Rekomendacijos 02/2021 dėl teisinio pagrindo saugoti kredito kortelių duomenis tik tam, kad būtų palengvinti internetiniai sandoriai ateityje

Priimta 2021 m. gegužės 19 d.

Europos duomenų apsaugos valdyba,

atsižvelgdama į 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 (toliau – BDAR) 70 straipsnio 1 dalies e punktą,

atsižvelgdama į EEE susitarimą, ypač į jo XI priedą ir 37 protokolą su pakeitimais, padarytais 2018 m. liepos 6 d. EEE jungtinio komiteto sprendimu Nr. 154/2018,

atsižvelgdama į Darbo tvarkos taisyklių 12 ir 22 straipsnius,

PRIĖMĖ ŠIAS REKOMENDACIJAS

1. COVID-19 pandemijos sąlygomis skaitmeninė ekonomika ir e. prekyba nuolat vystėsi. Dėl to išaugo ir rizika, susijusi su kredito kortelių duomenų naudojimu internete. Kaip teigiama 29 straipsnio darbo grupės Poveikio duomenų apsaugai vertinimo gairėse, kredito kortelių duomenų pažeidimai „*akivaizdžiai daro didelį poveikį duomenų subjekto kasdieniam gyvenimui*“, nes finansiniai duomenys gali būti naudojami „*sukčiavimui atliekant mokėjimus*“[1].

2. Todėl labai svarbu, kad duomenų valdytojai nustatytų tinkamas duomenų subjektų apsaugos priemones ir užtikrintų jiems galimybę kontroliuoti savo asmens duomenis, siekiant sumažinti neteisėto tvarkymo riziką ir sustiprinti pasitikėjimą skaitmenine aplinka. Europos duomenų apsaugos valdyba (EDAV) mano, kad šis pasitikėjimas yra labai svarbus tvariam skaitmeninės ekonomikos augimui.

3. Todėl šiomis rekomendacijomis siekiama skatinti darnų duomenų apsaugos taisyklių, susijusių su kredito kortelių duomenų tvarkymu Europos ekonominėje erdvėje (EEE), taikymą ir užtikrinti vienodą duomenų subjekto teisių apsaugą, visapusiškai laikantis pagrindinių duomenų apsaugos principų, kaip reikalaujama BDAR.

4. Konkrečiau, šiose rekomendacijose kalbama apie internetinių prekių tiekėjų ir paslaugų teikėjų atliekamą kredito kortelių duomenų saugojimą, siekiant vienintelio konkretaus tikslo – palengvinti tolesnį duomenų subjektų apsipirkimą[2]. Rekomendacijos apima atvejus, kai duomenų subjektas per interneto svetainę ar taikomąją programą perka produktą arba moka už paslaugą ir pateikia savo kredito kortelės duomenis, paprastai tam skirtoje formoje, kad sudarytų šį unikalų sandorį.

5. Kaip ir bet kokio kito duomenų tvarkymo atveju, duomenų valdytojas turi turėti galiojantį teisinį pagrindą saugoti šiuos duomenis pagal BDAR 6 straipsnį. Šiuo atžvilgiu reikėtų pažymėti, kad kai kurie BDAR 6 straipsnyje nurodyti teisiniai pagrindai šioje situacijoje nebūtų taikomi ir turėtų būti atmesti. Kreditinės kortelės duomenų saugojimas po sandorio, siekiant palengvinti tolesnius pirkimus, negali būti laikomas būtinu siekiant įvykdyti teisinę prievolę (BDAR 6 straipsnio 1 dalies

[1] 29 straipsnio darbo grupės Poveikio duomenų apsaugai vertinimo (PDAV) gairės, kuriomis Reglamento 2016/679 taikymo tikslais nurodoma, kaip nustatyti, ar duomenų tvarkymo operacijos „gali sukelti didelį pavojų“.

[2] Reikėtų pažymėti, kad rekomendacijos netaikomos mokėjimo įstaigoms, veikiančioms internetinėse parduotuvėse, ir valdžios institucijoms. Jos neapima ir kredito kortelės duomenų saugojimo jokiais kitais tikslais, pavyzdžiui, siekiant įvykdyti teisinę prievolę arba nustatyti periodinį mokėjimą, kai sudaroma tęstinio vykdymo sutartis arba užsakoma ilgalaikė paslauga (pvz., sutartis, kurioje numatyta kiekvieną mėnesį patiekti tam tikrą prekę, arba muzikos ar filmų transliavimo paslaugų abonementas).

c punktas) arba apsaugoti gyvybiškai svarbius fizinio asmens interesus (BDAR 6 straipsnio 1 dalies d punktas). Tinkamu teisiniu pagrindu negali būti laikoma ir užduotis, atliekama visuomenės labui arba įgyvendinant oficialius įgaliojimus, suteiktus duomenų valdytojui (BDAR 6 straipsnio 1 dalies e punktas).

6. Be to, kredito kortelės duomenų saugojimas po apmokėjimo už prekes ar paslaugas nėra būtinas sutarčiai vykdyti (BDAR 6 straipsnio 1 dalies b punktas). Nors, visų pirma, duomenų, susijusių su kredito kortele, kurią klientas naudoja mokėdamas, tvarkymas yra būtinas siekiant įvykdyti sutartį ir todėl taikytinas BDAR 6 straipsnio 1 dalies b punktas, šių duomenų saugojimas yra naudingas tik siekiant palengvinti galimą kitą sandorį ir palengvinti pardavimą. Toks tikslas negali būti laikomas būtinu vykdant duomenų subjekto jau apmokėtų prekių tiekimo ar paslaugų teikimo sutartį[3].

7. Kai duomenis reikia tvarkyti dėl duomenų valdytojo arba trečiosios šalies teisėtų interesų[4], EDAV pažymi, kad tam, jog duomenų valdytojas galėtų remtis BDAR 6 straipsnio 1 dalies f punktu, turi būti įvykdytos trys šiame straipsnyje nustatytos sąlygos[5]. Norint remtis šiuo teisiniu pagrindu, visų pirma reikia nustatyti ir apibrėžti teisėtą interesą, kurio siekia duomenų valdytojas arba trečioji šalis. Duomenų valdytojo arba trečiosios šalies interesas gali būti platesnis nei duomenų tvarkymo tikslas ir jis turi egzistuoti ir galioti duomenų tvarkymo dieną[6].

8. Antra, kad būtų galima remtis teisėtų interesų teisiniu pagrindu, būtina, kad asmens duomenys būtų tvarkomi siekiant teisėto intereso. Kalbant apie šią paskutinę sąlygą, jei duomenų valdytojas turi teisėtą interesą, kaip nurodyta pirmiau, nėra akivaizdu, kad kredito kortelės duomenų saugojimas, siekiant palengvinti būsimus pirkimus, yra būtinas siekiant šio teisėto intereso. Iš tiesų faktinis kito pirkimo vykdymas priklauso nuo vartotojo pasirinkimo, o ne nuo galimybės jį atlikti „vienu paspaudimu“.

9. Galiausiai pagal trečiąją sąlygą reikia nustatyti pusiausvyrą: duomenų valdytojo arba trečiosios šalies teisėtas interesas turi būti suderintas su duomenų subjekto interesais arba pagrindinėmis teisėmis ir laisvėmis, įskaitant duomenų subjekto teises į duomenų apsaugą ir privatumą. Nustatant pusiausvyrą reikia atsižvelgti į konkrečias duomenų tvarkymo aplinkybes[7]. Nustatant pusiausvyrą būtina atsižvelgti į galimą duomenų tvarkymo poveikį duomenų subjekto teisėms ir laisvėms[8]. Toks poveikis gali priklausyti nuo duomenų pobūdžio, konkretaus duomenų tvarkymo metodo ir trečiųjų šalių prieigos prie tokių duomenų. Kalbant apie duomenų pobūdžio kriterijų,

[3] Taip pat žr. EDAV gaires 2/2019 dėl asmens duomenų tvarkymo pagal Bendrojo duomenų apsaugos reglamento 6 straipsnio 1 dalies b punktą, kai duomenų subjektams teikiamos internetinės paslaugos, ypač 10 puslapį.

[4] Žr. 29 straipsnio darbo grupės nuomonę dėl duomenų valdytojo teisėto intereso sąvokos pagal Direktyvos 95/46/EB 7 straipsnį, kurią šiuo metu peržiūri EDAV (žr. 2021 m. kovo 16 d. priimtą EDAV 2021–2022 m. darbo programą).

[5] Žr. 2017 m. gegužės 4 d. ESTT sprendimo *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde / Rīgas pašvaldības SIA ‘Rīgas satiksme’,* C-13/16, ECLI:EU:C:2017:336, 28 punktą.

[6] Žr. 2019 m. gruodžio 11 d. ESTT sprendimo *TK / Asociaţia de Proprietari bloc M5A-ScaraA,* C-708/18, ECLI:EU:C:2019:1064, 44 punktą.

[7] Žr. 2011 m. lapkričio 24 d. ESTT sprendimo *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ir Federación de Comercio Electrónico y Marketing Directo (FECEMD) / Administración del Estado,* C-468/10 ir C-469/10, ECLI:EU:C:2011:777, 47 ir 48 punktus; 2016 m. spalio 19 d. ESTT sprendimo *Patrick Breyer / Vokietijos Federacinė Respublika,* C-582/14, ECLI:EU:C:2016:779, 62 punktą.

[8] Žr. pirmiau minėto ESTT 2011 m. lapkričio 24 d. sprendimo 44 punktą, pirmiau minėto ESTT 2019 m. gruodžio 11 d. sprendimo 56 punktą.

reikėtų pažymėti, kad 29 straipsnio darbo grupė finansinius duomenis laiko labai asmeninio pobūdžio duomenimis, nes jų pažeidimas akivaizdžiai daro didelį poveikį duomenų subjekto kasdieniam gyvenimui[9]. Taigi, nepaisant duomenų valdytojo prievolės įgyvendinti technines ir organizacines priemones, kad būtų užtikrintas tinkamas kredito kortelių duomenų saugumas pagal BDAR 5 straipsnio 1 dalies f punktą, ir nepaisant to, kad šie duomenys gali būti saugomi kitais tikslais, jų tvarkymas siekiant palengvinti tolesnius pirkimus gali padidinti kredito kortelių duomenų saugumo pažeidimų riziką, nes duomenys tvarkomi kitose sistemose. Kitas svarbus pusiausvyros nustatymo elementas, į kurį būtų galima atsižvelgti vertinant duomenų tvarkymo poveikį duomenų subjektams, yra pagrįsti duomenų subjektų lūkesčiai, grindžiami jų santykiais su duomenų valdytoju, taip pat asmens duomenų rinkimo aplinkybėmis bei tikslu[10]. Tačiau atrodo, kad pirkimo metu, pateikdamas kredito kortelės duomenis mokėjimui atlikti, duomenų subjektas pagrįstai nesitiki, kad jo kredito kortelės duomenys bus saugomi ilgiau, nei tai būtina atsiskaityti už perkamas prekes ar paslaugas. Todėl tikėtina, kad šiomis konkrečiomis aplinkybėmis asmens, kuriam taikoma duomenų apsauga, pagrindinės teisės ir laisvės būtų viršesnės už duomenų valdytojo interesus.

10. Šie aspektai leidžia daryti išvadą, kad sutikimas (GPDR 6 straipsnio 1 dalies a punktas) yra vienintelis tinkamas teisinis pagrindas, kad pirmiau aprašytas duomenų tvarkymas būtų teisėtas. Iš tiesų, siekiant sumažinti riziką saugumui, sudaryti sąlygas duomenų subjektui kontroliuoti savo duomenis ir aktyviai spręsti dėl savo kredito kortelės duomenų naudojimo, konkretus duomenų subjekto sutikimas turėtų būti gautas prieš saugant jo kredito kortelės duomenis po pirkimo. Šis sutikimas leidžia duomenų valdytojui parodyti asmens norą palengvinti tolesnius jo pirkimus konkrečioje interneto svetainėje ar taikomojoje programoje, kuris negali būti numanomas vien dėl to, kad asmuo sudarė vieną ar kelis pavienius sandorius.

11. Šis sutikimas negali būti numanomas, jis turi būti laisvas, konkretus, pagrįstas informacija ir nedviprasmiškas[11]. Jis turi būti pareikštas aiškiu patvirtinančiu veiksmu ir jo turi būti prašoma naudotojui patogiu būdu, pavyzdžiui, pačioje duomenų rinkimo formoje naudojant žymimąjį langelį, kuris neturėtų būti iš anksto pažymėtas[12]. Šis konkretus sutikimas turi būti atskirtas nuo sutikimo su paslaugų ar pardavimo sąlygomis ir neturi būti sandorio įvykdymo sąlyga.

12. Pagal BDAR 7 straipsnio 3 dalį duomenų subjektas turi teisę bet kada atšaukti savo sutikimą dėl kredito kortelės duomenų saugojimo tolesnių pirkimų palengvinimo tikslais. Duomenų subjektui turi būti suteikta galimybė atšaukti sutikimą nemokamai, paprastai ir taip pat lengvai, kaip ir duoti sutikimą. Atšaukus sutikimą, duomenų valdytojas turi veiksmingai ištrinti kredito kortelių duomenis, saugomus tik tam, kad palengvintų tolesnius sandorius.

Europos duomenų apsaugos valdybos vardu

Pirmininkė

(Andrea Jelinek)

[9] 29 straipsnio darbo grupės Poveikio duomenų apsaugai vertinimo (PDAV) gairės, kuriomis Reglamento 2016/679 taikymo tikslais nurodoma, kaip nustatyti, ar duomenų tvarkymo operacijos „gali sukelti didelį pavojų“.
[10] Žr. BDAR 47 konstatuojamąją dalį.
[11] Žr. EDAV gaires 05/2020 dėl sutikimo pagal Reglamentą 2016/679.
[12] *Ten pat*.