TEISINGUMO TEISMO (didžioji kolegija) SPRENDIMAS

2020 m. liepos 16 d.*

„Prašymas priimti prejudicinį sprendimą – Fizinių asmenų apsauga tvarkant asmens duomenis – Europos Sąjungos pagrindinių teisių chartija – 7, 8 ir 47 straipsniai – Reglamentas (ES) 2016/679–2 straipsnio 2 dalis – Taikymo sritis – Asmens duomenų perdavimai į trečiąsias valstybes komerciniais tikslais – 45 straipsnis – Komisijos sprendimas dėl tinkamumo – 46 straipsnis – Duomenų perdavimas taikant tinkamas apsaugos priemones – 58 straipsnis – Priežiūros institucijų įgaliojimai – Trečiosios valstybės valdžios institucijų atliekamas perduotų duomenų tvarkymas nacionalinio saugumo tikslais – Trečiojoje valstybėje užtikrinamo tinkamo apsaugos lygio vertinimas – Sprendimas 2010/87/ES – Standartinės į trečiąsias valstybes perduodamų asmens duomenų apsaugos sąlygos – Duomenų valdytojo užtikrinamos tinkamos apsaugos priemonės – Galiojimas – Įgyvendinimo sprendimas (ES) 2016/1250 – Europos Sąjungos ir Jungtinių Amerikos Valstijų „privatumo skydo“ užtikrinamos apsaugos tinkamumas – Galiojimas – Fizinio asmens, kurio duomenys buvo perduoti iš Europos Sąjungos į Jungtines Amerikos Valstijas, skundas“

Byloje C-311/18

dėl *High Court* (Aukštasis Teismas, Airija) 2018 m. gegužės 4 d. sprendimu, kurį Teisingumo Teismas gavo 2018 m. gegužės 9 d., pagal SESV 267 straipsnį pateikto prašymo priimti prejudicinį sprendimą byloje

Data Protection Commissioner

prieš

Facebook Ireland Ltd,

Maximilian Schrems,

dalyvaujant

The United States of America,

Electronic Privacy Information Centre,

BSA Business Software Alliance Inc.,

Digitaleurope,

* Proceso kalba: anglų.

TEISINGUMO TEISMAS (didžioji kolegija),

kurį sudaro pirmininkas K. Lenaerts, pirmininko pavaduotoja R. Silva de Lapuerta, kolegijų pirmininkai A. Arabadjiev, A. Prechal, M. Vilaras, M. Safjan, S. Rodin, P. G. Xuereb, L. S. Rossi ir I. Jarukaitis, teisėjai M. Ilešič, T. von Danwitz (pranešėjas) ir D. Šváby,

generalinis advokatas H. Saugmandsgaard Øe,

posėdžio sekretorė C. Strömholm, administratorė,

atsižvelgęs į rašytinę proceso dalį ir įvykus 2019 m. liepos 9 d. posėdžiui,

išnagrinėjęs pastabas, pateiktas:

– *Data Protection Commissioner*, atstovaujamo solisitoriaus D. Young, SC B. Murray bei M. Collins ir BL C. Donnelly,

– *Facebook Ireland Ltd*, atstovaujamos SC P. Gallagher ir N. Hyland, BL A. Mulligan ir F. Kieran, taip pat solisitorių P. Nolan, C. Monaghan, C. O'Neill ir R. Woulfe,

– M. Schrems, atstovaujamo *Rechtsanwalt* H. Hofmann, SC E. McCullough, J. Doherty, S. O'Sullivan ir solisitoriaus G. Rudden,

– *The United States of America*, atstovaujamų SC E. Barrington, BL S. Kingston ir solisitorių S. Barton ir B. Walsh,

– *Electronic Privacy Information Centre*, atstovaujamo solisitorės S. Lucey, BL G. Gilmore, A. Butler ir SC C. O'Dwyer,

– *BSA Business Software Alliance Inc.*, atstovaujamo *advocaten* B. Van Vooren ir K. Van Quathem,

– *Digitaleurope*, atstovaujamos baristerės N. Cahill, solisitoriaus J. Cahir ir SC M. Cush,

– Airijos, atstovaujamos A. Joyce ir M. Browne, padedamų BL D. Fennelly,

– Belgijos vyriausybės, atstovaujamos J.-C. Halleux ir P. Cottin,

– Čekijos vyriausybės, atstovaujamos M. Smolek, J. Vláčil, O. Serdula ir A. Kasalická,

– Vokietijos vyriausybės, atstovaujamos J. Möller, D. Klebs ir T. Henze,

– Prancūzijos vyriausybės, atstovaujamos A.-L. Desjonquères,

– Nyderlandų vyriausybės, atstovaujamos C. S. Schillemans, K. Bulterman ir M. Noort,

– Austrijos vyriausybės, atstovaujamos J. Schmoll ir G. Kunnert,

– Lenkijos vyriausybės, atstovaujamos B. Majczyna,

– Portugalijos vyriausybės, atstovaujamos L. Inez Fernandes, A. Pimenta ir C. Vieira Guerra,

– Jungtinės Karalystės vyriausybės, atstovaujamos S. Brandon, padedamo QC J. Holmes ir baristerio C. Knight,

– Europos Parlamento, atstovaujamo M. J. Martínez Iglesias ir A. Caiola,

– Europos Komisijos, atstovaujamos D. Nardi, H. Krämer ir H. Kranenborg,

– Europos duomenų apsaugos valdybos (EDAV), atstovaujamos A. Jelinek ir K. Behn,

susipažinęs su 2019 m. gruodžio 19 d. posėdyje pateikta generalinio advokato išvada,

priima šį

Sprendimą

1 Prašymas priimti prejudicinį sprendimą iš esmės pateiktas dėl:

– 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvos 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (OL L 281, 1995, p. 31; 2004 m. specialusis leidimas lietuvių k., 13 sk., 15 t., p. 355) 3 straipsnio 2 dalies pirmos įtraukos, 25 ir 26 straipsnių bei 28 straipsnio 3 dalies, siejamų su ESS 4 straipsnio 2 dalimi ir Europos Sąjungos pagrindinių teisių chartijos (toliau – Chartija) 7, 8 ir 47 straipsniais, išaiškinimo,

– 2010 m. vasario 5 d. Komisijos sprendimo 2010/87/ES dėl sutarčių standartinių sąlygų, nustatytų asmens duomenų perdavimui trečiosiose šalyse įsikūrusiems tvarkytojams pagal Direktyvos 95/46 nuostatas (OL L 39, 2010, p. 5), iš dalies pakeisto 2016 m. gruodžio 16 d. Komisijos įgyvendinimo sprendimu (ES) 2016/2297 (OL L 344, 2016, p. 100; toliau – SAS sprendimas), išaiškinimo ir galiojimo ir

– 2016 m. liepos 12 d. Komisijos įgyvendinimo sprendimo (ES) 2016/1250 dėl ES ir JAV „privatumo skydo“ užtikrinamos apsaugos tinkamumo pagal Direktyvą 95/46 (OL L 207, 2016, p. 1; toliau – „Privatumo skydo“ sprendimas) išaiškinimo ir galiojimo.

2 Šis prašymas pateiktas nagrinėjant *Data Protection Commissioner* (Duomenų apsaugos komisaras, Airija, toliau – komisaras) ginčą su *Facebook Ireland Ltd* ir Maximillian Schrems dėl šio asmens pateikto skundo dėl to, kad *Facebook Ireland* perdavė jo asmens duomenis *Facebook Inc.* į Jungtines Amerikos Valstijas.

Teisinis pagrindas

Direktyva 95/46

3 Direktyvos 95/46 3 straipsnio „Taikymo sritis“ 2 dalyje buvo nustatyta:

„Ši direktyva netaikoma tvarkant asmens duomenis:

– kai yra užsiimama tokia veikla, kuri nepatenka į Bendrijos teisės taikymo sritį, kaip antai veikla, kuri numatyta Europos Sąjungos sutarties V ir VI dalyse, taip pat kai atliekamos tvarkymo operacijos, susijusios su visuomenės saugumu, gynyba, valstybės saugumu (taip pat ir valstybės ekonomine gerove, kai tvarkymo operacija susijusi su valstybės saugumo klausimais) ir su valstybės veiksmais baudžiamosios teisės srityje;

<…>“

4 Šios direktyvos 25 straipsnyje buvo nurodyta:

„1. Valstybės narės numato, kad asmens duomenys <…> gali būti perduodami į trečiąją šalį tik tuo atveju, jeigu nepažeidžiant nacionalinių nuostatų, priimtų pagal kitas šios direktyvos nuostatas, ši trečioji šalis užtikrina adekvatų apsaugos lygį.

2. Apsaugos, kurią suteikia trečioji šalis, lygio adekvatumas įvertinamas atsižvelgiant į duomenų perdavimo operacijos ar operacijų grupės aplinkybes; <…>

<…>

6. 31 straipsnio 2 dalyje nurodyta tvarka Komisija gali išsiaiškinti, kad adekvatų apsaugos lygį, kaip numatyta šio straipsnio 2 dalyje, trečioji šalis užtikrina savo šalies įstatymais arba tarptautiniais įsipareigojimais, kuriuos ji yra prisiėmusi, ypač po 5 dalyje nurodytų derybų dėl asmenų privataus gyvenimo ir pagrindinių laisvių bei teisių apsaugos.

Valstybės narės imasi reikiamų priemonių, kad būtų laikomasi Komisijos sprendimo.“

5 Minėtos direktyvos 26 straipsnio 2 ir 4 dalyse buvo numatyta:

„2. Nepažeisdama šio straipsnio 1 dalies nuostatų, valstybė narė gali leisti perduoti asmens duomenis į trečiąją šalį, kuri neužtikrina adekvataus apsaugos lygio pagal 25 straipsnio 2 dalį, jeigu domenų valdytojas pateikia adekvačias apsaugos priemones asmenų privatumui ir pagrindinėms teisėms bei laisvėms apsaugoti ir atitinkamoms teisėms įgyvendinti; tokios apsaugos priemonės gali būti išdėstytos atitinkamuose sutarčių punktuose.

<…>

4. Jei 31 straipsnio 2 dalyje nurodyta tvarka Komisija nusprendžia, kad atitinkami standartiniai sutarčių punktai numato pakankamas apsaugos priemones, kaip reikalauja šio straipsnio 2 dalies nuostatos, valstybės narės imasi reikalingų priemonių, kad būtų laikomasi Komisijos sprendimo.“

6 Tos pačios direktyvos 28 straipsnio 3 dalyje buvo nustatyta:

„Kiekvienai valdžios institucijai suteikiami:

– įgaliojimai tirti, kaip antai: įgaliojimai sužinoti tvarkymo operacijų turinį ar įgaliojimai surinkti visą informaciją, reikalingą priežiūros funkcijoms atlikti,

– įgaliojimai veiksmingai įsikišti, pavyzdžiui, įgaliojimai pareikšti nuomonę, iš anksto įvertinus tvarkymo operacijas pagal 20 straipsnį, ir užtikrinti, kad tokios nuomonės būtų tinkamu būdu skelbiamos viešai, taip pat įgaliojimai nurodyti blokuoti, ištrinti arba sunaikinti duomenis, laikinai arba visiškai uždrausti tvarkyti duomenis, įspėti arba papeikti duomenų valdytoją arba įgaliojimai perduoti klausimą nacionaliniams parlamentams ar kitoms politinėms institucijoms svarstyti,

– įgaliojimai dalyvauti teismo procesuose, kai pažeidžiamos pagal šią direktyvą priimtos nacionalinės nuostatos, arba atkreipti teismo institucijų dėmesį į tokius pažeidimus.

<…>“

BDAR

7 Direktyva 95/46 buvo panaikinta ir pakeista 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (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, p. 1; klaidų ištaisymas OL L 127, 2018, p. 2; toliau – BDAR).

8 BDAR 6, 10, 101, 103, 104, 107–109, 114, 116 ir 141 konstatuojamosiose dalyse nurodyta:

„(6) dėl sparčios technologinės plėtros ir globalizacijos kyla naujų asmens duomenų apsaugos sunkumų. Žymiai išaugo asmens duomenų rinkimo ir keitimosi jais mastas. Technologijos leidžia privačioms bendrovėms ir valdžios institucijoms vykdant savo veiklą naudotis asmens duomenimis precedento neturinčiu mastu. Fiziniai asmenys vis dažniau viešina asmeninę informaciją pasaulio mastu. Technologijos pakeitė ekonominį ir socialinį gyvenimą ir turėtų sudaryti dar palankesnes sąlygas laisvam asmens duomenų judėjimui Sąjungoje ir jų perdavimui į trečiąsias valstybes bei tarptautinėms organizacijoms, kartu užtikrinant aukštą asmens duomenų apsaugos lygį;

<…>

(10) siekiant užtikrinti vienodo ir aukšto lygio fizinių asmenų apsaugą ir pašalinti asmens duomenų judėjimo Sąjungoje kliūtis, visose valstybėse narėse turėtų būti užtikrinama lygiavertė asmenų teisių ir laisvių apsauga tvarkant tokius duomenis. Visoje Sąjungoje turėtų būti užtikrintas nuoseklus ir vienodas taisyklių, reglamentuojančių fizinių asmenų pagrindinių teisių ir laisvių apsaugą tvarkant asmens duomenis, taikymas. Kalbant apie asmens duomenų tvarkymą siekiant laikytis teisinės prievolės, užduoties, vykdomos dėl viešojo intereso arba vykdant duomenų valdytojui pavestas viešosios valdžios funkcijas, atlikimui valstybėms narėms turėtų būti leidžiama išlaikyti arba nustatyti nacionalines nuostatas, kuriomis konkrečiau apibrėžiamas šiame reglamente nustatytų taisyklių taikymas. Kartu su bendraisiais ir horizontaliaisiais teisės aktais dėl duomenų apsaugos, kuriais įgyvendinama Direktyva 95/46/EB, valstybės narės turi keletą konkretiems sektoriams skirtų teisės aktų srityse, kuriose reikia konkretesnių nuostatų. Šiuo reglamentu valstybėms narėms taip pat suteikiama tam tikra veiksmų laisvė nustatyti savo taisykles, be kita ko, dėl specialių kategorijų asmens duomenų (neskelbtini duomenys) tvarkymo. Todėl šiuo reglamentu neužkertamas kelias taikyti valstybės narės teisę, kurioje nustatomos konkrečių duomenų tvarkymo atvejų aplinkybės, be kita ko, tiksliau apibrėžiant sąlygas, kuriomis duomenų tvarkymas yra teisėtas;

<…>

(101) asmens duomenų judėjimas į Sąjungai nepriklausančias valstybes ir tarptautines organizacijas ir iš jų reikalingas tarptautinės prekybos plėtrai ir tarptautiniam bendradarbiavimui. Išaugus tokiam judėjimui, atsirado naujų asmens duomenų apsaugos sunkumų ir rūpesčių. Tačiau kai asmens duomenys iš Sąjungos perduodami duomenų valdytojams, duomenų tvarkytojams ar kitiems gavėjams trečiosiose valstybėse arba tarptautinėms organizacijoms, neturėtų sumažėti Sąjungoje šiuo reglamentu fiziniams asmenims garantuojamos apsaugos lygis, be kita ko, tais atvejais, kai asmens duomenys toliau perduodami iš tos trečiosios valstybės ar tarptautinės organizacijos duomenų valdytojams, duomenų tvarkytojams toje pačioje arba kitoje trečiojoje valstybėje ar kitai tarptautinei organizacijai. Bet kuriuo atveju duomenys į trečiąsias valstybes ir tarptautinėms organizacijoms gali būti perduodami tik visapusiškai laikantis šio reglamento. Duomenys galėtų būti perduodami tik tuo atveju, jei duomenų valdytojas arba duomenų tvarkytojas įvykdo šio reglamento nuostatose, susijusiose su asmens duomenų perdavimu trečiosioms šalims ar tarptautinėms organizacijoms, nustatytas sąlygas, atsižvelgiant į kitas šio reglamento nuostatas;

<…>

(103) Komisija gali nuspręsti, sprendimui galiojant visoje Sąjungoje, kad trečioji valstybė, teritorija arba nurodytas sektorius trečiojoje valstybėje, arba tarptautinė organizacija užtikrina tinkamą duomenų apsaugos lygį, ir taip garantuoti teisinį tikrumą ir vienodą teisės taikymą visoje Sąjungoje, kiek tai susiję su trečiąja valstybe ar tarptautine organizacija, kurios laikomos užtikrinančiomis tokį apsaugos lygį. Šiais atvejais asmens duomenys į tokią trečią valstybę gali būti perduodami be papildomo leidimo. Komisija, įspėjusi trečiąją valstybę ar tarptautinę organizaciją ir pateikusi jai išsamias priežastis, taip pat gali nuspręsti tokį sprendimą atšaukti;

(104) atsižvelgdama į pagrindines vertybes, kuriomis grindžiama Sąjunga, visų pirma į žmogaus teisių apsaugą, Komisija, vertindama trečiąją šalį arba teritoriją, arba nurodytą sektorių trečiojoje šalyje, turėtų atsižvelgti į tai, kaip atitinkama trečioji šalis laikosi teisinės valstybės, teisės kreiptis į teismą principų, tarptautinių žmogaus teisių normų ir standartų, taip pat savo bendros ir sektorių teisės, įskaitant visuomenės saugumą, gynybą ir nacionalinį saugumą reglamentuojančius teisės aktus, ir viešosios tvarkos bei baudžiamosios teisės. Priimant teritorijai arba nurodytam sektoriui trečiojoje šalyje skirtą sprendimą dėl tinkamumo turėtų būti atsižvelgiama į aiškius ir objektyvius kriterijus, pavyzdžiui, konkrečią duomenų tvarkymo veiklą ir trečiojoje šalyje taikytinų teisinių standartų bei galiojančių teisės aktų taikymo sritį. Trečioji šalis turėtų suteikti garantijas, kuriomis būtų užtikrinama atitinkamo lygio apsauga, iš esmės lygiavertė Sąjungoje garantuojamai apsaugai, visų pirma tada, kai asmens duomenys tvarkomi viename ar keliuose nurodytuose sektoriuose. Visų pirma trečioji valstybė turėtų užtikrinti veiksmingą nepriklausomą duomenų apsaugos priežiūrą ir turėtų nustatyti bendradarbiavimo su valstybių narių duomenų apsaugos institucijomis mechanizmus, o duomenų subjektams turėtų būti užtikrintos veiksmingos bei įgyvendinamos teisės ir galimybė naudotis veiksmingomis administracinėmis ir teisminėmis teisių gynimo priemonėmis;

<…>

(107) Komisija gali pripažinti, kad trečioji valstybė, teritorija arba nurodytas sektorius trečiojoje valstybėje, arba tarptautinė organizacija nebeužtikrina tinkamo lygio duomenų apsaugos. Todėl perduoti asmens duomenis tai trečiajai šaliai arba tarptautinei organizacijai turėtų būti draudžiama, išskyrus atvejus, kai įvykdomi šiame reglamente nustatyti reikalavimai, susiję su perdavimu taikant tinkamas apsaugos priemones, įskaitant įmonei privalomas taisykles ir nukrypti leidžiančias nuostatas konkrečiais atvejais. Tokiu atveju turėtų būti numatyta, kad Komisija konsultuojasi su tokiomis trečiosiomis valstybėmis arba tarptautinėmis organizacijomis. Komisija turėtų laiku informuoti trečiąją valstybę arba tarptautinę organizaciją apie priežastis ir pradėti su ja konsultacijas, kad ji galėtų ištaisyti padėtį;

(108) jei sprendimas dėl tinkamumo nepriimtas, duomenų valdytojas arba duomenų tvarkytojas turėtų duomenų subjektams numatyti tinkamas apsaugos priemones nepakankamai duomenų apsaugai trečiojoje valstybėje kompensuoti. Tokios tinkamos apsaugos priemonės galėtų būti rėmimasis įmonei privalomomis taisyklėmis, Komisijos priimtomis standartinėmis duomenų apsaugos sąlygomis, priežiūros institucijos priimtomis standartinėmis duomenų apsaugos sąlygomis arba priežiūros institucijos pripažintomis sutarties sąlygomis. Tomis apsaugos priemonėmis turėtų būti užtikrinama, kad būtų laikomasi duomenų apsaugos reikalavimų, ir užtikrinamos tvarkant duomenis Sąjungoje tinkamos duomenų subjektų teisės, įskaitant galimybes naudotis vykdytinomis [įgyvendinamomis] duomenų subjekto teisėmis ir veiksmingomis teisių gynimo priemonėmis, be kita ko, naudotis veiksmingomis administracinėmis ar teisminėmis teisių gynimo priemonėmis ir reikalauti kompensacijos Sąjungoje ar trečiojoje valstybėje. Jos turėtų būti susijusios visų pirma su bendrųjų asmens duomenų tvarkymo principų, pritaikytosios ir standartizuotosios duomenų apsaugos principų laikymųsi; <…>

(109) galimybė duomenų valdytojui arba duomenų tvarkytojui remtis Komisijos ar priežiūros institucijos priimtomis standartinėmis duomenų apsaugos sąlygomis neturėtų užkirsti kelio duomenų valdytojams arba duomenų tvarkytojams standartines duomenų apsaugos sąlygas įtraukti į platesnes sutartis, tokias kaip duomenų tvarkytojo sutartis su kitais duomenų tvarkytojais, ar jas papildyti kitomis sąlygomis ar papildomomis apsaugos sąlygomis, jei jos tiesiogiai ar netiesiogiai neprieštarauja Komisijos ar priežiūros institucijos priimtoms standartinėms sutarčių sąlygoms ar nedaro poveikio duomenų subjektų pagrindinėms teisėms ir laisvėms. Duomenų valdytojai ir duomenų tvarkytojai turėtų būti skatinami taikyti dar griežtesnes apsaugos priemones numatant sutartinius įsipareigojimus, papildančius standartines duomenų apsaugos sąlygas;

<…>

(114) bet kuriuo atveju, kai Komisija nėra priėmusi sprendimo dėl tinkamo duomenų apsaugos lygio trečiojoje valstybėje, duomenų valdytojas arba duomenų tvarkytojas turėtų rinktis tokias galimybes, kuriomis duomenų subjektams užtikrinamos vykdytinos [įgyvendinamos] ir veiksmingos teisės jų duomenų tvarkymo Sąjungoje atžvilgiu, kai tie duomenys yra perduoti, kad jie ir toliau galėtų naudotis pagrindinėmis teisėmis ir apsaugos priemonėmis;

<…>

(116) kai asmens duomenys perduodami iš vienos valstybės į kitą už Sąjungos ribų, asmenims gali būti daug sunkiau pasinaudoti teisėmis į duomenų apsaugą, visų pirma apsisaugoti nuo neteisėto tų duomenų naudojimo arba atskleidimo. Be to, priežiūros institucijos gali nesugebėti nagrinėti skundų ar vykdyti tyrimų, susijusių su veikla už jų valstybės sienų. Jų pastangoms bendradarbiauti tarpvalstybiniu mastu taip pat gali kliudyti nepakankami įgaliojimai imtis prevencinių ar taisomųjų veiksmų, nenuoseklus teisinis reglamentavimas ir praktinės kliūtys, pavyzdžiui, riboti ištekliai <…>

<…>

(141) kiekvienas duomenų subjektas turėtų turėti teisę pateikti skundą vienai priežiūros institucijai, visų pirma valstybėje narėje, kurioje yra jo įprastinė gyvenamoji vieta, ir turėti teisę į veiksmingą teisminę teisių gynimo priemonę pagal Chartijos 47 straipsnį, jeigu duomenų subjektas mano, kad jo teisės pagal šį reglamentą yra pažeistos arba jeigu priežiūros institucija nesiima veiksmų dėl skundo, iš dalies arba visiškai atmeta skundą arba jo nepriima, arba nesiima veiksmų, kai tokie veiksmai yra būtini duomenų subjekto teisėms apsaugoti. <…>“

9 Šio reglamento 2 straipsnio 1 ir 2 dalyse numatyta:

„1. Šis reglamentas taikomas asmens duomenų tvarkymui, visiškai arba iš dalies atliekamam automatizuotomis priemonėmis, ir asmens duomenų, kurie sudaro susisteminto rinkinio dalį ar yra skirti ją sudaryti, tvarkymui ne automatizuotomis priemonėmis.

2. Šis reglamentas netaikomas asmens duomenų tvarkymui, kai:

a) duomenys tvarkomi vykdant veiklą, kuriai Sąjungos teisė netaikoma;

b) duomenis tvarko valstybės narės, vykdydamos veiklą, kuriai taikomas ES sutarties V antraštinės dalies 2 skyrius;

c) duomenis tvarko fizinis asmuo, užsiimdamas išimtinai asmenine ar namų ūkio veikla;

d) duomenis tvarko kompetentingos valdžios institucijos nusikalstamų veikų prevencijos, tyrimo, nustatymo ar patraukimo baudžiamojon atsakomybėn už jas, baudžiamųjų sankcijų vykdymo, įskaitant apsaugą nuo grėsmių visuomenės saugumui ir jų prevenciją, tikslais.“

10 Minėto reglamento 4 straipsnyje nurodyta:

„Šiame reglamente:

<…>

2) duomenų tvarkymas – bet kokia automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis ar asmens duomenų rinkiniais atliekama operacija ar operacijų seka, kaip antai rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, išgava, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimas arba sunaikinimas;

<…>

7) duomenų valdytojas – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuris vienas ar drauge su kitais nustato duomenų tvarkymo tikslus ir priemones; kai tokio duomenų tvarkymo tikslai ir priemonės nustatyti Sąjungos arba valstybės narės teisės, duomenų valdytojas arba konkretūs jo skyrimo kriterijai gali būti nustatyti Sąjungos arba valstybės narės teise;

8) duomenų tvarkytojas – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri duomenų valdytojo vardu tvarko asmens duomenis;

9) duomenų gavėjas – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuriai atskleidžiami asmens duomenys, nesvarbu, ar tai trečioji šalis ar ne. Tačiau valdžios institucijos, kurios pagal Sąjungos arba valstybės narės teisę gali gauti asmens duomenis vykdydamos konkretų tyrimą, nelaikomos duomenų gavėjais; tvarkydamos tuos duomenis, tos valdžios institucijos laikosi taikomų duomenų tvarkymo tikslus atitinkančių duomenų apsaugos taisyklių;

<…>“

11 To paties reglamento 23 straipsnyje nustatyta:

„1. Sąjungos ar valstybės narės teise, kuri taikoma duomenų valdytojui arba duomenų tvarkytojui, teisėkūros priemone gali būti apribotos 12–22 straipsniuose ir 34 straipsnyje, taip pat 5 straipsnyje tiek, kiek jo nuostatos atitinka 12–22 straipsniuose numatytas teises ir prievoles, nustatytos prievolės ir teisės, kai tokiu apribojimu gerbiama pagrindinių teisių ir laisvių esmė ir jis demokratinėje visuomenėje yra būtina ir proporcinga priemonė siekiant užtikrinti:

a) nacionalinį saugumą;

b) gynybą;

c) visuomenės saugumą;

d) nusikalstamų veikų prevenciją, tyrimą, nustatymą ar patraukimą už jas baudžiamojon atsakomybėn arba baudžiamųjų sankcijų vykdymą, įskaitant apsaugą nuo grėsmių visuomenės saugumui ir jų prevenciją;

<…>

2. Visų pirma visose 1 dalyje nurodytose teisėkūros priemonėse pateikiamos konkrečios nuostatos, susijusios tam tikrais atvejais bent su:

a) duomenų tvarkymo tikslais arba duomenų tvarkymo kategorijomis,

b) asmens duomenų kategorijomis,

c) nustatytų apribojimų apimtimi,

d) apsaugos priemonėmis, kuriomis siekiama užkirsti kelią piktnaudžiavimui arba neteisėtam susipažinimui su duomenimis ar jų perdavimui,

e) duomenų valdytojo arba duomenų valdytojų kategorijų apibūdinimu,

f) saugojimo laikotarpiais ir taikytinomis apsaugos priemonėmis, atsižvelgiant į duomenų tvarkymo arba duomenų tvarkymo kategorijų pobūdį, aprėptį ir tikslus,

g) pavojais duomenų subjektų teisėms ir laisvėms, ir

h) duomenų subjektų teise būti informuotiems apie apribojimą, nebent tai pakenktų apribojimo tikslui.“

12 BDAR V skyriuje „Asmens duomenų perdavimai į trečiąsias valstybes arba tarptautinėms organizacijoms“ yra šio reglamento 44–50 straipsniai. Šio reglamento 44 straipsnyje „Bendras duomenų perdavimo principas“ nustatyta:

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

13 Šio reglamento 45 straipsnio „Duomenų perdavimas remiantis sprendimu dėl tinkamumo“ 1–3 dalyse numatyta:

„1. Perduoti asmens duomenis į trečiąją valstybę arba tarptautinei organizacijai galima, jeigu Komisija nusprendė, kad atitinkama trečioji valstybė, teritorija arba vienas ar daugiau nurodytų sektorių toje trečiojoje valstybėje, arba atitinkama tarptautinė organizacija užtikrina tinkamo lygio apsaugą. Tokiam duomenų perdavimui specialaus leidimo nereikia.

2. Vertindama apsaugos lygio tinkamumą, Komisija visų pirma atsižvelgia į šiuos aspektus:

a) teisinės valstybės principą, pagarbą žmogaus teisėms ir pagrindinėms laisvėms, 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, duomenų apsaugos taisykles, profesines taisykles ir saugumo priemones, įskaitant taisykles dėl tolesnio asmens duomenų perdavimo į kitą trečiąją valstybę ar kitai tarptautinei organizacijai, kurių laikomasi toje valstybėje arba kurių laikosi ta tarptautinė organizacija, teismų praktikos precedentus, taip pat veiksmingas ir vykdytinas [įgyvendinamas] duomenų subjektų teises ir veiksmingas administracines bei teismines duomenų subjektų, kurių asmens duomenys yra perduodami, teisių gynimo priemones;

b) tai, ar yra ir ar veiksmingai veikia viena ar kelios nepriklausomos priežiūros institucijos trečiojoje šalyje arba kurioms yra pavaldi tarptautinė organizacija ir kurių atsakomybė yra užtikrinti, kad būtų laikomasi duomenų apsaugos taisyklių ir jos būtų vykdomos, įskaitant tinkamus vykdymo įgaliojimus padėti duomenų subjektams naudotis savo teisėmis ir patarti, kaip tai daryti, ir bendradarbiauti su valstybių narių priežiūros institucijomis; ir

c) atitinkamos trečiosios valstybės arba tarptautinės organizacijos prisiimtus tarptautinius įsipareigojimus ar kitus įsipareigojimus, atsirandančius dėl teisiškai privalomų konvencijų ar priemonių, taip pat dėl jų dalyvavimo daugiašalėse ar regioninėse sistemose, visų pirma kiek tai susiję su asmens duomenų apsauga.

3. Komisija, įvertinusi apsaugos lygio tinkamumą, gali nuspręsti, priimdama įgyvendinimo aktą, kad trečioji valstybė, teritorija arba vienas ar daugiau nurodytų sektorių toje trečiojoje valstybėje, arba tarptautinė organizacija užtikrina tinkamo lygio apsaugą, kaip apibrėžta šio straipsnio 2 dalyje. Įgyvendinimo akte numatomas periodinės peržiūros, atliekamos bent kas ketverius metus, kuria atsižvelgiama į visus atitinkamus pokyčius trečiojoje valstybėje ar tarptautinėje organizacijoje, mechanizmas. Įgyvendinimo akte nustatoma jo teritorinė ir sektorinė taikymo sritis ir, kai taikoma, nurodoma šio straipsnio 2 dalies b punkte nurodyta priežiūros institucija ar institucijos. Įgyvendinimo aktas priimamas laikantis 93 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.“

14 Minėto reglamento 46 straipsnio „Duomenų perdavimas taikant tinkamas apsaugos priemones“ 1–3 dalyse nurodyta:

„1. Jeigu nėra priimtas sprendimas pagal 45 straipsnio 3 dalį, duomenų valdytojas arba duomenų tvarkytojas gali perduoti asmens duomenis į trečiąją valstybę arba tarptautinei organizacijai tik tuo atveju, jeigu duomenų valdytojas arba duomenų tvarkytojas yra nustatęs tinkamas apsaugos priemones, su sąlyga, kad suteikiama galimybė naudotis vykdytinomis [įgyvendinamomis] duomenų subjektų teisėmis ir veiksmingomis duomenų subjektų teisių gynimo priemonėmis.

2. 1 dalyje nurodytos tinkamos apsaugos priemonės, nereikalaujant specialaus priežiūros institucijos leidimo, gali būti nustatomos:

a) teisiškai privalomu ir vykdytinu valdžios institucijų arba įstaigų tarpusavio dokumentu;

b) įmonėms privalomomis taisyklėmis pagal 47 straipsnį;

c) standartinėmis duomenų apsaugos sąlygomis, kurias Komisija priima laikydamasi 93 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros;

d) standartinėmis duomenų apsaugos sąlygomis, kurias priima priežiūros institucija ir pagal 93 straipsnio 2 dalyje nurodytą nagrinėjimo procedūrą patvirtina Komisija;

e) patvirtintu elgesio kodeksu pagal 40 straipsnį kartu su privalomais ir vykdytinais duomenų valdytojo arba duomenų tvarkytojo trečiojoje valstybėje įsipareigojimais taikyti tinkamas apsaugos priemones, be kita ko, susijusias su duomenų subjektų teisėmis; arba

f) patvirtintu sertifikavimo mechanizmu pagal 42 straipsnį kartu su privalomais ir vykdytinais duomenų valdytojo arba duomenų tvarkytojo trečiojoje valstybėje įsipareigojimais taikyti tinkamas apsaugos priemones, be kita ko, susijusias su duomenų subjektų teisėmis.

3. Gavus kompetentingos priežiūros institucijos leidimą, 1 dalyje nurodytos tinkamos apsaugos priemonės taip pat gali būti nustatomos, visų pirma:

a) duomenų valdytojo arba duomenų tvarkytojo ir duomenų valdytojo, duomenų tvarkytojo arba asmens duomenų gavėjo trečiojoje valstybėje arba tarptautinės organizacijos sutarčių sąlygomis; arba

b) nuostatomis, kurios turi būti įtrauktos į valdžios institucijų arba įstaigų tarpusavio administracinius susitarimus, kuriais numatomos vykdytinos [įgyvendinamos] ir veiksmingos duomenų subjektų teisės.“

15 To paties reglamento 49 straipsnyje „Nukrypti leidžiančios nuostatos konkrečiais atvejais“ nustatyta:

„1. Jeigu nepriimtas sprendimas dėl tinkamumo pagal 45 straipsnio 3 dalį arba nenustatytos tinkamos apsaugos priemonės pagal 46 straipsnį, įskaitant įmonei privalomas taisykles, asmens duomenų perdavimas į trečiąją valstybę arba tarptautinei organizacijai arba tokių perdavimų seka atliekami tik su viena iš šių sąlygų:

a) duomenų subjektas aiškiai sutiko su siūlomu duomenų perdavimu po to, kai buvo informuotas apie galimus tokių perdavimų pavojus duomenų subjektui dėl to, kad nepriimtas sprendimas dėl tinkamumo ir nenustatytos tinkamos apsaugos priemonės;

b) duomenų perdavimas yra būtinas duomenų subjekto ir duomenų valdytojo sutarčiai vykdyti arba ikisutartinėms priemonėms, kurių imtasi duomenų subjekto prašymu, įgyvendinti;

c) duomenų perdavimas yra būtinas, kad būtų sudaryta arba įvykdyta duomenų subjekto interesais sudaroma duomenų valdytojo ir kito fizinio ar juridinio asmens sutartis;

d) duomenų perdavimas yra būtinas dėl svarbių viešojo intereso priežasčių;

e) duomenų perdavimas yra būtinas siekiant pareikšti, vykdyti ar ginti teisinius reikalavimus;

f) duomenų perdavimas yra būtinas, kad būtų apsaugoti gyvybiniai duomenų subjekto arba kitų asmenų interesai, jeigu duomenų subjektas dėl fizinių ar teisinių priežasčių negali duoti sutikimo;

g) duomenys perduodami iš registro, pagal Sąjungos arba valstybės narės teisę skirto teikti informaciją visuomenei, su kuria gali susipažinti plačioji visuomenė arba bet kuris asmuo, galintis įrodyti teisėtą interesą, tačiau tik tiek, kiek konkrečiu atveju laikomasi pagal Sąjungos arba valstybės narės teisę nustatytų susipažinimo su tokiame registre esančia informacija sąlygų.

Kai perdavimas negali būti grindžiamas 45 arba 46 straipsnio nuostata, įskaitant nuostatas dėl įmonei privalomų taisyklių, ir netaikoma jokia pirmoje pastraipoje nurodyta konkrečioje situacijoje nukrypti leidžianti nuostata, perdavimas [į trečiąją šalį ar tarptautinei organizacijai galimas, jeigu] nėra kartojamas, yra susijęs tik su ribotu duomenų subjektų skaičiumi, yra būtinas įtikinamų [imperatyvių] duomenų valdytojo ginamų teisėtų interesų, kai nėra už juos viršesnių duomenų subjekto interesų ar teisių ir laisvių, tikslais, jeigu duomenų valdytojas yra įvertinęs visas su duomenų perdavimu susijusias aplinkybes ir, remdamasis tuo vertinimu, yra nustatęs tinkamas su asmens duomenų apsauga susijusias apsaugos priemones. Duomenų valdytojas praneša priežiūros institucijai apie duomenų perdavimą. Be 13 ir 14 straipsniuose nurodytos informacijos, duomenų valdytojas praneša duomenų subjektui apie duomenų perdavimą ir apie įtikinamus [imperatyvius] ginamus teisėtus interesus.

2. Jeigu duomenys perduodami pagal 1 dalies pirmos pastraipos g punktą, negali būti perduodami visi registre esantys asmens duomenys arba visi registre esantys tam tikrų kategorijų asmens duomenys. Jeigu registras yra skirtas tam, kad su jame esančia informacija susipažintų teisėtų interesų turintys asmenys, duomenys perduodami tik tų asmenų prašymu arba jeigu tie asmenys bus tų duomenų gavėjai.

3. 1 dalies pirmos pastraipos a, b ir c punktai bei jos antra pastraipa netaikomi veiklai, kurią valdžios institucijos atlieka vykdydamos savo viešuosius įgaliojimus.

4. 1 dalies pirmos pastraipos d punkte nurodytas viešasis interesas turi būti pripažintas Sąjungos teise arba duomenų valdytojui taikomos valstybės narės teise.

5. Jei sprendimas dėl tinkamumo nepriimtas, Sąjungos arba valstybės narės teisėje dėl svarbių viešojo intereso priežasčių gali būti aiškiai nustatytos konkrečių kategorijų asmens duomenų perdavimo į trečiąją valstybę ar tarptautinei organizacijai ribos. Valstybės narės tokias nuostatas praneša Komisijai.

6. Duomenų valdytojas arba duomenų tvarkytojas 30 straipsnyje nurodytuose įrašuose dokumentais pagrindžia vertinimą ir šio straipsnio 1 dalies antroje pastraipoje nurodytas tinkamas apsaugos priemones.“

16 BDAR 51 straipsnio 1 dalyje nustatyta:

„Kiekviena valstybė narė užtikrina, kad viena arba kelios nepriklausomos valdžios institucijos yra atsakingos už šio reglamento taikymo stebėseną, kad būtų apsaugotos fizinių asmenų pagrindinės teisės ir laisvės tvarkant duomenis ir sudarytos palankesnės sąlygos laisvam asmens duomenų judėjimui Sąjungoje (toliau – priežiūros institucija).“

17 Pagal šio reglamento 55 straipsnio 1 dalį „[k]iekviena priežiūros institucija turi kompetenciją savo valstybės narės teritorijoje vykdyti pagal šį reglamentą jai pavestas užduotis ir naudotis pagal šį reglamentą jai suteiktais įgaliojimais“.

18 Minėto reglamento 57 straipsnio 1 dalyje numatyta:

„Nedarant poveikio kitoms pagal šį reglamentą nustatytoms užduotims, kiekviena priežiūros institucija savo teritorijoje:

a) stebi, kaip taikomas šis reglamentas, ir užtikrina, kad jis būtų taikomas;

<…>

f) nagrinėja skundus, kuriuos <…> pateikė duomenų subjektas <…>, ir tinkamu mastu tiria skundo dalyką, taip pat per pagrįstą laikotarpį informuoja skundo pateikėją apie skundo tyrimo pažangą ir rezultatus, visų pirma tais atvejais, kai būtina tęsti tyrimą arba derinti veiksmus su kita priežiūros institucija;

<…>“

19 To paties reglamento 58 straipsnio 2 ir 4 dalyse nustatyta:

„2. Kiekviena priežiūros institucija turi visus šiuos įgaliojimus imtis taisomųjų veiksmų:

<…>

f) nustatyti laikiną arba galutinį duomenų tvarkymo apribojimą, įskaitant tvarkymo draudimą;

<…>

j) nurodyti sustabdyti duomenų srautus duomenų gavėjui trečiojoje valstybėje arba tarptautinei organizacijai.

<…>

4. Naudojimuisi pagal šį straipsnį priežiūros institucijai suteiktais įgaliojimais taikomos atitinkamos apsaugos priemonės, įskaitant veiksmingą apskundimą teismine tvarka ir tinkamą procesą, kaip nustatyta Sąjungos ir valstybės narės teisėje, laikantis Chartijos.“

20 BDAR 64 straipsnio 2 dalyje nurodyta:

„Bet kuri priežiūros institucija, [Europos duomenų apsaugos valdybos (EDAV)] pirmininkas arba Komisija gali prašyti, kad Valdyba išnagrinėtų bet kurį bendro pobūdžio klausimą arba klausimą, kuris daro poveikį daugiau nei vienoje valstybėje narėje, ir kad ji pateiktų nuomonę, visų pirma tais atvejais, kai kompetentinga priežiūros institucija nesilaiko su savitarpio pagalba susijusių prievolių pagal 61 straipsnį arba su bendromis operacijomis susijusių prievolių pagal 62 straipsnį.“

21 Šio reglamento 65 straipsnio 1 dalyje nustatyta:

„Siekiant užtikrinti tinkamą ir nuoseklų šio reglamento taikymą atskirais atvejais, Valdyba priima privalomą sprendimą šiais atvejais:

<…>

c) jeigu kompetentinga priežiūros institucija neprašo Valdybos pateikti nuomonę 64 straipsnio 1 dalyje nurodytais atvejais arba nesilaiko pagal 64 straipsnį pateiktos Valdybos nuomonės. Tuo atveju bet kuri susijusi priežiūros institucija arba Komisija gali pranešti apie šį klausimą Valdybai.“

22 Minėto reglamento 77 straipsnyje „Teisė pateikti skundą priežiūros institucijai“ nurodyta:

„1. Neapribojant galimybių imtis kitų administracinių arba teisminių teisių gynimo priemonių, kiekvienas duomenų subjektas turi teisę pateikti skundą priežiūros institucijai, visų pirma valstybėje narėje, kurioje yra jo nuolatinė gyvenamoji vieta, darbo vieta arba vieta, kurioje padarytas įtariamas pažeidimas, jeigu tas duomenų subjektas mano, kad su juo susijęs asmens duomenų tvarkymas atliekamas pažeidžiant šį reglamentą.

2. Priežiūros institucija, kuriai pateiktas skundas, informuoja skundo pateikėją apie skundo nagrinėjimo pažangą ir rezultatus, be kita ko, apie galimybę imtis teisminių teisių gynimo priemonių pagal 78 straipsnį.“

23 To paties reglamento 78 straipsnio „Teisė imtis veiksmingų teisminių teisių gynimo priemonių prieš priežiūros instituciją“ 1 ir 2 dalyse numatyta:

„1. Nedarant poveikio galimybei imtis kitų administracinių arba neteisminių teisių gynimo priemonių, kiekvienas fizinis ar juridinis asmuo turi teisę imtis veiksmingų teisminių teisių gynimo priemonių prieš priežiūros institucijos dėl jo priimtą teisiškai privalomą sprendimą.

2. Nedarant poveikio galimybei imtis kitų administracinių arba neteisminių teisių gynimo priemonių, kiekvienas duomenų subjektas turi teisę imtis veiksmingų teisminių teisių gynimo priemonių, jeigu priežiūros institucija, kuri yra kompetentinga pagal 55 straipsnį ir 56 straipsnius, skundo nenagrinėja arba per tris mėnesius nepraneša duomenų subjektui apie pagal 77 straipsnį pateikto skundo nagrinėjimo pažangą arba rezultatus.“

24 BDAR 94 straipsnyje nurodyta:

„1. Direktyva [95/46] panaikinama nuo 2018 m. gegužės 25 d.

2. Nuorodos į panaikintą direktyvą laikomos nuorodomis į šį reglamentą. Nuorodos į Direktyvos [95/46] 29 straipsniu įsteigtą Darbo grupę asmenų apsaugai tvarkant asmens duomenis laikomos nuorodomis į šiuo reglamentu įsteigtą Europos duomenų apsaugos valdybą.“

25 Šio reglamento 99 straipsnyje nustatyta:

„1. Šis reglamentas įsigalioja dvidešimtą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

2. Jis taikomas nuo 2018 m. gegužės 25 d.“

SAS sprendimas

26 SAS sprendimo 11 konstatuojamoji dalis suformuluota taip:

„Įgyvendinant šį sutarčių mechanizmą valstybių narių priežiūros institucijoms tenka svarbus vaidmuo – jos užtikrina, kad po perdavimo asmens duomenys būtų tinkamai apsaugoti. Išskirtiniais atvejais, kai duomenų eksportuotojai atsisako ar negali duoti tinkamų nurodymų duomenų importuotojui, ir todėl duomenų subjektams iškyla didelės žalos grėsmė, standartinės sutarčių sąlygos turėtų leisti priežiūros institucijoms atlikti duomenų importuotojų ir pagalbinių duomenų tvarkytojų patikrinimus ir, tam tikrais atvejais, priimti duomenų importuotojus ir pagalbinius duomenų tvarkytojus įpareigojančius sprendimus. Priežiūros institucijoms turėtų būti suteikta teisė sutarčių standartinių sąlygų pagrindu uždrausti ar sustabdyti duomenų perdavimą ar kelis duomenų perdavimus tais išimtiniais atvejais, kai nustatoma, jog pagal sutartį atliekamas duomenų perdavimas gali labai neigiamai paveikti garantijas ir įsipareigojimus, kuriais suteikiama tinkama apsauga duomenų subjektui.“

27 Šio sprendimo 1 straipsnyje nurodyta:

„Priede pateiktos standartinės sutarčių sąlygos laikomos užtikrinančiomis tinkamas apsaugos priemones pagal Direktyvos [95/46] 26 straipsnio 2 dalies reikalavimus, ginant privatumo teisę ir pagrindines asmens teises ir laisves, susijusias su atitinkamų teisių įgyvendinimu.“

28 Pagal minėto sprendimo 2 straipsnio antrą pastraipą jis „taikomas Europos Sąjungoje įsikūrusių duomenų valdytojų atliekamam asmens duomenų perdavimui gavėjams, kurie yra įsikūrę už Europos Sąjungos teritorijos ribų ir veikia tik kaip duomenų tvarkytojai“.

29 To paties sprendimo 3 straipsnyje nurodyta:

„Šio sprendimo tikslais taikomos šios apibrėžtys:

<…>

c) „duomenų eksportuotojas“ – duomenų valdytojas, kuris perduoda asmens duomenis;

d) „duomenų importuotojas“ – trečiojoje šalyje įsikūręs duomenų tvarkytojas, sutinkantis iš duomenų eksportuotojo gauti asmens duomenis ir gautus duomenis tvarkyti duomenų eksportuotojo vardu, laikydamasis jo duotų nurodymų bei šio sprendimo sąlygų, ir nepriklausantis trečiosios šalies tinkamos apsaugos užtikrinimo sistemai, kaip nustatyta [Direktyvos 95/46] 25 straipsnio 1 dalyje;

<…>

f) „taikytina duomenų apsaugos teisė“ – teisės aktai, ginantys pagrindines asmenų teises ir laisves (ypač jų teisę į privatų gyvenimą) tvarkant asmens duomenis, kurių turi laikytis duomenų valdytojas toje valstybėje narėje, kurioje įsikūręs duomenų eksportuotojas;

<…>“

30 Sprendimo 2010/87 4 straipsnio redakcijos, galiojusios prieš įsigaliojant Įgyvendinimo sprendimui 2016/2297, buvo numatyta:

„1. Nepažeidžiant valstybių narių kompetentingų institucijų teisių imtis veiksmų, kad būtų užtikrintas nacionalinių nuostatų, priimtų įgyvendinant Direktyvos [95/46] II, III, V ir VI skirsnių reikalavimus, vykdymas, jos gali pasinaudoti joms suteiktomis teisėmis uždrausti ar sustabdyti duomenų srautus į trečiąsias šalis, kad apsaugotų asmenis, kurių asmens duomenys yra tvarkomi, jeigu:

a) nustatoma, kad teisės aktu, kurio turi laikytis duomenų importuotojas arba pagalbinis duomenų tvarkytojas, jam keliami reikalavimai verčia nukrypti nuo taikomos duomenų apsaugos teisės ir tie reikalavimai viršija [Direktyvos 95/46] 13 straipsnyje nustatytus apribojimus, reikalingus demokratinėje visuomenėje, jei tie reikalavimai gali ypač neigiamai paveikti taikytiname [taikytinoje] duomenų apsaugos teisėje ar standartinėse sutarčių sąlygose nustatytas garantijas;

b) kompetentinga institucija nustato, kad duomenų importuotojas arba pagalbinis duomenų tvarkytojas nevykdo priede pateiktų standartinių sutarčių sąlygų; arba

c) yra reali tikimybė, kad priede pateiktos standartinės sutarčių sąlygos yra nevykdomos arba bus nevykdomos ir kad toliau perduodant duomenis duomenų subjektams iškils didelės žalos grėsmė.

2. Pagal 1 dalies sąlygas paskelbtas draudimas ar sustabdymas turi būti panaikintas iškart, kai tik nebelieka sustabdymo ar draudimo priežasčių.

3. Valstybės narės, priėmusios priemones pagal 1 ir 2 dalių sąlygas, privalo neatidėliodamos apie jas pranešti Komisijai, o Komisija tą informaciją perduos kitoms valstybėms narėms.“

31 Įgyvendinimo sprendimo 2016/2297, priimto paskelbus 2015 m. spalio 6 d. Sprendimą *Schrems* (C-362/14, EU:C:2015:650), 5 konstatuojamoji dalis suformuluota taip:

„*mutatis mutandis*, pagal Direktyvos [95/46] 26 straipsnio 4 dalį priimtas Komisijos sprendimas yra privalomas visoms valstybių narių institucijoms, kurioms jis skirtas, įskaitant jų nepriklausomas priežiūros institucijas, nes šiuo sprendimu pripažįstama, kad asmens duomenys yra perduodami remiantis jame nurodytomis standartinėmis sutarčių sąlygomis, kuriomis užtikrinama pakankama apsauga, kaip reikalaujama pagal tos direktyvos 26 straipsnio 2 dalį. Tai neužkerta kelio nacionalinei priežiūros institucijai naudotis savo įgaliojimais prižiūrėti duomenų srautus, įskaitant įgaliojimus sustabdyti arba uždrausti asmens duomenų perdavimą, kuomet ji nustato, kad duomenys perduodami pažeidžiant ES arba nacionalinės duomenų apsaugos teisės aktus, pavyzdžiui, kai duomenų importuotojas nesilaiko standartinių sutarčių sąlygų.“

32 Dabartinės redakcijos SAS sprendimo 4 straipsnyje, įtvirtintame Įgyvendinimo sprendimu 2016/2297, nustatyta:

„Kai valstybių narių kompetentingos institucijos įgyvendina savo įgaliojimus pagal Direktyvos [95/46] 28 straipsnio 3 dalį ir dėl šios priežasties sustabdomi arba neribotam laikui uždraudžiami duomenų srautai į trečiąsias šalis, kad apsaugotų asmenis atsižvelgiant į jų asmens duomenų tvarkymą, atitinkama valstybė narė nedelsdama informuoja Komisiją, kuri šią informaciją perduoda kitoms valstybėms narėms.“

33 SAS sprendimo priede „Standartinės sutarčių sąlygos (duomenų tvarkytojai)“ išdėstyta dvylika standartinių sąlygų. Šio priedo 3 sąlygoje „Trečiosios šalies naudos gavėjos sąlyga“ numatyta:

„1. Duomenų subjektas gali iškelti ieškinį duomenų eksportuotojui kaip trečiajai šaliai naudos gavėjai pagal šią sąlygą, 4 sąlygos b–i punktus, 5 sąlygos a–e ir g–j punktus, 6 sąlygos 1–2 dalis, 7 sąlygą, 8 sąlygos 2 dalį ir 9–12 sąlygas [Duomenų subjektas gali remtis šia sąlyga, 4 sąlygos b–i punktais, 5 sąlygos a–e ir g–j punktais, 6 sąlygos 1–2 dalimis, 7 sąlyga, 8 sąlygos 2 dalimi ir 9–12 sąlygomis prieš duomenų eksportuotoją kaip trečiosios šalies naudos gavėjas].

2. Duomenų subjektas gali iškelti ieškinį duomenų importuotojui pagal šią sąlygą, 5 sąlygos a–e ir g punktus, 6 sąlygą, 7 sąlygą, 8 sąlygos 2 dalį ir 9–12 sąlygas tais atvejais, kai duomenų eksportuotojas yra faktiškai dingęs, teisiškai nutraukė savo veiklą arba tapo nemokus, išskyrus atvejus, kai visus duomenų eksportuotojo teisinius įsipareigojimus sutartimi arba teisiniais veiksmais perėmė veiklos tęsėjas [Duomenų subjektas gali remtis šia sąlyga, 5 sąlygos a–e ir g punktais, 6 sąlyga, 7 sąlyga, 8 sąlygos 2 dalimi ir 9–12 sąlygomis prieš duomenų importuotoją tais atvejais, kai duomenų eksportuotojas yra faktiškai dingęs, teisiškai nutraukė savo veiklą arba tapo nemokus, išskyrus atvejus, kai visus duomenų eksportuotojo teisinius įsipareigojimus sutartimi arba pagal įstatymą perėmė veiklos tęsėjas]. Jis prisiima duomenų eksportuotojo teises ir įsipareigojimus, ir tokiu atveju duomenų subjektas gali iškelti tokiai įstaigai ieškinį [Jis prisiima duomenų eksportuotojo teises ir įsipareigojimus ir tokiu atveju duomenų subjektas gali [remtis tomis sąlygomis prieš šį asmenį].

<…>“

34 Šio priedo 4 sąlyga „Duomenų eksportuotojo įsipareigojimai“ suformuluota taip:

„Duomenų eksportuotojas sutinka ir užtikrina, kad:

a) asmens duomenų tvarkymas, įskaitant jų perdavimą, yra ir bus vykdomas laikantis susijusių taikytinos duomenų apsaugos teisės nuostatų (ir, jei taikytina, apie jį pranešta atitinkamoms valstybės narės, kurioje įsikūręs duomenų eksportuotojas, institucijoms) ir juo nepažeidžiamos atitinkamos tos valstybės nuostatos;

b) jis davė nurodymus duomenų importuotojui ir visą asmens duomenų tvarkymo paslaugų laikotarpį duos nurodymus tvarkyti perduotus asmens duomenis tik duomenų eksportuotojo vardu ir laikantis taikytinos duomenų apsaugos teisės ir šių sąlygų;

<…>

f) ypatingų kategorijų duomenų perdavimo atveju duomenų subjektui buvo pranešta arba bus pranešta prieš arba kuo greičiau po duomenų perdavimo, kad jo duomenys gali būti perduoti trečiajai šaliai, neužtikrinančiai reikiamos apsaugos pagal [Direktyvą 95/46];

g) persiųs bet kokį pranešimą, gautą iš duomenų importuotojo arba pagalbinio duomenų tvarkytojo pagal 5 sąlygos b punktą ir 8 sąlygos 3 dalį duomenų apsaugos priežiūros institucijai, jeigu duomenų eksportuotojas nusprendžia tęsti perdavimą arba nutraukti sustabdymą;

<…>“

35 Minėto priedo 5 sąlygoje „Duomenų importuotojo įsipareigojimai <…>“ nurodyta:

„Duomenų importuotojas sutinka ir užtikrina, kad:

a) tvarkys asmens duomenis tik duomenų eksportuotojo vardu ir laikysis jo nurodymų ir šių sąlygų; jeigu jis dėl bet kokių priežasčių negali užtikrinti atitikties, jis sutinka kuo skubiau pranešti duomenų importuotojui [eksportuotojui] apie tai, kad jis negali užtikrinti atitikties, ir tokiu atveju duomenų eksportuotojas turi teisę sustabdyti duomenų perdavimą ir (arba) nutraukti sutartį;

b) neturi pagrindo manyti, kad pagal jam taikytiną teisę jis negalės vykdyti iš duomenų eksportuotojo gautų nurodymų ir savo įsipareigojimų pagal sutartį, o jeigu ši teisė pakeičiama ir šie pakeitimai turi didelį neigiamą poveikį pagal šias sąlygas teikiamoms garantijoms ir prisiimtiems įsipareigojimams, jis kuo greičiau praneš apie šiuos pasikeitimus duomenų eksportuotojui, kai tik apie juos sužinos, o duomenų eksportuotojas tokiu atveju turi teisę sustabdyti duomenų perdavimą ir (arba) nutraukti sutartį;

<…>

d) kuo greičiau praneš duomenų eksportuotojui apie:
   i) bet kokį teisiškai įpareigojantį teisėsaugos institucijų prašymą atskleisti asmens duomenis, išskyrus atvejus, kai tai draudžiama, pvz., draudimas pagal baudžiamąją teisę, kuriuo siekiama užtikrinti teisėsaugos institucijų vykdomo tyrimo konfidencialumą;
   ii) bet kokią atsitiktinę arba nesankcionuotą prieigą prie duomenų; ir
   iii) bet kokius tiesioginius duomenų subjektų prašymus, neatsakydamas į juos, išskyrus atvejus, kai jis turi leidimą tai daryti;

<…>“

36 Išnašoje, į kurią daroma nuoroda šios 5 sąlygos antraštėje, nustatyta:

„Duomenų importuotojui taikytini privalomi nacionalinių teisės aktų reikalavimai, kurie, atsižvelgiant į Direktyvos [95/46] 13 straipsnio 1 dalį, neviršija demokratinėje visuomenėje reikalingų apribojimų, t. y. jeigu jie yra būtina priemonė užtikrinti nacionalinį saugumą, gynybą, visuomenės saugumą, baudžiamųjų nusikaltimų bei reglamentuojamų profesijų etikos pažeidimų prevenciją, tyrimą, išaiškinimą ir persekiojimą, svarbius valstybės ekonominius bei finansinius interesus, apsaugoti duomenų subjektą arba kitų asmenų teises ir laisves, neprieštarauja standartinėms sutarčių sąlygoms. <…>“

37 SAS sprendimo priedo 6 sąlygoje „Atsakomybė“ numatyta:

„1. Šalys susitaria, kad bet koks duomenų subjektas, kuriam bet kuri šalis arba pagalbinis duomenų tvarkytojas padarė žalą, nes neįvykdė 3 arba 11 sąlygoje nustatytų įsipareigojimų, turi teisę gauti kompensaciją iš duomenų eksportuotojo dėl patirtos žalos.

2. Jeigu duomenų subjektas negali reikalauti kompensacijos, kaip nustatyta 1 dalyje, iš duomenų eksportuotojo dėl duomenų importuotojo arba jo pagalbinio duomenų tvarkytojo padaryto bet kurio iš jų įsipareigojimų, įvardytų 3 arba 11 sąlygose, pažeidimo dėl to, kad duomenų eksportuotojas yra faktiškai dingęs, teisiškai nutraukė savo veiklą arba tapo nemokus, duomenų importuotojas sutinka, kad duomenų subjektas gali iškelti [pareikšti] ieškinį duomenų importuotojui, tarytum jis būtų duomenų eksportuotojas <…>.

<…>“

38 Šio priedo 8 sąlygos „Bendradarbiavimas su priežiūros institucijomis“ 2 dalyje nurodyta:

„Šalys sutinka, kad priežiūros institucija turi teisę atlikti duomenų importuotojo ir bet kurio pagalbinio duomenų tvarkytojo auditą, kuris būtų tokio paties masto ir kuriam būtų taikomos tokios pačios sąlygos kaip ir duomenų eksportuotojo auditui pagal taikytiną duomenų apsaugos teisę.“

39 Minėto priedo 9 sąlygoje „Reglamentuojantys teisės aktai“ nustatyta, kad šios sąlygos reglamentuojamos valstybės narės, kurioje įsikūręs duomenų eksportuotojas, teisės.

40 To paties priedo 11 sąlygoje „Pagalbinis duomenų tvarkymas“ nurodyta:

„1. Duomenų importuotojas nesudaro subrangos sutarties dėl duomenų tvarkymo veiksmų, atliekamų duomenų eksportuotojo vardu pagal šias sąlygas, negavęs išankstinio raštiško duomenų eksportuotojo sutikimo. Kai duomenų importuotojas, gavęs duomenų eksportuotojo sutikimą, sudaro subrangos sutartį, kuria perduoda savo įsipareigojimus pagal šias sąlygas, jis tai daro tik pasirašydamas rašytinį susitarimą su pagalbiniu duomenų tvarkytoju, kuriuo pagalbinis duomenų tvarkytojas prisiima tokius pačius įsipareigojimus, kuriuos pagal šias sąlygas prisiima duomenų importuotojas. <…>

2. Iš anksto sudarytoje duomenų importuotojo ir pagalbinio duomenų tvarkytojo rašytinėje sutartyje taip pat nustatoma trečiosios šalies naudos gavėjos sąlyga, kaip nustatyta 3 sąlygoje, skirta atvejams, kai duomenų subjektas negali reikalauti kompensacijos, nurodytos 6 sąlygos 1 dalyje, iš duomenų eksportuotojo arba duomenų importuotojo, nes jie yra faktiškai dingę, teisiškai nutraukė savo veiklą arba tapo nemokūs ir joks veiklos tęsėjas sutartimi arba teisiniais veiksmais neperėmė visų duomenų eksportuotojo arba duomenų importuotojo teisinių įsipareigojimų. Tokia pagalbinio duomenų tvarkytojo kaip trečiojo asmens atsakomybė apribojama jo paties vykdoma duomenų tvarkymo veikla pagal šias sąlygas.

<…>“

41 SAS sprendimo priedo 12 sąlygos „Įsipareigojimai nutraukus asmens duomenų tvarkymo paslaugų teikimą“ 1 dalyje nustatyta:

„Šalys sutinka, kad nutraukus asmens duomenų tvarkymo paslaugų teikimą duomenų importuotojas ir pagalbinis duomenų tvarkytojas duomenų eksportuotojo pasirinkimu grąžins visus perduotus asmens duomenis ir jų kopijas duomenų eksportuotojui arba sunaikins visus asmens duomenis ir išsiųs patvirtinimą duomenų eksportuotojui, kad tai buvo atlikta, išskyrus atvejus, kai pagal duomenų importuotojui taikytinus teisės aktus jam draudžiama grąžinti arba sunaikinti visus perduotus asmens duomenis arba jų dalį. <…>“

„Privatumo skydo“ sprendimas

42 2015 m. spalio 6 d. Sprendimu *Schrems* (C-362/14, EU:C:2015:650) Teisingumo Teismas pripažino negaliojančiu 2000 m. liepos 26 d. Komisijos sprendimą 2000/520/EB dėl Direktyvos 95/46 dėl saugaus uosto privatumo principų teikiamos apsaugos pakankamumo ir su tuo susijusių JAV komercijos departamento pateiktų Dažnai užduodamų klausimų (OL L 215, 2000, p. 7; 2004 m. specialusis leidimas lietuvių k., 16 sk., 1 t., p. 119); tame sprendime Komisija buvo konstatavusi, kad ši trečioji šalis užtikrina tinkamą apsaugos lygį.

43 Po šio teismo sprendimo paskelbimo Komisija priėmė „Privatumo skydo“ sprendimą; prieš priimdama šį sprendimą Komisija atliko Jungtinių Amerikos Valstijų teisės aktų vertinimą, kaip nurodyta minėto sprendimo 65 konstatuojamojoje dalyje:

„Komisija įvertino JAV teisėje nustatytus apribojimus ir apsaugos priemones, susijusias su JAV valdžios institucijų prieiga prie asmens duomenų, perduotų pagal [Europos Sąjungos] ir [Jungtinių Amerikos Valstijų] „privatumo skydo“ sistemą, ir šių duomenų naudojimu nacionalinio saugumo, teisėsaugos ir kitais viešojo intereso tikslais. Be to, JAV Vyriausybė per savo Nacionalinės žvalgybos direktoriaus biurą ([*Office of the Director of National Intelligence*], ODNI) pateikė Komisijai išsamius pareiškimus ir įsipareigojimus, kuri[e] išdėstyt[i] šio sprendimo VI priede. [JAV valstybės sekretoriaus pasirašytame] [r]ašte, kuris prie šio sprendimo pridedamas kaip III priedas, JAV Vyriausybė taip pat įsipareigojo sukurti naują nacionalinio saugumo priemonių priežiūros mechanizmą, t. y. „privatumo skydo“ ombudsmeną, kuris bus nepriklausomas nuo žvalgybos bendruomenės. Galiausiai JAV teisingumo departamento pareiškime, kuris pateiktas šio sprendimo VII priede, aprašomi valdžios institucijų prieigos prie duomenų ir jų naudojimo teisėsaugos ir kitais viešojo intereso tikslais apribojimai ir su tuo susijusios saugumo priemonės. Siekiant didinti skaidrumą ir užtikrinti šių įsipareigojimų teisinį pobūdį, kiekvienas šiame sprendime nurodytas ir prie jo pridėtas dokumentas bus skelbiamas JAV federaliniame registre.“

44 Komisijos atlikta šių apribojimų ir apsaugos priemonių analizė apibendrinta „Privatumo skydo“ sprendimo 67–135 konstatuojamosiose dalyse, o šios institucijos išvados dėl tinkamo pagal Europos Sąjungos ir Jungtinių Amerikos Valstijų „privatumo skydą“ užtikrinamos apsaugos lygio išdėstytos šio sprendimo 136–141 konstatuojamosiose dalyse.

45 Konkrečiai kalbant, šio sprendimo 68, 69, 76, 77, 109, 112–116, 120, 136 ir 140 konstatuojamosiose dalyse nurodyta:

„(68) pagal JAV Konstituciją nacionalinio saugumo užtikrinimas – prezidento prerogatyva, jis veikia kaip vyriausiasis vadas ir vykdomasis direktorius [vykdomosios valdžios atstovas], o užsienio žvalgybos srityje tvarko JAV užsienio reikalus <…>. Nors Kongresas, atsižvelgdamas į šias ribas, turi įgaliojimus nustatyti apribojimus ir tai darė įvairiais atvejais, [vis dėlto] [P]rezidentas gali nukreipti JAV žvalgybos bendruomenės veiklą, visų pirma priimdamas vykdomuosius įsakus arba [P]rezidento direktyvas. <…> Šiuo atžvilgiu dabar galioja dvi pagrindinės teisinės priemonės – tai vykdomasis įsakas (angl. *Executive Order*) Nr. 12333 (toliau – E.O. 12333) <…> ir Prezidento politinė direktyva Nr. 28 (angl. *Presidential Policy Directive*);

(69) 2014 m. sausio 17 d. priimtoje Prezidento politinėje direktyvoje Nr. 28 (PPD-28) nustatyti įvairūs signalų žvalgybos operacijų apribojimai <…>. Ši [P]rezidento direktyva turi privalomą galią JAV žvalgybos institucijoms <…> ir lieka toliau galioti pasikeitus JAV Administracijai <…>. PPD-28 yra ypač svarbi ne JAV asmenims, įskaitant ES duomenų subjektus; <…>

<…>

(76) nors [PPD-28 nustatyti] apribojimai nėra suformuluoti vartojant teisinius terminus, šiuose principuose įtvirtinti esminiai būtinumo ir proporcingumo principų aspektai; <…>

(77) kadangi šiuos reikalavimus direktyvos forma [P]rezidentas priėmė kaip vykdomasis direktorius [vykdomosios valdžios atstovas], jų privalo laikytis visa žvalgybos bendruomenė ir jie išsamiau apibūdinami agentūros taisyklėse ir procedūrose, kuriomis bendrieji principai perkeliami į konkrečias kasdienių operacijų instrukcijas; <…>

<…>

(109) priešingai, pagal [*Foreign Intelligence Surveillance Act*] (FISA) 702 straipsnį [*United States Foreign Intelligence Surveillance Court (FISC)* (Jungtinių Amerikos Valstijų užsienio žvalgybos priežiūros teismas)] neleidžia taikyti individualių stebėjimo priemonių; tiesą sakant, jis suteikia leidimus įgyvendinti stebėjimo programas (pvz., PRISM, UPSTREAM), remdamasis metiniais pažymėjimais, kuriuos parengė [*United States Attorney General* (generalinis prokuroras) ir [*Director of National Intelligence (DNI)* (Nacionalinės žvalgybos direktorius). <…> Kaip nurodyta, pažymėjimuose, kuriuos tvirtins FISC, nėra informacijos apie individualius asmenis, kurie bus sekami, vietoj to nustatomos užsienio žvalgybos informacijos kategorijos <…>. Nors FISC, atsižvelgdamas į pagrįstą tikimybę arba kitą standartą, nevertina, ar asmenys tinkamai sekami siekiant gauti užsienio žvalgybos informacijos <…>, vykdydamas kontrolę jis vadovaujasi sąlyga, kad „svarbus sekimo tikslas – gauti užsienio žvalgybos informacijos“; <…>

<…>

(112) pirma, Užsienio žvalgybos stebėjimo akte nustatytos įvairios teisių gynimo priemonės, kuriomis taip pat gali pasinaudoti ne JAV asmenys, kad ginčytų neteisėtą elektroninį stebėjimą <…>. Tai reiškia asmenų galimybę pareikšti civilinį ieškinį Jungtinėms Amerikos Valstijoms dėl materialinių nuostolių atlyginimo <…>, jeigu informacija apie juos buvo neteisėtai ir tyčia naudojama arba atskleista <…>; iškelti bylą JAV Vyriausybės pareigūnams kaip asmenims (pagal statutinę teisę [tarsi pagal įstatymą]) dėl materialinių nuostolių atlyginimo ir ginčyti stebėjimo teisėtumą (bei siekti panaikinti informaciją), jeigu JAV Vyriausybė ketina naudoti arba atskleisti bet kokią informaciją, gautą arba perimtą vykdant elektroninį asmens stebėjimą Jungtinėse Amerikos Valstijose nagrinėjamoje teisminėje arba administracinėje byloje; <…>

(113) antra, JAV Vyriausybė nurodė Komisijai įvairius papildomus būdus, kuriais ES duomenų subjektai galėtų pasinaudoti, siekdami teisinėmis priemonėmis apsiginti nuo Vyriausybės pareigūnų neteisėtos prieigos prie asmens duomenų arba jų naudojimo, įskaitant tariamus nacionalinio saugumo tikslus; <…>

(114) galiausiai JAV Vyriausybė nurodė, kad [*Freedom of information Act (FOIA)* (Informacijos laisvės įstatymas)] ne JAV asmenys gali naudotis kaip priemone, siekdami gauti prieigą prie esamų federalinių agentūros įrašų, įskaitant atvejus, kai juose yra asmens duomenų <…>. Atsižvelgiant į FOIA taikymo sritį, FOIA nenumatyti individualūs teisių gynimo nuo asmens duomenų ribojimo būdai, net jeigu tai iš esmės galėtų suteikti asmenims galimybę susipažinti su atitinkama informacija, kurią turi nacionalinės žvalgybos agentūros; <…>

(115) todėl, nors asmenys, įskaitant ES duomenų subjektus, gali pasinaudoti įvairiais teisių gynimo būdais, jei tapo neteisėto (elektroninio) stebėjimo nacionalinio saugumo tikslais aukomis, lygiai taip pat aišku, kad bent jau kai kurie teisiniai pagrindai [kai kuriems teisiniams pagrindams], kuriuos JAV žvalgybos institucijos gali naudoti (pvz., E.O. 12333), nėra taikomi [tai negalioja]. Be to, net jeigu galimybėmis pasinaudoti teisminėmis teisių gynimo priemonėmis iš esmės gali pasinaudoti ir ne JAV asmenys, pvz., stebėjimas pagal FISA, prieinami ieškinio pareiškimo pagrindai yra riboti <…>, o asmenų (įskaitant JAV asmenis) pareikšti ieškiniai bus paskelbti nepriimtinais, jeigu negalima įrodyti jų pagrįstumo <…>, todėl galimybė kreiptis į bendrosios kompetencijos teismus yra ribota; <…>

(116) siekdama suteikti galimybę pasinaudoti papildomu teisių gynimo būdu, kuris būtų prieinamas visiems ES duomenų subjektams, JAV Vyriausybė nusprendė sukurti naują instituciją – ombudsmeną, kaip nustatyta JAV valstybės sekretoriaus rašte Komisijai, kuris prie šio sprendimo pridedamas kaip III priedas. Šiai institucijai pagal PPD-28 vadovauja Valstybės departamente (sekretoriaus pavaduotojo lygmeniu) paskirtas vyresnysis koordinatorius, kuris veikia kaip kontaktinis centras, ne tik sprendžiantis užsienio vyriausybių iškeltus klausimus dėl JAV signalų žvalgybos veiklos, bet ir vykdantis daug įvairesnę veiklą, palyginti su pradine jo samprata;

<…>

(120) <…> JAV Vyriausybė įsipareigoja užtikrinti, kad vykdydamas savo funkcijas „privatumo skydo“ ombudsmenas galės kliautis bendradarbiavimu su kitomis pagal JAV teisę įkurtomis priežiūros ir atitikties peržiūros institucijomis. <…> Jeigu reikalavimų nesilaikymo atvejį nustatė kuri nors iš šių priežiūros institucijų, atitinkamas žvalgybos bendruomenės subjektas (pvz., žvalgybos agentūra) turės ištaisyti su tuo susijusią padėtį, nes tik taip obmudsmenas, atsižvelgdamas į šiuo tikslu duotą JAV Vyriausybės įsipareigojimą, galės pateikti teigiamą atsakymą asmeniui (t. y. atsakymą, kuriame nurodoma, kad ištaisyta bet kokia su reikalavimų nesilaikymu susijusi padėtis); <…>

<…>

(136) atsižvelgdama į šias išvadas, Komisija mano, kad Jungtinės Amerikos Valstijos užtikrina tinkamą asmens duomenų, kuriuos pagal ES ir JAV „privatumo skydą“ [Europos] Sąjunga perdavė Jungtinių Amerikos Valstijų autosertifikuotoms organizacijoms, apsaugos lygį;

<…>

(140) galiausiai, remdamasi prieinama informacija apie JAV teisinę tvarką, įskaitant JAV Vyriausybės pareiškimus ir įsipareigojimus, Komisija mano, kad bet kokia išimtis [bet koks suvaržymas], kurią [kurį] JAV valdžios institucijos, siekdamos nacionalinio saugumo, teisėsaugos ar kitų viešojo intereso tikslų, taiko asmenų, kurių duomenys perduodami iš Sąjungos į Jungtines Amerikos Valstijas pagal „privatumo skydą“, pagrindinėms teisėms, ir iš to išplaukiantys autosertifikuotoms organizacijoms nustatyti privalomi apribojimai, susiję su privatumo principų laikymusi, galios tik tiek, kiek tai yra griežtai būtina siekiant atitinkamo teisėto tikslo ir jeigu taikant tokias išimtis [tokius suvaržymus] galioja veiksminga teisinė apsauga.“

46 „Privatumo skydo“ sprendimo 1 straipsnyje nustatyta:

„1. Atsižvelgdamos į [Direktyvos 95/46] 25 straipsnio 2 dalį, Jungtinės Amerikos Valstijos užtikrina tinkamą asmens duomenų, kuriuos pagal ES ir JAV „privatumo skydą“ [Europos] Sąjunga perdavė Jungtinių Amerikos Valstijų organizacijoms, apsaugos lygį.

2. [Europos Sąjungos] ir [Jungtinių Amerikos Valstijų] „privatumo skydą“ sudaro 2016 m. liepos 7 d. JAV komercijos departamento paskelbti privatumo principai, kurie išdėstyti II priede[,] ir oficial[ūs] pareiškim[ai] ir įsipareigojim[ai], kurie pateikti I, III–VII prieduose nurodytuose dokumentuose.

3. Pagal šio straipsnio 1 dalį asmens duomenys perduodami pagal [Europos Sąjungos] ir [Jungtinių Amerikos Valstijų] „privatumo skydą“ tais atvejais, kai jie iš Sąjungos perduodami Jungtinių Amerikos Valstijų organizacijoms, įrašytoms į „privatumo skydo“ sąrašą, kurį pagal II priede išdėstytų privatumo principų I ir III skirsnius tvarko ir viešai skelbia JAV komercijos departamentas.“

47 „Privatumo skydo“ sprendimo II priedo „JAV komercijos departamento paskelbti [Europos Sąjungos] ir [Jungtinių Amerikos Valstijų] „privatumo skydo“ sistemos principai“ I.5 punkte numatyta, kad principų laikymasis, be kita ko, gali būti ribojamas „tiek, kiek tai būtina nacionalinio saugumo, viešojo intereso arba teisėsaugos reikalavimams įvykdyti“.

48 Šio sprendimo III priede pateiktas 2016 m. liepos 7 d. tuometinio *Secretary of State* (Jungtinių Amerikos Valstijų valstybės sekretorius) John Kerry raštas už teisingumą, vartotojų reikalus ir lygybę atsakingai Komisijos narei; šio rašto A priede pateiktas memorandumas „[Europos Sąjungos] ir [Jungtinių Amerikos Valstijų] „privatumo skydo“ ombudsmeno mechanizmas dėl signalų žvalgybos“, jame, be kita ko, nurodyta:

„Pripažįstant [Europos Sąjungos] ir [Jungtinių Amerikos Valstijų] „privatumo skydo“ sistemos svarbą, šiame memorandume nustatomas naujo mechanizmo, atitinkančio [PPD-28] ir susijusio su signalų žvalgyba, įgyvendinimo procesas.

<…> Prezidentas B. Obama paskelbė apie naujai priimtą politinę direktyvą – PPD-28, – kurioje aiškiai nurodoma, kokių veiksmų imamės užsienio žvalgybos srityje ir ko nedarome.

PPD-28 4 skirsnio d dalyje valstybės sekretoriui pavedama paskirti „Tarptautinės informacinių technologijų diplomatijos vyresnįjį koordinatorių“ (vyresnysis koordinatorius), „kuris <…> veiktų kaip kontaktinis centras, į kurį užsienio Vyriausybės galėtų kreiptis kilus klausimų dėl Jungtinių Amerikos Valstijų vykdomos signalų žvalgybos veiklos“.

<…>

1. [Vyresnysis koordinatorius] veiks kaip „privatumo skydo“ ombudsmen[as] ir <…> glaudžiai dirbs su atitinkamais kitų departamentų ir agentūrų pareigūnais, kurie atsako už prašymų nagrinėjimą pagal taikytiną Jungtinių Amerikos Valstijų teisę ir politiką. Ombudsmenas yra nepriklausomas nuo žvalgybos bendruomenės. Ombudsmenas atsiskaito tiesiogiai Valstybės sekretoriui, kuris užtikrina, kad ombudsmenas vykdytų savo funkcijas objektyviai ir nepriklausomai nuo jokios netinkamos įtakos, kuri gali būti daroma siekiant gauti atitinkamą sprendimą.

<…>“

49 „Privatumo skydo“ sprendimo VI priede pateiktas 2016 m. birželio 21 d. Nacionalinės žvalgybos direktoriaus biuro (*Office of the Director of National Intelligence*) raštas JAV komercijos departamentui ir Tarptautinės prekybos administracijai, kuriame nurodyta, kad pagal PPD-28 leidžiamas „masinis“ <… > gana didelio signalų žvalgybos informacijos kiekio arba duomenų [rinkimas] tais atvejais, kai žvalgybos bendruomenė negali panaudoti identifikatoriaus, susijusio su konkrečiu taikiniu <…>, kad galėtų tikslingai rinkti duomenis“.

Ginčas pagrindinėje byloje ir prejudiciniai klausimai

50 M. Schrems yra Austrijoje gyvenantis šios šalies pilietis; nuo 2008 m. jis yra socialinio tinklo *Facebook* (toliau – *Facebook*) naudotojas.

51 Visų Sąjungos teritorijoje gyvenančių asmenų, norinčių naudotis šiuo socialiniu tinklu, per registracijos procedūrą prašoma pasirašyti sutartį su *Facebook Ireland*, Jungtinėse Amerikos Valstijose įsikūrusios patronuojančiosios bendrovės *Facebook Inc.* patronuojamąja bendrove. Visi Sąjungos teritorijoje gyvenančių *Facebook Ireland* naudotojų duomenys arba jų dalis perduodami į *Facebook Inc.* serverius, kurie yra Jungtinių Amerikos Valstijų teritorijoje, ir šie duomenys ten tvarkomi. Sąjungos teritorijoje gyvenančių *Facebook Ireland* naudotojų asmens duomenys (visi arba jų dalis) perduodami į JAV teritorijoje esančius *Facebook Inc.* priklausančius serverius ir ten tvarkomi.

52 2013 m. birželio 25 d. M. Schrems pateikė komisarui skundą, jame iš esmės prašė uždrausti *Facebook Ireland* perduoti jo asmens duomenis į Jungtines Amerikos Valstijas ir teigė, kad šioje šalyje galiojanti teisė ir praktika neužtikrina pakankamos jos teritorijoje saugomų asmens duomenų apsaugos nuo šioje

šalyje viešosios valdžios institucijų vykdomos stebėjimo veiklos. Šis skundas buvo atmestas, be kita ko, motyvuojant tuo, kad Sprendime 2000/520 Komisija konstatavo, jog Jungtinės Valstijos užtikrina tinkamą duomenų apsaugos lygį.

53 *High Court* (Aukštasis teismas, Airija), kuriame M. Schrems apskundė šį atmetimą, kreipėsi į Teisingumo Teismą su prašymu priimti prejudicinį sprendimą dėl Sprendimo 2000/520 išaiškinimo ir galiojimo. 2015 m. spalio 6 d. Sprendimu *Schrems* (C-362/14, EU:C:2015:650) Teisingumo Teismas pripažino šį sprendimą negaliojančiu.

54 Po šio teismo sprendimo prašymą priimti prejudicinį sprendimą pateikęs teismas panaikino M. Schrems skundo atmetimą ir grąžino jį komisarui. Per komisaro pradėtą tyrimą *Facebook Ireland* paaiškino, kad didelė dalis asmens duomenų buvo perduota *Facebook Inc.* remiantis SAS sprendimo priede pateiktomis standartinėmis duomenų apsaugos sąlygomis. Atsižvelgdamas į šias aplinkybes komisaras paprašė M. Schrems performuluoti savo skundą.

55 2015 m. gruodžio 1 d. paduotame performuluotame skunde M. Schrems, be kita ko, teigė, kad pagal JAV teisę *Facebook Inc.* privalo jai perduodamus duomenis pateikti JAV valdžios institucijoms, kaip antai *National Security Agency (NSA)* ir *Federal Bureau of Investigation (FBI)*. Jis tvirtino: kadangi šie duomenys naudojami pagal įvairias stebėjimo programas su Chartijos 7, 8 ir 47 straipsniais nesuderinamu būdu, SAS sprendimu negali būti pateisinamas minėtų duomenų perdavimas į Jungtines Amerikos Valstijas. Tokiomis aplinkybėmis M. Schrems paprašė komisaro uždrausti arba sustabdyti jo asmens duomenų perdavimą *Facebook Inc.*

56 2016 m. gegužės 24 d. komisaras paskelbė „sprendimo projektą“, jame apibendrintos preliminarios jo tyrimo išvados. Šiame projekte jis preliminariai konstatavo, jog kyla pavojus, kad su Sąjungos piliečių asmens duomenimis, perduodamais į Jungtines Amerikos Valstijas, JAV valdžios institucijos gali susipažinti ir juos tvarkyti su Chartijos 7 ir 8 straipsniais nesuderinamu būdu ir kad pagal Jungtinių Amerikos Valstijų teisę šiems piliečiams nesuteikiamos su Chartijos 47 straipsniu suderinamos teisių gynimo priemonės. Komisaras nusprendė, kad SAS sprendimo priede pateiktos standartinės duomenų apsaugos sąlygos negali ištaisyti šio trūkumo, nes pagal jas duomenų subjektams suteikiamos tik sutartyje numatytos teisės duomenų eksportuotojo ir importuotojo atžvilgiu, tačiau jos nėra privalomos JAV valdžios institucijoms.

57 Manydamas, kad tokiomis aplinkybėmis performuluotame M. Schrems skunde buvo keliamas SAS sprendimo galiojimo klausimas, 2016 m. gegužės 31 d. komisaras, remdamasis 2015 m. spalio 6 d. Sprendime *Schrems* (C-362/14, EU:C:2015:650, 65 punktas) suformuota jurisprudencija, kreipėsi į *High Court* (Aukštasis teismas), kad šis pateiktų Teisingumo Teismui šį klausimą. 2018 m. gegužės 4 d. sprendimu *High Court* (Aukštasis teismas) pateikė Teisingumo Teismui šį prašymą priimti prejudicinį sprendimą.

58 Prie šio prašymo priimti prejudicinį sprendimą *High Court* (Aukštasis teismas) pridėjo 2017 m. spalio 3 d. paskelbtą sprendimą, jame buvo išdėstęs per nacionalinį procesą (jame dalyvavo JAV vyriausybė) jam pateiktų įrodymų tyrimo rezultatą.

59 Tame sprendime, į kurį prašyme priimti prejudicinį sprendimą kelis kartus daroma nuoroda, prašymą priimti prejudicinį sprendimą pateikęs teismas pažymėjo, jog iš principo jis turi ne tik teisę, bet ir pareigą išnagrinėti visas jam pateiktas faktines aplinkybes ir argumentus, kad jais remdamasis nuspręstų, ar reikia pateikti prašymą priimti prejudicinį sprendimą. Bet kuriuo atveju jis privalo atsižvelgti į teisės pakeitimus, kurie gali būti atlikti laikotarpiu nuo skundo pateikimo iki jo posėdžio surengimo. Tas teismas pažymėjo, kad nagrinėjant pagrindinę bylą jo vertinimas neapsiriboja komisaro pateiktais negaliojimo pagrindais, todėl jis taip pat gali *ex officio* nurodyti kitus negaliojimo pagrindus ir jais remdamasis pateikti prašymą priimti prejudicinį sprendimą.

60 Kaip konstatuota minėtame teismo sprendime, JAV valdžios institucijų žvalgybos veikla, susijusi su į Jungtines Amerikos Valstijas perduodamais asmens duomenimis, be kita ko, grindžiama FISA 702 straipsniu ir E.O. 12333.

61 Dėl FISA 702 straipsnio prašymą priimti prejudicinį sprendimą pateikęs teismas tame pačiame sprendime pažymėjo, kad pagal šį straipsnį generalinis prokuroras ir nacionalinės žvalgybos direktorius po FISC patvirtinimo gali kartu duoti leidimą stebėti ne JAV piliečius, esančius ne Jungtinėse Amerikos Valstijose, kad įgytų „užsienio žvalgybos informacijos“, ir kad šis straipsnis, be kita ko, yra stebėjimo programų PRISM ir UPSTREAM pagrindas. Kaip konstatavo tas teismas, pagal PRISM programą interneto paslaugų teikėjai privalo pateikti NSA visus iš „sekamo įrenginio“ išsiunčiamus ir į jį gaunamus pranešimus; dalis šių pranešimų taip pat perduodama FBI ir *Central Intelligence Agency (CIA)* (Centrinė žvalgybos agentūra).

62 Dėl UPSTREAM programos minėtas teismas konstatavo, kad pagal šią programą telekomunikacijų įmonės, eksploatuojančios pagrindinį interneto tinklą – t. y. kabelių, perjungiklių ir maršrutizatorių tinklą – privalo leisti NSA kopijuoti ir filtruoti interneto duomenų srautą siekiant gauti iš „sekamo įrenginio“ išsiunčiamus ir į jį gaunamus pranešimus arba pranešimus apie ne JAV pilietį. Kaip konstatavo tas pats teismas, pagal minėtą programą NSA turi prieigą tiek prie atitinkamų pranešimų metaduomenų, tiek prie jų turinio.

63 Dėl E.O. 12333 prašymą priimti prejudicinį sprendimą pateikęs teismas konstatuoja, kad pagal jį NSA leidžiama gauti prieigą prie į Jungtines Amerikos Valstijas „perduodamų“ duomenų, naudojantis Atlanto vandenyno dugne esančiais povandeniniais kabeliais, ir rinkti bei saugoti šiuos duomenis prieš jiems pasiekiant Jungtines Amerikos Valstijas ir prieš pradedant jiems taikyti FISA nuostatas. Jis pažymi, kad E.O. 12333 grindžiama veikla nėra reglamentuojama įstatymo.

64 Kiek tai susiję su žvalgybos veiklos apribojimais, prašymą priimti prejudicinį sprendimą pateikęs teismas pabrėžia, kad ne JAV asmenys patenka tik į PPD-28 taikymo sritį ir kad jame tik nurodyta, jog žvalgybos veikla turi būti „kuo tikslingesnė“ (*as tailored as feasible*). Remdamasis savo išvadomis minėtas teismas mano, kad Jungtinės Amerikos Valstijos tvarko didelį duomenų kiekį, neužtikrindamos apsaugos, kuri iš esmės būtų lygiavertė pagal Chartijos 7 ir 8 straipsnius užtikrinamai apsaugai.

65 Dėl teisminės apsaugos tas pats teismas nurodo, kad Sąjungos piliečiams nėra prieinamos tos pačios teisminės teisių gynimo priemonės dėl JAV valdžios institucijų atliekamo asmens duomenų tvarkymo kaip ir JAV piliečiams, nes *Constitution of the United States* (Jungtinių Amerikos Valstijų Konstitucija) Ketvirtoji pataisa, kurioje numatyta didžiausia apsauga nuo neteisėto stebėjimo JAV teisėje, netaikoma Sąjungos piliečiams. Šiuo klausimu prašymą priimti prejudicinį sprendimą pateikęs teismas pažymi, kad siekiant Sąjungos piliečiams pasinaudoti likusiomis teisių gynimo priemonėmis susiduriama su didelėmis kliūtimis, visų pirma pareiga – kurią, jo teigimu, pernelyg sudėtinga įvykdyti – pagrįsti savo teisę paduoti skundą. Be to, kaip konstatavo tas teismas, E.O. 12333 grindžiamai NSA veiklai netaikoma teismų kontrolė ir jos negalima apskųsti teismui. Galiausiai minėtas teismas laikosi nuomonės: kadangi, jo teigimu, „privatumo skydo“ ombudsmenas nėra teismas, kaip jis suprantamas pagal Chartijos 47 straipsnį, JAV teisėje Sąjungos piliečiams neužtikrinamas apsaugos lygis, kuris iš esmės būtų lygiavertis apsaugos lygiui, užtikrinamam šiame straipsnyje įtvirtinta pagrindine teise.

66 Prašyme priimti prejudicinį sprendimą jį pateikęs teismas dar pažymi, kad pagrindinės bylos šalys nesutaria, be kita ko, dėl Sąjungos teisės taikymo į trečiąją šalį perduodant asmens duomenis, kuriuos šios šalies valdžios institucijos gali tvarkyti, be kita ko, nacionalinio saugumo tikslais, ir dėl aplinkybių, į kurias reikia atsižvelgti vertinant tinkamą minėtos šalies užtikrinamą apsaugos lygį. Konkrečiai kalbant, šis teismas pažymi, kad, *Facebook Ireland* teigimu, Komisijos išvados, susijusios su trečiosios šalies užtikrinamo apsaugos lygio tinkamumu, kaip antai išdėstytos „Privatumo skydo“ sprendime, yra privalomos priežiūros institucijoms ir perduodant asmens duomenis remiantis SAS sprendimo priede pateiktomis standartinėmis apsaugos sąlygomis.

67 Kiek tai susiję su šiomis standartinėmis duomenų apsaugos sąlygomis, tam teismui kyla klausimas, ar SAS sprendimas gali būti laikomas galiojančiu, nors, to paties teismo teigimu, minėtos sąlygos nėra privalomos atitinkamos trečiosios šalies valdžios institucijoms, taigi jomis negali būti ištaisytas galimas tinkamo apsaugos lygio nebuvimas šioje šalyje. Šiuo aspektu jis laikosi nuomonės, kad Sprendimo 2010/87 redakcijos, galiojusios iki įsigaliojant Įgyvendinimo sprendimui 2016/2297, 4 straipsnio 1 dalies a punkte pripažinta valstybių narių kompetentingų valdžios institucijų galimybė uždrausti perduoti asmens duomenis į trečiąją šalį, importuotojui nustatant su tose pačiose standartinėse sąlygose išdėstytomis garantijomis nesuderinamas pareigas, įrodo, kad teisinė padėtis trečiojoje šalyje gali pateisinti draudimą perduoti duomenis, net jeigu tai daroma remiantis SAS sprendimo priede pateiktomis standartinėmis duomenų apsaugos sąlygomis, taigi rodo, kad šios sąlygos gali būti nepakankamos tinkamai apsaugai užtikrinti. Atsižvelgdamas į tai prašymą priimti prejudicinį sprendimą pateikęs teismas kelia klausimą dėl komisaro įgaliojimų uždrausti šiomis sąlygomis grindžiamą duomenų perdavimą apimties ir kartu laikosi nuomonės, kad diskrecijos nepakanka tinkamai apsaugai užtikrinti.

68 Tokiomis aplinkybėmis *High Court* (Aukštasis teismas) nusprendė sustabdyti bylos nagrinėjimą ir pateikti Teisingumo Teismui šiuos prejudicinius klausimus:

„1. Ar tais atvejais, kai privati bendrovė perduoda asmens duomenis iš [Sąjungos] valstybės narės privačiai bendrovei trečiojoje šalyje komerciniais tikslais pagal [SAS sprendimą], ir toje trečiojoje šalyje jos institucijos gali toliau tvarkyti tokius asmens duomenis ne tik nacionalinio saugumo tikslais, bet ir teisėsaugos bei trečiosios šalies užsienio politikos tikslais, tokių duomenų perdavimui taikoma Sąjungos teisė (įskaitant Chartiją), nepaisant ESS 4 straipsnio 2 dalies nuostatų dėl nacionalinio saugumo ir [Direktyvos 95/46] 3 straipsnio 2 dalies pirmos įtraukos nuostatų dėl visuomenės saugumo, gynybos ir valstybės saugumo?

2. a) Ar norint nustatyti, ar perdavus duomenis iš [Sąjungos] į trečiąją šalį pagal [SAS sprendimą], kur jie gali būti toliau tvarkomi nacionalinio saugumo tikslais, buvo pažeistos asmens teisės, pagal [Direktyvą 95/46] svarbus lyginamasis teisės šaltinis yra:
   i) Chartija, ESS, SESV, [Direktyva 95/46], [Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija, pasirašyta 1950 m. lapkričio 4 d. Romoje (toliau – EŽTK) (arba kuri nors kita [Sąjungos] teisės nuostata); ar
   ii) vienos arba daugiau valstybių narių nacionaliniai įstatymai?
   b) Jeigu svarbus lyginamasis teisės šaltinis yra nurodytas ii punkte, ar į jį turi būti įtraukta ir vienos arba daugiau valstybių narių taikoma su nacionalinio saugumo užtikrinimu susijusi praktika?

3. Ar norint įvertinti, ar trečioji šalis užtikrina pagal Sąjungos teisę reikalaujamą asmens duomenų, perduodamų į tą šalį pagal [Direktyvos 95/46] 26 straipsnį, apsaugos lygį, apsaugos lygis toje trečiojoje šalyje turėtų būti vertinamas atsižvelgiant į:
   a) toje trečiojoje šalyje taikomas nuostatas, kylančias iš jos nacionalinės teisės arba tarptautinių įsipareigojimų, ir tokių nuostatų laikymosi užtikrinimo praktiką, įskaitant profesines nuostatas ir saugumo priemones, kurių laikomasi toje trečiojoje šalyje;

   ar
   b) a punkte nurodytas nuostatas kartu su administracine, reguliavimo ir reikalavimų laikymosi užtikrinimo praktika bei politikos įgyvendinimo užtikrinimo priemonėmis, procedūromis, protokolais, priežiūros mechanizmais ir neteisminėmis gynybos priemonėmis, kurios yra taikomos trečiojoje šalyje?

4. Atsižvelgiant į *High Court* [(Aukštasis Teismas)] nustatytas faktines aplinkybes, susijusias su JAV teise, jeigu asmens duomenys pagal [SAS sprendimą] perduodami iš [Sąjungos] į JAV, ar taip pažeidžiamos Chartijos 7 ir (arba) 8 straipsniuose numatytos asmens teisės?

5. Atsižvelgiant į *High Court* [(Aukštasis Teismas)] nustatytas faktines aplinkybes, susijusias su JAV teise, jeigu asmens duomenys perduodami iš [Sąjungos] į JAV pagal [SAS sprendimą]:
   a) ar JAV suteikiama apsauga yra tokio lygio, kad ja užtikrinama asmens teisės pasinaudoti pagal Chartijos 47 straipsnį garantuojamomis teisminės gynybos priemonėmis, kai pažeidžiamos jo teisės į duomenų privatumą, esmė?

   Jeigu atsakymas į penktojo klausimo a punktą yra teigiamas:
   b) ar JAV teisėje numatyti asmens teisės pasinaudoti teisminės gynybos priemonėmis apribojimai, taikomi dėl JAV nacionalinio saugumo, yra proporcingi, kaip tai suprantama pagal Chartijos 52 straipsnį, ir jie neviršija to, kas būtina demokratinėje visuomenėje siekiant nacionalinio saugumo tikslų?

6. a) Kokio lygio apsaugą reikia užtikrinti asmens duomenims, perduodamiems į trečiąją šalį pagal sutarčių standartines sąlygas, nustatytas Komisijos sprendimu pagal 26 straipsnio 4 dalį, atsižvelgiant į [Direktyvos 95/46] nuostatas, visų pirma į jos 25 ir 26 straipsnius, aiškinamus atsižvelgiant į Chartiją?
   b) Į kokias aplinkybes reikia atsižvelgti, kai vertinama, ar pagal [SAS sprendimą] į trečiąją šalį perduodamiems duomenims suteikiamos apsaugos lygis atitinka [Direktyvos 95/46] ir Chartijos reikalavimus?

7. Ar aplinkybė, kad duomenų eksportuotojo ir duomenų importuotojo tarpusavio santykiams taikomos standartinės apsaugos sąlygos, nesaistančios trečiosios šalies nacionalinės valdžios institucijų, kurios gali pareikalauti duomenų importuotojo pateikti pagal [SAS sprendime] pateiktas sąlygas perduotus asmens duomenis toliau tvarkyti jos saugumo tarnyboms, reiškia, kad pagal šias sąlygas negali būti užtikrinamos adekvačios apsaugos priemonės, kaip numatyta [Direktyvos 95/46] 26 straipsnio 2 dalyje?

8. Ar, jeigu duomenų importuotojui iš trečiosios šalies taikomi stebėjimo įstatymai, kurie, duomenų apsaugos institucijos manymu, prieštarauja standartinėms apsaugos sąlygoms arba [Direktyvos 95/46] 25 ir 26 straipsniams ir (arba) Chartijai, duomenų apsaugos institucija privalo įgyvendinti pagal [Direktyvos 95/46] 28 straipsnio 3 dalį jai suteiktus vykdymo užtikrinimo įgaliojimus, kad sustabdytų duomenų srautus, ar tokie įgaliojimai gali būti įgyvendinami tik išimtiniais atvejais, atsižvelgiant į [Sprendimo 2010/87] 11 konstatuojamąją dalį, ar duomenų apsaugas institucija gali pasinaudoti diskrecija nestabdyti duomenų srautų?

9. a) Ar, atsižvelgiant į [Direktyvos 95/46] 25 straipsnio 6 dalį, [„Privatumo skydo“ sprendimas] yra visuotinai taikoma išvada, privaloma valstybių narių duomenų apsaugos institucijoms ir teismams, kiek jame numatyta, kad JAV savo šalies įstatymais arba prisiimtais tarptautiniais įsipareigojimais užtikrina adekvatų apsaugos lygį, kaip tai suprantama pagal [Direktyvos 95/46] 25 straipsnio 2 dalį?
   b) Jeigu taip nėra, kokią reikšmę [„Privatumo skydo“ sprendimas] turi (jeigu iš viso turi), kai vertinamas apsaugos priemonių, taikomų pagal [SAS sprendimą] į Jungtines Amerikos Valstijas perduodamiems duomenims, tinkamumas?

10. Ar, atsižvelgiant į *High Court* [(Aukštasis Teismas)] nustatytas su JAV teise susijusias aplinkybes, „privatumo skydo“ ombudsmeno institucijos įsteigimas pagal [„Privatumo skydo“ sprendimo] III priedo A priedą, vertinamą kartu su Jungtinėse Valstijose galiojančia sistema, užtikrina, kad JAV suteikia duomenų subjektams, kurių asmens duomenys perduodami į JAV pagal [SAS sprendimą], teisių gynybos priemones, atitinkančias Chartijos 47 straipsnio reikalavimus?

11. Ar [SAS sprendimas] pažeidžia Chartijos 7, 8 ir (arba) 47 straipsnius?“

Dėl prašymo priimti prejudicinį sprendimą priimtinumo

69 *Facebook Ireland* bei Vokietijos ir Jungtinės Karalystės vyriausybės teigia, kad prašymas priimti prejudicinį sprendimą yra nepriimtinas.

70 Dėl *Facebook Ireland* pareikšto prieštaravimo ši bendrovė pažymi, kad Direktyvos 95/46 nuostatos, kuriomis grindžiami prejudiciniai klausimai, buvo panaikintos BDAR.

71 Šiuo klausimu pažymėtina, kad nors Direktyva 95/46 pagal BDAR 94 straipsnio 1 dalį buvo iš tiesų panaikinta nuo 2018 m. gegužės 25 d., ji dar galiojo, kai 2018 m. gegužės 4 d. buvo suformuluotas šis prašymas priimti prejudicinį sprendimą, kurį Teisingumo Teismas gavo 2018 m. gegužės 9 d. Be to, Direktyvos 95/46 3 straipsnio 2 dalies pirma įtrauka, 25, 26 straipsniai ir 28 straipsnio 3 dalis, kurie nurodyti prejudiciniuose klausimuose, iš esmės pakartoti atitinkamai BDAR 2 straipsnio 2 dalyje bei ir 45, 46 ir 58 straipsniuose. Be to, reikia priminti, kad Teisingumo Teismas turi išaiškinti visas Sąjungos teisės nuostatas, kurių reikia nacionaliniams teismams, kad jie išspręstų nagrinėjamas bylas, net jei šios nuostatos nėra aiškiai nurodytos šių teismų jam pateiktuose klausimuose (2020 m. balandžio 2 d. Sprendimo *Ruska Federacija*, C-897/19 PPU, EU:C:2020:262, 43 punktas ir nurodyta jurisprudencija). Dėl šių įvairių motyvų aplinkybė, kad prašymą priimti prejudicinį sprendimą pateikęs teismas formulavo prejudicinius klausimus, remdamasis tik Direktyvos 95/46 nuostatomis, negali lemti šio prašymo priimti prejudicinį sprendimą nepriimtinumo.

72 Vokietijos vyriausybė savo nepriimtinumu grindžiamą prieštaravimą grindžia aplinkybe, kad, viena vertus, komisaras išreiškė tik abejonių, o ne galutinę nuomonę dėl SAS sprendimo galiojimo ir, kita vertus, prašymą priimti prejudicinį sprendimą pateikęs teismas nepatikrino, ar M. Schrems neabejotinai davė sutikimą pagrindinėje byloje aptariamam duomenų perdavimui, o dėl to, jei taip būtų, atsakymas į šį klausimą taptų nenaudingas. Galiausiai, Jungtinės Karalystės vyriausybės teigimu, prejudiciniai klausimai yra hipotetiniai, nes šis teismas nekonstatavo, kad šie duomenys iš tikrųjų buvo perduoti remiantis minėtu sprendimu.

73 Pagal suformuotą Teisingumo Teismo jurisprudenciją tik bylą nagrinėjantis nacionalinis teismas, atsakingas už sprendimo priėmimą, atsižvelgdamas į konkrečias bylos aplinkybes turi įvertinti tai, ar jo sprendimui priimti būtinas prejudicinis sprendimas, ir Teisingumo Teismui pateikiamų klausimų svarbą. Todėl iš principo Teisingumo Teismas turi priimti sprendimą tuo atveju, jei pateikiami klausimai susiję su Sąjungos teisės nuostatos išaiškinimu arba galiojimu. Vadinasi, nacionalinių teismų pateiktiems klausimams dėl Sąjungos teisės taikoma svarbos prezumpcija. Teisingumo Teismas gali atsisakyti priimti sprendimą dėl nacionalinio teismo pateikto prejudicinio klausimo, tik jeigu akivaizdu, kad prašomas išaiškinimas visiškai nesusijęs su ginčo pagrindinėje byloje aplinkybėmis ar dalyku, jeigu problema hipotetinė arba Teisingumo Teismas neturi informacijos apie faktines ir teisines aplinkybes, būtinos tam, kad naudingai atsakytų į tuos klausimus (2015 m. birželio 16 d. Sprendimo *Gauweiler ir kt.*, C-62/14, EU:C:2015:400, 24 ir 25 punktai; 2018 m. spalio 2 d. Sprendimo *Ministerio Fiscal*, C-207/16, EU:C:2018:788, 45 punktas ir 2019 m. gruodžio 19 d. Sprendimo *Dobersberger*, C-16/18, EU:C:2019:1110, 18 ir 19 punktai).

74 Šiuo atveju prašyme priimti prejudicinį sprendimą nurodytos faktinės ir teisinės aplinkybės, kurių pakanka, kad būtų galima suprasti prejudicinių klausimų turinį. Be to, visų pirma Teisingumo Teismo turimoje bylos medžiagoje nėra jokių duomenų, kuriais remiantis būtų galima konstatuoti, jog prašomas Sąjungos teisės išaiškinimas yra nesusijęs su ginčo pagrindinėje byloje aplinkybėmis arba hipotetinis, be kita ko, dėl to, kad pagrindinėje byloje nagrinėjamas asmens duomenų perdavimas grindžiamas aiškiu duomenų subjekto sutikimu su šiuo perdavimu, o ne SAS sprendimu. Remiantis šiame prašyme pateikta informacija, *Facebook Ireland* pripažino, kad perduoda Sąjungoje gyvenančių savo registruotų naudotojų asmens duomenis *Facebook Inc.* ir kad didelė šių perdavimų, kurių teisėtumą ginčija M. Schrems, dalis atliekama remiantis SAS sprendimo priede pateiktomis standartinėmis duomenų apsaugos sąlygomis.

75 Be to, šio prašymo priimti prejudicinį sprendimą priimtinumui neturi įtakos tai, kad komisaras neišreiškė galutinės nuomonės dėl šio sprendimo galiojimo, nes prašymą priimti prejudicinį sprendimą pateikęs teismas mano, jog atsakymas į prejudicinius klausimus dėl Sąjungos teisės normų išaiškinimo ir galiojimo yra būtinas ginčui pagrindinėje byloje išspręsti.

76 Darytina išvada, kad prašymas priimti prejudicinį sprendimą yra priimtinas.

Dėl prejudicinių klausimų

77 Pirmiausia reikia priminti, jog šis prašymas priimti prejudicinį sprendimą pateiktas byloje, pradėtoje gavus M. Schrems skundą, kuriuo siekta, kad komisaras nurodytų sustabdyti arba uždrausti ateityje *Facebook Ireland* atliekamą jo asmens duomenų perdavimą *Facebook Inc*. Nors prejudiciniuose klausimuose nurodytos Direktyvos 95/46 nuostatos, neginčijama, kad komisaras dar nebuvo priėmęs galutinio sprendimo dėl šio skundo, kai ši direktyva nuo 2018 m. gegužės 25 d. buvo panaikinta ir pakeista BDAR.

78 Dėl šio nacionalinio sprendimo nebuvimo pagrindinėje byloje nagrinėjama situacija skiriasi nuo situacijų, dėl kurių priimti 2019 m. rugsėjo 24 d. Sprendimas *Google (Nuorodų pašalinimo teritorinė taikymo sritis)* (C-507/17, EU:C:2019:772) ir 2019 m. spalio 1 d. Sprendimas *Planet49* (C-673/17, EU:C:2019:801); šiuose sprendimuose buvo nagrinėti sprendimai, priimti iki minėtos direktyvos panaikinimo.

79 Taigi į prejudicinius klausimus reikia atsakyti atsižvelgiant į BDAR, o ne Direktyvos 95/46, nuostatas.

Dėl pirmojo klausimo

80 Pirmuoju klausimu prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės siekia išsiaiškinti, ar BDAR 2 straipsnio 1 dalis bei 2 straipsnio 2 dalies a, b ir d punktai, siejami su ESS 4 straipsnio 2 dalimi, turi būti aiškinami taip, kad į šio reglamento taikymo sritį patenka asmens duomenų perdavimas, atliktas valstybėje narėje įsteigto ūkio subjekto kitam trečiojoje šalyje įsteigtam ūkio subjektui, jei atliekant šį perdavimą ar po jo šios trečiosios šalies valdžios institucijos gali tvarkyti šiuos duomenis visuomenės saugumo, gynybos ir valstybės saugumo tikslais.

81 Šiuo aspektu pirmiausia reikia pažymėti, kad ESS 4 straipsnio 2 dalyje esanti nuostata, pagal kurią Sąjungoje kiekviena valstybė narė išimtinai išlieka atsakinga už savo nacionalinį saugumą, skirta tik Sąjungos valstybėms narėms. Todėl nagrinėjamu atveju ši nuostata nėra reikšminga aiškinant BDAE 2 straipsnio 1 dalį ir 2 straipsnio 2 dalies a, b bei d punktus.

82 Pagal BDAR 2 straipsnio 1 dalį šis reglamentas taikomas asmens duomenų tvarkymui, visiškai arba iš dalies atliekamam automatizuotomis priemonėmis, ir asmens duomenų, kurie sudaro susisteminto rinkinio dalį ar yra skirti jai sudaryti, tvarkymui ne automatizuotomis priemonėmis. Šio reglamento 4 straipsnio 2 punkte sąvoka „duomenų tvarkymas“ apibrėžta kaip „bet kokia automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis ar asmens duomenų rinkiniais atliekama operacija ar operacijų seka“ ir kaip pavyzdys nurodytas „atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę <…> naudotis“, nedarant skirtumo pagal tai, ar šios operacijos vykdomos Sąjungoje arba ar turi sąsają su trečiąja šalimi. Be to, minėtame reglamente asmens duomenų perdavimui į trečiąsias šalis taikomos specialios taisyklės, išdėstytos jo V skyriuje „Asmens duomenų perdavimai į trečiąsias valstybes arba tarptautinėms organizacijoms“, ir taip pat šiuo tikslu priežiūros institucijoms suteikti specialūs įgaliojimai, išdėstyti to paties reglamento 58 straipsnio 2 dalies j punkte.

83 Darytina išvada, kad asmens duomenų perdavimo iš valstybės narės į trečiąją šalį operacija savaime yra asmens duomenų tvarkymas, kaip jis suprantamas pagal BDAR 4 straipsnio 2 punktą, atliekamas valstybės narės teritorijoje; tokiam tvarkymui šis reglamentas taikomas pagal jo 2 straipsnio 1 dalį (pagal analogiją dėl Direktyvos 95/46 2 straipsnio b punkto ir 3 straipsnio 1 dalies žr. 2015 m. spalio 6 d. Sprendimo *Schrems*, C-362/14, EU:C:2015:650, 45 punktą ir nurodytą jurisprudenciją).

84 Dėl klausimo, ar tokią operaciją galima laikyti nepatenkančia į BDAR taikymo sritį pagal jo 2 straipsnio 2 dalį, reikia priminti, kad šioje nuostatoje numatytos šio reglamento taikymo srities, apibrėžtos jo 2 straipsnio 1 dalyje, išimtys, kurios turi būti aiškinamos siaurai (pagal analogiją dėl Direktyvos 95/46 3 straipsnio 2 dalies žr. 2018 m. liepos 10 d. Sprendimo *Jehovan todistajat*, C-25/17, EU:C:2018:551, 37 punktą ir nurodytą jurisprudenciją).

85 Kadangi pagrindinėje byloje nagrinėjamu atveju *Facebook Ireland* perduoda asmens duomenis *Facebook Inc.*, t. y. duomenys perduodami tarp dviejų juridinių asmenų, šis perdavimas nepatenka į RGPD 2 straipsnio 2 dalies c punkto, kuris susijęs su fizinio asmens atliekamu duomenų tvarkymu užsiimant išimtinai asmenine ar namų ūkio veikla, taikymo sritį. Minėtam perdavimui taip pat netaikomos šio reglamento 2 straipsnio 2 dalies a, b ir d punktuose numatytos išimtys, nes juose kaip pavyzdžiai nurodytos veiklos sritys visais atvejais yra pačių valstybių ar jų valdžios institucijų veikla, kuri nėra privačių asmenų veikla (pagal analogiją dėl Direktyvos 95/46 3 straipsnio 2 dalies žr. 2018 m. liepos 10 d. Sprendimo *Jehovan todistajat*, C-25/17, EU:C:2018:551, 38 punktą ir nurodytą jurisprudenciją).

86 Galimybė, kad komerciniais tikslais tarp dviejų ūkio subjektų perduotus asmens duomenis atliekant perdavimą arba po jo atitinkamos trečiosios šalies valdžios institucijos tvarko visuomenės saugumo, gynybos ir valstybės saugumo tikslais, nereiškia, kad minėtas perdavimas nepatenka į BDAR taikymo sritį.

87 Be to, iš pačios šio reglamento 45 straipsnio 2 dalies a punkto, kuriame aiškiai nustatyta pareiga Komisijai, vertinant trečiosios šalies suteikiamo apsaugos lygio tinkamumą, be kita ko, 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“, formuluotės matyti, kad trečiosios šalies galbūt atliekamas atitinkamų duomenų tvarkymas visuomenės saugumo, gynybos ir valstybės saugumo tikslais nepaneigia minėto reglamento taikytinumo nagrinėjamam perdavimui.

88 Darytina išvada, jog toks perdavimas negali nepatekti į BDAR taikymo sritį dėl to, kad atitinkamus duomenis atliekant šį perdavimą arba po jo gali tvarkyti atitinkamos trečiosios šalies valdžios institucijos visuomenės saugumo, gynybos ir valstybės saugumo tikslais.

89 Taigi į pirmąjį klausimą reikia atsakyti: BDAR 2 straipsnio 1 ir 2 dalys turi būti aiškinamos taip, kad į šio reglamento taikymo sritį patenka asmens duomenų perdavimas, atliktas komerciniais tikslais valstybėje narėje įsteigto ūkio subjekto kitam trečiojoje šalyje įsteigtam ūkio subjektui, nepaisant to, ar atliekant šį perdavimą arba po jo atitinkamos trečiosios šalies valdžios institucijos gali tvarkyti šiuos duomenis visuomenės saugumo, gynybos ir valstybės saugumo tikslais.

Dėl antrojo, trečiojo ir šeštojo klausimų

90 Antruoju, trečiuoju ir šeštuoju klausimais prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės Teisingumo Teismo klausia dėl BDAR 46 straipsnio 1 dalyje ir 46 straipsnio 2 dalies c punkte reikalaujamo apsaugos lygio perduodant asmens duomenis į trečiąją šalį remiantis standartinėmis duomenų apsaugos sąlygomis. Konkrečiai tas teismas prašo Teisingumo Teismo paaiškinti aspektus, į kuriuos reikia atsižvelgti siekiant nustatyti, ar toks apsaugos lygis užtikrinamas tokio perdavimo atveju.

91 Kiek tai susiję su reikalaujamu apsaugos lygiu, iš siejamų šių nuostatų matyti, kad, jei nepriimtas sprendimas dėl tinkamumo pagal 45 straipsnio 3 dalį, duomenų valdytojas arba duomenų tvarkytojas gali perduoti asmens duomenis į trečiąją šalį tik tuo atveju, jeigu duomenų valdytojas arba duomenų tvarkytojas yra nustatęs „tinkamas apsaugos priemones“ ir su sąlyga, kad duomenų subjektai turėtų „vykdytinas [įgyvendinamas] teises ir veiksmingas teisių gynimo priemones“; šios tinkamos apsaugos priemonės, be kita ko, gali būti suteiktos Komisijos priimtomis standartinėmis duomenų apsaugos sąlygomis.

92 Nors BDAR 46 straipsnyje aiškiai nenurodytas iš šios nuorodos kylančių reikalavimų, susijusių su „tinkamomis apsaugos priemonėmis“, „vykdytinomis [įgyvendinamomis] teisėmis“ ir „veiksmingomis teisių gynimo priemonėmis“, pobūdis, pažymėtina, kad šis straipsnis yra šio reglamento V skyriuje, taigi turi būti aiškinamas atsižvelgiant į minėto reglamento 44 straipsnį „Bendras duomenų perdavimo principas“, kuriame nurodyta, kad „[v]isos [šio] skyriaus nuostatos taikomos siekiant užtikrinti, kad nebūtų pakenkta šiuo reglamentu garantuojamam fizinių asmenų apsaugos lygiui“. Todėl šis apsaugos lygis turi būti užtikrintas, kad ir kokia būtų to skyriaus nuostata, kuria remiantis asmens duomenys perduodami į trečiąją šalį.

93 Kaip savo išvados 117 punkte pažymėjo generalinis advokatas, BDAR V skyriumi siekiama užtikrinti šio aukšto apsaugos lygio tęstinumą, kai asmens duomenys perduodami į trečiąją šalį, vadovaujantis šio reglamento 6 konstatuojamojoje dalyje nurodytu tikslu.

94 BDAR 45 straipsnio 1 dalies pirmame sakinyje numatyta, kad galima leisti perduoti asmens duomenis į trečiąją šalį Komisijai priėmus sprendimą, pagal kurį ši trečioji šalis, teritorija arba vienas ar daugiau jame nurodytų sektorių toje šalyje užtikrina tinkamo lygio apsaugą. Šiuo aspektu pažymėtina, jog nereikalaujant, kad atitinkama trečioji šalis užtikrintų tokį patį apsaugos lygį, koks garantuojamas Sąjungos teisinėje sistemoje, žodžių junginys „tinkamas apsaugos lygis“ turi būti suprantamas, kaip patvirtina šio reglamento 104 konstatuojamoji dalis, kaip reikalaujantis, kad ši trečioji šalis savo nacionalinės teisės aktais arba tarptautiniais įsipareigojimais iš tikrųjų užtikrintų pagrindinių laisvių ir teisių apsaugos lygį, kuris būtų iš esmės lygiavertis tam, kuris garantuojamas Sąjungoje minėtu reglamentu, siejamu su Chartija. Be šio reikalavimo šio sprendimo ankstesniame punkte minėto tikslo faktiškai būtų nepaisoma (pagal analogiją dėl Direktyvos 95/46 25 straipsnio 6 dalies žr. 2015 m. spalio 6 d. Sprendimo *Schrems*, C-362/14, EU:C:2015:650, 73 punktą).

95 Šiomis aplinkybėmis BDAR 107 konstatuojamojoje dalyje nurodyta, kad jeigu „trečioji valstybė, teritorija arba nurodytas sektorius trečiojoje valstybėje <…> nebeužtikrina tinkamo lygio duomenų apsaugos[,] <…> perduoti asmens duomenis tai trečiajai šaliai <…> turėtų būti draudžiama, išskyrus atvejus, kai įvykdomi šiame reglamente nustatyti reikalavimai, susiję su perdavimu taikant tinkamas apsaugos priemones“. Šiuo tikslu minėto reglamento 108 konstatuojamojoje dalyje nurodyta, kad jei sprendimas dėl tinkamumo nepriimtas, tinkamos apsaugos priemonės, kurių pagal to paties reglamento 46 straipsnio 1 dalį turi imtis duomenų valdytojas arba duomenų tvarkytojas, turi „[kompensuoti] nepakankam[ą] duomenų apsaug[ą] trečiojoje valstybėje“ siekiant „užtikrin[ti], kad būtų laikomasi duomenų apsaugos reikalavimų, ir užtikrin[ti] tvarkant duomenis Sąjungoje tinkam[a]s duomenų subjektų teis[e]s“.

96 Iš to matyti, jog, kaip savo išvados 115 punkte pažymėjo generalinis advokatas, šiomis tinkamomis apsaugos priemonėmis turi būti užtikrinta, kad asmenims, kurių asmens duomenys perduodami į trečiąją šalį remiantis standartinėmis duomenų apsaugos sąlygomis, kaip ir perduodant duomenis pagal sprendimą dėl tinkamumo, būtų suteikiamas iš esmės lygiavertis apsaugos lygis, koks garantuojamas Sąjungoje.

97 Prašymą priimti prejudicinį sprendimą pateikusiam teismui taip pat kyla klausimas, ar šis apsaugos lygis, iš esmės lygiavertis Sąjungoje garantuojamam apsaugos lygiui, turi būti nustatytas atsižvelgiant į Sąjungos teisę, be kita ko, į Chartijoje garantuojamas teises, ir (arba) į pagrindines teises, įtvirtintas Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijoje (toliau – EŽTK), arba net atsižvelgiant į valstybių narių nacionalinę teisę.

98 Šiuo klausimu reikia priminti, kad nors, kaip patvirtina ESS 6 straipsnio 3 dalis, EŽTK įtvirtintos pagrindinės teisės sudaro Sąjungos teisės bendruosius principus ir nors pagal Chartijos 52 straipsnio 3 dalį Chartijoje numatytoms teisėms, atitinkančioms EŽTK užtikrinamas teises, suteikiama ta pati prasmė ir apimtis, kaip suteikta minėtos konvencijos, pastaroji, kol Sąjunga prie jos neprisijungė, nėra į jos teisinę sistemą formaliai įtraukta teisės priemonė (2013 m. vasario 26 d. Sprendimo *Åkerberg Fransson*, C-617/10, EU:C:2013:105, 44 punktas ir nurodyta jurisprudencija ir 2018 m. kovo 20 d. Sprendimo *Menci*, C-524/15, EU:C:2018:197, 22 punktas).

99 Tokiomis aplinkybėmis Teisingumo Teismas nusprendė, kad Sąjungos teisė turi būti aiškinama ir Sąjungos teisės aktų galiojimas turi būti vertinamas atsižvelgiant į Chartijoje užtikrinamas pagrindines teises (pagal analogiją žr. 2018 m. kovo 20 d. Sprendimo *Menci*, C-524/15, EU:C:2018:197, 24 punktą).

100 Be to, pagal suformuotą jurisprudenciją Sąjungos teisės nuostatų galiojimas ir, nesant aiškios nuorodos į valstybių narių nacionalinę teisę, jų aiškinimas negali būti vertinami atsižvelgiant į nacionalinę teisę, net konstitucinio statuso, ypač į pagrindines teises, kaip antai išdėstytas nacionalinėse konstitucijose (šiuo klausimu žr. 1970 m. gruodžio 17 d. Sprendimo *Internationale Handelsgesellschaft*, 11/70, EU:C:1970:114, 3 punktą; 1979 m. gruodžio 13 d. Sprendimo *Hauer*, 44/79, EU:C:1979:290, 14 punktą ir 2016 m. spalio 18 d. Sprendimo *Nikiforidis*, C-135/15, EU:C:2016:774, 28 punktą ir nurodytą jurisprudenciją).

101 Darytina išvada: kadangi, viena vertus, asmens duomenų perdavimas, kaip antai nagrinėjamas pagrindinėje byloje, kurį komerciniais tikslais atlieka valstybėje narėje įsteigtas ūkio subjektas kitam trečiojoje šalyje įsteigtam ūkio subjektui, kaip matyti iš atsakymo į pirmąjį klausimą, patenka į BDAR taikymo sritį, ir, kita vertus, šiuo reglamentu, kaip matyti iš jo 10 konstatuojamosios dalies, siekiama užtikrinti vienodo ir aukšto lygio fizinių asmenų apsaugą visoje Sąjungoje ir šiuo tikslu – nuoseklų ir vienodą taisyklių, reglamentuojančių šių asmenų pagrindinių teisių ir laisvių apsaugą tvarkant asmens duomenis, taikymą, šio reglamento 46 straipsnio 1 dalyje reikalaujamas pagrindinių teisių apsaugos lygis turi būti nustatytas remiantis to paties reglamento nuostatomis, siejamomis su Chartijoje užtikrinamomis pagrindinėmis teisėmis.

102 Prašymą priimti prejudicinį sprendimą pateikęs teismas taip pat siekia išsiaiškinti, į kokius aspektus reikia atsižvelgti norint nustatyti apsaugos lygio tinkamumą perduodant asmens duomenis į trečiąją šalį, remiantis standartinėmis duomenų apsaugos sąlygomis, priimtomis pagal BDAR 46 straipsnio 2 dalies c punktą.

103 Šiuo aspektu pažymėtina, kad nors šioje nuostatoje neišvardyti įvairūs veiksniai, į kuriuos reikia atsižvelgti vertinant apsaugos lygio, kurio turi būti laikomasi atliekant tokį perdavimą, tinkamumą, šio reglamento 46 straipsnio 1 dalyje nurodyta, kad duomenų subjektams turi būti suteiktos tinkamos garantijos ir jie turi turėti įgyvendinamas teises ir veiksmingas teisių gynimo priemones.

104 Šiuo tikslu atliekant tokio perdavimo kontekste reikalaujamą vertinimą, be kita ko, turi būti atsižvelgta ir į duomenų valdytojo ar jo duomenų tvarkytojo, įsteigtų Sąjungoje, ir perduodamų duomenų gavėjo, įsteigto atitinkamoje trečiojoje šalyje, sudarytų sutarčių sąlygas, ir, kiek tai susiję su galima šios trečiosios šalies valdžios institucijų prieiga prie perduotų asmens duomenų, į atitinkamus šios šalies teisinės sistemos aspektus. Pastaruoju klausimu pažymėtina, kad aspektai, į kuriuos reikia atsižvelgti, kalbant apie minėto reglamento 46 straipsnį, atitinka aspektus, kurių neišsamus sąrašas pateiktas jo 45 straipsnio 2 dalyje.

105 Taigi į antrąjį, trečiąjį ir šeštąjį klausimus reikia atsakyti: BDAR 46 straipsnio 1 dalis ir 2 dalies c punktas turi būti aiškinami taip, kad šiose nuostatose reikalaujamomis tinkamomis apsaugos priemonėmis, įgyvendinamomis teisėmis ir veiksmingomis duomenų subjektų teisių gynimo priemonėmis turi būti užtikrinama, kad asmenų, kurių asmens duomenys perduodami į trečiąją šalį remiantis standartinėmis duomenų apsaugos sąlygomis, teisių apsaugos lygis būtų iš esmės lygiavertis tam, kuris garantuojamas Sąjungoje šiuo reglamentu, siejamu su Chartija. Šiuo tikslu, vertinant tokio perdavimo atveju užtikrinamą apsaugos lygį, be kita ko, turi būti atsižvelgta ir į duomenų valdytojo ar jo duomenų tvarkytojo, įsteigtų Sąjungoje, ir perduodamų duomenų gavėjo, įsteigto atitinkamoje trečiojoje šalyje, sudarytų sutarčių sąlygas, ir, kiek tai susiję su galima šios trečiosios šalies valdžios institucijų prieiga prie taip perduotų asmens duomenų, į atitinkamus šios šalies teisinės sistemos aspektus, be kita ko, nurodytus to reglamento 45 straipsnio 2 dalyje.

Dėl aštuntojo klausimo

106 Aštuntuoju klausimu prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės siekia išsiaiškinti, ar BDAR 58 straipsnio 2 dalies f ir j punktai turi būti aiškinami taip, kad kompetentinga priežiūros institucija turi sustabdyti arba uždrausti asmens duomenų perdavimą į trečiąją šalį, grindžiamą Komisijos priimtomis standartinėmis duomenų apsaugos sąlygomis, jei mano, kad šioje trečiojoje šalyje šių sąlygų nesilaikoma arba jų negalima laikytis ir kad negalima užtikrinti pagal Sąjungos teisę, visų pirma pagal BDAR 45 bei 46 straipsnius ir Chartiją, reikalaujamos perduodamų duomenų apsaugos, ar vis dėlto taip, kad pasinaudoti šiais įgaliojimais galima tik išimtiniais atvejais.

107 Pagal Chartijos 8 straipsnio 3 dalį, BDAR 51 straipsnio 1 dalį ir 57 straipsnio 1 dalies a punktą nacionalinės priežiūros institucijos yra atsakingos už Sąjungos taisyklių, susijusių su fizinių asmenų apsauga tvarkant asmens duomenis, laikymosi kontrolę. Todėl kiekviena iš jų turi kompetenciją patikrinti, ar asmens duomenų perdavimas iš valstybės narės, kuriai ji priklauso, į trečiąją šalį atitinka šiame reglamente nustatytus reikalavimus (pagal analogiją dėl Direktyvos 95/46 28 straipsnio žr. 2015 m. spalio 6 d. Sprendimo *Schrems*, C-362/14, EU:C:2015:650, 47 punktą).

108 Iš šių nuostatų matyti, kad priežiūros institucijų pagrindinė užduotis yra kontroliuoti BDAR taikymą ir užtikrinti jo laikymąsi. Šios užduoties vykdymas ypač svarbus, kai asmens duomenys perduodami į trečiąją šalį, nes, kaip matyti iš pačios šio reglamento 116 konstatuojamosios dalies formuluotės, „kai asmens duomenys perduodami iš vienos valstybės į kitą už Sąjungos ribų, asmenims gali būti daug sunkiau pasinaudoti teisėmis į duomenų apsaugą, visų pirma apsisaugoti nuo neteisėto tų duomenų naudojimo arba atskleidimo“. Tokiu atveju, kaip nurodyta toje pačioje konstatuojamojoje dalyje, „priežiūros institucijos gali nesugebėti nagrinėti skundų ar vykdyti tyrimų, susijusių su veikla už jų valstybės sienų“.

109 Be to, pagal BDAR 57 straipsnio 1 dalies f punktą kiekviena priežiūros institucija savo teritorijoje privalo nagrinėti skundus, kuriuos pagal šio reglamento 77 straipsnio 1 dalį turi teisę pateikti bet kuris asmuo, kai mano, kad tvarkant jo asmens duomenis pažeistas minėtas reglamentas, ir tinkamu mastu tirti šių skundų dalyką. Priežiūros institucija turi ypač kruopščiai, kaip to reikalaujama, išnagrinėti tokį skundą (pagal analogiją dėl Direktyvos 95/46 25 straipsnio 6 dalies žr. 2015 m. spalio 6 d. Sprendimo *Schrems*, C-362/14, EU:C:2015:650, 63 punktą).

110 BDAR 78 straipsnio 1 ir 2 dalyse kiekvienam asmeniui pripažįstama teisė imtis veiksmingų teisminių teisių gynimo priemonių, be kita ko, kai priežiūros institucija neišnagrinėja jo skundo. Šio reglamento 141 konstatuojamojoje dalyje taip pat nurodyta „teisė į veiksmingą teisminę teisių gynimo priemonę pagal Chartijos 47 straipsnį“ tuo atveju, jei ši priežiūros institucija „nesiima veiksmų, kai tokie veiksmai yra būtini duomenų subjekto teisėms apsaugoti“.

111 Tam, kad būtų išnagrinėti pateikti skundai, BDAR 58 straipsnio 1 dalyje kiekvienai priežiūros institucijai suteikti dideli tyrimo įgaliojimai. Kai atlikusi tyrimą tokia institucija mano, jog duomenų subjektui, kurio asmens duomenys buvo perduoti į trečiąją šalį, toje šalyje nėra suteikiamas tinkamas apsaugos lygis, ji pagal Sąjungos teisę privalo tinkamai reaguoti, kad būtų ištaisytas nustatytas nepakankamumas, nepaisant šio nepakankamumo kilmės ar pobūdžio. Šiuo tikslu šio reglamento 58 straipsnio 2 dalyje išvardyti įvairūs taisomieji veiksmai, kurių gali imtis priežiūros institucija.

112 Nors tinkamą ir reikiamą priemonę turi pasirinkti priežiūros institucija ir tai daryti ji turi atsižvelgdama į visas atitinkamo asmens duomenų perdavimo aplinkybes, ši institucija privalo ypač kruopščiai, kaip to reikalaujama, vykdyti savo užduotį – užtikrinti visapusišką BDAR laikymąsi.

113 Šiuo klausimu, kaip savo išvados 148 punkte taip pat nurodė generalinis advokatas, pažymėtina, kad minėta institucija pagal šio reglamento 58 straipsnio 2 dalies f ir j punktus privalo sustabdyti arba uždrausti asmens duomenų perdavimą į trečiąją šalį, jeigu, atsižvelgdama į visas šio perdavimo aplinkybes, mano, kad šioje trečiojoje šalyje nėra arba negali būti laikomasi standartinių duomenų apsaugos sąlygų ir kad pagal Sąjungos teisę reikalaujamos apsaugos negalima užtikrinti kitomis priemonėmis, ir jeigu duomenų valdytojas arba duomenų tvarkytojas, įsteigti Sąjungoje, patys nesustabdė ar nenutraukė šio perdavimo.

114 Pirmesniame punkte pateikto aiškinimo nepaneigia komisaro argumentai, kad prieš įsigaliojant Įgyvendinimo sprendimui 2016/2297 galiojusios redakcijos Sprendimo 2010/87 4 straipsniu, siejamu su šio sprendimo 11 konstatuojamąja dalimi, priežiūros institucijų įgaliojimai sustabdyti arba uždrausti asmens duomenų perdavimą į trečiąją šalį buvo apriboti iki tam tikrų išimtinių atvejų. Iš tiesų SAS sprendimo 4 straipsnio redakcijoje su pakeitimais, padarytais Įgyvendinimo sprendimu 2016/2297, nurodyti dabar pagal BDAR 58 straipsnio 2 dalies f ir j punktus šių institucijų turimi įgaliojimai sustabdyti arba uždrausti tokį perdavimą, naudojimosi šiais įgaliojimais niekaip neapribojant išimtinėmis aplinkybėmis.

115 Bet kuriuo atveju Komisijai pagal BDAR 46 straipsnio 2 dalies c punktą pripažintais įgyvendinimo įgaliojimais priimti standartines duomenų apsaugos sąlygas jai nesuteikiama kompetencija apriboti priežiūros institucijų pagal šio reglamento 58 straipsnio 2 dalį turimus įgaliojimus (pagal analogiją dėl Direktyvos 95/46 25 straipsnio 6 dalies ir 28 straipsnio žr. 2015 m. spalio 6 d. Sprendimo *Schrems*, C-362/14, EU:C:2015:650, 102 ir 103 punktus). Be to, Įgyvendinimo sprendimo 2016/2297 5 konstatuojamojoje dalyje patvirtinta, kad SAS sprendimas „neužkerta kelio <…> priežiūros institucijai naudotis savo įgaliojimais prižiūrėti duomenų srautus, įskaitant įgaliojimus sustabdyti arba uždrausti asmens duomenų perdavimą, kuomet ji nustato, kad duomenys perduodami pažeidžiant ES arba nacionalinės duomenų apsaugos teisės aktus, pavyzdžiui, kai duomenų importuotojas nesilaiko standartinių sutarčių sąlygų“.

116 Vis dėlto reikia paaiškinti, kad kompetentingos priežiūros institucijos įgaliojimai turi būti įgyvendinami visapusiškai laikantis sprendimo, kuriame Komisija prireikus pagal BDAR 45 straipsnio 1 dalies pirmą sakinį konstatuoja, kad tam tikra trečioji šalis užtikrina tinkamą apsaugos lygį. Tokiu atveju iš šio reglamento 45 straipsnio 1 dalies antro sakinio, siejamo su jo 103 konstatuojamąja dalimi, matyti, kad asmens duomenys gali būti perduodami į atitinkamą trečiąją šalį be būtinybės gauti specialų leidimą.

117 Pagal SESV 288 straipsnio ketvirtą pastraipą Komisijos sprendimas dėl tinkamumo privalomas visas visoms valstybėms narėms, kurioms skirtas, taigi ir visoms jų institucijoms, tiek, kiek juo konstatuojama, kad atitinkama trečioji šalis užtikrina tinkamą apsaugos lygį ir kiek pagal jį leidžiamas šis duomenų perdavimas (pagal analogiją dėl Direktyvos 95/46 25 straipsnio 6 dalies žr. 2015 m. spalio 6 d. Sprendimo *Schrems*, C-362/14, EU:C:2015:650, 51 punktą ir nurodytą jurisprudenciją).

118 Taigi tol, kol Teisingumo Teismas nepripažįsta negaliojančiu sprendimo dėl tinkamumo, valstybės narės ir jų institucijos, tarp kurių yra jų nepriklausomos priežiūros institucijos, negali imtis šiam sprendimui prieštaraujančių priemonių, kaip antai priimti privalomų aktų, kuriais siekiama

konstatuoti, kad minėtame sprendime nurodyta trečioji šalis neužtikrina tinkamo apsaugos lygio (2015 m. spalio 6 d. Sprendimo *Schrems*, C-362/14, EU:C:2015:650, 52 punktas ir nurodyta jurisprudencija), ir dėl to sustabdyti arba uždrausti asmens duomenų perdavimą į šią trečiąją šalį.

119 Vis dėlto pagal BDAR 45 straipsnio 3 dalį Komisijos priimtas sprendimas dėl tinkamumo negali užkirsti kelio asmenims, kurių asmens duomenys buvo ar galėjo būti perduoti į trečiąją šalį, pagal BDAR 77 straipsnio 1 dalį paduoti kompetentingai nacionalinei priežiūros institucijai skundą dėl jų teisių ir laisvių apsaugos tvarkant šiuos duomenis. Be to, tokio pobūdžio sprendimu negali būti panaikinti ar apriboti įgaliojimai, nacionalinės priežiūros institucijoms aiškiai suteikti pagal Chartijos 8 straipsnio 3 dalį, minėto reglamento 51 straipsnio 1 dalį ir 57 straipsnio 1 dalies a punktą (pagal analogiją dėl Direktyvos 95/46 25 straipsnio 6 dalies ir 28 straipsnio žr. 2015 m. spalio 6 d. Sprendimo *Schrems*, C-362/14, EU:C:2015:650, 53 punktą).

120 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 (pagal analogiją dėl Direktyvos 95/46 25 straipsnio 6 dalies ir 28 straipsnio žr. 2015 m. spalio 6 d. Sprendimo *Schrems*, C-362/14, EU:C:2015:650, 57 ir 65 punktus).

121 Atsižvelgiant į tai, kas išdėstyta, į aštuntąjį klausimą reikia atsakyti: BDAR 58 straipsnio 2 dalies f ir j punktai turi būti aiškinami taip, kad, nebent Komisija yra teisėtai priėmusi sprendimą dėl tinkamumo, kompetentinga priežiūros institucija turi sustabdyti arba uždrausti duomenų perdavimą į trečiąją šalį, grindžiamą Komisijos priimtomis standartinėmis duomenų apsaugos sąlygomis, jei, atsižvelgdama į visas konkrečias šio perdavimo aplinkybes, mano, kad šioje trečiojoje šalyje šių sąlygų nesilaikoma arba jų negalima laikytis ir kad kitomis priemonėmis negalima užtikrinti pagal Sąjungos teisę, visų pirma pagal BDAR 45 bei 46 straipsnius ir Chartiją, reikalaujamos perduodamų duomenų apsaugos, jeigu Sąjungoje įsteigtas duomenų valdytojas arba duomenų tvarkytojas pats nesustabdė arba nenutraukė duomenų perdavimo.

Dėl septintojo ir vienuoliktojo klausimų

122 Septintuoju ir vienuoliktuoju klausimais, kuriuos reikia nagrinėti kartu, prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės klausia Teisingumo Teismo dėl SAS sprendimo galiojimo atsižvelgiant į Chartijos 7, 8 ir 47 straipsnius.

123 Konkrečiai kalbant, kaip matyti iš pačios septintojo klausimo formuluotės ir prašyme priimti prejudicinį sprendimą pateiktų dėl jo pateiktų paaiškinimų, prašymą priimti prejudicinį sprendimą pateikusiam teismui kyla klausimas, ar SAS sprendimu gali būti užtikrintas tinkamas į trečiąsias šalis perduodamų asmens duomenų apsaugos lygis, atsižvelgiant į tai, kad jame numatytos standartinės duomenų apsaugos sąlygos nėra privalomos šių trečiųjų šalių valdžios institucijoms.

124 SAS sprendimo 1 straipsnyje nurodyta, kad šio sprendimo priede pateiktos standartinės duomenų apsaugos sąlygos laikomos užtikrinančiomis tinkamas apsaugos priemones asmenų privatumui, pagrindinėms teisėms ir laisvėms apsaugoti pagal Direktyvos 95/46 26 straipsnio 2 dalies reikalavimus. Pastaroji nuostata iš esmės buvo pakartota BDAR 46 straipsnio 1 dalyje ir 2 dalies c punkte.

125 Vis dėlto, nors šios sąlygos yra privalomos Sąjungoje įsteigtam duomenų valdytojui ir trečiojoje šalyje įsteigtam perduodamų asmens duomenų gavėjui, jeigu jie yra sudarę sutartį pagal šias sąlygas, neginčijama, kad minėtos sąlygos negali saistyti šios trečiosios šalies institucijų, nes jos nėra sutarties šalys.

126 Vadinasi, nors yra atvejų, kai, atsižvelgiant į atitinkamoje trečiojoje šalyje galiojančią teisę ir esamą praktiką, tokių perduodamų duomenų gavėjas gali užtikrinti būtiną duomenų apsaugą, remdamasis vien standartinėmis duomenų apsaugos sąlygomis, yra ir kitų atvejų, kai šiose sąlygose išdėstytos nuostatos gali nebūti pakankama priemonė praktiškai užtikrinti veiksmingą atitinkamoje trečiojoje šalyje perduodamų asmens duomenų apsaugą. Taip, be kita ko, yra tuo atveju, jei pagal šios trečiosios šalies teisę jos valdžios institucijoms leidžiama varžyti duomenų subjektų teises, susijusias su šiais duomenimis.

127 Taigi kyla klausimas, ar Komisijos sprendimas dėl standartinių duomenų apsaugos sąlygų, priimtas remiantis RGPD 46 straipsnio 2 dalies c punktu, negalioja, kai tame sprendime nėra garantijų, kuriomis galima remtis prieš trečiųjų šalių, į kurias asmens duomenys yra arba gali būti perduoti remiantis šiomis sąlygomis, valdžios institucijas.

128 BDAR 46 straipsnio 1 dalyje numatyta, kad jeigu nėra priimta sprendimo dėl tinkamumo, duomenų valdytojas arba duomenų tvarkytojas gali perduoti asmens duomenis į trečiąją valstybę tik tuo atveju, jei duomenų valdytojas arba duomenų tvarkytojas yra nustatęs tinkamas apsaugos priemones, su sąlyga, kad suteikiama galimybė naudotis įgyvendinamomis duomenų subjektų teisėmis ir veiksmingomis duomenų subjektų teisių gynimo priemonėmis. Pagal šio reglamento 46 straipsnio 2 dalies c punktą šios garantijos gali būti suteiktos Komisijos priimtomis standartinėmis duomenų apsaugos sąlygomis. Tačiau šiose nuostatose nenurodyta, kad visos minėtos garantijos būtinai turi būti numatytos Komisijos sprendime, kaip antai SAS sprendime.

129 Šiuo klausimu reikia pažymėti, jog toks sprendimas skiriasi nuo pagal RGPD 45 straipsnio 3 dalį priimto sprendimo dėl tinkamumo, kuriuo, išnagrinėjus atitinkamos trečiosios šalies teisės aktus, atsižvelgiant, be kita ko, į atitinkamus teisės aktus dėl nacionalinio saugumo ir valdžios institucijų prieigos prie asmens duomenų, siekiama privalomai konstatuoti, kad trečioji šalis, teritorija arba vienas ar daugiau nurodytų sektorių toje šalyje užtikrina tinkamą apsaugos lygį ir kad dėl to minėtos šalies valdžios institucijų prieiga prie tokių duomenų netrukdo duomenų perdavimui į šią trečiąją šalį. Taigi tokį sprendimą dėl tinkamumo Komisija gali priimti tik su sąlyga, kad konstatavo, jog atitinkamais šios trečiosios šalies teisės aktais šioje srityje iš tikrųjų suteikiamos visos reikiamos garantijos, leidžiančios manyti, kad jais užtikrinamas tinkamas apsaugos lygis.

130 Vis dėlto, kalbant apie Komisijos sprendimą, kuriuo priimamos standartinės duomenų apsaugos sąlygos, kaip antai SAS sprendimą, pažymėtina: kadangi toks sprendimas nesusijęs su trečiąja šalimi, teritorija arba vienu ar daugiau nurodytų sektorių toje šalyje, remiantis BDAR 46 straipsnio 1 dalimi ir 46 straipsnio 2 dalies c punktu negalima daryti išvados, kad prieš priimdama tokį sprendimą Komisija privalo įvertinti trečiosiose šalyse, į kurias asmens duomenys gali būti perduoti remiantis tokiomis sąlygomis, užtikrinamo apsaugos lygio tinkamumą.

131 Šiuo klausimu reikia priminti, kad pagal šio reglamento 46 straipsnio 1 dalį, jei Komisija nėra priėmusi sprendimo dėl tinkamumo, duomenų valdytojas arba duomenų tvarkytojas, įsteigti Sąjungoje, turi, be kita ko, numatyti tinkamas apsaugos priemones. Minėto reglamento 108 ir 114 konstatuojamosiose dalyse patvirtinta, kad jei Komisija nėra priėmusi sprendimo dėl duomenų apsaugos lygio trečiojoje valstybėje tinkamumo, duomenų valdytojas arba prireikus duomenų tvarkytojas „turėtų duomenų subjektams numatyti tinkamas apsaugos priemones nepakankamai duomenų apsaugai trečiojoje valstybėje kompensuoti“, ir kad „[t]omis apsaugos priemonėmis turėtų būti užtikrinama, kad būtų laikomasi duomenų apsaugos reikalavimų, ir užtikrinamos tvarkant duomenis Sąjungoje tinkamos duomenų subjektų teisės, įskaitant galimybes naudotis vykdytinomis [įgyvendinamomis] duomenų subjekto teisėmis ir veiksmingomis teisių gynimo priemonėmis <…> Sąjungoje ar trečiojoje valstybėje“.

132 Kadangi, kaip matyti iš šio sprendimo 125 punkto, standartinių duomenų apsaugos sąlygų sutartiniam pobūdžiui būdinga tai, kad jos negali saistyti trečiųjų šalių valdžios institucijų, tačiau pagal BDAR 44 straipsnį, 46 straipsnio 1 dalį ir 46 straipsnio 2 dalies c punktą, siejamus su Chartijos 7, 8 ir 47 straipsniais, reikalaujama užtikrinti, kad nebūtų pakenkta šiuo reglamentu garantuojamam fizinių

asmenų apsaugos lygiui, gali būti būtina papildyti šiose standartinėse duomenų apsaugos sąlygose nustatytas garantijas. Šiuo aspektu minėto reglamento 109 konstatuojamojoje dalyje nustatyta, kad „galimybė duomenų valdytojui <…> remtis Komisijos <…> priimtomis standartinėmis duomenų apsaugos sąlygomis neturėtų užkirsti kelio duomenų valdytojams <…> jas papildyti kitomis sąlygomis ar papildomomis apsaugos sąlygomis“, ir konkrečiai nurodyta, kad duomenų valdytojai „turėtų būti skatinami taikyti dar griežtesnes apsaugos priemones <…>, papildanči[a]s standartines duomenų apsaugos sąlygas“.

133 Taigi Komisijos pagal to paties reglamento 46 straipsnio 2 dalies c punktą priimtomis standartinėmis duomenų apsaugos sąlygomis tik siekiama duomenų valdytojams arba duomenų tvarkytojams, įsteigtiems Sąjungoje, suteikti sutartines garantijas, kurios būtų vienodai taikomos visose trečiosiose šalyse, taigi neatsižvelgiant į kiekvienoje iš jų užtikrinamą apsaugos lygį. Kadangi, atsižvelgiant į šių standartinių duomenų apsaugos sąlygų pobūdį, jomis negali būti suteiktos garantijos, viršijančios sutartinę prievolę užtikrinti, kad būtų laikomasi pagal Sąjungos teisę reikalaujamo apsaugos lygio, dėl šių sąlygų, atsižvelgiant į padėtį vienoje ar kitoje trečiojoje šalyje, duomenų valdytojui gali būti būtina imtis papildomų priemonių šio apsaugos lygio laikymuisi užtikrinti.

134 Šiuo aspektu pažymėtina, kad, kaip savo išvados 126 punkte nurodė generalinis advokatas, BDAR 46 straipsnio 2 dalies c punkte numatytas sutartinis mechanizmas grindžiamas duomenų valdytojo arba duomenų tvarkytojo, įsteigtų Sąjungoje, ir subsidiariai kompetentingos priežiūros institucijos atsakomybe. Todėl šis duomenų valdytojas arba duomenų tvarkytojas, visų pirma kiekvienu atveju ir prireikus bendradarbiaudamas su duomenų gavėju, turi patikrinti, ar pagal paskirties trečiosios šalies teisę užtikrinama tinkama, atsižvelgiant į Sąjungos teisę, asmens duomenų, perduodamų remiantis standartinėmis duomenų apsaugos sąlygomis, apsauga ir prireikus suteikiama papildomų garantijų, be tų, kurios numatytos šiose sąlygose.

135 Jeigu duomenų valdytojas arba duomenų tvarkytojas, įsteigti Sąjungoje, negali imtis papildomų priemonių, kurių pakaktų tokiai apsaugai užtikrinti, jie arba subsidiariai kompetentinga priežiūros institucija privalo sustabdyti arba nutraukti asmens duomenų perdavimą į atitinkamą trečiąją šalį. Taip, be kita ko, yra tuo atveju, kai šios trečiosios šalies teisėje iš Sąjungos perduodamų asmens duomenų gavėjui nustatytos pareigos, prieštaraujančios minėtoms sąlygoms, taigi ir galinčios daryti poveikį apsaugos nuo tos trečiosios šalies valdžios institucijų prieigos prie šių duomenų tinkamo lygio sutartinei garantijai.

136 Taigi vien tai, kad pagal BDAR 46 straipsnio 2 dalies c punktą priimtame Komisijos sprendime pateiktos standartinės duomenų apsaugos sąlygos, kaip antai išdėstytos SAS sprendimo priede, nėra privalomos trečiųjų šalių, į kurias gali būti perduodami asmens duomenys, valdžios institucijoms, negali turėti įtakos šio sprendimo galiojimui.

137 Vis dėlto šis galiojimas priklauso nuo to, ar, remiantis iš BDAR 46 straipsnio 1 dalies ir 2 dalies c punkto, siejamų su Chartijos 7, 8 ir 47 straipsniais, kylančiu reikalavimu, tokiame sprendime yra įtvirtinti veiksmingi mechanizmai, leidžiantys praktiškai užtikrinti, kad būtų laikomasi Sąjungos teisėje reikalaujamo apsaugos lygio ir kad asmens duomenų perdavimas, grindžiamas tokiomis sąlygomis, būtų sustabdytas arba uždraustas pažeidus šias sąlygas arba nesant galimybės jų laikytis.

138 Kiek tai susiję su garantijomis, nustatytomis SAS sprendimo priede pateiktose standartinėse duomenų apsaugos sąlygose, iš šio priedo 4 sąlygos a ir b punktų, 5 sąlygos a punkto, 9 sąlygos ir 11 sąlygos 1 dalies matyti, kad Sąjungoje įsteigtas duomenų valdytojas, perduodamų asmens duomenų gavėjas ir galbūt šio gavėjo duomenų tvarkytojas tarpusavyje įsipareigoja, kad šių duomenų tvarkymas, įskaitant jų perdavimą, yra ir bus vykdomas laikantis „taikytinos duomenų apsaugos teisės“, t. y. pagal minėto sprendimo 3 straipsnio f punkte pateiktą apibrėžtį „teisės aktų, ginančių pagrindines asmenų teises ir laisves (ypač jų teisę į privatų gyvenimą) tvarkant asmens duomenis, kurių turi laikytis duomenų valdytojas toje valstybėje narėje, kurioje įsikūręs duomenų eksportuotojas“. BDAR nuostatos, siejamos su Chartija, yra šių teisės aktų dalis.

139 Be to, trečiojoje šalyje įsteigtas perduodamų asmens duomenų gavėjas pagal šios 5 sąlygos a punktą įsipareigoja kuo skubiau pranešti duomenų eksportuotojui apie tai, kad negali laikytis pareigų pagal sudarytą sutartį. Kalbant konkrečiai, pagal minėtos 5 sąlygos b punktą šis duomenų gavėjas patvirtina, jog neturi jokio pagrindo manyti, kad pagal jam taikytiną teisę negalės vykdyti pareigų pagal sudarytą sutartį, ir įsipareigoja kuo greičiau, kai tik apie tai sužinos, pranešti duomenų valdytojui apie visus jam taikytinų nacionalinės teisės aktų pakeitimus, kurie gali turi didelį neigiamą poveikį pagal SAS sprendimo priede pateiktas standartines duomenų apsaugos sąlygas teikiamoms garantijoms ir prisiimtiems įsipareigojimams. Be to, nors pagal tos pačios 5 sąlygos d punkto i papunktį perduodamų asmens duomenų gavėjui leidžiama nepranešti Sąjungoje įsteigtam duomenų valdytojui apie bet kokį teisiškai įpareigojantį teisėsaugos institucijų prašymą atskleisti asmens duomenis, jei pagal teisės aktus jam tai draudžiama, pavyzdžiui, nustatytas draudimas pagal baudžiamąją teisę, kuriuo siekiama užtikrinti teisėsaugos institucijų vykdomo tyrimo konfidencialumą, jis vis tiek pagal SAS sprendimo priedo 5 sąlygos a punktą privalo informuoti duomenų valdytoją, kad negali laikytis standartinių duomenų apsaugos sąlygų.

140 Abiem šios 5 sąlygos a ir b punktuose nurodytais atvejais pagal šią sąlygą Sąjungoje įsteigtam duomenų valdytojui suteikiama teisė sustabdyti duomenų perdavimą ir (arba) nutraukti sutartį. Atsižvelgiant į reikalavimus, kylančius iš BDAR 46 straipsnio 1 dalies ir 46 straipsnio 2 dalies c punkto, siejamų su Chartijos 7 ir 8 straipsniais, duomenų perdavimo sustabdymas ir (arba) sutarties nutraukimas yra privalomi duomenų valdytojui, kai duomenų gavėjas negali arba nebegali laikytis standartinių duomenų apsaugos sąlygų. Priešingu atveju duomenų valdytojas pažeistų reikalavimus, jam tenkančius pagal SAS sprendimo priedo 4 sąlygos a punktą, siejamą su BDAR ir Chartijos nuostatomis.

141 Taigi šio priedo 4 sąlygos a punkte ir 5 sąlygos a ir b punktuose Sąjungoje įsteigtas duomenų valdytojas ir perduodamų asmens duomenų gavėjas įpareigojami, prieš perduodant asmens duomenis į paskirties trečiąją šalį, įsitikinti, kad pagal šios trečiosios šalies teisės aktus minėtam gavėjui sudaromos sąlygos laikytis SAS sprendimo priede pateiktų standartinių duomenų apsaugos sąlygų. Kalbant apie šį patikrinimą, pažymėtina, jog su minėta 5 sąlyga susijusioje išnašoje nurodyta, kad privalomi šių teisės aktų reikalavimai, neviršijantys demokratinėje visuomenėje reikalingų apribojimų, be kita ko, siekiant užtikrinti nacionalinį saugumą, gynybą ir visuomenės saugumą, neprieštarauja šioms standartinėms duomenų apsaugos sąlygoms. Atvirkščiai, kaip savo išvados 131 punkte pažymėjo generalinis advokatas, paskirties trečiosios šalies teisėje įtvirtintos pareigos, viršijančios tai, kas būtina tokiais tikslais, laikymasis turi būti laikomas minėtų sąlygų pažeidimu. Šiems subjektams vertinant tokios pareigos būtinumą, prireikus turi būti atsižvelgta į atitinkamos trečiosios šalies užtikrinamo apsaugos lygio tinkamumo konstatavimą, pateiktą pagal BDAR 45 straipsnio 3 dalį priimtame Komisijos sprendime dėl tinkamumo.

142 Iš to matyti, kad Sąjungoje įsteigtas duomenų valdytojas ir perduodamų asmens duomenų gavėjas turi iš anksto patikrinti, ar atitinkamoje trečiojoje šalyje laikomasi Sąjungos teisėje reikalaujamo apsaugos lygio. Šių duomenų gavėjas prireikus pagal tos pačios 5 sąlygos b punktą privalo informuoti duomenų valdytoją, jei negali laikytis šių sąlygų, o duomenų valdytojas tuomet turi sustabdyti duomenų perdavimą ir (arba) nutraukti sutartį.

143 Jei į trečiąją šalį perduodamų asmens duomenų gavėjas pagal SAS sprendimo priedo 5 sąlygos b punktą pranešė duomenų valdytojui, kad pagal atitinkamos trečiosios šalies teisės aktus jam nesudaromos sąlygos laikytis šiame priede pateiktų standartinių duomenų apsaugos sąlygų, iš minėto priedo 12 sąlygos matyti, kad duomenys, kurie jau buvo perduoti į šią trečiąją šalį, ir jų kopijos turi būti grąžinamos arba sunaikintos. Bet kuriuo atveju to paties priedo 6 sąlygoje numatyta sankcija už šių standartinių sąlygų nesilaikymą, duomenų subjektui suteikiant teisę gauti kompensaciją dėl patirtos žalos.

144 Reikia pridurti, kad pagal SAS sprendimo priedo 4 sąlygos f punktą tuo atveju, kai ypatingų kategorijų duomenys gali būti perduoti į tinkamo apsaugos lygio neužtikrinančią trečiąją šalį, Sąjungoje įsteigtas duomenų valdytojas įsipareigoja apie tai pranešti duomenų subjektui prieš arba kuo greičiau po

duomenų perdavimo. Gavęs šią informaciją šis subjektas gali pasinaudoti jam šio priedo 3 sąlygos 1 dalyje suteikta teise į teisinę gynybą duomenų valdytojo atžvilgiu, kad šis valdytojas sustabdytų numatomą duomenų perdavimą, nutrauktų su perduodamų asmens duomenų gavėju sudarytą sutartį, arba prireikus pareikalauti, kad šis duomenų gavėjas grąžintų arba sunaikintų perduotus duomenis.

145 Galiausiai, remiantis minėto priedo 4 sąlygos g punktu, kai perduodamų asmens duomenų gavėjas pagal jo 5 sąlygos b punktą Sąjungoje įsteigtam duomenų valdytojui praneša apie jam taikytinų teisės aktų pakeitimus, kurie gali turi didelį neigiamą poveikį pagal standartines duomenų apsaugos sąlygas teikiamoms garantijoms ir prisiimtiems įsipareigojimams, šis duomenų valdytojas turi persiųsti šį pranešimą kompetentingai priežiūros institucijai, jeigu, nepaisydamas minėto pranešimo, nusprendžia tęsti perdavimą arba nutraukti sustabdymą. Tokio pranešimo persiuntimas šiai priežiūros institucijai ir jos teisė pagal to paties priedo 8 sąlygos 2 dalį atlikti perduodamų asmens duomenų gavėjo patikrinimus sudaro sąlygas šiai priežiūros institucijai patikrinti, ar reikia sustabdyti arba uždrausti numatomą duomenų perdavimą siekiant užtikrinti tinkamą apsaugos lygį.

146 Šiomis aplinkybėmis SAS sprendimo 4 straipsniu, siejamu su Įgyvendinimo sprendimo 2016/2297 5 konstatuojamąja dalimi, patvirtinama, kad SAS sprendimu kompetentingai priežiūros institucijai visiškai netrukdoma sustabdyti ar prireikus uždrausti asmens duomenų perdavimą į trečiąją šalį, atliekamą remiantis šio sprendimo priede pateiktomis standartinėmis duomenų apsaugos sąlygomis. Šiuo aspektu pažymėtina, kad, kaip matyti iš atsakymo į aštuntąjį klausimą, nebent Komisija yra teisėtai priėmusi sprendimą dėl tinkamumo, kompetentinga priežiūros institucija pagal BDAR 58 straipsnio 2 dalies f ir j punktus turi sustabdyti arba uždrausti tokį duomenų perdavimą, jei, atsižvelgdama į visas konkrečias šio perdavimo aplinkybes, mano, kad šioje trečiojoje šalyje šių sąlygų nesilaikoma arba jų negalima laikytis ir kad kitomis priemonėmis negalima užtikrinti Sąjungos teisėje reikalaujamos perduodamų duomenų apsaugos, jeigu Sąjungoje įsteigtas duomenų valdytojas arba duomenų tvarkytojas pats nesustabdė arba nenutraukė duomenų perdavimo.

147 Dėl komisaro nurodytos aplinkybės, kad dėl asmens duomenų perdavimo į tokią trečiąją šalį įvairių valstybių narių priežiūros institucijos gali priimti skirtingus sprendimus, reikia pridurti, kad, kaip matyti iš BDAR 55 straipsnio 1 dalies ir 57 straipsnio 1 dalies a punkto, užduotis užtikrinti šio reglamento laikymąsi iš principo patikėta kiekvienai valstybės narės priežiūros institucijai jos valstybės narės teritorijoje. Be to, siekiant išvengti skirtingų sprendimų, minėto reglamento 64 straipsnio 2 dalyje numatyta priežiūros institucijos, kuri mano, kad apskritai turi būti uždrausta perduoti duomenis į trečiąją šalį, galimybė kreiptis į Europos duomenų apsaugos valdybą (EDAV), kad ši pateiktų nuomonę; ši valdyba pagal to paties reglamento 65 straipsnio 1 dalies c punktą gali priimti privalomą sprendimą, be kita ko, jei priežiūros institucija nesilaiko pateiktos nuomonės.

148 Darytina išvada, jog SAS sprendime numatyti veiksmingi mechanizmai, praktiškai sudarantys sąlygas užtikrinti, kad asmens duomenų perdavimas į trečiąją šalį remiantis šio sprendimo priede pateiktomis standartinėmis duomenų apsaugos sąlygomis būtų sustabdytas arba uždraustas, jei duomenų gavėjas nesilaiko arba negali laikytis tų sąlygų.

149 Atsižvelgiant į visa tai, kas išdėstyta, į septintąjį ir vienuoliktąjį klausimus reikia atsakyti taip: išnagrinėjus SAS sprendimą atsižvelgiant į Chartijos 7, 8 ir 47 straipsnius nenustatyta nieko, kas galėtų turėti įtakos šio sprendimo galiojimui.

Dėl ketvirtojo, penktojo, devintojo ir dešimtojo klausimų

150 Devintuoju klausimu prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės siekia išsiaiškinti, ar valstybės narės priežiūros institucija yra saistoma „Privatumo skydo“ sprendime pateiktų išvadų, kad Jungtinės Amerikos Valstijos užtikrina tinkamą apsaugos lygį, ir kiek. Ketvirtuoju, penktuoju ir dešimtuoju klausimais šis teismas iš esmės siekia išsiaiškinti, ar, atsižvelgiant į tai, ką jis pats konstatavo dėl Jungtinių Amerikos Valstijų teisės, perduodant asmens duomenis į šią trečiąją šalį

remiantis SAS sprendimo priede pateiktomis standartinėmis duomenų apsaugos sąlygomis pažeidžiamos Chartijos 7, 8 ir 47 straipsniuose garantuojamas teisės, ir konkrečiai Teisingumo Teismo klausia, ar „Privatumo skydo“ sprendimo III priede nurodytos ombudsmeno institucijos įsteigimas suderinamas su šiuo 47 straipsniu.

151 Pirmiausia reikia pažymėti, kad nors komisaro pateiktu skundu pagrindinėje byloje keliamos abejonės vien dėl SAS sprendimo galiojimo, šis skundas prašymą priimti prejudicinį sprendimą pateikusiam teismui buvo paduotas prieš priimant „Privatumo skydo“ sprendimą. Kadangi ketvirtuoju ir penktuoju klausimais tas teismas apskritai klausia Teisingumo Teismo dėl apsaugos, kuri turi būti užtikrinta pagal Chartijos 7, 8 ir 47 straipsnius vykdant tokį perdavimą, Teisingumo Teismui atliekant nagrinėjimą turi būti atsižvelgta į per tą laiką įvykusio „Privatumo skydo“ sprendimo priėmimo pasekmes. Taip juo labiau yra dėl to, kad minėtas teismas dešimtuoju klausimu aiškiai siekia išsiaiškinti, ar pagal 47 straipsnį reikalaujama apsauga užtikrinama per pastarajame sprendime nurodytą ombudsmeną.

152 Be to, iš prašyme priimti prejudicinį sprendimą pateiktos informacijos matyti, jog nagrinėjant pagrindinę bylą *Facebook Ireland* teigė, kad „Privatumo skydo“ sprendimas komisarui sukelia privalomų padarinių, kiek tai susiję su Jungtinių Amerikos Valstijų užtikrinamo apsaugos lygio tinkamumo konstatavimu ir atitinkamai su asmens duomenų perdavimo į šią trečiąją šalį remiantis SAS sprendimo priede pateiktomis standartinėmis duomenų apsaugos sąlygomis teisėtumu.

153 Kaip matyti iš šio sprendimo 59 punkto, 2017 m. spalio 3 d. sprendime, pridėtame prie prašymo priimti prejudicinį sprendimą, šį prašymą pateikęs teismas pabrėžė, kad turi atsižvelgti į teisės pakeitimus, atliktus nuo skundo pateikimo iki jo posėdžio surengimo. Taigi, siekdamas išspręsti ginčą pagrindinėje byloje, tas teismas privalo atsižvelgti į aplinkybių pasikeitimą dėl „Privatumo skydo“ sprendimo priėmimo ir jo galimus privalomus padarinius.

154 Kalbant konkrečiai, „Privatumo skydo“ sprendime pateikto tinkamo apsaugos lygio Jungtinėse Amerikos Valstijose konstatavimo privalomų padarinių buvimas yra svarbus vertinant tiek šio sprendimo 141 ir 142 punktuose nurodytas duomenų valdytojo ir remiantis SAS sprendimo priede pateiktomis standartinėmis duomenų apsaugos sąlygomis į trečiąją šalį perduodamų asmens duomenų gavėjo pareigas, tiek prireikus priežiūros institucijai tenkančias pareigas sustabdyti arba uždrausti tokį duomenų perdavimą.

155 Kalbant apie privalomus „Privatumo skydo“ sprendimo padarinius, pažymėtina, kad šio sprendimo 1 straipsnio 1 dalyje nurodyta, kad atsižvelgdamos į BDAR 45 straipsnio 1 dalį „Jungtinės Amerikos Valstijos užtikrina tinkamą asmens duomenų, kuriuos pagal ES ir JAV „privatumo skydą“ Sąjunga perdavė Jungtinių Amerikos Valstijų organizacijoms, apsaugos lygį“. Pagal minėto sprendimo 1 straipsnio 3 dalį laikoma, kad asmens duomenys perduodami pagal šį „privatumo skydą“, kai jie iš Sąjungos perduodami Jungtinėse Amerikos Valstijose įsteigtoms organizacijoms, įrašytoms į „privatumo skydo“ sąrašą, kurį pagal to sprendimo II priede išdėstytų privatumo principų I ir III skirsnius tvarko ir viešai skelbia JAV komercijos departamentas.

156 Kaip matyti iš šio sprendimo 117 ir 118 punktuose nurodytos jurisprudencijos, „Privatumo skydo“ sprendimas yra privalomas priežiūros institucijoms tiek, kiek jame konstatuojama, kad Jungtinės Amerikos Valstijos užtikrina tinkamą apsaugos lygį, todėl jo poveikis yra susijęs su tuo, kad pagal jį leidžiama perduoti asmens duomenis pagal Europos Sąjungos ir Jungtinių Amerikos Valstijų „privatumo skydą“. Taigi tol, kol Teisingumo Teismas nepripažino šio sprendimo negaliojančiu, kompetentinga priežiūros institucija negali sustabdyti ar uždrausti asmens duomenų perdavimo organizacijai, įrašytai į „privatumo skydo“ sąrašą, motyvuodama tuo, kad, priešingai tame sprendime Komisijos pateiktam vertinimui, ji mano, jog Jungtinių Amerikos Valstijų teisės aktais, kuriais reglamentuojama prieiga prie asmens duomenų, perduodamų pagal tą „privatumo skydą“, ir šios trečiosios šalies valdžios institucijų atliekamu šių duomenų naudojimu nacionalinio saugumo, teisėsaugos ir kitais viešojo intereso tikslais neužtikrinamas tinkamas apsaugos lygis.

157 Vis dėlto pagal šio sprendimo 119 ir 120 punktuose nurodytą jurisprudenciją kompetentinga priežiūros institucija, gavusi asmens skundą, turi visiškai nepriklausomai išnagrinėti, ar perduodant atitinkamus asmens duomenis laikytasi BDAR nustatytų reikalavimų, ir, jeigu mano, kad šio asmens pateikti argumentai siekiant užginčyti sprendimo dėl tinkamumo galiojimą yra pagrįsti, kreiptis į nacionalinius teismus, kad jie pateiktų Teisingumo Teismui prašymą priimti prejudicinį sprendimą dėl to sprendimo galiojimo įvertinimo.

158 Pagal BDAR 77 straipsnio 1 dalį pateiktas skundas, kuriame asmuo, kurio asmens duomenys buvo arba galėjo būti perduoti į trečiąją šalį, teigia, kad, nepaisant to, ką Komisija konstatavo pagal šio reglamento 45 straipsnio 3 dalį priimtame sprendime, pagal šios šalies teisę ir praktiką nėra užtikrinamas tinkamas apsaugos lygis, iš esmės turi būti suprantamas kaip susijęs su šio sprendimo suderinamumu su privataus gyvenimo bei asmenų pagrindinių teisių ir laisvių apsauga (pagal analogiją dėl Direktyvos 95/46 25 straipsnio 6 dalies ir 28 straipsnio 4 dalies žr. 2015 m. spalio 6 d. Sprendimo *Schrems*, C-362/14, EU:C:2015:650, 59 punktą).

159 Nagrinėjamu atveju M. Schrems iš esmės paprašė komisaro uždrausti arba sustabdyti *Facebook Ireland* atliekamą jo asmens duomenų perdavimą Jungtinėse Amerikos Valstijose įsteigtai *Facebook Inc.*, motyvuodamas tuo, kad ši trečioji šalis neužtikrina tinkamo apsaugos lygio. Kadangi komisaras, atlikęs M. Schrems teiginių tyrimą, kreipėsi į prašymą priimti prejudicinį sprendimą pateikusį teismą, šis teismas, atsižvelgdamas į jam pateiktus įrodymus ir jame vykusius rungimosi principu pagrįstus teisminius ginčus, kelia klausimą dėl M. Schrems abejonių dėl toje trečiojoje šalyje užtikrinamo apsaugos lygio tinkamumo, nepaisant to, ką Komisija per tą laiką konstatavo „Privatumo skydo“ sprendime; dėl to tas teismas pateikė Teisingumo Teismui ketvirtąjį, penktąjį ir dešimtąjį prejudicinius klausimus.

160 Taigi, kaip savo išvados 175 punkte pažymėjo generalinis advokatas, šiuos prejudicinius klausimus reikia suprasti taip, kad jais iš esmės kvestionuojama „Privatumo skydo“ sprendime pateikta Komisijos išvada, kad Jungtinės Amerikos Valstijos užtikrina tinkamą iš Sąjungos į šią trečiąją šalį perduodamų asmens duomenų apsaugos lygį, taigi ir šio sprendimo galiojimas.

161 Taigi, atsižvelgiant į tai, kas išdėstyta šio sprendimo 121 ir 157–160 punktuose, ir siekiant pateikti išsamų atsakymą prašymą priimti prejudicinį sprendimą pateikusiam teismui reikia išnagrinėti, ar „Privatumo skydo“ sprendimas atitinka reikalavimus, kylančius iš BDAR, siejamo su Chartija (pagal analogiją žr. 2015 m. spalio 6 d. Sprendimo *Schrems*, C-362/14, EU:C:2015:650, 67 punktą).

162 Komisijai pagal BDAR 45 straipsnio 3 dalį priimant sprendimą dėl tinkamumo reikalaujama, kad ji tinkamai motyvuodama konstatuotų, kad atitinkama trečioji šalis savo nacionalinės teisės aktais arba tarptautiniais įsipareigojimais iš tikrųjų užtikrina pagrindinių laisvių ir teisių apsaugos lygį, kuris iš esmės yra lygiavertis tam, kuris garantuojamas Sąjungos teisinėje sistemoje (pagal analogiją dėl Direktyvos 95/46 25 straipsnio 6 dalies žr. 2015 m. spalio 6 d. Sprendimo *Schrems*, C-362/14, EU:C:2015:650, 96 punktą).

Dėl „Privatumo skydo“ sprendimo turinio

163 „Privatumo skydo“ sprendimo 1 straipsnio 1 dalyje Komisija konstatavo, kad Jungtinės Amerikos Valstijos užtikrina tinkamą asmens duomenų, perduodamų iš Sąjungos Jungtinėse Amerikos Valstijose įsteigtoms organizacijoms pagal Europos Sąjungos ir Jungtinių Amerikos Valstijų „privatumo skydą“, apsaugos lygį; pagal šio sprendimo 1 straipsnio 2 dalį šį „apsaugos skydą“, be kita ko, sudaro 2016 m. liepos 7 d. JAV komercijos departamento paskelbti privatumo principai, išdėstyti to sprendimo II priede, ir oficialūs pareiškimai ir įsipareigojimai, pateikti minėto sprendimo I, III–VII prieduose nurodytuose dokumentuose.

164 Vis dėlto „Privatumo skydo“ sprendimo II priedo „[Europos Sąjungos ir Jungtinių Amerikos Valstijų] „privatumo skydo“ sistemos principai“ I.5 punkte taip pat nurodyta, kad šių principų laikymasis, be kita ko, gali būti ribojamas „tiek, kiek tai būtina nacionalinio saugumo, viešojo intereso arba teisėsaugos reikalavimams įvykdyti“. Taigi tame sprendime, kaip ir Sprendime 2000/520, įtvirtinta šių reikalavimų viršenybė minėtų principų atžvilgiu; pagal šią viršenybę autosertifikuotos Jungtinių Amerikos Valstijų organizacijos, gaunančios asmens duomenis iš Sąjungos, privalo be apribojimų netaikyti šių principų, jeigu jie prieštarauja minėtiems reikalavimams ir dėl to yra su jais nesuderinami (pagal analogiją dėl Sprendimo 2000/520 žr. 2015 m. spalio 6 d. Sprendimo *Schrems*, C-362/14, EU:C:2015:650, 86 punktą).

165 Atsižvelgiant į tai, kad „Privatumo skydo“ sprendimo II priedo I.5 punkte numatyta nukrypti leidžianti nuostata yra bendro pobūdžio, remiantis ja taip pat galima nustatyti asmenų, kurių asmens duomenys yra arba gali būti perduoti iš Sąjungos į Jungtines Amerikos Valstijas, pagrindinių teisių suvaržymus, grindžiamus reikalavimais, susijusiais su nacionaliniu saugumu, viešuoju interesu ir Jungtinių Amerikos Valstijų nacionalinės teisės aktų laikymusi (pagal analogiją dėl Sprendimo 2000/520 žr. 2015 m. spalio 6 d. Sprendimo *Schrems*, C-362/14, EU:C:2015:650, 87 punktą). Kalbant konkrečiai, kaip konstatuota „Privatumo skydo“ sprendime, tokių suvaržymų gali kilti dėl prieigos prie asmens duomenų, perduodamų iš Sąjungos į Jungtines Amerikos Valstijas, ir dėl to, kad Jungtinių Amerikos Valstijų valdžios institucijos naudoja šiuos duomenis pagal FISA 702 straipsniu grindžiamas stebėjimo programas PRISM bei UPSTREAM ir remdamosi E.O. 12333.

166 Šiomis aplinkybėmis „Privatumo skydo“ sprendimo 67–135 konstatuojamosiose dalyse Komisija įvertino Jungtinių Amerikos Valstijų teisės aktuose, be kita ko, FISA 702 straipsnyje, E.O. 12333 ir PPD-28, numatytus apribojimus ir apsaugos priemones, kiek tai susiję su prieiga prie pagal Europos Sąjungos ir Jungtinių Amerikos Valstijų „privatumo skydą“ perduodamų asmens duomenų ir JAV valdžios institucijų atliekamu šių duomenų naudojimu nacionalinio saugumo, teisėsaugos ir kitais viešojo intereso tikslais.

167 Atlikusi šį vertinimą Komisija to sprendimo 136 konstatuojamojoje dalyje konstatavo, kad „Jungtinės Amerikos Valstijos užtikrina tinkamą asmens duomenų, kuriuos <…> Sąjunga perdavė Jungtinių Amerikos Valstijų autosertifikuotoms organizacijoms, apsaugos lygį“ ir jo 140 konstatuojamojoje dalyje nusprendė, kad „rem[iantis] prieinama informacija apie JAV teisinę tvarką <…> bet kokia išimtis [bet koks suvaržymas], kurią [kurį] JAV valdžios institucijos, siekdamos nacionalinio saugumo, teisėsaugos ar kitų viešojo intereso tikslų, taiko asmenų, kurių duomenys perduodami iš Sąjungos į Jungtines Amerikos Valstijas pagal „privatumo skydą“, pagrindinėms teisėms, ir iš to išplaukiantys autosertifikuotoms organizacijoms nustatyti privalomi apribojimai, susiję su privatumo principų laikymusi, galios tik tiek, kiek tai yra griežtai būtina siekiant atitinkamo teisėto tikslo ir jeigu taikant tokias išimtis [tokius suvaržymus] galioja veiksminga teisinė apsauga“.

Dėl tinkamo apsaugos lygio konstatavimo

168 Atsižvelgiant į aplinkybes, kurias „Privatumo skydo“ sprendime nurodė Komisija, ir aplinkybes, kurias nagrinėdamas pagrindinę bylą nustatė prašymą priimti prejudicinį sprendimą pateikęs teismas, tam teismui kyla abejonių dėl to, ar pagal Jungtinių Amerikos Valstijų teisę iš tikrųjų užtikrinamas tinkamas apsaugos lygis, kurio reikalaujama BDAR 45 straipsnyje, siejamame su Chartijos 7, 8 ir 47 straipsniuose garantuojamomis pagrindinėmis teisėmis. Kalbant konkrečiai, minėtas teismas mano, kad šios trečiosios šalies teisėje nenumatyta apribojimų ir apsaugos priemonių, būtinų atsižvelgiant į pagal jo nacionalinės teisės aktus leidžiamus suvaržymus, ir taip pat neužtikrinama veiksminga teisminė apsauga nuo tokių suvaržymų. Pastaruoju aspektu jis priduria manantis, kad „privatumo skydo“ ombudsmeno institucijos įsteigimas negali pašalinti šių trūkumų, nes ombudsmenas negali būti prilygintas teismui, kaip jis suprantamas pagal Chartijos 47 straipsnį.

169 Pirma, dėl Chartijos 7 ir 8 straipsnių, kurie svarbūs užtikrinant Sąjungoje reikalaujamą apsaugos lygį, kurio laikymąsi turi konstatuoti Komisija, prieš priimdama sprendimą dėl tinkamumo pagal BDAR 45 straipsnio 1 dalį, reikia priminti, jog pagal Chartijos 7 straipsnį kiekvienam asmeniui užtikrinama teisė į tai, kad būtų gerbiamas jo privatus ir šeimos gyvenimas, būsto neliečiamybė ir komunikacijos slaptumas. Kalbant apie Chartijos 8 straipsnio 1 dalį, pažymėtina, kad ja kiekvienam asmeniui aiškiai suteikiama teisė į jo asmens duomenų apsaugą.

170 Taigi prieiga prie asmens duomenų, siekiant juos saugoti ar naudoti, daro poveikį asmens pagrindinei teisei į privatų gyvenimą, užtikrinamai Chartijos 7 straipsnyje; ši teisė susijusi su bet kokia informacija apie fizinį asmenį, kurio tapatybė yra nustatyta arba gali būti nustatyta. Minėtam duomenų tvarkymui taikomas ir Chartijos 8 straipsnis, nes tai yra asmens duomenų tvarkymas, kaip tai suprantama pagal šį straipsnį, taigi jis būtinai turi atitikti šiame straipsnyje numatytus duomenų apsaugos reikalavimus (šiuo klausimu žr. 2010 m. lapkričio 9 d. Sprendimo *Volker und Markus Schecke ir Eifert*, C-92/09 ir C-93/09, EU:C:2010:662, 49 ir 52 punktus; 2014 m. balandžio 8 d. Sprendimo *Digital Rights Ireland ir kt.*, C-293/12 ir C-594/12, EU:C:2014:238, 29 punktą ir 2017 m. liepos 26 d. Nuomonės 1/15 (*ES ir Kanados PNR susitarimas*), EU:C:2017:592, 122 ir 123 punktus).

171 Teisingumo Teismas jau yra nusprendęs, kad asmens duomenų perdavimas trečiajam asmeniui, kaip antai valdžios institucijai, yra Chartijos 7 ir 8 straipsnyje įtvirtintų pagrindinių teisių suvaržymas, nesvarbu, kaip perduoda informacija bus naudojama vėliau. Tas pats taikytina asmens duomenų saugojimui ir prieigai prie tų duomenų, kai juos siekia panaudoti valdžios institucijos, nepaisant to, ar atitinkama su privačiu gyvenimu susijusi informacija yra jautri ir ar dėl šio suvaržymo suinteresuotieji asmenys patyrė nepatogumų (šiuo klausimu žr. 2003 m. gegužės 20 d. Sprendimo *Österreichischer Rundfunk ir kt.*, C-465/00, C-138/01 ir C-139/01, EU:C:2003:294, 74 ir 75 punktus; 2014 m. balandžio 8 d. Sprendimo *Digital Rights Ireland ir kt.*, C-293/12 ir C-594/12, EU:C:2014:238, 33–36 punktus ir 2017 m. liepos 26 d. Nuomonės 1/15 (*ES ir Kanados PNR susitarimas*), EU:C:2017:592, 124 ir 126 punktus).

172 Vis dėlto Chartijos 7 ir 8 straipsniuose įtvirtintos teisės nėra absoliučios ir turi būti vertinamos atsižvelgiant į jų visuomeninę paskirtį (šiuo klausimu žr. 2010 m. lapkričio 9 d. Sprendimo *Volker und Markus Schecke ir Eifert*, C-92/09 ir C-93/09, EU:C:2010:662, 48 punktą ir nurodytą jurisprudenciją; 2013 m. spalio 17 d. Sprendimo *Schwarz*, C-291/12, EU:C:2013:670, 33 punktą ir nurodytą jurisprudenciją ir 2017 m. liepos 26 d. Nuomonės 1/15 (*ES ir Kanados PNR susitarimas*), EU:C:2017:592, 136 punktą).

173 Šiuo klausimu taip pat pažymėtina, kad pagal Chartijos 8 straipsnio 2 dalį asmens duomenys, be kita ko, turi būti tvarkomi „tik konkretiems tikslams ir tik atitinkamam asmeniui sutikus ar kitais įstatymo nustatytais teisėtais pagrindais“.

174 Be to, pagal Chartijos 52 straipsnio 1 dalies pirmą sakinį bet koks Chartijos pripažintų teisių ir laisvių įgyvendinimo apribojimas turi būti numatytas įstatymo ir nekeisti šių teisių ir laisvių esmės. Pagal Chartijos 52 straipsnio 1 dalies antrą sakinį, remiantis proporcingumo principu, tokių teisių ir laisvių apribojimai galimi tik tuo atveju, kai jie būtini ir tikrai atitinka Sąjungos pripažintus bendrus interesus arba reikalingi kitų teisėms ir laisvėms apsaugoti.

175 Pastaruoju aspektu reikia pridurti, jog reikalavimas, kad bet koks pagrindinių teisių įgyvendinimo apribojimas būtų numatytas įstatyme, reiškia, kad pačiame teisiniame pagrinde, kuriuo leidžiamas šių teisių suvaržymas, būtų apibrėžta atitinkamos teisės įgyvendinimo apribojimo apimtis (žr. 2017 m. liepos 26 d. Nuomonės 1/15 (*ES ir Kanados PNR susitarimas*), EU:C:2017:592, 139 punktą ir nurodytą jurisprudenciją).

176 Galiausiai siekiant įvykdyti proporcingumo reikalavimą, kad nukrypti nuo asmens duomenų apsaugos leidžiančios nuostatos ir šios apsaugos apribojimai neviršytų to, kas yra griežtai būtina, nagrinėjamame suvaržymą nustatančiame teisės akte turi būti numatytos aiškios ir tikslios taisyklės, kuriomis būtų

reglamentuojama atitinkamos priemonės apimtis ir taikymas 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 (šiuo klausimu žr. 2017 m. liepos 26 d. Nuomonės 1/15 (*ES ir Kanados PNR susitarimas*), EU:C:2017:592, 140 ir 141 punktus ir nurodytą jurisprudenciją).

177 Šiuo tikslu BDAR 45 straipsnio 2 dalies a punkte nustatyta, kad vertindama trečiosios šalies užtikrinamo apsaugos lygio tinkamumą Komisija, be kita ko, atsižvelgia į „veiksmingas ir vykdytinas [įgyvendinamas] duomenų subjektų [kurių asmens duomenys perduodami] teises“.

178 Nagrinėjamu atveju „Privatumo skydo“ sprendime Komisijos padaryta išvada, kad Jungtinės Amerikos Valstijos užtikrina apsaugos lygį, iš esmės lygiavertį tam, kuris garantuojamas Sąjungoje BDAR, siejamu su Chartijos 7 ir 8 straipsniais, buvo užginčyta, be kita ko, remiantis tuo, kad suvaržymams, kylantiems iš FISA 702 straipsniu ir E.O. 12333 grindžiamų stebėjimo programų, netaikomi reikalavimai, kuriais, laikantis proporcingumo principo, būtų užtikrinamas apsaugos lygis, iš esmės lygiavertis tam, kuris garantuojamas Chartijos 52 straipsnio 1 dalies antru sakiniu. Taigi reikia išnagrinėti, ar šios stebėsenos programos įgyvendinamos laikantis tokių reikalavimų, ir nebūtina iš anksto patikrinti, ar ši trečioji šalis laikosi sąlygų, iš esmės lygiaverčių toms, kurios numatytos Chartijos 52 straipsnio 1 dalies pirmame sakinyje.

179 Šiuo klausimu, kiek tai susiję su FISA 702 straipsniu grindžiamomis stebėsenos programomis, „Privatumo skydo“ sprendimo 109 konstatuojamojoje dalyje Komisija konstatavo, kad pagal minėtą straipsnį „FISC neleidžia taikyti individualių stebėjimo priemonių; tiesą sakant, jis suteikia leidimus įgyvendinti stebėjimo programas (pvz., PRISM, UPSTREAM), remdamasis metiniais pažymėjimais, kuriuos parengė generalinis prokuroras ir Nacionalinės žvalgybos direktorius“. Taigi, kaip matyti iš tos pačios konstatuojamosios dalies, FISC vykdoma kontrole siekiama patikrinti, ar šios stebėjimo programos atitinka tikslą gauti užsienio žvalgybos informacijos, bet atliekant šią kontrolę nėra vertinama, „ar asmenys tinkamai sekami siekiant gauti užsienio žvalgybos informacijos“.

180 Taigi iš FISA 702 straipsnio jokiu būdu nematyti, kad jame yra įtvirtintų įgaliojimų įgyvendinti stebėjimo programas užsienio žvalgybos tikslais apribojimų ar garantijų ne JAV asmenims, kuriems gali būti taikomos šios programos. Šiomis aplinkybėmis, kaip savo išvados 291, 292 ir 297 punktuose iš esmės pažymėjo generalinis advokatas, pagal šį straipsnį negali būti užtikrintas apsaugos lygis, iš esmės lygiavertis tam, kuris garantuojamas Chartija, kaip antai išaiškinta šio sprendimo 175 ir 176 punktuose nurodytoje jurisprudencijoje, pagal kurią tam, kad būtų įvykdytas proporcingumo principas, pačiame teisiniame pagrinde, kuriuo leidžiami pagrindinių teisių suvaržymai, turi būti apibrėžta atitinkamos teisės įgyvendinimo ribojimo apimtis ir numatytos aiškios, tikslios taisyklės, kuriomis būtų reglamentuojama atitinkamos priemonės apimtis ir taikymas ir nustatomi minimalūs reikalavimai.

181 Remiantis tuo, kas konstatuota „Privatumo skydo“ sprendime, FISA 702 straipsniu grindžiamos stebėjimo programos, be abejo, turi būti įgyvendinamos laikantis iš PPD-28 kylančių reikalavimų. Tačiau, nors „Privatumo skydo“ sprendimo 69 ir 77 konstatuojamosiose dalyse Komisija pabrėžė, jog tokie reikalavimai yra privalomi JAV žvalgybos tarnyboms, atsakydama į Teisingumo Teismo klausimą JAV vyriausybė pripažino, kad pagal PPD-28 duomenų subjektams nesuteikiamos įgyvendinamos teisės, kuriomis jie galėtų remtis teismuose JAV valdžios institucijų atžvilgiu. Todėl, priešingai, nei reikalaujama BDAR 45 straipsnio 2 dalies a punkte, PPD-28 negali būti užtikrintas apsaugos lygis, iš esmės lygiavertis tam, kuris kyla iš Chartijos; BDAR 45 straipsnio 2 dalies a punkte nustatyta, kad šio lygio konstatavimas, be kita ko, priklauso nuo to, ar duomenų subjektai, kurių duomenys buvo perduoti į atitinkamą trečiąją šalį, turi veiksmingas ir įgyvendinamas teises.

182 Kalbant apie E.O. 12333 grindžiamas stebėjimo programas, iš Teisingumo Teismo turimos bylos medžiagos matyti, kad šiuo dekretu taip pat nesuteikta įgyvendinamų teisių, kuriomis būtų galima remtis teismuose JAV valdžios institucijų atžvilgiu.

183 Reikia pridurti, kad, kaip nurodyta „Privatumo skydo“ sprendimo VI priede pateiktame 2016 m. birželio 21 d. Nacionalinės žvalgybos direktoriaus biuro (*Office of the Director of National Intelligence*) rašte JAV komercijos departamentui ir Tarptautinės prekybos administracijai, pagal PPD-28, kurios turi būti laikomasi taikant pirmesniuose dviejuose punktuose nurodytas programas, leidžiamas „masinis“ <…> gana didelio signalų žvalgybos informacijos kiekio arba duomenų [rinkimas] tais atvejais, kai žvalgybos bendruomenė negali panaudoti identifikatoriaus, susijusio su konkrečiu taikiniu <…>, kad galėtų tikslingai rinkti duomenis“. Bet kuriuo atveju šia galimybe, kuria pagal E.O. 12333 grindžiamas stebėjimo programas suteikiama prieiga prie į Jungtines Amerikos Valstijas perduodamų duomenų, šiai prieigai netaikant jokios teismų kontrolės, nėra pakankamai aiškiai ir tiksliai nustatytos tokio masinio asmens duomenų rinkimo apimties ribos.

184 Taigi nei FISA 702 straipsnis, nei E.O. 12333, aiškinami kartu su PPD-28, neatitinka minimalių reikalavimų, Sąjungos teisėje siejamų su proporcingumo principu, vadinasi, negalima konstatuoti, kad šiomis nuostatomis grindžiamos stebėjimo programos neviršija to, kas griežtai būtina.

185 Šiomis aplinkybėmis asmens duomenų apsaugos apribojimai, kurie kyla iš Jungtinių Amerikos Valstijų nacionalinės teisės aktų, susijusių su JAV valdžios institucijų prieiga prie tokių duomenų, perduodamų iš Sąjungos į Jungtines Amerikos Valstijas, ir šių institucijų atliekamu jų naudojimu, ir kuriuos Komisija įvertino „Privatumo skydo“ sprendime, nėra sureglamentuoti taip, kad atitiktų reikalavimus, iš esmės lygiaverčius tiems, kurie Sąjungos teisėje nustatyti Chartijos 52 straipsnio 1 dalies antrame sakinyje.

186 Antra, dėl Chartijos 47 straipsnio, kuris taip pat svarbus užtikrinant Sąjungos teisėje reikalaujamą apsaugos lygį ir kurio laikymąsi Komisija turi konstatuoti prieš priimdama sprendimą dėl tinkamumo pagal BDAR 45 straipsnio 1 dalį, reikia priminti, jog šio 47 straipsnio pirmoje pastraipoje reikalaujama, kad kiekvienas asmuo, kurio teisės ir laisvės, garantuojamos Sąjungos teisės, yra pažeistos, turėtų teisę į veiksmingą jų gynybą teisme šiame straipsnyje nustatytomis sąlygomis. Kaip nurodyta minėto straipsnio antroje pastraipoje, kiekvienas asmuo turi teisę, kad jo bylą išnagrinėtų nepriklausomas ir nešališkas teismas.

187 Pagal suformuotą jurisprudenciją pats veiksmingos teisminės kontrolės, skirtos Sąjungos teisės nuostatų laikymuisi užtikrinti, egzistavimas neatsiejamas nuo teisinės valstybės egzistavimo. Taigi reglamentavimu, nenumatančiu asmeniui 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 (2015 m. spalio 6 d. Sprendimo *Schrems*, C-362/14, EU:C:2015:650, 95 punktas ir nurodyta jurisprudencija).

188 Šiuo tikslu BDAR 45 straipsnio 2 dalies a punkte reikalaujama, kad vertindama trečiosios šalies užtikrinamo apsaugos lygio tinkamumą Komisija, be kita ko, atsižvelgtų į „veiksmingas administracines bei teismines duomenų subjektų, kurių asmens duomenys yra perduodami, teisių gynimo priemones“. Šiuo aspektu BDAR 104 konstatuojamojoje dalyje pabrėžta, kad „trečioji valstybė turėtų užtikrinti veiksmingą nepriklausomą duomenų apsaugos priežiūrą ir nustatyti bendradarbiavimo su valstybių narių duomenų apsaugos institucijomis mechanizmus“, ir nurodyta, kad „duomenų subjektams turėtų būti užtikrintos veiksmingos bei įgyvendinamos teisės ir galimybė naudotis veiksmingomis administracinėmis ir teisminėmis teisių gynimo priemonėmis“.

189 Tokių veiksmingų teisių gynimo priemonių buvimas atitinkamoje trečiojoje šalyje yra ypač svarbus asmens duomenų perdavimo į šią trečiąją šalį atveju, nes, kaip matyti iš BDAR 116 konstatuojamosios dalies, duomenų subjektai gali susidurti su situacija, kai valstybių narių administracinių ir teisminių

institucijų įgaliojimai ir priemonės, siekiant naudingai išnagrinėti jų skundus, grindžiamus tariamai neteisėtu taip perduotų jų duomenų tvarkymu šioje trečiojoje šalyje, būtų nepakankami ir dėl to jie būtų priversti kreiptis į tos trečiosios šalies nacionalines institucijas ir teismus.

190 Nagrinėjamu atveju „Privatumo skydo“ sprendime Komisijos padaryta išvada, kad Jungtinės Amerikos Valstijos užtikrina apsaugos lygį, iš esmės lygiavertį tam, kuris garantuojamas Chartijos 47 straipsnyje, buvo užginčyta, be kita ko, remiantis tuo, kad įsteigus „privatumo skydo“ ombudsmeno instituciją negali būti pašalintos pačios Komisijos konstatuotos spragos, kiek tai susiję su asmenų, kurių asmens duomenys perduodami į šią trečiąją šalį, teismine apsauga.

191 Šiuo aspektu „Privatumo skydo“ sprendimo 115 punkte Komisija pažymėjo, kad „nors asmenys, įskaitant [Sąjungos] duomenų subjektus, gali pasinaudoti įvairiais teisių gynimo būdais, jei tapo neteisėto (elektroninio) stebėjimo nacionalinio saugumo tikslais aukomis, lygiai taip pat aišku, kad bent jau kai kurie teisiniai pagrindai [kai kuriems teisiniams pagrindams], kuriuos JAV žvalgybos institucijos gali naudoti (pvz., E.O. 12333), nėra taikomi [tai negalioja]“. Taigi dėl E.O. 12333 Komisija minėtoje 115 konstatuojamojoje dalyje pabrėžė, kad nėra jokių teisių gynimo priemonių. Pagal šio sprendimo 187 punkte nurodytą jurisprudenciją tokia teisminės apsaugos spraga atsižvelgiant į suvaržymus, susijusius su šiuo prezidento dekretu grindžiamomis žvalgybos programomis, kliudo konstatuoti, kaip tai padarė Komisija „Privatumo skydo“ sprendime, kad pagal Jungtinių Amerikos Valstijų teisę užtikrinamas apsaugos lygis, iš esmės lygiavertis tam, kuris garantuojamas Chartijos 47 straipsnyje.

192 Be to, kiek tai susiję su stebėjimo programomis, grindžiamomis FISA 702 straipsniu, ir stebėjimo programomis, grindžiamomis E.O. 12333, šio sprendimo 181 ir 182 punktuose pažymėta, kad nei pagal PPD-28, nei pagal E.O. 12333 duomenų subjektams nesuteikiamos įgyvendinamos teisės, kuriomis jie galėtų remtis teismuose JAV valdžios institucijų atžvilgiu, todėl šie asmenys neturi teisės į veiksmingą teisinę gynybą.

193 Vis dėlto „Privatumo skydo“ sprendimo 115 ir 116 konstatuojamosiose dalyse Komisija konstatavo, kad dėl JAV valdžios institucijų nustatyto ombudsmeno mechanizmo, kaip antai apibūdinto rašte, kurį 2016 m. liepos 7 d. JAV valstybės sekretorius išsiuntė už teisingumą, vartotojų reikalus ir lyčių lygybę atsakingai Europos Komisijos narei ir kuris pateiktas to sprendimo III priede, ir dėl ombudsmenui pavestos užduoties, šiuo atveju – „tarptautinės informacinių technologijų diplomatijos vyresniojo koordinatoriaus“ funkcijų, pobūdžio Jungtinės Amerikos Valstijos gali būti laikomos užtikrinančiomis apsaugos lygį, iš esmės lygiavertį tam, kuris garantuojamas Chartijos 47 straipsnyje.

194 Klausimas, ar „Privatumo skydo“ sprendime nurodytu ombudsmeno mechanizmu iš tikrųjų gali būti pašalinti Komisijos konstatuoti teisės į veiksmingą teisminę apsaugą apribojimai, turi būti, remiantis iš Chartijos 47 straipsnio ir šio sprendimo 187 punkte nurodytos jurisprudencijos kylančiais reikalavimais, nagrinėjamas vadovaujantis principu, kad teisės subjektai turi turėti galimybę pasinaudoti teisių gynimo priemonėmis nepriklausomame ir nešališkame teisme, kad galėtų susipažinti su savo asmens duomenimis arba reikalauti, kad tokie duomenys būtų ištaisyti arba ištrinti.

195 Nors šio sprendimo 193 punkte nurodytame rašte „privatumo skydo“ ombudsmenas apibūdintas kaip „nepriklausomas nuo žvalgybos tarnybų“, jis buvo pristatytas kaip „atsiskait[antis] tiesiogiai Valstybės sekretoriui, kuris užtikrina, kad ombudsmenas vykdytų savo funkcijas objektyviai ir nepriklausomai nuo jokios netinkamos įtakos, kuri gali būti daroma siekiant gauti atitinkamą sprendimą“. Be to, nepaisant to, kad, kaip „Privatumo skydo“ sprendimo 116 konstatuojamojoje dalyje konstatavo Komisija, ombudsmeną skiria Valstybės sekretorius ir jis įeina į Jungtinių Amerikos Valstijų Valstybės departamento sudėtį, minėtame sprendime, kaip savo išvados 337 punkte pažymėjo generalinis advokatas, nėra jokios informacijos apie tai, kad ombudsmeno atšaukimui iš pareigų ar jo paskyrimo panaikinimui būtų taikomos ypatingos garantijos, o dėl to gali kilti abejonių dėl ombudsmeno nepriklausomumo nuo vykdomosios valdžios (šiuo klausimu žr. 2020 m. sausio 21 d. Sprendimo *Banco de Santander*, C-274/14, EU:C:2020:17, 60 ir 63 punktus ir nurodytą jurisprudenciją).

196 Be to, kaip savo išvados 338 punkte pažymėjo generalinis advokatas, nors „Privatumo skydo“ sprendimo 120 konstatuojamojoje dalyje pabrėžtas JAV vyriausybės įsipareigojimas, kad atitinkamas žvalgybos tarnybų padalinys turės ištaisyti kiekvieną „privatumo skydo“ ombudsmeno nustatytą taikytinų normų pažeidimą, tame sprendime visiškai nenurodyta, jog šis ombudsmenas būtų įgaliotas priimti šioms tarnyboms privalomus sprendimus, taip pat nekalbama apie jokias teisines garantijas, kurios būtų siejamos su šiuo įsipareigojimu ir kuriomis galėtų remtis duomenų subjektai.

197 Taigi „Privatumo skydo“ sprendime nurodytu ombudsmeno mechanizmu nesuteikiama teisių gynimo priemonė institucijoje, kurioje asmenims, kurių duomenys perduodami į Jungtines Amerikos Valstijas, būtų suteiktos garantijos, iš esmės lygiavertės toms, kurios reikalaujamos Chartijos 47 straipsnyje.

198 Vadinasi, „Privatumo skydo“ sprendimo 1 straipsnio 1 dalyje konstatavusi, kad Jungtinės Amerikos Valstijos užtikrina tinkamą asmens duomenų perdavimą iš Sąjungos šioje trečiojoje šalyje įsteigtoms organizacijoms pagal Europos Sąjungos ir Jungtinių Amerikos Valstijų „privatumo skydą“, Komisija nesilaikė reikalavimų, kylančių iš BDAR 45 straipsnio 1 dalies, siejamos su Chartijos 7, 8 ir 47 straipsniais.

199 Darytina išvada, kad „Privatumo skydo“ sprendimo 1 straipsnis nesuderinamas su BDAR 45 straipsnio 1 dalimi, siejama su Chartijos 7, 8 ir 47 straipsniais, todėl negalioja.

200 Kadangi „Privatumo skydo“ sprendimo 1 straipsnis yra neatsiejamas nuo jo 2–6 straipsnių ir priedų, jo negaliojimas turi įtakos viso šio sprendimo galiojimui.

201 Atsižvelgiant į visa tai, kas išdėstyta, darytina išvada, kad „Privatumo skydo“ sprendimas negalioja.

202 Dėl klausimo, ar reikia palikti galioti šio sprendimo padarinius siekiant išvengti teisės spragos atsiradimo (šiuo klausimu žr. 2016 m. balandžio 28 d. Sprendimo *Borealis Polyolefine ir kt.*, C-191/14, C-192/14, C-295/14, C-389/14 ir C-391/14–C-393/14, EU:C:2016:311, 106 punktą), reikia pažymėti, kad bet kuriuo atveju, atsižvelgiant į BDAR 49 straipsnį, panaikinus sprendimą dėl tinkamumo, kaip antai „Privatumo skydo“ sprendimą, negali atsirasti tokia teisės spraga. Iš tiesų šiame straipsnyje išsamiai nustatytos sąlygos, kuriomis asmens duomenys gali būti perduodami į trečiąsias šalis nepriėmus sprendimo dėl tinkamumo pagal minėto reglamento 45 straipsnio 3 dalį arba tinkamų apsaugos priemonių pagal to paties reglamento 46 straipsnį.

Dėl bylinėjimosi išlaidų

203 Kadangi šis procesas pagrindinės bylos šalims yra vienas iš etapų prašymą priimti prejudicinį sprendimą pateikusio teismo nagrinėjamoje byloje, bylinėjimosi išlaidų klausimą turi spręsti šis teismas. Išlaidos, susijusios su pastabų pateikimu Teisingumo Teismui, išskyrus tas, kurias patyrė minėtos šalys, nėra atlygintinos.

Remdamasis šiais motyvais, Teisingumo Teismas (didžioji kolegija) nusprendžia:

1. **2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) 2 straipsnio 1 ir 2 dalys turi būti aiškinamos taip, kad į šio reglamento taikymo sritį patenka asmens duomenų perdavimas, atliktas komerciniais tikslais valstybėje narėje įsteigto ūkio subjekto kitam trečiojoje šalyje įsteigtam ūkio subjektui, nepaisant to, ar atliekant šį perdavimą arba po jo atitinkamos trečiosios šalies valdžios institucijos gali tvarkyti šiuos duomenis visuomenės saugumo, gynybos ir valstybės saugumo tikslais.**

2. **Reglamento 2016/679 46 straipsnio 1 dalis ir 2 dalies c punktas turi būti aiškinami taip, kad šiose nuostatose reikalaujamomis tinkamomis apsaugos priemonėmis, įgyvendinamomis teisėmis ir veiksmingomis duomenų subjektų teisių gynimo priemonėmis turi būti užtikrinama, kad asmenų, kurių asmens duomenys perduodami į trečiąją šalį remiantis standartinėmis duomenų apsaugos sąlygomis, teisių apsaugos lygis būtų iš esmės lygiavertis tam, kuris garantuojamas Europos Sąjungoje šiuo reglamentu, siejamu su Europos Sąjungos pagrindinių teisių chartija. Šiuo tikslu, vertinant tokio perdavimo atveju užtikrinamą apsaugos lygį, be kita ko, turi būti atsižvelgta ir į duomenų valdytojo ar jo duomenų tvarkytojo, įsteigtų Europos Sąjungoje, ir perduodamų duomenų gavėjo, įsteigto atitinkamoje trečiojoje šalyje, sudarytų sutarčių sąlygas, ir, kiek tai susiję su galima šios trečiosios šalies valdžios institucijų prieiga prie taip perduotų asmens duomenų, į atitinkamus šios šalies teisinės sistemos aspektus, be kita ko, nurodytus to reglamento 45 straipsnio 2 dalyje.**

3. **Reglamento 2016/679 58 straipsnio 2 dalies f ir j punktai turi būti aiškinami taip, kad, nebent Europos Komisija yra teisėtai priėmusi sprendimą dėl tinkamumo, kompetentinga priežiūros institucija turi sustabdyti arba uždrausti duomenų perdavimą į trečiąją šalį, grindžiamą Komisijos priimtomis standartinėmis duomenų apsaugos sąlygomis, jei, atsižvelgdama į visas konkrečias šio perdavimo aplinkybes, mano, kad šioje trečiojoje šalyje šių sąlygų nesilaikoma arba jų negalima laikytis ir kad kitomis priemonėmis negalima užtikrinti pagal Sąjungos teisę, visų pirma pagal šio reglamento 45 bei 46 straipsnius ir Pagrindinių teisių chartiją, reikalaujamos perduodamų duomenų apsaugos, jeigu Sąjungoje įsteigtas duomenų valdytojas arba duomenų tvarkytojas pats nesustabdė arba nenutraukė duomenų perdavimo.**

4. **Išnagrinėjus 2010 m. vasario 5 d. Komisijos sprendimą 2010/87/ES dėl sutarčių standartinių sąlygų, nustatytų asmens duomenų perdavimui trečiosiose šalyse įsikūrusiems tvarkytojams pagal Europos Parlamento ir Tarybos direktyvos 95/46/EB nuostatas, iš dalies pakeistą 2016 m. gruodžio 16 d. Komisijos įgyvendinimo sprendimu (ES) 2016/2297, atsižvelgiant į Pagrindinių teisių chartijos 7, 8 ir 47 straipsnius nenustatyta nieko, kas galėtų turėti įtakos šio sprendimo galiojimui.**

5. **2016 m. liepos 12 d. Komisijos įgyvendinimo sprendimas (ES) 2016/1250 dėl ES ir JAV „privatumo skydo“ užtikrinamos apsaugos tinkamumo pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB negalioja.**

Parašai.