VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

Automobilių nuomos bendrovei skirta bauda dėl duomenų saugumo pažeidimo pagal Bendrąjį duomenų apsaugos reglamentą

(privatus sektorius, 110 tūkst. Eur bauda)

2021 m.

Asmens duomenų apsaugos priežiūros institucija Valstybinė duomenų apsaugos inspekcija (VDAI) 2021 m. lapkričio 29 d. sprendimu skyrė 110 tūkst. eurų administracinę baudą trumpalaikės automobilių nuomos platformą „CityBee“ valdančiai UAB „Prime Leasing“. VDAI savo iniciatyva atliko tyrimą atsižvelgdama į 2021 m. vasario mėn. viešoje erdvėje pasirodžiusią informaciją dėl galimai įvykusio bendrovės klientų asmens duomenų saugumo pažeidimo (ADSP). Bauda bendrovei skirta dėl Bendrojo duomenų apsaugos reglamento (BDAR) 32 straipsnio 1 dalies a, b, d punktų, reglamentuojančių pareigą užtikrinti asmens duomenų tvarkymo saugumą, pažeidimų.

ATVEJO KILMĖ

UAB „Prime Leasing“ tyrimas pradėtas VDAI iniciatyva, atsižvelgus į gautą informaciją, kad buvo paviešinti bendrovės klientų asmens duomenys, įskaitant ir asmens kodus. Tyrimo metu bendrovė teisės aktų nustatyta tvarka pateikė priežiūros institucijai savo pranešimą apie ADSP bendrovės IT infrastruktūroje. Bendrovės teigimu, ji apie šį pažeidimą sužinojo iš kitos kibernetinio saugumo paslaugas teikiančios įmonės, kuri informavo, kad „CityBee“ klientų duomenys CSV formatu yra paskelbti RaidForums.com interneto svetainėje. Tyrimo metu nustatyta, kad paviešinti duomenys gauti iš neapsaugotai laikomo duomenų bazės atsarginės kopijos BACPAC failo (DB failas), kurio sukūrimo data yra 2018-02-27. Paaiškėjo, kad tiksli išorinės prieigos prie minėto failo panaikinimo data 2021-02-16 11:15. Nepateikus jokių faktinių įrodymų, kurie leistų teigti, kad minėtas failas buvo viešai pasiekiamas ne visą šį laikotarpį, buvo konstatuota, kad ADSP tęsėsi nuo 2018-02-27 iki 2021-02-16.

Atsižvelgiant į nustatytą trunkamąjį ADSP pobūdį bei įvertinus BDAR taikymo pradžią, priežiūros institucijos tyrimo metu buvo vertintos bendrovei taikomos BDAR numatytos prievolės, susijusios tiek su ADSP, tiek ir su reikalavimais asmens duomenų saugumo užtikrinimui.

PAGRINDINIAI TYRIMO REZULTATAI

Atlikus tyrimą nustatyta:

- DB failo, kuriame esančių asmens duomenų pagrindu sukurtas ir viešai paskelbtas bendrovės klientų asmens duomenų rinkinys CSV formatu, sukūrimo data buvo 2018-02-27.
- Atskleisti ir viešai paskelbti 110 302 „CityBee“ vartotojų duomenys.
- Nustatyti 433 vartotojai, kurie buvo pateikę savo gyvenamosios vietos adresą kitose Europos Sąjungos ir (ar) Europos Ekonominės Erdvės valstybėse.
- DB faile atviru tekstu buvo saugomi šie saugumo požiūriu keliantys didesnę riziką asmens duomenys: asmenų vardai, pavardės, adresai, telefono numeriai, el. pašto adresai, asmens kodai, vairuotojo pažymėjimo numeriai, mokėjimo kortelės tipas ir paskutiniai 4 jos numerio skaičiai, mokėjimo kortelės galiojimo data bei vartotojo „Braintree“ sistemoje identifikatorius (*token*).
- Bendrovė neužtikrino tinkamo asmens duomenų saugumo valdymo ir kontrolės:

- ✓ nepaskyrė tinkamą kompetenciją turinčio asmens atsakingu už saugumo užtikrinimą ir rizikos valdymą;
- ✓ neatskyrė IT kūrimo ir priežiūros srities pareigų ir atsakomybių ribų nuo kibernetinio saugumo srities pareigų ir atsakomybių ribų;
- ✓ neužtikrino prieigos prie DB failo žurnalinių įrašų fiksavimo ir kaupimo, bei neužtikrino atliekamų veiksmų su DB failų fiksavimo, stebėsenos ir vertinimo;
- ✓ DB failą saugojo nešifruotą, todėl techninių žinių turintis asmuo galėjo parsisiuntęs failą gauti pilną prieigą prie jame esančių duomenų. Asmens kodai DB faile taip pat buvo saugomi atviru tekstu, neapsaugoti naudojant maišos ar šifravimo algoritmus;
- ✓ DB faile esančius slaptažodžius šifravo silpnu ir gana nesaugiu laikomu SHA-1 šifravimo algoritmu. Techninių žinių turintys asmenys, pasinaudodami viešai internete prieinamais ir (ar) specializuotais įrankiais, galėjo nesunkiai sužinoti faile saugomų dalies (ar visų) slaptažodžių tikrąsias (neužmaskuotas maišos (angl. *hash*) būdu) reikšmes;
- ✓ vartotojai turėjo galimybę naudoti bendrovės IT saugumo politikos slaptažodžiams keliamų reikalavimų neatitinkantį slaptažodį.

- Bendrovė nevertino, nevaldė ir negalėjo valdyti rizikos, susijusios su šiame DB faile esančių asmens duomenų konfidencialumo praradimu (taikydama tinkamas organizacines ir technines saugumo priemones), nes, jos teigimu, ji nežinojo, kad jos valdomoje IT infrastruktūroje egzistuoja šis DB failas. Tai tiesiogiai lėmė ADSP bei buvo sudarytos sąlygos (anksčiau ar vėliau) jam įvykti.

Inspekcijos vertinimu, DB faile saugomų asmens duomenų konfidencialumą būtų apsaugojusios tinkamai panaudotos bent viena iš toliau nurodytų bazinių saugumo priemonių: autentifikuota prieiga prie DB failo tik bendrovės darbuotojams; prisijungimas prie saugyklos tik iš vidinio bendrovės kompiuterių tinklo; DB failo saugojimas užšifravus (šifravimo raktus patikint tik įgaliotiems bendrovės darbuotojams); tinkama informacinių išteklių stebėsena.

Pažymėtina, kad bendrovė ėmėsi reikiamų priemonių siekiant pašalinti ADSP ar sumažinti jo pasekmes ir tinkamai vykdė BDAR 33 straipsnio 3 dalies reikalavimus.

SPRENDIMAS

Kaip numato BDAR (83 straipsnio 4 dalies a punktas), UAB „Prime Leasing“ administracinė bauda skirta atsižvelgiant į bendrovės ankstesnių finansinių metų (2020 m.) bendrą metinę pasaulinę apyvartą ir įvertinus byloje pateiktas aplinkybes. VDAI sprendimu, už nustatytus BDAR 32 straipsnio 1 dalies a, b, d punktų pažeidimus administracinė 110 tūkst. eurų dydžio bauda leis pasiekti BDAR tikslus ir bus atgrasanti bei proporcinga.

VDAI, spręsdama dėl baudos dydžio, atsižvelgė į šiuos bendrovės atsakomybę sunkinančius ir švelninančius veiksnius:

- Sunkinantis veiksnys. DB failo saugumas nebuvo užtikrintas nuo pat jo sukūrimo, dėl ko įvyko ADSP, kurio metu buvo pažeistas didelio duomenų subjektų skaičiaus asmens duomenų konfidencialumas (BDAR 83 straipsnio 2 dalies a punktas). Nors žalos duomenų subjektams dydis nebuvo neaiškus bylos nagrinėjimo metu, tačiau tai nereiškia, kad ši žala ateityje nekils, juolab, kad dėl pačios bendrovės tinkamo duomenų saugumo neužtikrinimo, nėra aišku, kiek asmenų turėjo neteisėtą prieigą prie DB failo ir kiek plačiai šie duomenys jau yra pasklidę, tik dar nėra panaudoti, taip pat nėra aišku, kur ir kaip plačiai jau yra panaudoti, tik dar nežinomi tokie panaudojimo atvejai.
- Sunkinantis veiksnys. Dėl netinkamo duomenų saugumo užtikrinimo buvo pažeistas asmens unikalaus identifikatoriaus (asmens kodo), kuris nėra keičiamas, kurį draudžiama skelbti viešai (Asmens duomenų teisinės apsaugos įstatymo 3 straipsnio 2 dalis) bei pagal kurį daugelyje Lietuvos Respublikos registrų ir informacinių sistemų tarpusavyje siejama įvairi informacija, konfidencialumas. Be to, aptariamame DB faile išsaugota visuma asmens duomenų tiesiogiai ir

nedviprasmiškai identifikuoja konkretų fizinį asmenį. Pažymėtina, kad šie asmens duomenys buvo saugomi be jokios papildomos techninės apsaugos, nebuvo šifruoti (BDAR 83 straipsnio 2 dalies g punktas).

- Bendrovė asmens duomenų migracijos procesui netaikė rizikos vertinimo, pasikliovė tik įsitikinimu, kad taip, kaip jis yra atliekamas, yra saugu. Bendrovė, kaip duomenų valdytojas, turėjo pareigą užtikrinti asmens duomenų saugumą ne tik duomenų migracijos proceso metu, bet ir tolimesnio DB failo tvarkymo metu. Toks bendrovės elgesys vertintas kaip aplaidumas (BDAR 83 straipsnio 2 dalies b punktas). Aplinkybė, jog bendrovės veiksmuose nustatyta ne tyčia, o aplaidumas, yra pagrindas atsakomybę bendrovei švelninti.

Aplinkybės, į kurias atsižvelgta, tačiau jos nebuvo vertinamos nei kaip atsakomybę švelninantys, nei kaip sunkinantys veiksniai:

- Bendrovė, įvykus ADSP, ėmėsi priemonių siekiant pašalinti ADSP ar sumažinti jo pasekmes ir įvykus ADSP tinkamai vykdė BDAR 33 straipsnio 3 dalies reikalavimus (BDAR 83 straipsnio 2 dalies c punktas).
- Bendrovė tiesiogiai, kaip duomenų valdytoja, atsakinga už netinkamą BDAR 32 straipsnio reikalavimų neužtikrinimą nurodyto failo atžvilgiu (BDAR 83 straipsnio 2 dalies d punktas).
- Bendrovės atžvilgiu iki nagrinėjamo atvejo nebuvo taikytos jokios poveikio priemonės už BDAR 24 straipsnio ir (ar) 32 straipsnio nuostatų pažeidimą (BDAR 83 straipsnio 2 dalies e punktas).
- Bendrovė atliekant tikrinimą bendradarbiavo su VDAI, tačiau bendradarbiavimas nėra sietinas su siekiu atitaisyti pažeidimą ar sumažinti jo galimo neigiamo poveikio laipsnį.
- Nors VDAI bendrovės tyrimą pradėjo savo iniciatyva gautos informacijos pagrindu, tačiau visuomenę apie įvykusį ADSP, kurio kontekste buvo tikrintas bendrovės saugumas, informavo pati bendrovė. Be to, bendrovė, nepraleidusi BDAR 34 straipsnyje nustatytų terminų, apie įvykusį ADSP informavo VDAI (BDAR 83 straipsnio 2 dalies h punktas). Atsižvelgiant į tai, nelaikytina, kad bendrovė būtų siekusi nuslėpti ADSP nuo VDAI.

VDAI bylą dėl administracinės baudos skyrimo išnagrinėjo žodinės procedūros tvarka uždarame posėdyje, dalyvaujant VDAI ir UAB „Prime leasing“ atstovams. Atsižvelgiant į tai, kad ADSP buvo susijęs ir su kitų Europos Sąjungos valstybių narių piliečių asmens duomenimis, vadovaujantis BDAR priimtas sprendimas suderintas ir su tų valstybių asmens duomenų apsaugos priežiūros institucijomis. Susijusiomis priežiūros institucijomis save laikė šių valstybių priežiūros institucijos: Airijos, Vokietijos, Austrijos, Italijos, Portugalijos, Estijos, Belgijos, Danijos, Olandijos, Ispanijos, Latvijos, Švedijos, Liuksemburgo, Prancūzijos, Norvegijos, Suomijos, Slovakijos, Slovėnijos.

Šis sprendimas Lietuvos Respublikos administracinių bylų teisenos nustatyta tvarka per vieną mėnesį nuo jo įteikimo dienos gali būti skundžiamas Vilniaus apygardos administraciniam teismui.

2021-12-29 bendrovė paskelbė viešai, kad VDAI sprendimo teismui neskųs.