VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

Mokėjimo iniciavimo paslaugas teikiančiai bendrovei skirta bauda dėl BDAR pažeidimų
(privatus sektorius, 61,5 tūkst. Eur bauda)

2019 m.

Valstybinė duomenų apsaugos inspekcija už Bendrojo duomenų apsaugos reglamento pažeidimus skyrė administracinę baudą, siekiančią 61 500 eurų. Sankcijos UAB „MisterTango“ pritaikytos dėl minėto reglamento 5, 32 ir 33 straipsnių pažeidimų – dėl asmens duomenų saugumo pažeidimo mokėjimo iniciavimo paslaugų sistemoje, apie kurį, be kita ko, nebuvo pranešta priežiūros institucijai. Inspekcijos nuomone, pradėtos skirti baudos pagal Bendrąjį duomenų apsaugos reglamentą turėtų būti reikšmingas signalas ir kitoms įmonėms, tik deklaratyviai įgyvendinančioms šio teisės akto nuostatas.

Valstybinė duomenų apsaugos inspekcija (Inspekcija) atliko tyrimą ir skyrė baudą, atsižvelgdama į gautą informaciją apie paviešintus bankų klientų asmens duomenis bei galimai įvykusį asmens duomenų saugumo pažeidimą UAB „MisterTango“. Tai įmonė, veikianti tarptautiniu mastu ir teikianti mokėjimo paslaugas tiek Lietuvos, tiek ir užsienio gyventojams bei įmonėms. Ji yra įsteigusi savo padalinį ir Latvijoje, paslaugas teikė ir kitose valstybėse. Lietuvos priežiūros institucija, pagal Bendrojo duomenų apsaugos reglamento (BDAR) nuostatas derindama savo sprendimą su Latvijos asmens duomenų apsaugos priežiūros institucija, turėjo progą gauti kolegų patvirtinimą dėl padarytų išvadų teisingumo. Šis atvejis taip pat parodo, kad įmonės turėtų daugiau dėmesio skirti duomenų saugumo pažeidimų valdymui ir bendradarbiavimui su priežiūros institucija tyrimų metu.

Inspekcija, atlikusi tyrimą, nustatė, kad įmonė pažeidė BDAR reikalavimus netinkamai tvarkydama asmens duomenis momentiniuose ekrano vaizduose (MEV), paviešindama asmens duomenis ir nepateikdama pranešimo apie asmens duomenų saugumo pažeidimą asmens duomenų apsaugos priežiūros institucijai.

Dėl netinkamo asmens duomenų tvarkymo. Įvertinus tyrimo metu surinktą informaciją ir pateiktus paaiškinimus, nustatyta, kad UAB „MisterTango“ tvarko (prieina, renka) daugiau asmens duomenų, negu pati nurodo esant būtina mokėtojo inicijuotam mokėjimui įvykdyti. Inspekcijos nuomone, įgyvendinant asmens duomenų kiekio mažinimo principą, turėtų būti renkami tik mokėjimo atlikimui būtini tokie duomenys kaip mokėtojo vardas, pavardė, jei mokėtojas pageidauja, jo identifikavimo kodas, banko sąskaitos numeris, valiuta ir likutis, mokėjimo paskirtis / įmokos kodas. Tačiau be šių duomenų įmonė rinko ir tokius pertekliniais laikytinus duomenis, pavyzdžiui, neperžiūrėtų elektroninių sąskaitų pateikimo datos, siuntėjų pavadinimai bei sumos; neperskaitytų pranešimų pateikimo datos, temos ir dalis pranešimo teksto; turimų paskolų paskirtys, pobūdžiai, sumos; pensijų fondų pavadinimai, sukaupti vienetai, jų vertė, sukauptos sumos; kredito tipai (pvz., būsto), mokėtini likučiai, kitų mokėjimų sumos bei

datos, išduotų mokėjimo kortelių numeriai ir jose esančios sumos. Be to, nustatyta, kad įmonė duomenis saugo ilgiau, negu pati yra nustačiusi bei nurodo esant reikalinga, t. y. tyrimo metu buvo pateikta duomenų dėl saugojimo 216 dienų, vietoje nustatytų 10 minučių. Pagal BDAR 5 straipsnį įmonė yra pati atsakinga, kad įgyvendintų atskaitomybės principą, t. y. laikytųsi BDAR reikalavimų ir sugebėtų tai įrodyti, tačiau tyrimo metu įmonė pakankamų įrodymų priežiūros institucijai nepateikė.

Dėl asmens duomenų paviešinimo. Tyrimo metu nustatyta, kad ne mažiau kaip 2 dienas (2018 m. liepos 9–10 d.) internete buvo prieinamas tinklalapis su UAB „MisterTango“ apdorotų mokėjimų sąrašu. Jame buvo matomi įvairių bankų įstaigų klientų atlikti mokėjimai per UAB „MisterTango“ mokėjimo iniciavimo paslaugų sistemą su tų klientų asmens duomenimis. Taip pat daugiau kaip 9 000 MEV su 12 skirtingų bankų, esančių skirtingose valstybėse, klientų mokėjimo sesijų detalių puslapiais. Be kita ko, nustatyta, kad įmonėje saugos užtikrinimą ir valdymą bei visos įmonės IT infrastruktūros (techninės ir programinės) valdymą, diegimą ir priežiūrą vykdė vienas darbuotojas. Vienas darbuotojas vykdė tarpusavyje konkuruojančias funkcijas. Taip nebuvo užtikrintas tinkamas neautorizuotų ar netyčinių modifikacijų galimybių minimizavimas ir tinkamos asmens duomenų apsaugos politikos įgyvendinimas. Taigi, UAB „MisterTango“ nepasirinko atitinkamų techninių ar organizacinių priemonių, kurios padėtų užtikrinti pavojų atitinkančio lygio saugumą, įskaitant apsaugą nuo neteisėto tvarkymo, atskleidimo, ir tuo pažeidė BDAR 5 ir 32 str.

Dėl pranešimo apie asmens duomenų saugumo pažeidimą nepateikimo. Pagal BDAR toks incidentas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga, yra duomenų saugumo pažeidimas. Inspekcijos nuomone, pirmiau minėtas incidentas, kai 2 dienas internete neautorizuotiems asmenims buvo sudaryta galimybė prieiti prie asmens duomenų, laikytinas tokiu duomenų saugumo pažeidimu, apie kurį privaloma pranešti priežiūros institucijai. Todėl UAB „MisterTango“ privalėjo nepagrįstai nedelsdama ir, jei įmanoma, praėjus ne daugiau kaip 72 valandoms nuo tada, kai sužinojo apie asmens duomenų saugumo pažeidimą, apie tai pranešti Inspekcijai. Apie šį pažeidimą nepranešdama priežiūros institucijai UAB „MisterTango“ pažeidė BDAR 33 str.

Inspekcija, spręsdama dėl administracinės baudos dydžio, įvertino visas aplinkybes, reikšmingas taikant atsakomybę UAB „MisterTango“, pavyzdžiui, kad įmonė asmens duomenis tvarkė neskaidriai, didesne apimtimi ir ilgiau, negu tai yra būtina duomenų tvarkymo tikslui pasiekti, neteisėtą asmens duomenų tvarkymą atliko sistemingai, asmens duomenų saugumo pažeidimo metu neužtikrino asmens duomenų saugumo, priežiūros institucijai nepranešė apie įvykusį asmens duomenų saugumo pažeidimą, kuris turėjo poveikį asmens duomenims, pagal kuriuos buvo galima tiesiogiai nustatyti asmens tapatybę, be to, šie duomenys sudarė banko paslaptį ir buvo tvarkomi nešifruoti bei asmens duomenų saugumo pažeidimo metu buvo tvarkomi neužtikrinant prieigos kontrolės prie šių duomenų. Skiriant įmonei 61 500 eurų administracinę baudą taip pat atsižvelgta ir į įmonės metinę pasaulinę apyvartą. Šis Inspekcijos sprendimas yra neįsiteisėjęs ir gali būti skundžiamas teismui.

Inspekcijos turimais duomenimis, reikšmingas baudas pagal BDAR jau yra skyrusi Prancūzija, Ispanija, Vokietija, Lenkija, Austrija, Bulgarija, Kipras, Malta.