TOP-3
2023 M. VALSTYBINĖS DUOMENŲ APSAUGOS INSPEKCIJOS SKIRTOS DIDŽIAUSIOS BAUDOS

Baudos už BDAR pažeidimus Lietuvoje ženklios, tačiau lyginant su TOP 3 didžiausiomis baudomis pasaulyje , skirtomis Meta Platforms Ireland Ltd.– dv baudos -1,2 mlrd. ir 390 mln. Eur, TikTok Ltd – 345 mln. Eur, neišsiskiriame.

1. **---20 tūkst. Eur bauda**

Valstybinėje duomenų apsaugos inspekcijoje gautas pranešimas apie asmens duomenų saugumo pažeidimą, kurio metu buvo pažeistas virš 50 000 duomenų subjektų (klientų) asmens duomenų konfidencialumas. Šio ADSP pagrindu Inspekcija savo iniciatyva atliko Bendrovės tikrinimą.

Tikrinimo metu nustatyta, kad ADSP metu:

1) nebuvo įgyvendintos priemonės, užtikrinančios tinkamą IT sistemų administratorių ir kitų privilegijuotų naudotojų (pavyzdžiui, programuotojų) prieigų kontrolę ir autentifikavimą:

− jungiantis prie IT sistemos duomenų bazės administravimo panelės nebuvo įdiegtas prieigos ribojimas tik įgaliotiems asmenims;

− įvedant naudotojų prisijungimo duomenis sistemos duomenų bazės administravimo panelėje nebuvo naudojama kelių veiksnių autentifikacija (angl. MFA – Multi-factor authentication),

nebuvo užtikrinama pakankamo lygio apsauga nuo slaptažodžių parinkimo ar kitų panašaus pobūdžio kibernetinių atakų, nebuvo įdiegtos priemonės nuo slaptažodžių spėliojimo;

− nebuvo tinkamai užtikrinama IT sistemų administratorių ir kitų privilegijuotų naudotojų prisijungimo prie sistemos prieigos kontrolė, neatliekamas sistemos naudotojų veiksmų ir žurnalinių įrašų stebėjimas. Inspekcija padarė išvadą, kad tiriamas ADSP įvyko dėl nepakankamai užtikrinamos prieigų kontrolės ir autentifikavimo, jungiantis prie IT sistemų techninio administravimo tikslu, todėl neišvengta neteisėtos prieigos prie Bendrovės valdomos sistemos duomenų bazės, nebuvo užtikrinamas tinkamas IT sistemų žurnalinių įrašų kaupimas ir saugojimas, nesilaikoma žurnalinių įrašų saugojimo terminų ir stebėsenos rekomendacijų.

ADSP tyrimo metu taip pat nustatyta, kad įvykus ADSP Bendrovė nedelsiant sustabdė IT sistemos veikimą, t. y. ėmėsi tinkamų veiksmų įvykusiam ADSP suvaldyti. Taip pat tikrinimo metu nustatyta, kad Bendrovė neįrodė, jog nustatytas 5 metų saugojimo terminas yra būtinas visiems klientams ir proporcingas siekiamiems tikslams, todėl Inspekcija padarė išvadą, kad Bendrovė, IT sistemoje esančių klientų asmens duomenis saugodama 5 metus, pažeidė BDAR 5 straipsnyje įtvirtintą duomenų saugojimo trukmės apribojimo principą. Šiuo atveju, Bendrovė pateiktus argumentus siejo su siekiu supaprastinti klientams paslaugų užsakymą ir naudojimąsi paslaugomis, siekiu valdyti galimus klientų įsiskolinimus bei siekiu užtikrinti Bendrovės teisių gynimą, tačiau Inspekcija padarė išvadą, kad nei vienas iš argumentų negalėtų būti taikomas visų klientų atžvilgiu. BDAR konstatuojamosios dalies 39 punkte, be kita ko, nurodyta: „ Asmens duomenys turėtų būti tinkami, susiję su tikslais, kuriais jie tvarkomi, ir riboti pagal tai, kiek jų yra būtina turėti atsižvelgiant į tikslus, kuriais jie tvarkomi; tam pirmiausia reikia užtikrinti, kad asmens duomenų saugojimo laikotarpis būtų tikrai minimalus. Asmens duomenys turėtų būti tvarkomi tik tuomet, jei asmens duomenų tvarkymo tikslo pagrįstai negalima pasiekti kitomis priemonėmis. Siekiant užtikrinti, kad duomenys nebūtų laikomi ilgiau nei būtina, duomenų valdytojas turėtų nustatyti duomenų ištrynimo arba periodinės peržiūros terminus.“ Pagal pateiktą teisinį reglamentavimą nustatant asmens duomenų saugojimo

terminus turi būti atsižvelgiama į du pagrindinius aspektus: duomenis reikia saugoti kuo trumpesnį laiką; kiekvienas saugojimo laikotarpis turi būti siejamas su konkrečiu asmens duomenų tvarkymo tikslu.

2. --- 10 tūkst. Eur bauda:

Valstybinė duomenų apsaugos inspekcija išnagrinėjusi pareiškėjo skundą, priėmė sprendimą, kuriuo skundo dalį dėl teisės apriboti duomenų tvarkymą pažeidimo pripažino pagrįsta ir teikė Bendrovei nurodymą – atsakyti pareiškėjui, ar buvo apribotas jo asmens duomenų tvarkymas pagal jo prašymą ir, jeigu nebuvo, tuomet teisiškai pagrįsti pareiškėjui, kodėl nebuvo bei apie nurodymo įvykdymą informuoti Inspekciją raštu, pateikiant tai patvirtinančius įrodymus. Atsakymo apie Nurodymo vykdymą Bendrovė Inspekcijai nepateikė.

Apie Nurodymo įvykdymą Bendrovė turėjo informuoti Inspekciją raštu iki nurodyto termino, pateikiant tai patvirtinančius įrodymus. Pažymėtina, kad Bendrovė Inspekcijos sprendimo, kuriuo buvo teiktas Nurodymas, teismui neskundė. Sprendimu teiktas Nurodymas yra galiojantis ir nenuginčytas, dėl to jo turi būti laikomasi ir jis turi būti vykdomas, tačiau duomenų apie Nurodymo įvykdymą Bendrovė Inspekcijai nepateikė, nors Inspekcija raštu kelis kartus prašė Bendrovės pateikti informaciją apie Nurodymo įvykdymą. Esant nurodytoms aplinkybėms, Inspekcija darė išvadą, kad Nurodymas nebuvo įvykdytas. Šią išvadą patvirtino ir Bendrovės administracinės baudos skyrimo procedūros metu pateikti paaiškinimai, iš kurių matyti, kad Nurodymo nesilaikoma, jis nebuvo įvykdytas, nes Bendrovė su juo iš esmės nesutiko. Bendrovė, nesutikdama su Inspekcijos sprendimu bei jame teiktu Nurodymu, turėjo teisę skųsti jį teismui teisės aktų nustatyta tvarka, tačiau šia teise nepasinaudojo. Įsiteisėjęs Inspekcijos Nurodymas yra privalomas ir turi būti vykdomas, o jeigu nesilaikoma priežiūros institucijos nurodymo, taip pat jei nesuteikiama prieigos galimybė pažeidžiant BDAR 58 straipsnio 1 dalį, gali būti skiriama administracinė bauda.

3.--- 8 tūkst. Eur bauda:

Valstybinėje duomenų apsaugos inspekcijoje 2022 m. liepos mėn. gautas fizinio asmens skundas dėl Bendrovėje tinkamai neįgyvendintos pareiškėjo teisės susipažinti su Bendrovėje tvarkomais jo asmens duomenimis. Bendrovė pareiškėjui nepateikė informacijos apie jo asmens duomenų tvarkymo tikslus ir teisinius asmens duomenų tvarkymo pagrindus, asmens duomenų gavėjus, asmens duomenų kategorijas ir asmens duomenų saugojimo laikotarpį, taip pat informacijos apie kitus šaltinius, iš kurių buvo gauti pareiškėjo asmens duomenys, nepateikė ir tvarkomų asmens duomenų kopijos. Duomenų subjekto teisė susipažinti su savo duomenimis ir atitinkama duomenų valdytojo pareiga supažindinti duomenų subjektą su jo duomenimis detalizuoja vieną iš pagrindinių duomenų apsaugos teisės – skaidrumo – principą. Taikant skaidrumo principą, fiziniams asmenims turėtų būti aišku, kaip su jais susiję asmens duomenys yra renkami, naudojami, su jais susipažįstama arba jie yra kitaip tvarkomi, taip pat kokiu mastu tie asmens duomenys yra ar bus tvarkomi (BDAR preambulės 39 punktas). Be to, duomenų subjektas turi turėti teisę susipažinti su apie jį surinktais asmens duomenimis ir galimybę ta teise lengvai ir pagrįstais laiko tarpais pasinaudoti, kad žinotų apie duomenų tvarkymą ir galėtų patikrinti jo teisėtumą (BDAR preambulės 63 punktas). Nagrinėjamu atveju nustatytas pažeidimas – pareiškėjo teisės susipažinti su asmens duomenimis tinkamas neįgyvendinimas, lėmė tai, kad pareiškėjui nebuvo sudaryta galimybė patikrinti, kokiu teisiniu pagrindu (ar pagrindais) pareiškėjo asmens duomenys tvarkomi, kokie konkrečiai duomenys ir kokiais tikslais tvarkomi, kiek laiko jie bus saugomi ir kt.

Šaltinis: VDAI sprendimai (baudos, nurodymai ir kt.) - Valstybinė duomenų apsaugos inspekcija (lrv.lt)