

Pareiškimas



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

Pareiškimas 03/2021 dėl E. privatumo reglamento Priimtas 2021 m. kovo 9 d.

Europos duomenų apsaugos valdyba priėmė šį pareiškimą:

EDAV palankiai vertina Tarybos patvirtintus sutartus derybų įgaliojimus dėl privatumo apsaugos ir konfidencialumo naudojantis elektroninių ryšių paslaugomis (toliau – Tarybos pozicija) kaip teigiamą poslinkį rengiant naują E. privatumo reglamentą. Labai svarbu, kad ES bendroji duomenų apsaugos sistema būtų skubiai papildyta suderintomis elektroniniams ryšiams taikomomis taisyklėmis.

Kaip jau ne kartą minėta¹, E. privatumo reglamentu jokiais aplinkybėmis neturėtų būti sumažintas šiuo metu galiojančia E. privatumo direktyva nustatytas apsaugos lygis, tačiau juo turėtų būti papildytas Bendrasis duomenų apsaugos reglamentas (BDAR), suteikiant papildomas dideles konfidencialumo ir visų rūšių elektroninių ryšių apsaugos garantijas. E. privatumo reglamentas jokiu būdu negali būti naudojamas siekiant *de facto* pakeisti BDAR. Atsižvelgiant į tai Tarybos pozicija kelia nemažai susirūpinimo ir EDAV norėtų nurodyti klausimus, kurie turėtų būti sprendžiami būsimose derybose.

Šis pareiškimas neturi poveikio galimam būsimam išsamesniam EDAV pareiškimui ar nuomonei dėl teisėkūros institucijų pozicijų.

Susirūpinimas dėl elektroninių ryšių duomenų tvarkymo ir saugojimo teisėsaugos ir nacionalinio saugumo užtikrinimo tikslais

Kalbant apie 6 straipsnio 1 dalies d punktą ir 7 straipsnio 4 dalį, EDAV pakartoja, kad teisėkūros priemonės, pagal kurias reikalaujama, kad elektroninių ryšių paslaugų teikėjai saugotų elektroninius duomenis, turi atitikti:

-) ES pagrindinių teisių chartijos (toliau – Chartija) 7 ir 8 straipsnius,
-) naujausią ES Teisingumo Teismo (toliau – ESTT) praktiką², taip pat

¹ Žr. EDAV ir 29 straipsnio darbo grupės parengtų dokumentų dėl e. privatumo taisyklių išsamų sąrašą, pateiktą šio pareiškimo priede.

² ESTT sujungtos bylos C-511/18, C-512/18 ir C-520/18, byla C-623/17.

) Europos žmogaus teisių konvencijos 8 straipsnį.

EDAV mano, kad E. privatumo reglamentu negalima nukrypti nuo naujausios ESTT praktikos taikymo: pagal ją visų pirma nustatyta, kad Chartijos 7, 8, 11 straipsniai ir 52 straipsnio 1 dalis turi būti aiškinami kaip draudžiantys teisėkūros priemonės, kuriomis, kaip prevencine priemone, būtų nustatomas bendras ir nediferencijuojamas srauto ir vietos nustatymo duomenų saugojimas. Todėl pagal Chartiją neleidžiama suteikti teisinio pagrindo jokiais kitais atvejais, išskyrus tikslinį duomenų saugojimą teisės saugos ir nacionalinio saugumo užtikrinimo tikslais, ir bet kuriuo atveju jam turėtų būti taikomi griežti laiko ir materialiniai apribojimai, taip pat Teismo arba nepriklausomos institucijos peržiūra.

Kalbant apie tai, jog elektroninių ryšių paslaugų teikėjų vykdoma duomenų tvarkymo veikla neįtraukta į reglamento taikymo sritį, EDV mano, kad tokia išimtis prieštarauja nuoseklios ES duomenų apsaugos sistemos prielaidai. Tuo atveju, jei išimtis nustatoma, EDV vis dėlto pabrėžia, kad yra taikomas BDAR.

Elektroninių ryšių konfidencialumui užtikrinti reikia konkrečių apsaugos priemonių (6, 6a, 6b ir 6c straipsniai)

Pranešimų slaptumas yra viena iš pagrindinių teisių, ginamų pagal Chartijos 7 straipsnį, kuri jau įgyvendinama pagal E. privatumo direktyvą. Ši teisė į slaptumą turi būti taikoma visiems elektroniniams pranešimams, nepriklausomai nuo jų siuntimo priemonių, kai jie saugomi arba siunčiami visu keliu nuo siuntėjo iki gavėjo, taip pat turi būti užtikrintas kiekvieno naudotojo galinio įrenginio nepažeidžiamumas.

Bendrieji draudimai su siauromis asmens duomenų tvarkymo išimtimis

EDV visiškai pritaria požiūriui, grindžiamam bendraisiais draudimais su siauromis, konkrečiomis ir aiškiai apibrėžtomis (orientuotomis į tikslą) išimtimis.

Tačiau EDV kelia susirūpinimą tai, kad susidaro įspūdis, jog pagal kai kurias Tarybos nustatytas išimtis (visų pirma 6 straipsnio 1 dalies c punkte, 6b straipsnio 1 dalies e ir f punktuose ir 6c straipsnyje) leidžiamas labai įvairių tipų duomenų tvarkymas, ir primena, kad reikia tas išimtis susiaurinti, kad jos būtų taikomos tik konkrečiais ir aiškiai apibrėžtais tikslais. Bet kuriuo atveju tie konkretūs tikslai turėtų būti aiškiai išvardyti, kad būtų galima užtikrinti teisinį tikrumą ir kuo aukštesnį apsaugos lygį.

Be to, pagal išimtis 6 straipsnio 1 dalies b, c ir d punktuose, pagal kurias leidžiama prieiga prie elektroninių ryšių duomenų, įskaitant turinį, siekiant užtikrinti tinklo ir galutinio naudotojo įrenginio saugumą, galėtų būti leidžiama visiška elektroninių ryšių paslaugų teikėjo arba duomenų tvarkytojų prieiga prie visų galutinio naudotojo pranešimų turinio. Kadangi tokios išimties galėtų pakenkti galutinio naudotojo teisei į konfidencialumą ir jo su privatumu susijusiems lūkesčiams, jos turi būti proporcingos ir turėtų būti susiaurintos, bent jau siekiant priminti, kad tai negali lemti nuolatinės elektroninių pranešimų turinio stebėsenos, ar leisti paslaugų teikėjams arba duomenų tvarkytojams apeiti bet kokį šifravimą.

Galiausiai, reglamente turėtų būti pabrėžtas anoniminimo, kaip pagrindinės garantijos, kuri turi būti nuolatos suteikiama naudojant elektroninių ryšių duomenis, vaidmuo.

Stiprus ir patikimas šifravimas – šiuolaikinio skaitmeninio pasaulio būtinybė

Stiprus pažangiausiasiais metodais grindžiamas šifravimas turėtų būti bendrai taikomas, siekiant užtikrinti saugų, laisvą ir patikimą duomenų srautą tarp piliečių, įmonių ir vyriausybių, ir yra labai svarbus norint užtikrinti, kad būtų laikomasi BDAR saugumo įpareigojimų, pavyzdžiui, sveikatos duomenų, ir didėjančių grėsmių aplinkoje taikoma IT sistemų apsauga. Ištinis šifravimas nuo siuntėjo

iki gavėjo taip pat yra vienintelis būdas užtikrinti visišką duomenų apsaugą jų perdavimo metu. Bet koks galimas mėginimas susilpninti šifravimą, netgi tokiais tikslais kaip nacionalinis saugumas, dėl galimo neteisėto jo naudojimo visiškai panaikintų tuos apsaugos mechanizmus. Šifravimas turi išlikti standartizuotas, stiprus ir veiksmingas³.

Naujuoju reglamentu turi būti užtikrinta, kad būtų laikomasi reikalavimo gauti sutikimą naudoti slapukus ir panašias technologijas, o paslaugų teikėjams būtų suteiktos techninės priemonės tokiam sutikimui lengvai gauti (8 straipsnis⁴)

Poreikis taikyti privatumo išsaugojimo požiūrį priimant „viskas arba nieko“ sprendimus

Reikėtų priminti, kad BDAR nuostatos dėl sutikimo taikomos e. privatumo taisyklių kontekste. Todėl EDAV mano, kad būtinybė gauti tikrą laisva valia duotą sutikimą užkirstų kelią paslaugų teikėjams vykdyti nesąžiningą veiklą, pavyzdžiui, siūlyti „viskas arba nieko“ sprendimus, pagal kuriuos paslaugomis ir funkcijomis galima naudotis su sąlyga, kad naudotojas duoda sutikimą saugoti informaciją, arba gauti prieigą prie naudotojo galiniame įrenginyje jau saugomos informacijos (vadinamosios slapukų sienos)⁵.

EDAV pabrėžia būtinybę į E. privatumo reglamentą įtraukti aiškią nuostatą siekiant įtvirtinti šį draudimą, kad naudotojai galėtų sutikti su profiliavimu arba jo atsisakyti. Todėl tie patys paslaugų teikėjai naudotojams turi pasiūlyti sąžiningas pasirinkimo galimybes. Šie principai turėtų būti vienodai taikomi visiems paslaugų teikėjams, nepriklausomai nuo jų veiklos sektoriaus ar dabartinio finansavimo modelio (žr. Tarybos pozicijos 21aa konstatuojamąją dalį).

Auditorijos dydžio nustatymas turi apsiriboti neįkyria veikla, kuria, tikėtina, naudotojų privatumui nesukeliama rizika

Tarybos pozicijoje pagal 29 straipsnio darbo grupės pasiūlymą nurodoma nauja išimtis auditorijos dydžio nustatymui⁶. Tačiau ši auditorijos dydžio nustatymui taikoma Tarybos siūloma nukrypti leidžianti nuostata suformuluota per plačiai ir galėtų sudaryti sąlygas pernelyg plačiam šios nukrypti leidžiančios nuostatos taikymo srities aiškinimui ir dėl to sumažinti galutinių naudotojų galinių įrenginių apsaugos lygį.

Todėl EDAV pabrėžia, kad nukrypti leidžianti nuostata dėl auditorijos dydžio nustatymo turėtų būti apribota žemo lygio analitika, kuri reikalinga naudotojo prašomos paslaugos teikimo analizei atlikti, ji turėtų būti naudojama tik statistikai paslaugų operatoriui teikti ir ją turi įdiegti paslaugų operatorius arba duomenų tvarkytojai. Todėl šios duomenų tvarkymo veiklos, pačios savaime arba kartu su kitais sekimo sprendimais, paslaugų teikėjas ar kiti duomenų valdytojai negali naudoti kaip nors naudotojams išskirti arba profiliuoti. Be to, naudojantis auditorijos dydžio nustatymo paslauga neturėtų būti leidžiama rinkti naršymo informaciją, susijusią su įvairių svetainių ir (arba) taikomųjų programų naudotojais, ir turėtų būti siūlomas patogus naudoti mechanizmas, kad būtų galima atsisakyti duomenų rinkimo.

³ 2018 m. balandžio 11 d. 29 straipsnio darbo grupės pareiškimas dėl šifravimo ir jo poveikio asmenų apsaugai tvarkant jų asmens duomenis ES, pateiktas adresu: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622229.

⁴ Taip pat susijusios konstatuojamosios dalys (20aaaa ir 21aa Tarybos pozicijoje).

⁵ Kaip anksčiau yra pareiškusi EDAV 2018 m. gegužės 25 d. priimtame pareiškime dėl E. privatumo reglamento, pateiktame adresu: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_en.pdf, ir EDAV gairėse 05/2019 dėl sutikimo pagal Reglamento 2016/679 39 dalį, pateiktose adresu: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

⁶ Taip pat žr. Nuomonę 04/2012 dėl slapukams taikomos reikalavimo gauti sutikimą išimties (WP 194), p. 10–11. Pateikiama adresu: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf.

Veiksmingas būdas gauti sutikimą svetainėse ir mobiliosiose programėlėse (4a straipsnis)

EDAV mano, kad taikant E. privatumo reglamentą dabartinė padėtis turėtų pagerėti grąžinus kontrolę naudotojams ir sprendžiant „sutikimo davimo nuovargio“ problemą. 4a straipsnis turėtų būti išplėstas ir jame turėtų būti reikalaujama, kad naršyklėse bei operacinėse sistemose būtų įdiegti patogūs naudoti ir veiksmingi mechanizmai duomenų valdytojams gauti sutikimą, kad būtų galima visiems dalyviams sudaryti vienodas sąlygas. Į reglamento taikymo sritį taip pat reikėtų aiškiai įtraukti naršyklės bei operacinės sistemos teikėjus.

Privatumo nustatymuose paprastai turi būti numatyta asmens duomenų apsaugos ir naudotojų galinių įrenginių nepažeidžiamumo teisė ir turėtų būti numatyta galimybė lengvai, privalomai ir vykdytinai duoti ir atsiimti sutikimą visų šalių atžvilgiu.

Tolesnis duomenų tvarkymas suderinamais tikslais (6c straipsnis ir 8 straipsnio 1 dalies g punktas)

Kalbant apie vykstančias diskusijas dėl tolesnio elektroninių ryšių metaduomenų ir (arba) duomenų, surinktų naudojant slapukus ir panašias technologijas, tvarkymo, EDAV pakartoja, kad pritaria E. privatumo reglamente išdėstytam požiūriui, kurį iš pradžių pasiūlė Europos Komisija ir jam pritarė Europos Parlamentas, pagrįstą bendroju draudimu, siauromis išimtimis ir sutikimo naudojimu. Tolesnis duomenų tvarkymas suderinamais tikslais susijęs su apsaugos, kuri užtikrinama E. privatumo reglamentu, sumažinimo rizika, ypač elektroninių ryšių metaduomenų tvarkymo srityje, leidžiant juos tvarkyti bet kuriuo tikslu, kurį paslaugos teikėjas laiko atitinkančiu „suderinamumo“ sąlygą, nors teisės aktų leidėjas aiškiai siekė, nesant sutikimo, apriboti jų tvarkymą konkrečiais tikslais. EDAV nori pabrėžti, kad pirmiau minėti duomenys gali būti toliau tvarkomi be sutikimo ir nesukeliant rizikos naudotojams juos anoniminius.

Būsimas priežiūros institucijų, EDAV ir bendradarbiavimo mechanizmo vaidmuo (18–20 straipsniai)

EDAV primena, kad norint užtikrinti vienodas sąlygas bendrojoje skaitmeninėje rinkoje, būtina visoje ES užtikrinti visų E. privatumo reglamento duomenų tvarkymo nuostatų suderintą aiškinimą ir vykdymą.

Siekiant tolesnio nuoseklumo, privatumo nuostatų priežiūra pagal E. privatumo reglamentą turėtų būti pagal BDAR patikėta kompetentingoms priežiūros institucijoms

EDAV norėtų priminti, kad esama aiškios kompetencijų sąsajos tarp nacionalinių institucijų, kompetentingų pagal galiojančią E. privatumo direktyvą, ir duomenų apsaugos institucijų. Būsimo E. privatumo reglamento nuostatos, susijusios su privatumo apsauga, neturėtų būti taikomos atskirai, kadangi jos yra glaudžiai susijusios su asmens duomenų tvarkymu ir BDAR.

Taigi, siekiant suderinti aukšto lygio asmens duomenų apsaugą ir teisinį bei procedūrinį tikrumą, už BDAR vykdymo užtikrinimą atsakingoms nacionalinėms institucijoms turėtų būti patikėta būsimo E. privatumo reglamento nuostatų, susijusių su asmens duomenų tvarkymu, priežiūra, kaip iš pradžių siūlė Komisija⁷.

⁷ Europos Komisija, 2017 m. sausio 10 d. pasiūlymas dėl Europos Parlamento ir Tarybos reglamento dėl teisės į privatumą gyvenimą ir asmens duomenų apsaugos elektroninių ryšių sektoriuje, kuriuo panaikinama Direktyva 2002/58/EB (Reglamentas dėl privatumo ir elektroninių ryšių), pateikiamas adresu: <https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A52017PC0010>, ir 29 straipsnio darbo grupės susijusi nuomonė, pateikiama adresu: https://ec.europa.eu/newsroom/document.cfm?doc_id=44103.

EDAV pažymi, kad, skirtingai nei pirminiame Europos Komisijos pasiūlyme, visos nuorodos į bendradarbiavimo ir nuoseklumo užtikrinimo mechanizmą, kaip nustatyta BDAR VII skyriuje, iš Tarybos pozicijos buvo pašalintos. Dėl pirmiau minėtų priežasčių EDAV pakartoja, kad tik visiškas suderinimas su BDAR bendradarbiavimo ir nuoseklumo užtikrinimo sistema leistų E. privatumo reglamentui pasiekti savo tikslų, išvengti fragmentiškumo vykdymo užtikrinimo procese ir taikant reglamentą, taip pat sumažinti našatę paslaugų teikėjams, kurie kitu atveju turėtų kreiptis į galimai daugiau nei 27 priežiūros institucijas.

Tuo atveju, jei nacionalinės kompetentingos institucijos, kurios nėra EDAV narės, turėtų palaikyti ryšius su EDAV, kaip šiuo metu numatyta Tarybos pozicijoje, jų galimybė laiku prisidėti prie nuoseklaus E. privatumo reglamento taikymo sumažėtų ir skaitmeninės ekonomikos, ir pagrindinių teisių apsaugos nenaudai.

Europos duomenų apsaugos valdybos vardu

Pirmininkė

(Andrea Jelinek)

PRIEDAS. EDAV ir 29 straipsnio darbo grupės anksčiau parengtų dokumentų sąrašas

-) Nuomonė 1/2009 dėl pasiūlymų, iš dalies keičiančių Direktyvą 2002/58/EB dėl privatumo ir elektroninių ryšių (E. privatumo direktyva), pateikiama adresu: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp159_lt.pdf.
-) Nuomonė 04/2012 dėl slapukams taikomos reikalavimo gauti sutikimą išimties (WP 194), pateikiama adresu: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_lt.pdf.
-) Nuomonė 03/2016 dėl E. privatumo direktyvos vertinimo ir peržiūros (WP 240), pateikiama adresu: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=645254.
-) 29 straipsnio darbo grupės nuomonė dėl pasiūlymo dėl Europos Parlamento ir Tarybos reglamento dėl teisės į privatų gyvenimą ir asmens duomenų apsaugos elektroninių ryšių sektoriuje, kuriuo panaikinama Direktyva 2002/58/EB (Reglamentas dėl privatumo ir elektroninių ryšių), pateikiama adresu: https://ec.europa.eu/newsroom/document.cfm?doc_id=44103.
-) 29 straipsnio darbo grupės pareiškimas dėl šifravimo ir jo poveikio asmenų apsaugai tvarkant jų asmens duomenis ES, Briuselis, 2018 m. balandžio 11 d., pateikiamas adresu: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622229.
-) 2018 m. gegužės 25 d. priimtas EDAV pareiškimas dėl E. privatumo reglamento peržiūros ir jo poveikio asmenų apsaugai, susijusiai su jų pranešimų privatumu ir konfidencialumu, pateikiamas adresu: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_en.pdf.
-) 2019 m. kovo 13 d. priimtas EDAV pareiškimas 3/2019 dėl E. privatumo reglamento, pateikiamas adresu: https://edpb.europa.eu/sites/edpb/files/files/file1/201903_edpb_statement_eprivacyregulation_en.pdf.
-) 2020 m. lapkričio 19 d. priimtas EDAV pareiškimas dėl E. privatumo reglamento ir būsimo priežiūros institucijų bei EDAV vaidmens, pateikiamas adresu: https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-eprivacy-regulation-and-future-role-supervisory_en.