliekant tolesnę analizę, Europos duomenų apsaugos valdyba (toliau – EDAV) toliau nagrinėjant ir vertinant Europos Sąjungos Teisingumo Teismo (toliau – Teisingumo Teismas) sprendimą.

Sprendimas C–311/18 yra paskelbtas čia; Teisingumo Teismo pranešimas spaudai – čia.

1) Ką nusprendė Teisingumo Teismas šiuo sprendimu?

➔ Šiame sprendime Teisingumo Teismas nagrinėjo Europos Komisijos sprendimo 2010/87/EB dėl sutarčių standartinių sąlygų (toliau – SSS) galiojimą ir pripažino jį galiojančiu. Iš tikrųjų to sprendimo galiojimas nėra kvestionuojamas vien dėl to, kad jo standartinės duomenų apsaugos sąlygos, kurios yra sutartinio pobūdžio, nėra privalomos trečiosios šalies valdžios institucijoms, kurioms gali būti perduodami duomenys.

Tačiau šis galiojimas, priduria Teisingumo Teismas, priklauso nuo to, ar Sprendime 2010/87/EB yra įtvirtinti veiksmingi mechanizmai, leidžiantys praktiškai užtikrinti, kad būtų laikomasi apsaugos lygio, iš esmės lygiaverčio tam, kuris užtikrinamas ES pagal BDAR, ir kad asmens duomenų perdavimas, grindžiamas tokiomis sąlygomis, būtų sustabdytas arba uždraustas pažeidus šias sąlygas arba nesant galimybės jų laikytis.

Šiuo požiūriu Teisingumo Teismas, visų pirma, pažymi, kad Sprendimu 2010/87/EB nustatoma prievolė duomenų eksportuotojui ir duomenų gavėjui (duomenų importuotojui) prieš duomenų perdavimą ir atsižvelgiant į perdavimo aplinkybes patikrinti, ar atitinkamoje trečiojoje šalyje laikomasi Sąjungos teisėje reikalaujamo apsaugos lygio, ir kad pagal Sprendimą 2010/87/EB duomenų importuotojas privalo informuoti duomenų eksportuotoją, jei negali laikytis standartinių duomenų apsaugos sąlygų ir prireikus bet kokių papildomų priemonių, be užtikrinamų tomis sąlygomis, o duomenų eksportuotojas tuomet privalo sustabdyti duomenų perdavimą ir (arba) nutraukti sutartį su duomenų importuotoju.

➔ Teisingumo Teismas taip pat išnagrinėjo „Privatumo skydo“ sprendimo (Sprendimas 2016/1250 dėl ES ir JAV „privatumo skydo“ užtikrinamos apsaugos tinkamumo) galiojimą, nes dėl duomenų perdavimo tarp ES ir Jungtinių Amerikos Valstijų (JAV) kilo nacionalinis ginčas ir dėl jo buvo pateiktas prašymas priimti prejudicinį sprendimą.

Teisingumo Teismas konstatavo, kad asmens duomenų apsaugos apribojimai, kurie kyla iš Jungtinių Amerikos Valstijų nacionalinės teisės aktų ir, visų pirma, tam tikrų programų, susijusių su JAV valdžios institucijų prieiga prie asmens duomenų, perduodamų iš ES į JAV nacionalinio saugumo tikslais, nėra sureglamentuoti taip, kad atitiktų reikalavimus, iš esmės lygiaverčius tiems, kurie yra nustatyti ES teisėje[1], ir kad pagal tą teisės aktą duomenų subjektams nesuteikiamos įgyvendinamos teisės, kuriomis jie galėtų remtis teismuose JAV valdžios institucijų atžvilgiu.

Dėl tokio nesuderinamumo su asmenų, kurių duomenys yra perduodami į tą trečiąją šalį, pagrindinėmis teisėmis Teisingumo Teismas pripažino „Privatumo skydo“ tinkamumo sprendimą negaliojančiu.

2) Ar, be „privatumo skydo“, Teisingumo Teismo sprendimas daro poveikį kitoms duomenų perdavimo priemonėms?

➔ Apskritai trečiųjų šalių atveju Teisingumo Teismo nustatyta ribinė vertė taip pat taikoma visoms kitoms tinkamoms apsaugos priemonėms, pagal BDAR 46 straipsnį naudojamoms perduodant duomenis iš EEE į bet kokią trečiąją šalį. Teisingumo Teismo nurodytas JAV teisės aktas (t. y. FISA 702 straipsnis ir EO 12333) taikomas bet kokiam duomenų perdavimo elektroninėmis priemonėmis į JAV, patenkančiam į to teisės akto taikymo sritį, neatsižvelgiant į tokiam perdavimui naudojamą perdavimo priemonę[2].

3) Ar yra koks nors atidėjimo laikotarpis, per kurį galiu ir toliau perduoti duomenis į JAV nevertindamas perdavimo teisinio pagrindo?

➔ Ne, Teisingumo Teismas pripažino „Privatumo skydo“ sprendimą negaliojančiu ir jis nebetaikomas, nes Teisingumo Teismo išnagrinėtais JAV įstatymais nėra užtikrinamas apsaugos lygis, kuris būtų iš esmės lygiavertis ES apsaugos lygiui. Perduodant duomenis į JAV į šį vertinimą būtina atsižvelgti.

4) Anksčiau perduodavau duomenis JAV duomenų importuotojui pagal „privatumo skydo“ mechanizmą. Ką turėčiau daryti dabar?

➔ Perdavimas remiantis šia teisine sistema yra neteisėtas. Jeigu norite ir toliau perduoti duomenis į JAV, turite patikrinti, ar galite tai daryti toliau nustatytomis sąlygomis.

5) Su JAV duomenų importuotoju naudoju SSS. Ką turėčiau daryti?

[1] Teisingumo Teismas pabrėžia, kad tam tikrose stebėjimo programose, pagal kurias JAV valdžios institucijoms suteikiama prieiga prie asmens duomenų, perduodamų iš ES į JAV nacionalinio saugumo tikslais, nėra jokių JAV valdžios institucijoms suteikiamų įgaliojimų apribojimų ar garantijų ne JAV asmenims, kuriems gali būti taikomos šios programos.

[2] FISA 702 straipsnis taikomas visiems „elektroninių ryšių paslaugų teikėjams“ (žr. apibrėžtį USC 50 1881 straipsnio b punkto 4 papunktyje), o pagal EO 12333 organizuojamas elektroninis stebėjimas, apibrėžtas kaip „neviešos komunikacijos elektroninėmis priemonėmis įgijimas neturint elektroninės komunikacijos šalimi esančio asmens sutikimo arba, neelektroninės komunikacijos atveju, neturint asmens, kuris akivaizdžiai yra komunikacijos vietoje, sutikimo, bet neįskaitant radijo krypties nustatymo įrangos naudojimo tik siųstuvo buvimo vietai nustatyti“ (3.4 straipsnio b punktas).

➔ Teisingumo Teismas yra nusprendęs, kad JAV įstatymu (t. y. FISA 702 straipsniu ir EO 12333) nėra užtikrinamas iš esmės lygiavertis apsaugos lygis.

Ar perduodate asmens duomenis pagal SSS ar ne, priklausys nuo jūsų vertinimo rezultato atsižvelgiant į perdavimo aplinkybes ir papildomas priemones, kurių galite imtis. Kartu su SSS taikomomis papildomomis priemonėmis, vertinant perdavimo aplinkybes kiekvienu konkrečiu atveju, reikėtų užtikrinti, kad JAV įstatymais nebūtų pažeidžiamas tinkamas užtikrinamos apsaugos lygis.

Jeigu padarote išvadą, kad atsižvelgiant į perdavimo aplinkybes ir galimas papildomas priemones, tinkamos apsaugos priemonės nėra užtikrinamos, asmens duomenų perdavimą privalote sustabdyti arba nutraukti. Tačiau, jeigu ketinate ir toliau perduoti duomenis nepaisydami padarytos išvados, privalote pranešti apie tai kompetentingai PI[3].

6) Bendradarbiaudamas su JAV subjektu taikau įmonei privalomas taisykles (ĮPT). Ką turėčiau daryti?

➔ Atsižvelgiant į Teisingumo Teismo sprendimą, kuriuo „privatumo skydas“ yra pripažintas negaliojančiu, nes pagal JAV teisę nėra užtikrinamos asmenų, kurių duomenys yra perduodami į tą trečiąją šalį, pagrindinės teisės, ir į tai, kad „privatumo skydas“ buvo sukurtas taip pat siekiant užtikrinti duomenų, perduodamų naudojant kitas priemones, kaip antai ĮPT, apsaugą, Teisingumo Teismo vertinimas taikomas ir ĮPT, nes JAV teisė bus viršesnė ir už šią priemonę.

Ar perduodate asmens duomenis pagal ĮPT, ar ne, priklausys nuo jūsų vertinimo rezultato atsižvelgiant į perdavimo aplinkybes ir papildomas priemones, kurių galite imtis. Šiomis kartu su ĮPT taikomomis papildomomis priemonėmis, vertinant perdavimo aplinkybes kiekvienu konkrečiu atveju, reikėtų užtikrinti, kad JAV įstatymais nebūtų pažeidžiamas tinkamas užtikrinamos apsaugos lygis.

Jeigu padarote išvadą, kad, atsižvelgiant į perdavimo aplinkybes ir galimas papildomas priemones, tinkamos apsaugos priemonės nėra užtikrinamos, asmens duomenų perdavimą privalote sustabdyti arba nutraukti. Tačiau, jeigu ketinate ir toliau perduoti duomenis nepaisydami padarytos išvados, privalote pranešti apie tai kompetentingai PI[4].

7) Kaip dėl kitų perdavimo priemonių pagal BDAR 46 straipsnį?

➔ EDAV įvertins Teisingumo Teismo sprendimo pasekmes kitoms perdavimo priemonėms, kurios nėra SSS ir ĮPT. Sprendime patikslinama, kad tinkamos apsaugos priemonės pagal BDAR 46 straipsnį turi būti „iš esmės lygiavertės“.

Kaip pabrėžia Teisingumo Teismas, reikėtų pažymėti, kad 46 straipsnis yra BDAR V skyriuje, tad jį reikėtų taikyti atsižvelgiant į BDAR 44 straipsnį, kuriame yra nustatyta: „*Visos šio skyriaus*

[3] Žr., visų pirma, Teisingumo Teismo sprendimo 145 punktą ir Komisijos sprendimo 2010/87/ES 4 sąlygos g punktą, taip pat Komisijos sprendimo 2001/497/EB 5 sąlygos a punktą ir Komisijos sprendimo 2004/915/EB priedo II rinkinio c punktą.

[4] Žr., visų pirma, Teisingumo Teismo sprendimo 145 punktą ir Komisijos sprendimo 2010/87/ES 4 sąlygos g punktą. Taip pat žr. WP 256 1-osios peržiūrėtos redakcijos 6.3 skirsnį (29 straipsnio darbo grupės darbinis dokumentas, kuriuo nustatoma EDAV patvirtintų įmonei privalomose taisyklėse turinčių būti elementų ir principų lentelė: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109) ir WP 257 1-osios peržiūrėtos redakcijos 6.3 skirsnį (29 straipsnio darbo grupės darbinis dokumentas, kuriuo nustatoma EDAV patvirtintų įmonėms duomenų tvarkytojoms privalomose taisyklėse turinčių būti elementų ir principų lentelė: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110).

nuostatos taikomos siekiant užtikrinti, kad nebūtų pakenkta šiuo reglamentu garantuojamam fizinių asmenų apsaugos lygiui“.

8) Ar perduodamas duomenis į JAV galiu taikyti vieną iš BDAR 49 straipsnyje numatytų nukrypti leidžiančių nuostatų?

➔ Duomenis iš EEE į JAV vis dar galima perduoti remiantis BDAR 49 straipsnyje numatytomis nukrypti leidžiančiomis nuostatomis, jeigu taikomos šiame straipsnyje nustatytos sąlygos. EDAV daro nuorodą į savo gaires dėl šios nuostatos[5].

Visų pirma, reikėtų priminti, kad perduodant duomenis turint duomenų subjekto sutikimą jis turėtų būti:

- Aiškus,
- Duodamas dėl konkretaus duomenų perdavimo ar perdavimų sekos (t. y. duomenų eksportuotojas privalo užtikrinti, kad gaus konkretų sutikimą prieš atliekant duomenų perdavimą, net jeigu jis gaunamas jau surinkus duomenis) ir
- Grindžiamas informacija, visų pirma apie galimus perdavimo pavojus (t. y. duomenų subjektas taip pat turėtų būti informuojamas apie konkrečius pavojus, susijusius su jų duomenų perdavimu į valstybę, kurioje neužtikrinama tinkama apsauga ir netaikomos tinkamos apsaugos priemonės, kuriomis siekiama užtikrinti duomenų apsaugą).

Kalbant apie duomenų perdavimą, būtiną duomenų subjekto ir duomenų valdytojo sutarčiai vykdyti, reikėtų turėti omenyje, kad asmens duomenys gali būti perduodami tik jeigu tai daroma nereguliariai. Ar duomenų perdavimas yra reguliarus ar nereguliarus, reikėtų nustatyti kiekvienu konkrečiu atveju. Bet kuriuo atveju šia nukrypti leidžiančia nuostata galima vadovautis tik kai duomenų perdavimas yra objektyviai būtinas sutarčiai vykdyti.

Kalbant apie duomenų perdavimą, kuris yra būtinas dėl svarbių viešojo intereso priežasčių (tai turi būti pripažinta ES ar valstybių narių[6] teisėje), EDAV primena, kad esminis šios nukrypti leidžiančios nuostatos taikymo reikalavimas yra nustatyti ne organizacijos rūšį, o svarbų viešąjį interesą ir kad šią nukrypti leidžiančią nuostatą galima taikyti ne tik nereguliariam duomenų perdavimui, bet tai nereiškia, kad, remiantis svarbių viešųjų interesų nukrypti leidžiančia nuostata, duomenis galima perduoti dideliu mastu ir sistemingai. Iš tikrųjų, reikia laikytis bendrojo principo, pagal kurį BDAR 49 straipsnyje nustatytos nukrypti leidžiančios nuostatos praktiškai neturi tapti taisykle ir turi būti taikomos tik konkrečiais atvejais, o kiekvienas duomenų eksportuotojas turi užtikrinti, kad duomenų perdavimas atitiktų griežtą būtinumo kriterijų.

9) Ar galiu ir toliau naudoti SSS ar ĮPT duomenims perduoti į kitą trečiąją šalį, ne JAV?

➔ Teisingumo Teismas yra nurodęs, kad SSS paprastai vis dar galima naudoti perduodant duomenis į trečiąją šalį, tačiau Teisingumo Teismo nustatyta ribinė vertė dėl duomenų perdavimo į JAV taikoma bet kokiai trečiajai šaliai. Tas pats pasakytina apie ĮPT.

Teisingumo Teismas pažymėjo, kad įvertinti, ar atitinkamoje trečiojoje šalyje yra užtikrinamas pagal ES teisę reikalaujamas apsaugos lygis, turi duomenų eksportuotojas ir duomenų importuotojas, jeigu jie nori nustatyti, ar pagal SSS ar ĮPT užtikrinamas garantijas galima įgyvendinti praktiškai. Jeigu ne, turėtumėte įvertinti, ar galite įgyvendinti papildomas priemones,

[5] Žr. 2018 m. gegužės 25 d. priimtas EDAV gaires Nr. 2/2018 dėl leidžiančių nukrypti nuostatų pagal Reglamento 2016/679 49 straipsnį, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_lt.pdf, p. 3.

[6] Daromos nuorodos į valstybes nares turėtų būti suprantamos kaip nuorodos į EEE valstybes nares.

kad užtikrintumėte iš esmės lygiavertį apsaugos lygį, kaip EEE, ir ar trečiosios šalies teisės aktai nedarys poveikio šioms papildomoms priemonėms taip, kad jos taptų neveiksmingos.

Galite kreiptis į savo duomenų importuotoją, kad išsiaiškintumėte dėl jo šalies teisės aktų ir atliktumėte šį vertinimą kartu. Jeigu jūs ar jūsų duomenų importuotojas trečiojoje šalyje nustatote, kad perduodant duomenis pagal SSS ar ĮPT nėra užtikrinamas apsaugos lygis, iš esmės lygiavertis EEE užtikrinamam apsaugos lygiui, turėtumėte nedelsdami sustabdyti duomenų perdavimą. Jeigu to nepadarote, privalote apie tai informuoti kompetentingą PI[7].

➔ Nors, kaip yra pažymėjęs Teisingumo Teismas, ar pagal paskirties trečiosios šalies teisės aktus duomenų importuotojas gali laikytis standartinių duomenų apsaugos sąlygų arba ĮPT, prieš perduodami duomenis tai trečiajai šaliai turi įvertinti patys duomenų eksportuotojai ir duomenų importuotojai, PI taip pat atliks svarbų vaidmenį įgyvendinant BDAR priimdamos tolesnius sprendimus dėl duomenų perdavimo į trečiąsias šalis.

Kaip siūlo Teisingumo Teismas, siekiant išvengti skirtingų sprendimų, jos toliau dirbs EDAV, kad būtų užtikrinamas nuoseklumas, ypač jeigu reikia uždrausti perduoti duomenis į trečiąsias šalis.

10) Kokių papildomų priemonių galiu imtis, jeigu perduodu duomenis į trečiąsias šalis pagal SSS arba ĮPT?

➔ Prireikus galite numatyti papildomas priemones kiekvienu konkrečiu atveju atsižvelgdami į visas duomenų perdavimo aplinkybes ir įvertinę trečiosios šalies įstatymus, kad patikrintumėte, ar jais užtikrinamas tinkamas apsaugos lygis.

Teisingumo Teismas yra pažymėjęs, kad už tokį vertinimą ir būtinų papildomų priemonių įgyvendinimą atsako, visų pirma, duomenų eksportuotojas ir duomenų importuotojas.

EDAV šiuo metu nagrinėja Teisingumo Teismo sprendimą, kad nustatytų, kokias papildomas (teisines, technines ar organizacines) priemones, be SSS ar ĮPT, galima numatyti perduodant duomenis į trečiąsias šalis, kai vien SSS ar ĮPT nepavyksta užtikrinti pakankamo garantijų lygio.

➔ EDAV toliau vertina, kas galėtų sudaryti tas papildomas priemones, ir pateiks papildomų gairių.

11) Dirbu su duomenų tvarkytoju, tvarkančiu duomenis, už kuriuos esu atsakingas kaip jų valdytojas. Kaip sužinoti, ar tas duomenų tvarkytojas perduoda duomenis į JAV ar kitą trečiąją šalį?

➔ Pagal BDAR 28 straipsnio 3 dalį jūsų sudarytoje sutartyje su duomenų tvarkytoju turi būti numatyta, ar duomenis galima perduoti ar ne (reikėtų turėti omenyje, kad duomenų perdavimu laikomas net prieigos prie duomenų iš trečiosios šalies suteikimas, pavyzdžiui, administraciniais tikslais).

➔ Leidimo taip pat reikia dėl duomenų tvarkytojų naudojimosi pagalbinių duomenų tvarkytojų paslaugomis perduodant duomenis į trečiąsias šalis. Turėtumėte būti atidūs ir atsargūs, nes yra daug įvairių kompiuterinių sprendimų, kuriuose gali būti numatytas asmens duomenų perdavimas į trečiąją šalį (pvz., saugojimo ar techninės priežiūros tikslais).

[7] Žr., visų pirma, Teisingumo Teismo sprendimo 145 punktą. Dėl SSS žr. Komisijos sprendimo 2010/87/ES 4 sąlygos g punktą, taip pat Komisijos sprendimo 2001/497/EB 5 sąlygos a punktą ir Komisijos sprendimo 2004/915/EB priedo II rinkinio c punktą. Dėl ĮPT žr. WP 256 1-osios peržiūrėtos redakcijos (patvirtintos EDAV) 6.3 skirsnį ir WP 257 1-osios peržiūrėtos redakcijos (patvirtintos EDAV) 6.3 skirsnį.

12) Ką galiu padaryti, kad galėčiau ir toliau naudotis savo duomenų tvarkytojo paslaugomis, jeigu pagal BDAR 28 straipsnio 3 dalį pasirašytoje sutartyje nurodoma, kad duomenys gali būti perduodami į JAV ar kitą trečiąją šalį?

➔ Jeigu jūsų duomenys gali būti perduodami į JAV ir neįmanoma įgyvendinti jokių papildomų priemonių siekiant užtikrinti, kad dėl JAV įstatymų nenukentėtų duomenų perdavimo priemonėmis užtikrinamas apsaugos lygis, iš esmės lygiavertis EEE apsaugos lygiui, ir nėra taikomos nukrypti leidžiančios nuostatos pagal BDAR 49 straipsnį, vienintelis sprendimas yra derėtis dėl jūsų sutarties pakeitimo ar papildomos sąlygos, kad duomenų perdavimas į JAV būtų uždraustas. Duomenys turėtų būti ne tik saugomi, bet ir administruojami ne JAV.

➔ Jeigu jūsų duomenys gali būti perduodami į kitą trečiąją šalį, taip pat turėtumėte patikrinti tos trečiosios šalies teisės aktus, ar jie atitinka Teisingumo Teismo reikalavimus ir ar jais užtikrinamas asmens duomenų apsaugos lygis, kurio tikimasi. Jeigu nepavyksta rasti tinkamo pagrindo perduoti duomenis į trečiąją šalį, asmens duomenys neturėtų būti perduodami už EEE teritorijos ribų ir visa duomenų tvarkymo veikla turėtų būti vykdoma EEE.

Europos duomenų apsaugos valdybos vardu

Pirmininkė

Andrea Jelinek