VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

Valstybinė duomenų apsaugos inspekcija, atlikusi tyrimą, priėmė sprendimą dėl neužtikrinto tinkamo asmens duomenų konfidencialumo, vientisumo, prieinamumo ir atsparumo bei pažeisto duomenų saugojimo trukmės principo

2023 m.

SUTRUMPINTAS APIBENDRINIMAS

Sprendimo kontekstas

Sprendimo data: 2023-04-20
Nacionalinis atvejis
Valdytojas: privatus juridinis asmuo (toliau – Bendrovė)
Teisinės nuorodos: *gebėjimas užtikrinti duomenų saugojimo trukmės apribojimo bei konfidencialumo principus (pagal BDAR[1] 5 straipsnio 1 dalies e ir f punktus bei 32 straipsnio 1 dalies b ir d punktus)*
Sprendimas: *administracinė bauda 20 000 Eur*

Sprendimo santrumpa

Bylos priežastis

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

Pagrindinės išvados

Tikrinimo metu nustatyta, kad ADSP metu Bendrovės informacinėje sistemoje, kurioje įvyko incidentas (toliau – IT sistema), nebuvo įgyvendintos priemonės, užtikrinančios tinkamą IT sistemų administratorių ir kitų privilegijuotų naudotojų prieigų kontrolę ir autentifikavimą.

Taip pat nustatyta, kad Bendrovė neįrodė, jog jos nustatytas asmens duomenų saugojimo terminas yra būtinas visų klientų asmens duomenų saugojimui ir proporcingas siekiamiems tikslams.

Sprendimas

Už nustatytus BDAR 5 straipsnio 1 dalies e ir f punktų bei 32 straipsnio 1 dalies b ir d punktų nuostatų pažeidimus Bendrovei skirta 20 000 Eur dydžio administracinė bauda.

[1] 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 (Bendrasis duomenų apsaugos reglamentas)

PLATESNIS APIBENDRINIMAS

Inspekcijos tyrimo priežastys

Inspekcija gavo pranešimą, kuriame nurodyta, kad Bendrovėje 2022-06-30 įvyko ADSP, kaip jis apibrėžiamas BDAR 4 straipsnio 12 punkte, kurio metu buvo pažeistas virš 50 000 duomenų subjektų (Bendrovės klientų) asmens duomenų, įskaitant klientų vardus, pavardes, el. pašto adresus, telefono numerius, automobilių valstybinius numerius, konfidencialumas. Toks ADSP vertintinas kaip galintis kelti didelį pavojų fizinių asmenų (duomenų subjektų) teisėms ir laisvėms, todėl Inspekcija savo iniciatyva pradėjo tyrimą, susijusį su galimu BDAR nuostatų pažeidimu.

Tyrimui aktualios BDAR nuostatos

Pagal BDAR 5 straipsnio 1 dalies e punktą, asmens duomenys turi būti laikomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, nei tai yra būtina tais tikslais, kuriais asmens duomenys yra tvarkomi; asmens duomenis galima saugoti ilgesnius laikotarpius, jeigu asmens duomenys bus tvarkomi tik archyvavimo tikslais viešojo intereso labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais pagal BDAR 89 straipsnio 1 dalį, įgyvendinus atitinkamas technines ir organizacines priemones, kurių reikalaujama šiuo reglamentu siekiant apsaugoti duomenų subjekto teises ir laisves (saugojimo trukmės apribojimo principas).

BDAR 5 straipsnio 1 dalies f punkte nustatyta, kad asmens duomenys turi būti tvarkomi tokiu būdu, kad taikant atitinkamas technines ar organizacines priemones būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo (vientisumo ir konfidencialumo principas).

Pagal BDAR 5 straipsnio 2 dalį, duomenų valdytojas yra atsakingas už tai, kad būtų laikomasi BDAR 5 straipsnio 1 dalies, ir turi sugebėti įrodyti, kad jos laikomasi (atskaitomybės principas).

Pagal BDAR 24 straipsnio 1 dalį, atsižvelgdamas į duomenų tvarkymo pobūdį, aprėptį, kontekstą bei tikslus, taip pat į įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas įgyvendina tinkamas technines ir organizacines priemones, kad užtikrintų ir galėtų įrodyti, kad duomenys tvarkomi laikantis šio reglamento. Tos priemonės prireikus peržiūrimos ir atnaujinamos.

Vadovaujantis BDAR 32 straipsnio 1 dalimi, atsižvelgdamas į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas bei duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas ir duomenų tvarkytojas įgyvendina tinkamas technines ir organizacines priemones, kad būtų užtikrintas pavojų atitinkančio lygio saugumas, įskaitant gebėjimą užtikrinti nuolatinį duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą (b punktas) bei reguliarų techninių ir organizacinių priemonių, kuriomis užtikrinamas duomenų tvarkymo saugumas, tikrinimo, vertinimo ir veiksmingumo vertinimo procesą (d punktas).

Pagal BDAR 32 straipsnio 2 dalį, nustatant tinkamo lygio saugumą, visų pirma, atsižvelgiama į pavojus, kurie kyla dėl duomenų tvarkymo, visų pirma, dėl netyčinio arba neteisėto persiųstų, saugomų ar kitaip tvarkomų duomenų sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jų.

Nustatant asmens duomenims kylantį pavojų ir rizikas bei vertinant, ar duomenų valdytojas įgyvendina tinkamas technines ir organizacines saugumo priemones, yra atsižvelgiama į ISO/IEC 27002 standartą „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“.

Tyrimo metu nustatytos aplinkybės

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 (ISO/IEC 27002:2017 9.4 punktas „Prieigos prie sistemų ir taikomųjų programų valdymas“).

2) nebuvo užtikrinamas tinkamas IT sistemų žurnalinių įrašų kaupimas ir saugojimas, nesilaikoma žurnalinių įrašų saugojimo terminų ir stebėsenos rekomendacijų (ISO/IEC 27002:2017 12.4 punktas „Registravimas ir stebėsena“, 2020-06-18 „Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams“), todėl konstatuota, kad Bendrovė neįgyvendino priemonių, kuriomis gebėtų tikrinti ir vertinti naudojamų techninių ir organizacinių priemonių, kuriomis užtikrinamas duomenų tvarkymo saugumas, veiksmingumą, ir tokiu neveikimu pažeidė BDAR 32 straipsnio 1 dalies d punkto nuostatas.

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.

Administracinės baudos skyrimo motyvai ir baudos dydžio nustatymas[2]

[2] Priimant sprendimą dėl administracinės baudos skyrimo Inspekcija atsižvelgė į 29 straipsnio darbo grupės 2017-10-03 priimtas Administracinių baudų taikymo ir nustatymo pagal Reglamentą 216/679 gaires bei Europos duomenų apsaugos valdybos 2022-05-16 priimtas Gaires 04/22 dėl administracinių baudų apskaičiavimo pagal BDAR

Tikrinimo metu Inspekcija nenustatė, kad Bendrovės padarytas pažeidimas būtų padarytas tyčia ar būtų susijęs su specialių kategorijų asmens duomenų tvarkymu (BDAR 83 straipsnio 2 dalies b ir g punktai), todėl šios aplinkybės laikytos neutraliomis), tačiau ADSP buvo susijęs su poveikiu dideliam skaičiui duomenų subjektų (BDAR 83 straipsnio 2 dalies a punktas), todėl ši aplinkybė laikyta sunkinančia. Kitų BDAR 83 straipsnio 2 dalyje nustatytų veiksnių įvertinimas (iš Bendrovei taikytų 8 veiksnių, pagal 2 veiksnius nustatytos Bendrovės atsakomybę sunkinančios aplinkybės[3], pagal vieną veiksnį – lengvinančios[4]) siejamas su Bendrovės metine apyvarta, todėl plačiau nekomentuojamas.

[3]Viena jau minėta aplinkybė – nustatyta BDAR 83 straipsnio 2 dalies a punkte, kita – BDAR 83 straipsnio 2 dalies d punkte ir vertinta kaip pagrindinis pažeidimas, t. y. duomenų valdytojo įgyvendintos techninės ir organizacinės priemonės

[4] T. y. veiksmai, kurių Bendrovė ėmėsi, kad būtų sumažinta duomenų subjektų patiriama žala (BDAR 83 straipsnio 2 dalies c punktas)