



VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

SPRENDIMAS

2026 m. kovo d. Nr. 3R- (2.13-1.E)
Vilnius

Valstybinė duomenų apsaugos inspekcija (toliau – Inspekcija) žodinės procedūros tvarka, 2026-02-19 vykusiamе uždaramе posėdyje, dalyvaujant [DUOMENYS NESKELBTINI] išnagrino bylą dėl administracinės baudos skyrimo UAB DELSKA Lithuania¹ (toliau ir – Bendrovė, Tikrinamas asmuo), juridinio asmens kodas 302527488.

1. Inspekcijos patikrinimo inicijavimo aplinkybės

2026 m. kovo mėn. Inspekcija gavo tris pranešimus apie asmens duomenų saugos pažeidimus (1. [DUOMENYS NESKELBTINI] 2025-03-06 pranešimą apie asmens duomenų saugumo pažeidimą (toliau – ADSP) (Inspekcijos reg. Nr. 1R-1473 (2.23.E)); 2. [DUOMENYS NESKELBTINI] 2025-03-07 pranešimą apie asmens duomenų saugumo pažeidimą (Inspekcijos reg. Nr. 1R-1497 (2.23.E)); 3. [DUOMENYS NESKELBTINI] 2025-03-06 pranešimą apie asmens duomenų saugumo pažeidimą (Inspekcijos reg. Nr. 1R-1512 (2.23.E)), susijusius su 2025-03-03 15:00 val. UAB „Rakrėjus“ (Tikrinamo asmens) viešosios debesijos paslaugų platformoje [DUOMENYS NESKELBTINI] įvykusi kibernetinio saugumo incidentu (toliau – Incidentas).

2025-03-06 [DUOMENYS NESKELBTINI] Inspekcijai pateiktame pranešime (Inspekcijos reg. Nr. 1R-1473 (2.23.E)) nurodoma, kad 2025-03-03 15:00 val. buvo paveikta [DUOMENYS NESKELBTINI] viešosios debesijos platforma. Incidento sukėlėjai užšifravo dalį saugomų atsarginių kopijų ir virtualiuose serveriuose esančių klientų sistemų. Bandant surasti sprendimus atšifruoti ir atkurti paslaugų teikimą, buvo susidurta su kenkėjiškos programinės įrangos veikimo iššūkiais, ko pasekoje klientų esami virtualūs resursai ir atsarginės duomenų kopijos yra nepasiekiamos. Atsarginės duomenų kopijos laikotarpiu nuo 2025-03-03 15:00 val. yra prarastos ir negalės būti atkurtos. [DUOMENYS NESKELBTINI] pranešime buvo nurodyta, kad Incidentu buvo paveikti apytiksliai 180 fizinių asmenų duomenys (asmens kodai, gimimo datos, vardai, pavardės, adresai, telefono numeriai, el. pašto adresai, banko sąskaitų numeriai), esantys buhalterinės apskaitos programoje [DUOMENYS NESKELBTINI]. Atsakydama į Inspekcijos 2025-03-07 raštą Nr. 2R-990 (2.23.E) [DUOMENYS NESKELBTINI] nurodė, kad ADSP tyrimą planuojama baigti iki 2025-03-27. [DUOMENYS NESKELBTINI] pažymėjo, kad sutartis su Tikrinamu asmeniu buvo elektroninė ir saugoma su kitais įmonės elektroniniais dokumentais, todėl dėl įvykusio incidento jos pateikti negali. [DUOMENYS NESKELBTINI] nurodė, kad kaip 2025-03-13 informavo Tikrinamas asmuo, [DUOMENYS NESKELBTINI] virtuali mašina atkurta naujoje virtualaus duomenų centro aplinkoje, tačiau dėl prieigos nebuvimo nėra galimybės patikrinti ar visi duomenys ir dokumentai yra tinkamai atkurti. [DUOMENYS NESKELBTINI] taip pat nurodė, kad už atsarginių kopijų saugojimą buvo atsakingas Tikrinamas asmuo. Kartu su atsakymu [DUOMENYS NESKELBTINI] pridėjo kovo mėnesio PVM sąskaitą faktūrą, kurioje detalizuotai matosi teikiamos „Back-Up“ paslaugos.

2025-03-07 [DUOMENYS NESKELBTINI] pateiktame pranešime (Inspekcijos reg. Nr. 1R-1497 (2.23.E)) nurodoma, kad iš Tikrinamo asmens 2025-03-04 15:19 val. el. paštu gauta informacija apie

¹ UAB „Rakrėjus“ turto, teisių ir pareigų perėmėja pagal 2025-01-24 reorganizavimo sąlygas ir 2025-04-28 turto, teisių ir pareigų perdavimo–priėmimo aktą.

kibernetinio saugumo incidentą, kurio metu buvo paveikta [DUOMENYS NESKELBTINI] viešosios debesijos platforma. [DUOMENYS NESKELBTINI] paaiškino, kad dėl įvykusio Incidento buvo suformuotas Krizių valdymo komitetas, kuris atlieka bei koordinuoja strateginius ir taktinius situacijos valdymo veiksmus. Be to, lygiagrečiai vykdomas vidinis Incidento tyrimas, kuriame dalyvauja vadovas, duomenų apsaugos pareigūnė, IT projektų vadovas, IT infrastruktūros administratorius, informacinės saugos ekspertas, taip pat pasitelkti išoriniai teisininkai. [DUOMENYS NESKELBTINI] pažymėjo, kad savo infrastruktūros lygyje bendrą kibernetinio incidento tyrimą atlieka ir paslaugų teikėjas – Tikrinimas asmuo. Kadangi Incidentas įvyko Tikrinamo asmens infrastruktūroje ir paveikė ne vien tik [DUOMENYS NESKELBTINI] duomenis, pagrindinį vaidmenį tiriant ir valdant visą incidentą atlieka iš esmės Tikrinamas asmuo, su kuriuo [DUOMENYS NESKELBTINI] palaiko nuolatinį tiesioginį ryšį, vykdamas tiesioginę ir nenutrūkstamą komunikaciją. [DUOMENYS NESKELBTINI] nurodė, kad 2025-03-04 kreipėsi į Tikrinamą asmenį dėl papildomos informacijos pateikimo apie Incidentą, prašydamas nurodyti: 1) kokio pobūdžio ir masto yra Incidentas, pateikiant jo faktines aplinkybes, kas lėmė jo atsiradimą, trukmę, pašalinimo terminus, ar šiuo metu Incidentas yra visiškai suvaldytas ir kitą esminę informaciją; 2) ar trečiosioms šalims atskleisti ir/arba trečiosios šalys neteisėtai įgijo prieigas prie bet kokių banko, įskaitant jo klientų duomenų (įskaitant asmens duomenis). Jei taip, kokie banko duomenys ir kokioje apimtyje tapo prieinami trečiosioms šalims; 3) nurodyti, kokių priemonių yra imtasi ir kokie veiksmai šiuo metu yra atliekami, siekiant užkirsti kelią neigiamoms pasekmėms atsirasti dėl patirto Incidento. Anot [DUOMENYS NESKELBTINI], 2025-03-05 pateiktame Tikrinamo asmens atsakyme buvo nurodyta, kad buvo susidurta su kenkėjiška duomenų šifravimo programa [DUOMENYS NESKELBTINI], kuri didelę dalį duomenų užšifravo, dėl ko naudojimas duomenimis yra negalimas. Nepaisant to, patikrinus ryšio grafikus ir įvykių sekoje matomus veiksmus įsitikinta, kad duomenys nebuvo pasisavinti. Tikrinimas asmuo taip pat nurodė, kad 1) patikrinus sistemų žurnalus buvo rastas pažeidimas ir sudaryta chronologinė įvykių seka; 2) patikrinus ryšio grafikus ir įvykių sekoje matomus veiksmus įsitikinta, kad duomenys nebuvo pasisavinti; 3) duomenų iššifravimui Tikrinamo asmens komanda naudojo oficialius iššifravimo įrankius, tačiau iki šiol visi bandymai nebuvo sėkmingi; 4) Tikrinamas asmuo kreipėsi į Nacionalinį kibernetinio saugumo centrą (toliau – NKSC) dėl Incidento bei pateikė surinktą informaciją apie Incidentą; 5) Tiesioginiai ryšiai tarp sistemų buvo panaikinti, kita dalis sistemų izoliuota (kitoje aplinkoje bei [DUOMENYS NESKELBTINI]), peržiūrėti vartotojai ir pakeisti jų prisijungimo duomenys [DUOMENYS NESKELBTINI], pažeistos sistemos lokalizuotos ir neturi sąsajos su „išore“. [DUOMENYS NESKELBTINI] taip pat nurodė, kad siekiant atkurti veiklos tęstinumą, nedelsiant pradėtas duomenų atkūrimas visiškai naujoje debesijos platformoje, nesusijusioje su [DUOMENYS NESKELBTINI], iš kritinių sistemų atsarginių kopijų. [DUOMENYS NESKELBTINI] pažymėjo, kad kritinės sistemos turėjo nuo debesijos platformos [DUOMENYS NESKELBTINI] atskirtas atsargines kopijas, kurios nebuvo sukompromituotos, jų prieinamumas prarastas nebuvo. Visi duomenys, išskyrus vartojimo kredito paraiškas ir jose esančią informaciją, buvo sėkmingai atkurti. Vartojimo kredito paraiškos ir jose esanti informacija (t.y., savo pobūdžiu archyvinė informacija) nebuvo saugomi kritinėse sistemose, todėl, tikėtina, kad šių duomenų atkurti artimoje ateityje nepavyks. Be to, šiuo metu nėra atkurtos kai kurių archyvinių duomenų kopijos, kurios neturi įtakos kasdieninėms [DUOMENYS NESKELBTINI] operacijoms. Kartu su Inspekcijai pateiktais papildomais 2025-04-22 paaiškinimais (Inspekcijos reg. Nr. 1R-2554 (2.23 Mr)), [DUOMENYS NESKELBTINI] pateikė galutinę ADSP ataskaitą, iš kurios matyti, kad dėl Incidento buvo laikinai prarastas prieinamumas prie tvarkomų asmens duomenų – duomenys tapo neprieinami dėl jų užšifravimo kenkėjiška programa [DUOMENYS NESKELBTINI]. Preliminariu [DUOMENYS NESKELBTINI] vertinimu, dėl Incidento buvo paveikti 2 252 klientų ir 107 darbuotojų asmens duomenys (vardai, pavardės, elektroniniai paštai, telefono numeriai, asmens tapatybės dokumentų duomenys, nuotraukos, IP adresai, interneto banko prisijungimo duomenys, naršymo informacija (kada ir iš kur buvo prisijungta prie banko sistemų), mokesčių mokėtojo identifikaciniai numeriai,

duomenys apie klientų sandorius su banku ir sudarytas sutartis (banko sąskaitų numeriai, indėliai, mokėjimo nurodymai ir kitos mokėjimo operacijos, naudojamos mokėjimo priemonės ir jų naudojimo duomenys, piniginių lėšų įnešimo, išėmimo operacijų duomenys), duomenys, susiję su kredituojamu ar lizinguojamu turtu ir jo savininkais (turto adresas, unikalus numeris, automobilio VIN, savininko duomenys, lizingo objekto (turto) pardavėjo duomenys), klientų duomenys, susiję su duomenų subjekto patikimumu ir veiklos vertinimu (finansinės operacijos, duomenys apie žalą, padarytą bankui, informacija, reikalinga pinigų plovimo ir teroristų finansavimo prevencijai, informacija apie tarptautinių sankcijų vykdymą, verslo veikla ir turto kilmės šaltinis, sandorių šalys, galutiniai naudos gavėjai), klientų finansiniai duomenys (informacija apie esamą ar buvusią darbovietę, vykdomą ūkinę komercinę veiklą, sąskaitų numeriai, turimas/turėtas turtas, sandoriai, paskolos, pajamos (įskaitant prognozuojamas pajamas ir jų stabilumą), išlaidos, įsipareigojimai, finansinė patirtis, kredito istorija ir kreditingumas, duomenys apie draudimą, sudarytos vartojimo kredito sutartys). Be to, pagal [DUOMENYS NESKELBTINI] pateiktą informaciją buvo paveikti specialių kategorijų asmens duomenys (klientų duomenys, susiję su duomenų subjekto patikimumu ir veiklos vertinimu, įskaitant informaciją apie tai, ar duomenų subjektas yra politikoje dalyvaujantis asmuo (PEP) ir darbuotojų, kuriems taikomas reikalavimas būti neteistiems, duomenys apie teistumą / neteistumą). ADSP ataskaitoje taip pat nurodoma, kad bendradarbiaujant su Tikrinamu asmeniu ir pasitelkus išorinį informacijos saugumo vadovą, [DUOMENYS NESKELBTINI] pavyko atkurti reikšmingą dalį duomenų, kurie nebuvo saugomi [DUOMENYS NESKELBTINI] infrastruktūroje – tiek pasitelkiant atsargines kopijas, tiek taikant specializuotas technines priemones jų atkūrimui. Nepaisant taikytų priemonių, skirtų sumažinti pažeidimo pasekmes ir atkurti duomenis, dalies duomenų atkurti nepavyko - [DUOMENYS NESKELBTINI] sistemoje buvo prarasti 1) terminuotų indėlių sutarčių PDF formato failai (per paskutinius 13 mėnesių sudarytų sutarčių failai, jei sutartis buvo sudaryta naudojantis [DUOMENYS NESKELBTINI] interneto banku, kiekis – apie 1 436 failų); ir 2) mokėjimų nurodymų PDF formato failai, generuoti naudojantis [DUOMENYS NESKELBTINI] interneto banku nuo jo paleidimo (maždaug nuo 2015 m.). Taip pat [DUOMENYS NESKELBTINI] sistemoje buvo prarasta apie 130 vartojimo kredito paraiškų, kurios buvo pateiktos po paskutinės prieinamos atsarginės kopijos sukūrimo datos.

2025-03-06 [DUOMENYS NESKELBTINI] pateiktame pranešime (Inspekcijos reg. Nr. 1R-1512 (2.23.E)) nurodoma, kad 2025-03-03 17:09 val. pastaroji gavo iš Tikrinamo asmens pranešimą, kad nuo 2025-03-03 15:00 val. buvo paveikta [DUOMENYS NESKELBTINI] viešosios debesijos platforma. Atliekant išsamią Incidento analizę, paaiškėjo, kad Incidento sukėlėjai užšifravo dalį saugomų atsarginių kopijų ir virtualiuose serveriuose esančių klientų sistemų. Anot [DUOMENYS NESKELBTINI], Tikrinamas asmuo paaiškino, kad atsarginės duomenų kopijos yra prarastos ir negalės būti atkurtos, o Tikrinamo asmens virtualūs resursai ir jo saugomos atsarginės duomenų kopijos yra nepasiekiamos. [DUOMENYS NESKELBTINI] pranešime nurodyta, kad buvo paveikti darbuotojų, klientų (fizinių asmenų ir juridinių asmenų atstovų), tiekėjų (fizinių asmenų ir juridinių asmenų atstovų) asmens duomenys – vardai, pavardės, darbo užmokesčio duomenys, darbo laiko apskaitos duomenys, taip pat kita informacija, esanti buhalterinės apskaitos sistemoje.

Inspekcijos direktoriaus 2025-03-25 įsakymu Nr. 1T-38 (1.12 E) Tikrinamo asmens atžvilgiu nuspręsta pradėti neplaninį tikrinimą savo iniciatyva, susijusį su galimu 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) (toliau – BDAR) nuostatų pažeidimu.

2. Tikrinamo asmens pateikta informacija

2025-04-15 Inspekcijai pateiktuose paaiškinimuose (Inspekcijos reg. Nr. 1R-2414 (2.23 Mr)), Tikrinamas asmuo nurodė, kad 2025-03-03 15:00 val. buvo paveiktos [DUOMENYS NESKELBTINI] viešosios debesijos platforma bei [DUOMENYS NESKELBTINI] atsarginių kopijų sistemos. Anot Tikrinamo asmens, atliekant išsamią Incidento analizę paaiškėjo, kad Incidento sukėlėjai užšifravo dalį saugomų atsarginių kopijų ir virtualiuose serveriuose esančių klientų sistemų. Techniniam skyriui bandant surasti sprendimus atšifruoti ir atkurti paslaugų teikimą, buvo susidurta su kenkėjiška duomenų šifravimo programa [DUOMENYS NESKELBTINI], kuri nedidelę dalį duomenų užšifravo ir jais laikinai nebuvo techninių galimybių naudotis.

Pasisakydamas dėl veiksmų, kurių buvo imtasi sprendžiant Incidentą, Tikrinamas asmuo nurodė, kad [DUOMENYS NESKELBTINI].

Tikrinamas asmuo pažymėjo, kad teikdamas paslaugas savo klientams, neturi prieigos prie virtualių serverių turinio. Klientai yra laisvi pasirinkti, kokius duomenis (asmens ar kitus) pageidauja saugoti naudojantis Tikrinamo asmens duomenų centru ir kitomis paslaugomis. Kadangi Tikrinamas asmuo neturi jokios galimybės prieiti prie virtualių serverių turinio, pastarasis negali patvirtinti, ar išvis buvo paveikti asmens duomenys. Atsižvelgiant į nurodytas aplinkybes, Tikrinamas asmuo laikosi pozicijos, kad neturėjo pagrindo pradėti tyrimo dėl ADSP, nes negalėjo žinoti, ar klientas saugojo asmens duomenis ir atitinkamai įvertinti incidento galimą poveikį būtent asmens duomenims. Tikrinamas asmuo taip pat nurodė, kad dėl techninės konfigūracijos, kuri neleidžia Tikrinamam asmeniui pasiekti klientų virtualių serverių turinio, piktavaliai, įsilaužę ir užšifravę klientų virtualius serverius, taip pat negalėjo peržiūrėti jų turinio. Anot Tikrinamo asmens, jeigu asmens duomenys buvo saugomi, Incidento metu galėjo būti paveiktas tik jų prieinamumas.

2025-05-23 Inspekcijai pateiktuose paaiškinimuose (Inspekcijos reg. Nr. 1R-3407 (2.23 Mr)), pasisakydamas dėl techninių ir organizacinių saugumo priemonių, kurios buvo įgyvendintos iki Incidento, Tikrinamas asmuo nurodė, kad šios priemonės nustatytos Tikrinamo asmens parengtoje ir patvirtintoje informacijos saugumo valdymo sistemoje (toliau – ISVS), kuri parengta remiantis ISO/IEC 27001:2017 standartu. [DUOMENYS NESKELBTINI].

Pasisakydamas dėl priemonių, kurių imtasi, kad tokio pobūdžio incidentai nepasikartotų ateityje, Tikrinamas asmuo nurodė, kad [DUOMENYS NESKELBTINI].

Tikrinamas asmuo nurodė, kad turi ISO/IEC 27001:2017 sertifikatą ir yra nusistatęs informacijos saugumo incidentų valdymo veiksmus vadybos sistemos procedūroje „Įvykių, neatitikčių ir incidentų valdymas“.

Kartu su paaiškinimais Tikrinamas asmuo Inspekcijai pateikė Incidento tyrimo ataskaitą.

3. Teisinis reglamentavimas

Pagal BDAR 4 straipsnio 1 punktą, asmens duomenys yra bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (duomenų subjektas); fizinis asmuo, kurio tapatybę galima nustatyti, yra asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti, visų pirma pagal identifikatorių, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius.

Remiantis BDAR 4 straipsnio 2 punktu, duomenų tvarkymu laikoma bet kokia automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis ar asmens duomenų rinkiniais atliekama operacija ar operacijų seka, kaip antai rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, išgava, susipažinimas, naudojimas, atskleidimas

persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimasis arba sunaikinimas.

BDAR 4 straipsnio 7 punktą nustato, kad duomenų valdytojas – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuris vienas ar drauge su kitais nustato duomenų tvarkymo tikslus ir priemones; kai tokio duomenų tvarkymo tikslai ir priemonės nustatyti Sąjungos arba valstybės narės teisės, duomenų valdytojas arba konkretūs jo skyrimo kriterijai gali būti nustatyti Sąjungos arba valstybės narės teise. Tuo metu pagal to paties straipsnio 8 punktą, duomenų tvarkytojas – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri duomenų valdytojo vardu tvarko asmens duomenis.

Atsižvelgiant į nurodytą teisinį reglamentavimą ir į tai, kad Tikrinamas asmuo teikia viešosios debesijos platformos paslaugas, sudarančias sąlygas klientams saugoti duomenis (įskaitant asmens duomenis) virtualiuose serveriuose, darytina išvada, jog tokia veikla atitinka duomenų tvarkymo sampratą, kaip ji apibrėžta BDAR 4 straipsnio 2 punkte.

Vertinant Tikrinamo asmens vaidmenį atliekant duomenų tvarkymo veiklą, atsižvelgtina į Europos duomenų apsaugos valdybos (toliau – EDAV) gaires Nr. 07/2020 dėl sąvokų „duomenų valdytojas“ ir „duomenų tvarkytojas“ pagal BDAR (toliau – EDAV gairės). EDAV gairių 76 punkte nurodoma, kad subjektas būtų laikomas duomenų tvarkytoju yra būtinos dvi sąlygos: a) jis turi būti atskiras subjektas duomenų valdytojo atžvilgiu ir b) turi tvarkyti asmens duomenis duomenų valdytojo vardu.

EDAV gairių 77 punktą numato, kad atskiras subjektas reiškia, kad duomenų valdytojas nusprendžia visą duomenų tvarkymo veiklą arba jos dalį perduoti išorės organizacijai.

EDAV gairių 79-81 punktuose nurodoma, kad tvarkant asmens duomenis duomenų valdytojo vardu, pirmiausia reikia, kad atskiras subjektas tvarkytų asmens duomenis duomenų valdytojo naudai. Antra, duomenys turi būti tvarkomi duomenų valdytojo vardu, bet ne jam tiesiogiai vadovaujant ar kontroliuojant. Veikimas „kito vardu“ reiškia tarnavimą kieno nors kito interesams ir primena teisinę sąvoką „delegavimas“. Duomenų valdytojo nurodymuose vis tiek gali būti palikta tam tikra veiksmų laisvė, kaip geriausiai tenkinti duomenų valdytojo interesus, leidžiant duomenų tvarkytojui pasirinkti tinkamiausias technines ir organizacines priemones. Veikimas „kito vardu“ taip pat reiškia, kad duomenų tvarkytojas negali tvarkyti duomenų savo paties tikslu (-ais).

Nagrinėjamu atveju iš Tikrinimo metu surinktos informacijos nustatyta, kad Tikrinamas asmuo duomenų valdytojų (teikiamų paslaugų klientų) atžvilgiu yra laikytinas atskiru subjektu. Be to, Tikrinamas asmuo tvarko asmens duomenis duomenų valdytojų vardu ir jų naudai, nes jis nusprendžia dėl duomenų tvarkymo tikslų ar duomenų turinio, o tik sudaro technines sąlygas duomenų valdytojams saugoti ir tvarkyti asmens duomenis. Tai, kad Tikrinamam asmeniui paliekama tam tikra diskrecija renkant technines ir organizacines priemones, nepaneigia jo, kaip duomenų tvarkytojo, statuso, kadangi tokia veiksmų laisvė yra suderinama su veikimu klientų naudai.

Aplinkybę, kad viešosios debesijos platformos paslaugas teikiantys subjektai įprastai laikytini duomenų tvarkytojais tiesiogiai patvirtina ir su tuo susiję EDAV įvardijami pavyzdžiai (žr. EDAV gairių 14 ir 29 puslapius).

Šiame kontekste taip pat pažymėtina, kad [DUOMENYS NESKELBTINI] kartu su 2025-03-18 paaiškinimais Inspekcijai (Inspekcijos reg. Nr. 1R-1724 (2.23 Mr)) pateikė tarp Tikrinamo asmens ir [DUOMENYS NESKELBTINI] sudarytą [DUOMENYS NESKELBTINI] asmens duomenų tvarkymo susitarimą Nr. 1 (toliau – Susitarimas). Susitarimo preambulėje nurodoma, kad Susitarimas sudaromas atsižvelgiant į tai, kad „Vykdamas Pagrindinėje sutartyje nustatytas prievolės Duomenų valdytojas perduoda Duomenų tvarkytojui tvarkyti asmens duomenis, Duomenų tvarkytojas šiuos duomenis tvarko vadovaudamasis Duomenų valdytojo instrukcijomis bei šio susitarimo ir jo priedų, nuostatomis.“ Susitarimo 1 priede „Informacija apie asmens duomenų tvarkymą“ nurodoma, kad duomenų tvarkymo tikslas yra duomenų saugojimas Tikrinamo asmens duomenų centre, o

duomenų subjektų kategorijų skiltyje nurodoma, kad bus saugomi [DUOMENYS NESKELBTINI] darbuotojų, klientų ir jų atstovų, taip pat konsultantų, partnerių asmens duomenys. Susitarimo 3 priede nurodoma, kad „Duomenų tvarkytojas tvarkys Duomenų valdytojo duomenis tik pagal atskirus Duomenų valdytojo nurodymus ir/arba užsakymus <...>.“

EDAV gairėse pabrėžiama, kad išskirtinis naujas BDAR bruožas – nuostatos, kuriomis tiesiogiai nustatomos prievolės duomenų tvarkytojams. Pavyzdžiui, duomenų tvarkytojas privalo užtikrinti, kad asmenys, įgalioti tvarkyti asmens duomenis, būtų įsipareigoję laikytis konfidencialumo (28 straipsnio 3 dalis); duomenų tvarkytojas privalo tvarkyti visų kategorijų duomenų tvarkymo veiklos įrašus (30 straipsnio 2 dalis) ir įgyvendinti tinkamas technines ir organizacines priemones (32 straipsnis). Tam tikromis sąlygomis duomenų tvarkytojas taip pat privalo paskirti duomenų apsaugos pareigūną (37 straipsnis) ir, sužinojęs apie asmens duomenų saugumo pažeidimą, privalo nepagrįstai nedelsdamas apie tai pranešti duomenų valdytojui (33 straipsnio 2 dalis). Be to, duomenų perdavimo į trečiąsias valstybes taisyklės (V skyrius) taikomos ir duomenų tvarkytojams, ir duomenų valdytojams (EDAV gairių 93 punktas).

Pagal BDAR 4 straipsnio 12 punktą, ADSP, tai saugumo pažeidimas, 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.

Atsižvelgiant į tai, kad Incidento metu buvo paveikti asmens duomenys (žr. [DUOMENYS NESKELBTINI] Inspekcijai pateiktą informaciją), Incidentas laikytinas ADSP, kaip apibrėžiama BDAR 4 straipsnio 12 punkte.

BDAR 32 straipsnio 1 dalyje reglamentuota, kad 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, inter alia, jei reikia: a) pseudonimų suteikimą asmens duomenims ir jų šifravimą; b) gebėjimą užtikrinti nuolatinį duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą; c) gebėjimą laiku atkurti sąlygas ir galimybes naudotis asmens duomenimis fizinio ar techninio incidento atveju; d) reguliarių techninių ir organizacinių priemonių, kuriomis užtikrinamas duomenų tvarkymo saugumas, tikrinimo, vertinimo ir veiksmingumo vertinimo procesą.

BDAR preambulės 83 punkte paaiškinta, kad siekiant užtikrinti saugumą ir užkirsti kelią šį reglamentą pažeidžiančiam duomenų tvarkymui, duomenų valdytojas arba duomenų tvarkytojas turėtų įvertinti su duomenų tvarkymu susijusius pavojus ir įgyvendinti jo mažinimo priemones, pavyzdžiui, šifravimą. Šiomis priemonėmis turėtų būti užtikrintas tinkamo lygio saugumas, įskaitant konfidencialumą, atsižvelgiant į techninių galimybių išsivystymo lygį ir įgyvendinimo sąnaudas pavojų ir saugotinių asmens duomenų pobūdžio atžvilgiu.

Pažymėtina, kad BDAR nenustato detalių saugumo reikalavimų, todėl vertinant duomenų valdytojo taikomas saugumo priemones asmens duomenų saugumui užtikrinti, remiamasi ne tik BDAR, bet ir Europos Sąjungos kibernetinio saugumo agentūros (ENISA) metodinėmis rekomendacijomis dėl duomenų saugumo bei atitinkamais saugumo (ISO/IEC) standartais. Be to, Inspekcija, remiantis Europos Sąjungos kibernetinio saugumo agentūros (ENISA) rekomendacijomis („Handbook on Security of Personal Data Processing“, 2018 m.) ir ISO standartais LST ISO/IEC 27001:2022 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo valdymo sistemos. Reikalavimai“ (toliau – ISO 27001:2022 standartas), LST ISO/IEC 27002:2022 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo kontrolės priemonės“ (toliau – ISO 27002:2022 standartas) bei ISO/IEC 27701:2019 „Saugumo metodai – ISO/IEC 27001 ir ISO/IEC 27002 papildymas dėl privatumo valdymo – Reikalavimai ir gairės“ yra parengusi ir Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gaires duomenų valdytojams ir duomenų tvarkytojams (toliau – VDAI gairės) .

Kaip jau minėta, 32 straipsnio 1 dalies b punkto nuostatos tiesiogiai įpareigoja duomenų tvarkytoją įgyvendinti tinkamas technines ir organizacines priemones, atsižvelgiant į duomenų tvarkymo keliamus skirtingos tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms. Pažymėtina, kad duomenų tvarkytojas objektyviai negalėtų įgyvendinti nurodytos pareigos, t. y., parinkti ir įdiegti tinkamų saugumo priemonių, nežinodamas, kokio pobūdžio duomenis apskritai ketinama saugoti. Atsižvelgiant į tai, Tikrinamas asmuo, būdamas profesionaliu viešosios debesijos platformos paslaugų teikėju ir veikdamas kaip savo srities specialistas, prieš pradėdamas teikti duomenų centro nuomos paslaugą turi pareigą įsitikinti, ar konkretus paslaugos gavėjas ketina duomenų centre saugoti asmens duomenis.

4. Inspekcijos išvados²:

[DUOMENYS NESKELBTINI]

Atsižvelgiant į nurodytas aplinkybes ir aptartą teisinį reglamentavimą, Inspekcija vertina, kad ADSP metu Tikrinamas asmuo nebuvo įgyvendinęs pakankamų organizacinių ir techninių saugumo priemonių, kurios būtų užkirtusios kelią ADSP. Atitinkamai, darytina išvada, kad tokiu būdu Tikrinamas asmuo pažeidė BDAR 32 straipsnio 1 dalies b punkto reikalavimus.

Įvertinus nustatytus Tikrinamo asmens pažeidimus, Inspekcija 2025-12-18 raštu Nr. 2R-6121 (2.14 E) (toliau – Siūlymas skirti administracinę baudą) nusprendė pradėti administracinės baudos skyrimo procedūrą.

Vadovaudamasi ADTAĮ 34 straipsnio 1 dalimi, Inspekcija Siūlymu skirti administracinę baudą Tikrinamo asmens pareikalavo pateikti: 1) Savo paaiškinimus dėl Siūlyme skirti administracinę baudą išdėstytų aplinkybių, išskyrus tai, kas jau buvo Inspekcijai pateikta atliekant tikrinimą, bei suteikti informacijos, reikšmingos skiriant administracinę baudą (BDAR 83 straipsnio 2 dalis); 2) Nuomonę dėl bylos nagrinėjimo procedūros; 3) Informaciją apie UAB „Rakrėjus“ 2024 finansinių metų bendrą metinę pasaulinę apyvartą.

5. Po siūlymo skirti baudą gauti rašytiniai paaiškinimai

Inspekcijoje 2026-01-26 gauti Tikrinamo asmens paaiškinimai dėl Siūlymo skirti baudą (Inspekcijos reg. Nr. 1R-666 (2.14 E)), kuriuose nurodoma, kad Tikrinamas asmuo nesutinka su inspekcijos išvadamis ir laiko jas nepagrįstomis. 2025-03-03 15:15 val. įvyko ADSP, kurio metu nežinomas išorės kibernetinis pažeidėjas įvykdė Tikrinamo asmens debesijos paslaugų [DUOMENYS NESKELBTINI] platformos ir atsarginių duomenų kopijų paslaugos sistemos [DUOMENYS NESKELBTINI] kibernetinę ataką, dėl kurios buvo užšifruoti duomenų valdytojų valdomi duomenys. Sužinojęs apie ADSP, Tikrinamas asmuo nedelsdamas informavo paveiktus klientus, Lietuvos policiją bei ėmėsi priemonių ADSP suvaldymui ir poveikio mažinimui. Valdant ADSP buvo vadovaujamosi Nacionalinio standartų ir technologijų instituto (angl. National Institute of Standards and Technology, toliau – NIST) Specialiame leidinyje (SP) 800-61 aprašytu incidento reagavimo ciklu. Incidento tyrimas buvo atliktas naudojantis „Microsoft“, NKSC ir NIST paremtais metodais.

Tikrinamas asmuo nurodė, kad valdant ADPS buvo imtasi šių veiksmų: [DUOMENYS NESKELBTINI].

Tikrinamas asmuo pažymėjo, kad šiai dienai iš papildomų atsarginių duomenų kopijų yra sėkmingai atstatyti visi [DUOMENYS NESKELBTINI] ir [DUOMENYS NESKELBTINI] duomenys, taip pat didžioji dalis [DUOMENYS NESKELBTINI] duomenų, t.y., beveik visi duomenys vėl tapo prieinami. Tokiu būdu galimos neigiamos ADSP pasekmės buvo praktiškai pilna apimtimi pašalintos. Kartu,

² Pagal Inspekcijos Informacinių technologijų skyriaus 2025-12-16 išvadą Nr. 4R-667 (2.14 E) „DĖL UAB „RAKRĖJUS“ ĮGYVENDINAMŲ ASMENS DUOMENŲ SAUGUMO PRIEMONIŲ TINKAMUMO (toliau – Išvada).

ADPS tyrimo eigoje buvo nustatyta, kad ADSP metu duomenys nebuvo pasisavinti ar atskleisti neautorizuotoms šalims, t.y. duomenų konfidencialumas nebuvo prarastas. Galiausiai, Tikrinamas asmuo neturi informacijos, kad paveikti duomenų subjektai ([DUOMENYS NESKELBTINI] klientai, kurių duomenų nepavyko atstatyti) būtų kreipęsi į [DUOMENYS NESKELBTINI] dėl patirtų neigiamų pasekmių. Vadinasi, realios žalos ADSP paveikti duomenų subjektai nepatyrė. Šios aplinkybės patvirtina, kad iki ADSP Tikrinamo asmens taikytos techninės priemonės sėkmingai užtikrino, kad 1) Išorinis pažeidėjas neprieitų prie asmens duomenų (buvo užtikrintas duomenų konfidencialumas ir vientisumas), bei 2) pavyktų atkurti paveiktus duomenis (buvo atkurtas duomenų prieinamumas), taip užkertant kelią neigiamų pasekmių atsiradimui duomenų subjektų atžvilgiu. Kartu pažymėtina, kad paties ADSP visiškai išvengti objektyviai nebuvo įmanoma, nes net ir taikant pažangiausias bei geriausią praktiką atitinkančias saugumo priemones absoliutus informacijos saugumas nėra įmanomas. Be to, Tikrinamo asmens teiktos paslaugos duomenų valdytojams nebuvo ir nėra licencijuojamos Lietuvoje, todėl nesant imperatyviai nustatytų techninių reikalavimų, Tikrinamas asmuo pagrįstai rėmėsi taikytina gerąja praktika bei rizika grįstu saugumo priemonių parinkimu. Tikrinamo asmens nesutikimas su Inspekcijos išvadomis grindžiamas šiais argumentais:

1) Tikrinamas asmuo veikė kaip duomenų tvarkytojas, atsakingas už virtualių resursų prieinamumą, tačiau neadministravo duomenų valdytojų valdomose virtualiose mašinose veikiančių sistemų ir jose tvarkomų asmens duomenų, neatliko šių sistemų saugumo konfigūracijos. Atsakomybė už duomenų tvarkymo tikslų, priemonių, rizikų vertinimo ir papildomų saugumo reikalavimų nustatymą pagal BDAR 32 straipsnį pirmiausia tenka duomenų valdytojams, tačiau jų veiksmai ar neveikimas iki ADSP Inspekcijos nebuvo vertinti;

2) Iki ADSP Tikrinamas asmuo taikė rizikai proporcingas technines ir organizacines priemones, turėjo galiojantį ISO 27001:2017 sertifikatą, o nepriklausomų sertifikavimo auditų metu nebuvo nustatyta kritinių neatitikčių. Kartu, nei ISO standartai, nei Inspekcijos Gairės nėra teisiškai privalomi, todėl jų netaikymas ar dalinis taikymas negali savaime būti laikomas BDAR pažeidimu;

3) [DUOMENYS NESKELBTINI] auditas nebuvo nepriklausomas trečiosios šalies auditas, o įvykęs ADSP nebuvo įtrauktas į audito imtį ir nebuvo minėto audito vertinimo objektas, tad juo remtis nėra pagrindo;

4) Inspekcijos išvados dėl to, kad ADSP neva „nebūtų įvykęs“, jeigu būtų taikytos papildomos techninės priemonės, yra retrospektyvios ir hipotetinės, nes nėra pagrįstos technine atakos kelio analize, be to nebuvo nustatytas priežastinis ryšys tarp ADSP ir konkrečių iki ADSP taikytų ar netaikytų saugumo kontrolės priemonių;

5) Informacijos, kad duomenų valdytojai veikė proaktyviai (vertino su duomenų tvarkymu susijusias rizikas ir rinko tinkamiausias saugumo priemones, vertino ir auditavo duomenų tvarkytoją, reguliariai peržiūrėjo taikomas saugumo priemones, siekiant įvertinti jų pakankamumą) iki ADSP, nėra;

6) Tikrinamo asmens prieigos apsauga buvo įgyvendinama apjungiant organizacines ir technines priemones, kurios atitiko rizika grindžiamą požiūrį ir buvo realiai taikomos iki ADSP. Jungimuisi prie Tikrinamo asmens vidinio tinklo tiek iki ADSP, tiek ir po jo buvo įdiegtas ir realiai naudojamas [DUOMENYS NESKELBTINI]. Buvo naudojami kiti patikimi autentifikavimo būdai, atsižvelgiant į konkrečios sistemos pobūdį ir riziką;

7) Nustatytais tinklų naudojimo kontrolės principais, buvo įgyvendintas loginis (funkcinis) sistemų, prieigų ir tinklų atskyrimas, paremtas naudotojų vaidmenimis ir funkcijomis. Buvo užtikrintas loginis ir resursinis virtualių mašinų atskyrimas, atitinkantis platformos veikimo principus;

8) Atsarginių informacijos kopijų darymas Tikrinamo asmens buvo sistemingai įgyvendintas, o atsarginių duomenų kopijų formavimas [DUOMENYS NESKELBTINI] aplinkoje yra standartinė ir plačiai taikoma techninė praktika, leidžianti užtikrinti operacinį atkuriamumą, ir savaime nereiškia, kad atsarginės kopijos buvo neapsaugotos ar laikomos nesaugiai.

Paaškinimuose Tikrinamas asmuo taip pat išdėstė, jo manymu, aktualias lengvinančias aplinkybes tuo atveju, jeigu Inspekcija visgi nuspręstų skirti administracinę baudą:

1) Tokios apimties ir pobūdžio ADSP Tikrinamas asmuo patyrė pirmą kartą, o išorinio pažeidėjo neteisėta prieiga buvo vienkartinė ir vyko trumpą laiką, todėl įvykęs ADSP nebuvo tęstinės veikos rezultatas. Įvykus ADSP Tikrinamas asmuo nedelsiant ėmėsi visų įmanomų priemonių galimoms neigiamoms pasekmėms pašalinti. Tikrinamas asmuo į ADSP reagavo nedelsdamas ir sistemiškai, laikydamasis tarptautiniu mastu pripažintų incidentų valdymo praktikų, o iš incidento tyrimo ir valdymo ataskaitos matyti, jog buvo taikyti struktūruoti reagavimo veiksmai, atitinkantys NIST standartus ir nacionalinių kibernetinio saugumo institucijų rekomendacijas;

2) Tikrinamas asmuo aktyviai neprisidėjo prie ADSP, nes prieiga prie Tikrinamo asmens sistemų buvo gauta neteisėtu būdu, nesant tame Tikrinamo asmens kaltės ir pačiam Tikrinamam asmeniui būnant šios neteisėtos veikos auka. Be to, įvykdyta kibernetinė ataka yra viena pavojingiausių kibernetinių atakų formų (*angl. ransomware*), kuri gali būti įvykdyta, net ir turint 100 procentinį pasiruošimą;

3) Tikrinamo asmens taikytos techninės priemonės sėkmingai užkirto kelią kilti konfidencialumo ir vientisumo pažeidimui, o taip pat padėjo beveik pilnai (iš 44 paveiktų virtualių mašinų buvo atstatytos 42) atkurti duomenis, paveiktus prieinamumo pažeidimo;

4) Tikrinamas asmuo, kaip atsakingas duomenų tvarkytojas, darė viską, ką gali, kad sumažintų ADSP galimas neigiamas pasekmes, t.y. laikantis nustatytų terminų apie incidentą pranešė visiems paveiktiems duomenų valdytojams; įdiegė papildomas technines ir organizacines priemones; apie įvykusį kibernetinį incidentą pranešė NKSC; atsakinėjo į kiekvieną duomenų valdytojų paklausimą; glaudžiai bendradarbiavo siekiant atstatyti paveiktus duomenis; noriai ir sklandžiai teikė informaciją Inspekcijai vykdant ADSP tyrimą. Tikrinamo asmens vertinimu, įdėtos pastangos viršija teisės aktų numatomą bendradarbiavimo su institucijomis minimumą;

5) [DUOMENYS NESKELBTINI] ir [DUOMENYS NESKELBTINI] iki šiol naudojami Tikrinamo asmens paslaugomis. Jeigu šios įmonės laikytų, kad Tikrinamas asmuo netinkamai teikia paslaugas, jos būtų nutraukusios sutartis ir savo duomenis perkėlusios kitiems paslaugų teikėjams. Tikrinamo asmens vertinimu, baudos skyrimas šiuo atveju nebūtų nei veiksmingas, nei proporcingas, nei atgrasomas pagal BDAR 83 straipsnio 1 dalį, o priešingai galėtų būti vertinamas kaip perteklinė ir neadekvati priemonė. ADSP kilo laikotarpiu, kai paslaugas teikė ne UAB DELSKA Lithuania, bet UAB „Rakrėjus“, t.y. juridinis asmuo, kuris po ADSP buvo prijungtas prie UAB DELSKA Lithuania ir šiuo metu nebeegzistuoja kaip atskiras subjektas. Nors UAB DELSKA Lithuania perėmė UAB „Rakrėjus“ teises ir pareigas, UAB DELSKA Lithuania nėra vien tik UAB „Rakrėjus“ teisinis tęsinys ar formalus pertvarkymas, bet veikia kaip atskiras juridinis asmuo, turintis kitokią organizacinę struktūrą, kitokią techninę ir informacijos saugumo valdymo komandą, procesus ir rizikos profilį. Pažymėtina, kad UAB DELSKA Lithuania yra ir nepriekaištingą reputaciją turinčios buvusios UAB „Duomenų logistikos centras“ tąsa, perėmusi būtent šio juridinio asmens kodą, o prijungus UAB „Rakrėjus“ prie UAB DELSKA Lithuania, UAB „Rakrėjus“ nustojo egzistuoti. Atsižvelgiant į tai, reikšmingos administracinės baudos skyrimas UAB DELSKA Lithuania už veiksmus ir aplinkybes, susijusias su subjektu, kuris faktiškai jau nebevykdo veiklos, neatitiktų veiksmingumo, proporcingumo ir atgrasomumo kriterijų, nes baudos poveikis būtų nukreiptas į kitą subjektą, o ne į tą, kurio veiklos metu kilo ADSP. Be to, didelės baudos skyrimas galėtų turėti neproporcingai neigiamą poveikį ir faktiškai sukelti rimtų sunkumų UAB DELSKA Lithuania veiklos tęstinumui ir neigiamai paveiktų būtent UAB DELSKA Lithuania, o ne UAB „Rakrėjus“ reputaciją.

Kartu su paaškinimais Tikrinamas asmuo Inspekcijai nurodė, kad ataskaitiniu laikotarpiu nuo 2024-01-01 iki 2024-12-31 UAB „Rakrėjus“ metinė apyvarta buvo 5 904 909 EUR.

Inspekcijoje 2026-02-17 gauti papildomi Tikrinamo asmens paaškinimai (Inspekcijos reg. Nr. 1R-1194 (2.14 E)), kuriuose nurodoma, kad papildomos peržiūros metu nustatyta, kad NKSC UAB „Rakrėjus“ IP adresų ruožų stebėseną vykdo bent jau nuo 2015 metų. Anot Tikrinamo asmens, tai

patvirtina nuolatinį ir sistemingą bendradarbiavimą su kompetentinga nacionaline institucija kibernetinio saugumo srityje. Tikrinamas asmuo pažymėjo, kad atlikus papildomą patikrinimą nenustatyta, jog iki Inspekcijos nagrinėjamo ADSP NKSC būtų pateikęs informaciją apie konkrečius pažeidžiamumus, kuriuos savo rašte nustatė Inspekcija. Šią informaciją Tikrinamas asmuo prašo vertinti kaip lengvinančią aplinkybę nagrinėjant bylą.

6. Žodinio bylos nagrinėjimo metu gauti paaiškinimai

Žodinio bylos nagrinėjimo metu Tikrinamas asmuo pateikė iš esmės analogiškus paaiškinimus, kurie buvo nurodyti po Siūlymo skirti baudą pateiktuose 2026-01-26 ir 2026-02-17 rašytiniuose paaiškinimuose. Papildomai paaiškino, kad [DUOMENYS NESKELBTINI] yra komercinis klientas, kuris pasirinko konkretų technologinį sprendimą ir pats atliko sistemų administravimą viešojoje debesijoje. [DUOMENYS NESKELBTINI] vertindamas rizikas savo organizacijos viduje sąmoningai pasirinko viešosios debesijos sprendimą, tam, kad saugoti duomenų subjektų duomenis. Papildomai pažymėjo, kad laikyti atsargines kopijas nekeičiamoje būsenoje (angl. *immutable storage*) reiškia papildomus kaštus, kurie paprastai tiekėjo nėra įgyvendinami, nebent to reikalauja pats valdytojas. Papildomos paslaugos, tokios kaip papildomas duomenų šifravimas, perkėlimas yra papildomi paslaugos teikėjo kaštai. Taip pat, kad [DUOMENYS NESKELBTINI] ir kiti valdytojai niekada nedavė instrukcijų elgtis kitaip negu Tikrinamas asmuo elgėsi.

Posėdžio metu Inspekcijai nurodžius, kad remiantis Tikrinamo asmens Incidento tyrimo ataskaita buvo nustatyta, kad [DUOMENYS NESKELBTINI] Tikrinamo asmens atstovai nurodė, kad kadangi tai yra techninio pobūdžio klausimas, nuodugniai šio klausimo pakomentuoti negali, tačiau išsami techninė Incidento tyrimo analizė yra pateikta Tikrinamo asmens Incidento tyrimo ataskaitoje.

7. Po Siūlymo skirti baudą iš Tikrinamo asmens gautų paaiškinimų vertinimas

7.1. Dėl duomenų valdytojų atsakomybės

Paaiškinimuose nurodoma, kad Tikrinamas asmuo teikė duomenų valdytojams viešų virtualių resursų (viešos debesijos) nuomos paslaugas, pagal kurias jiems suteikiamos virtualios mašinos. Pagal prisiimtus sutartinius įsipareigojimus, Tikrinamas asmuo atsakė už virtualių resursų prieinamumą, tačiau neadministravo virtualiose mašinose veikiančių operacinių sistemų, informacinių sistemų, jose esančios informacijos ir neatliko šių sistemų saugumo konfigūracijos, kadangi tokios paslaugos nebuvo iš anksto užsakytos minėtų duomenų valdytojų. Patys duomenų valdytojai buvo ir yra techniškai ir teisiškai atsakingi už šiose virtualiose mašinose veikiančių sistemų administravimą, atnaujinimus, saugumo parametrų nustatymus, antivirusinę apsaugą bei jose tvarkomų duomenų saugumą. Tokios priežiūros veiksmai buvo ir yra atliekami pačių duomenų valdytojų arba jų pasirinktų trečiųjų šalių. Esant tokiai paslaugų teikimo apimčiai, tik duomenų valdytojai, žinodami, kokius duomenis planuoja tvarkyti naudodamiesi Tikrinamo asmens paslaugomis, galėjo atlikti realų ir visapusišką rizikų vertinimą, ir pagal jį nuspręsti, kokios konkrečiai techninės ir organizacinės priemonės turėtų būti taikomos, siekiant užtikrinti tokių asmens duomenų saugumą, kaip to reikalauja BDAR 32 straipsnio 1 dalis.

BDAR 32 straipsnio 1 dalies b punkte įtvirtinta, kad 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.

EDAV gairių 93 punkte nurodoma, kad išskirtinis naujas BDAR bruožas – nuostatos, kuriomis tiesiogiai nustatomos prievolės duomenų tvarkytojams. Pavyzdžiui, duomenų tvarkytojas privalo užtikrinti, kad asmenys, įgalioti tvarkyti asmens duomenis, būtų įsipareigoję laikytis konfidencialumo (28 straipsnio 3 dalis); duomenų tvarkytojas privalo tvarkyti visų kategorijų duomenų tvarkymo veiklos įrašus (30 straipsnio 2 dalis) ir įgyvendinti tinkamas technines ir organizacines priemones (32 straipsnis).

Nors pagal BDAR 32 str. duomenų valdytojai taip pat turi pareigą imtis techninių ir organizacinių priemonių asmens duomenų saugumui užtikrinti, nagrinėjamu atveju pagal Tikrinimo metu surinktą medžiagą nustatyta, kad ADSP įvyko ne dėl konkrečių duomenų valdytojų veiksmų arba neveikimo, o dėl Tikrinamo asmens netinkamai įgyvendintų techninių ir organizacinių priemonių, t. y. nustatyti trūkumai buvo susiję ne su duomenų valdytojų administruojamų virtualių mašinų konfigūracija ar jose veikiančių informacinių sistemų saugumo nustatymais, bet su pačios Tikrinamo asmens teikiamos debesijos infrastruktūros saugumu. Kaip nustatyta Tikrinimo metu, [DUOMENYS NESKELBTINI]. Šios aplinkybės yra susijusios su debesijos infrastruktūros architektūra ir jos saugumo priemonėmis, kurios patenka būtent į paslaugos teikėjo – t. y. Tikrinamo asmens – atsakomybės sritį.

Papildomai pažymėtina, kad po ADSP būtent Tikrinamas asmuo, o ne duomenų valdytojai, ėmėsi organizacinių ir techninių priemonių, skirtų analogiškų incidentų pasikartojimo rizikai sumažinti. Kaip nustatyta tikrinimo metu, [DUOMENYS NESKELBTINI]. Ši aplinkybė patvirtina, kad minėtos priemonės patenka būtent į Tikrinamo asmens, kaip debesijos infrastruktūros valdytojo, kompetencijos ir kontrolės sritį. Atitinkamai, tai rodo, kad Tikrinamas asmuo turėjo realias galimybes šias priemones įgyvendinti ir iki ADSP įvykimo.

Šiame kontekste Inspekcija taip pat atkreipia dėmesį į tarp Tikrinamo asmens ir [DUOMENYS NESKELBTINI] sudaryto Susitarimo 12 punktą, kuriame nustatyta, kad „Pagal Reglamento 32 straipsnį Duomenų tvarkytojas, nepriklausomai nuo Duomenų valdytojo, taip pat įvertina duomenų tvarkymo riziką, susijusią su asmens duomenų tvarkymo veikla, kuriai atlikti Duomenų valdytojas pasitarkė Duomenų tvarkytoją, galinčią kilti fizinių asmenų teisėms ir laisvėms, ir įgyvendina priemones šiai rizikai sumažinti <...>.“ Susitarimo 3 priedo „Nurodymai, kaip tvarkyti asmens duomenis“ 2 punkte nustatyta, kad „Duomenų tvarkytojas turi teisę ir privalo priimti sprendimus dėl techninių ir organizacinių saugumo priemonių naudojimo užtikrinti reikiamą (ir suderintą) duomenų saugumo lygį“. Susitarimo 1 priede „Informacija apie asmens duomenų tvarkymą“ nurodoma, kad duomenų tvarkymo tikslas yra duomenų saugojimas Tikrinamo asmens duomenų centre, o duomenų subjektų kategorijų skiltyje nurodoma, kad bus saugomi [DUOMENYS NESKELBTINI] darbuotojų, klientų ir jų atstovų, taip pat konsultantų, partnerių asmens duomenys. Atsižvelgiant į tai, darytina išvada, kad, priešingai nei nurodoma paaiškinimuose, Tikrinamas asmuo ne tik faktiškai valdė debesijos infrastruktūros saugumo priemones, bet ir sutartiniais įsipareigojimais buvo prisiėmęs pareigą savarankiškai vertinti riziką bei įgyvendinti tinkamas technines ir organizacines priemones.

Atsižvelgiant į tai, kas išdėstyta, Tikrinamo asmens argumentai, kad pagrindinė atsakomybė už duomenų saugumo užtikrinimą nagrinėjamu atveju teko duomenų valdytojams, nepaneigia jo, kaip duomenų tvarkytojo, savarankiškų pareigų pagal BDAR, ir negali būti laikomi pagrindu atleisti jį nuo atsakomybės už jo valdomos infrastruktūros saugumo trūkumus.

7.2. Dėl ISO standartų ir VDAI gairių privalomumo

Atkreiptinas dėmesys, kad BDAR – tai Europos Sąjungos reglamentas, nustatantis taisykles, susijusias su fizinių asmenų apsauga tvarkant jų asmens duomenis.

Nors BDAR nenumato konkrečių techninių ir organizacinių priemonių, kurias privalo įgyvendinti duomenų tvarkytojas, tai nereiškia, kad Inspekcijos Informacinių technologijų skyrius rengdamas Išvadą, taip pat Inspekcija, priimdama Siūlymą skirti baudą, negali remtis visuotinai pripažintais saugumo standartais ir jų pagrindu parengtomis gerosios praktikos gairėmis. Priešingu atveju, t. y. pripažinus, jog BDAR 32 straipsnyje nesant konkrečiai įvardytų techninių ir organizacinių priemonių duomenų valdytojai ir duomenų tvarkytojai turi visišką diskreciją jų neįgyvendinti, būtų paneigtas pačios šios nuostatos veiksmingumas. Tokia interpretacija reikštų, kad duomenų tvarkytojai faktiškai negalėtų būti traukiami atsakomybėn už nepakankamų saugumo priemonių taikymą, nors būtent BDAR 32 straipsnis aiškiai įtvirtina duomenų tvarkytojo pareigą užtikrinti atitinkamo lygio duomenų saugumą, atsižvelgiant į su duomenų tvarkymu susijusią riziką. Tai reiškia, kad taikytų techninių ir organizacinių priemonių pakankamumas kiekvienu atveju yra vertinamas atsižvelgiant į konkretaus atvejo aplinkybes. Tai patvirtina ir Europos Sąjungos Teisingumo Teismo (toliau – ESTT) praktika, kur išaiškinta, kad BDAR 32 straipsnis įtvirtina duomenų tvarkytojo pareigą įgyvendinti tinkamas technines ir organizacines priemones, kuriomis būtų užtikrinamas pavojų atitinkantis asmens duomenų saugumo lygis, atsižvelgiant į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas bei konkretaus duomenų tvarkymo pobūdį, apimtį, kontekstą ir tikslus. Teismas taip pat pažymi, kad BDAR nustatyta rizika grindžiama sistema, kuria nesiekama visiškai eliminuoti asmens duomenų saugumo pažeidimų rizikos, tačiau reikalaujama, kad duomenų tvarkytojas imtųsi priemonių, kuriomis būtų siekiama kiek įmanoma išvengti tokių pažeidimų. Tokių priemonių tinkamumas turi būti vertinamas konkrečiai, atsižvelgiant į su atitinkamu duomenų tvarkymu susijusius pavojus ir į tai, ar duomenų tvarkytojas faktiškai įgyvendino priemones, atitinkančias šiuos pavojus.³

Kaip jau buvo minėta, nagrinėjamu atveju Inspekcijai įvertinus ADSP priežastis nustatyta, [DUOMENYS NESKELBTINI]. Šių trūkumų kontekste Inspekcija vertino, kad Tikrinamas asmuo nebuvo įsidiegęs pakankamų techninių ir organizacinių priemonių, kurios būtų užkirtusios kelią ADSP arba sumažinusios jo mastą, o ISO standartų ir VDAI gairių nuostatos buvo pasitelktos kaip visuotinai pripažintos gerosios praktikos rekomendacijos, padedančios nustatyti priemonių pakankumą atsižvelgiant į techninių galimybių išsivystymo lygį.

Inspekcijos vertinimu, atsižvelgiant į Tikrinamo asmens teikiamų paslaugų pobūdį, nurodytų priemonių – [DUOMENYS NESKELBTINI] – nebuvimas buvo laikomas nepakankamu techninių ir organizacinių priemonių įgyvendinimu pagal BDAR 32 straipsnio 1 dalies b punktą, o ne ISO standartų ar VDAI gairių pažeidimu.

Atitinkamai, nėra pagrindo daryti išvadą, kad nagrinėjamu atveju Inspekcija inicijavo administracinės baudos skyrimo procedūrą už ISO standartų arba VDAI gairių, kaip privalomai taikytinų teisės aktų, pažeidimus. Siūlyme skirti baudą Inspekcijai aiškiai nurodė, kad administracinės baudos skyrimo procedūra inicijuojama dėl BDAR 32 straipsnio 1 dalies b punkto pažeidimo.

7.3. Dėl [DUOMENYS NESKELBTINI] atlikto audito

Priimdama Siūlymą skirti baudą, Inspekcija, be kita ko, rėmėsi ir po ADSP [DUOMENYS NESKELBTINI] atliktoje Tikrinamo asmens informacinių ir ryšių technologijų, skaitmeninės ir operacinės atsparumo rizikos valdymo įgyvendinimo audito ataskaitoje pateikta informacija. Ataskaitoje buvo nurodyta, kad [DUOMENYS NESKELBTINI].

Paaikškinimuose Inspekcijai Tikrinamas asmuo nurodo, kad Inspekcija ataskaitos išvadomis rėmėsi nepagrįstai. Nurodo, kad minėtas auditas nebuvo nepriklausomas trečiosios šalies auditas, o buvo atliktas suinteresuotos šalies, t.y. [DUOMENYS NESKELBTINI] iniciatyva ir jo interesais jau po įvykusio ADSP. Anot Tikrinamo asmens, tokio pobūdžio auditas negali būti laikomos objektyviu,

³ ESTT 2023-12-14 sprendimas byloje Nr. C-340/21, 26-31 punktai.

neutraliu ir galutiniu pagrindu konstatuoti, kad Tikrinamas asmuo sistemingai ar iš esmės nesilaikė ISO 27001 standarto, sutartinių įsipareigojimų ar kokių nors teisės aktų reikalavimų. Tikrinamas asmuo taip pat pažymi, kad audito išvados yra grindžiamos ex post perspektyva, vertinant, kokios papildomos techninės ir organizacinės priemonės būtų tikslingos ar reikalingos siekiant užkirsti kelią analogiškiems incidentams ateityje, todėl tai savaime nereiškia, kad iki ADSP taikytos priemonės buvo nepakankamos ar neatitiko tuo metu galiojusių BDAR 32 straipsnio reikalavimų. Tikrinamas asmuo taip pat pažymi, kad ADSP nebuvo įtrauktas į audito imtį ir nebuvo minėto audito vertinimo objektas.

Pasisakydama dėl šių Tikrinamo asmens argumentų Inspekcija pažymi, kad išvados dėl Tikrinamo asmens BDAR 32 straipsnio 1 dalies b punkto pažeidimo buvo padarytos remiantis, visų pirma, Inspekcijos Išvada (Informacinių technologijų skyriaus 2025-12-16 išvada Nr. 4R-667 (2.14 E)), o ne [DUOMENYS NESKELBTINI] audite nurodyta informacija. Kaip matyti iš pačios Inspekcijos Išvados, [DUOMENYS NESKELBTINI] atliktas auditas joje apskritai nėra minimas ar analizuojamas.

Tuo tarpu Siūlyme skirti baudą kai kuri [DUOMENYS NESKELBTINI] audito ataskaitoje pateikta informacija yra paminėta tik siekiant pažymėti, kad [DUOMENYS NESKELBTINI] ir Inspekcijos išvados dėl priemonių, kurias įgyvendinus būtų buvę galima užkirsti kelią ADSP, iš dalies sutampa. Nors Tikrinamas asmuo teisingai nurodo, kad įvykęs ADSP nebuvo įtrauktas į [DUOMENYS NESKELBTINI] atlikto audito apimtį, pažymėtina, kad, kaip matyti iš šio audito ataskaitos priedo Nr. 1 „2025-03-03 įvykusio incidento aplinkybės“, [DUOMENYS NESKELBTINI] taip pat padarė išvadą, jog Incidento buvo galima išvengti arba reikšmingai sumažinti jo pasekmes, [DUOMENYS NESKELBTINI].

Atsižvelgiant į tai, kad Inspekcijos Išvada buvo priimta išanalizavus Tikrinamo asmens pateiktą informaciją ir kitus tikrinimo metu surinktus duomenis, nėra pagrindo sutikti su Tikrinamo asmens argumentais, kad Siūlymas skirti baudą buvo grindžiamas šališku ir neobjektyviu trečiosios šalies auditu. Siūlyme skirti baudą paminėtos [DUOMENYS NESKELBTINI] audito išvados yra nurodytos tik siekiant papildomai pagrįsti, kad nuo ADSP nukentėjęs duomenų valdytojas, išanalizavęs turimą informaciją, taip pat priėjo prie išvados, jog įgyvendinus tam tikras technines ir organizacines priemones ADSP būtų neįvykęs arba būtų mažesnio masto.

Inspekcija taip pat pažymi, kad vien tai, jog Inspekcijos ir [DUOMENYS NESKELBTINI] išvados dėl priemonių, kurias įgyvendinus būtų buvę galima išvengti ADSP, iš dalies sutampa, nesudaro pagrindo teigti, kad Inspekcijos Išvada ar Siūlymas skirti baudą buvo priimti remiantis ne Inspekcijos atlikto tikrinimo metu surinktos informacijos visumos vertinimu, o vien [DUOMENYS NESKELBTINI] audito išvadomis.

7.4. Dėl Tikrinamo asmens saugumo architektūros iki ADSP

Paaikškinimuose Tikrinamas asmuo nurodo, kad Inspekcijos ir [DUOMENYS NESKELBTINI] šališka pozicija, grindžiama po ADSP atliktais vertinimais ir audito ataskaitos išvadomis, iš esmės reiškia retrospektyvų saugumo lūkesčių taikymą, kai saugumo priemonių pakankamumas vertinamas jau žinant ADSP pasekmes. Toks vertinimo metodas neatitinka nei BDAR 32 straipsnio rizika grindžiamos logikos, nei šalių sutartiniuose įsipareigojimuose nustatyto šalių atsakomybės pasidalijimo. Saugumo priemonių tinkamumas turi būti vertinamas tik *ex ante*, atsižvelgiant į iki ADSP atliktus rizikos vertinimus, duomenų tvarkytojo tikrinimus, jam teiktus galiojusių nurodymus, sutartinius susitarimus ir kitą aktualų šalių faktinį elgesį. Tikrinamo asmens teigimu, Inspekcijos pateikiama išvada, jog ADSP neva nebūtų įvykęs, jeigu iki ADSP būtų buvusios taikytos tam tikros papildomos techninės priemonės [DUOMENYS NESKELBTINI], nėra pagrįsta faktine ar technine analize.

Dėl prieigų valdymo nurodo, kad prieiga prie Tikrinamo asmens debesijos informacinių sistemų buvo valdoma vadovaujantis „Informacijos saugumo politikoje“ nustatytais vidaus reikalavimais ir taisyklėmis, kurie realiai buvo taikomi praktikoje. [DUOMENYS NESKELBTINI].

Dėl tinklų atskyrimo nurodo, kad šis aspektas buvo aiškiai numatytas pagal taikomumo pareiškimą ir tai reglamentavo patvirtinta „Informacijos saugumo politika“. [DUOMENYS NESKELBTINI].

Dėl atsarginių kopijų darymo nurodo, kad šis aspektas buvo numatytas pagal taikomumo pareiškimą ir buvo įgyvendintas per IT infrastruktūros valdymą. [DUOMENYS NESKELBTINI].

Pasisakydama dėl Tikrinamo asmens argumentų Inspekcija pažymi, kad vien tai, jog taikytų organizacinių ir techninių priemonių vertinimas buvo atliktas jau po įvykusio ADSP ir žinant jo pasekmes, savaime nesudaro pagrindo vertinti Inspekcijos išvados kaip nepagrįstos teisine, technine ar faktine, prasmėmis. Iš esmės kiekvienas tyrimas dėl įvykusio asmens duomenų saugos pažeidimo yra atliekamas jau po įvykusio incidento ir siekiant nustatyti jo priežastis yra vertinama visa tokio tyrimo metu pateikta ir prieinama informacija. Nagrinėjamu atveju pagrindinis šaltinis, kuriuo pagrindu Inspekcija priėmė išvadą, buvo paties Tikrinamo asmens pateikta Incidento tyrimo ataskaita, kurioje detalai aprašyta koku būdu įvyko įsilaužimas. 2026-02-19 vykusio baudos skyrimo posėdžio metu Tikrinamo asmens atstovai taip pat pripažino, kad išsami informacija apie ADSP aplinkybes yra aprašyta Incidento tyrimo ataskaitoje. Kaip matyti iš išvados, Inspekcijos Informacinių technologijų skyrius, remdamasis Incidento tyrimo ataskaita išanalizavo ADSP aplinkybes, įskaitant prieinamą informaciją apie tai, koku būdu buvo prisijungta prie Tikrinamo asmens valdomos infrastruktūros bei remiantis tuo padarė išvadą dėl 1) priežasčių, dėl kurių įvyko ADSP ir 2) techninių ir organizacinių priemonių, kurioms esant ADSP nebūtų įvykęs.

Remiantis nurodytu, nėra pagrindo spręsti, kad Inspekcijos išvada dėl saugumo priemonių pakankamumo būtų atlikta netinkamai arba nepakankamai išsamiai. Be to, vien tai, kad toks vertinimas buvo atliktas jau po įvykusio ADSP taip pat joku būdu nesuponuoja, kad išvada yra nepagrįsta. Priešingu atveju, iš esmės kiekvienas tyrimas dėl asmens duomenų saugos pažeidimo galėtų būti laikomas nepagrįstu. Inspekcija taip pat pažymi, kad kaip jau buvo minėta šio sprendimo 7.1 dalyje, tikrinimo metu nebuvo Inspekcija nenustatė, kad ADSP būtų įvykęs dėl duomenų valdytojų veiksmų ar neveikimo. Incidento tyrimo ataskaitoje, kurią Tikrinamas asmuo taip pat pripažįsta pagrindiniu ADSP aplinkybių šaltiniu, taip pat nėra jokios informacijos apie tai, kad asmens duomenys buvo paveikti dėl pačių duomenų valdytojų veiksmų ar neveikimo.

Pasisakydama dėl Tikrinamo asmens argumentų, susijusių su prieigų valdymu, Inspekcija neturi pagrindo sutikti su tuo, kad ADSP metu buvo taikytas [DUOMENYS NESKELBTINI]. Nors ši priemonė iš tiesų yra aprašyta Tikrinamo asmens informacijos saugumo politikoje, nurodant jog, [DUOMENYS NESKELBTINI] iš tikrinimo metu surinktos informacijos Inspekcija negali daryti išvados, kad ADSP metu ši priemonė faktiškai veikė. 2026-02-19 vykusio baudos skyrimo posėdžio metu Inspekcijai paklausus Tikrinamo asmens atstovų, koku būdu Incidento tyrimo ataskaitoje aprašytomis aplinkybėmis trečiasis asmuo galėjo įgyti prieigą prie Tikrinamo asmens valdomos infrastruktūros, jeigu buvo taikytos Tikrinamo asmens paaiškinimuose nurodytos priemonės ([DUOMENYS NESKELBTINI]), Tikrinamo asmens atstovai nurodė, kad visa informacija apie ADSP aplinkybes yra nurodyta Incidento tyrimo ataskaitoje. Visgi, kaip matyti iš šios ataskaitos, prisijungimui prie Tikrinamo asmens vidinio tinklo, trečiasis asmuo neturėjo naudoti [DUOMENYS NESKELBTINI]. Taip pat, net jeigu tokia priemonė ir buvo taikyta, Incidento tyrimo ataskaitoje nėra jokios informacijos apie tai, koku būdu trečiasis asmuo šią priemonę sugebėjo apeiti. Aplinkybę, kad ADSP metu nebuvo taikomas [DUOMENYS NESKELBTINI] taip pat patvirtina ir 2025-05-23 Inspekcijai pateiktuose paaiškinimuose (Inspekcijos reg. Nr. 1R-3407 (2.23 Mr)) esanti informacija, kuriuose Tikrinamas asmuo, pasisakydamas dėl priemonių kurių imtasi, kad tokio pobūdžio incidentai nepasikartotų ateityje, nurodė, kad infrastruktūroje buvo įdiegtas informacinių sistemų valdymas naudojantis [DUOMENYS NESKELBTINI]. Remiantis nurodytu, Inspekcija neturi pagrindo sutikti su tuo, kad ši priemonė ADSP metu buvo faktiškai taikyta.

Nors Tikrinamas asmuo nurodo, kad buvo taikomos ir kitos prieigos kontrolės priemonės [DUOMENYS NESKELBTINI], Inspekcijos vertinimu, šios priemonės nagrinėjamu atveju negali būti

vertinamos kaip pakankamos. Kaip matyti iš Incidento tyrimo ataskaitos, [DUOMENYS NESKELBTINI], tačiau netaikant papildomų saugumo priemonių [DUOMENYS NESKELBTINI], trečiasis asmuo, [DUOMENYS NESKELBTINI], įgijo prieigą prie Tikrinamo asmens infrastruktūros, įskaitant atsarginių kopijų ir funkcinę aplinką, bei galėjo pasiekti skirtingų duomenų valdytojų duomenis. Atsižvelgiant į tai, vien aplinkybė, kad buvo taikomos tam tikros bazinės saugumo priemonės, nesudaro pagrindo laikyti jas pakankamomis BDAR 32 straipsnio 1 dalies b punkto prasme, jeigu jos nebuvo derinamos su papildomomis priemonėmis, reikalingomis atsižvelgiant į nustatytą riziką.

Pasisakant dėl Tikrinamo asmens argumentų, susijusių su tinklų ir sistemų atskyrimu, pažymėtina, kad Inspekcijos išvados dėl saugumo spragų buvo padarytos įvertinus faktines ADSP aplinkybes, iš kurių matyti, jog trečiajam asmeniui, pasinaudojus [DUOMENYS NESKELBTINI] ir įgijus prieigą prie Tikrinamo asmens valdomos infrastruktūros, atsirado galimybė netrukdomai pasiekti ir kitus infrastruktūros komponentus, įskaitant 45 virtualiąsias mašinas, kuriose buvo saugomi paveikti duomenys. Ši aplinkybė rodo, kad, priešingai nei nurodo Tikrinamas asmuo, taikytos tinklų ir sistemų atskyrimo priemonės nebuvo pakankamos [DUOMENYS NESKELBTINI], kadangi jos neužkirto kelio prieigos plitimui tarp skirtingų infrastruktūros dalių.

Nors Tikrinamas asmuo pagrįstai pažymi, kad įprastomis sąlygomis skirtingų duomenų valdytojų virtualiosios mašinos buvo logiškai atskirtos ir klientai neturėjo prieigos prie vieni kitų duomenų, ši aplinkybė savaime nepatvirtina tinkamo infrastruktūros tinkle atskyrimo. Tinkamas sistemų atskyrimas turi užtikrinti ne tik klientų IT infrastruktūros izoliaciją įprastomis naudojimo sąlygomis, bet ir riboti galimą prieigos plitimą bei privilegijuotos prieigos išnaudojimą tuo atveju, kai yra paveikiama viena iš infrastruktūros dalių. Nagrinėjamu atveju nustatyta, kad [DUOMENYS NESKELBTINI]. Atsižvelgiant į tai, Inspekcija neturi pagrindo sutikti su Tikrinamo asmens argumentais, kad taikytos tinklų atskyrimo priemonės buvo pakankamos BDAR 32 straipsnio 1 dalies b punkto prasme.

Pasisakydama dėl Tikrinamo asmens argumentų, susijusių su atsarginių duomenų kopijų darymu, Inspekcija pažymi, kad nors atsarginių kopijų darymas iš tiesų yra standartinė ir būtina techninė praktika, užtikrinanti duomenų prieinamumą ir veiklos tęstinumą, ši aplinkybė savaime nepaneigia pareigos užtikrinti tinkamą šių sistemų saugumą. Antai, BDAR 32 straipsnis įpareigoja užtikrinti ne tik duomenų atkuriamumą, bet ir jų apsaugą nuo neteisėtos prieigos. Taigi, nors sutiktina su Tikrinamo asmens argumentais, jog [DUOMENYS NESKELBTINI] infrastruktūroje galėtų būti kuriamos [DUOMENYS NESKELBTINI] aplinkoje saugomų duomenų atsarginės kopijos, tarp šių sistemų turi egzistuoti techninė sąsaja, tokia sąsaja turi būti sukonfigūruota taip, kad nesudarytų galimybių neautorizuotai prieigai plisti tarp skirtingų bendros infrastruktūros dalių.

Be to, kaip matyti iš Incidento tyrimo ataskaitos, viena iš priemonių, kurių Tikrinamas asmuo ėmėsi siekdamas išvengti analogiškų incidentų ateityje, buvo [DUOMENYS NESKELBTINI]. Tai patvirtina, kad toks atskyrimas yra techniškai įmanomas ir suderinamas su Tikrinamo asmens teikiamomis viešosios debesijos paslaugomis. Atsižvelgiant į tai, nėra pagrindo sutikti su Tikrinamo asmens argumentais, kad Inspekcijos išvada dėl nepakankamo šių sistemų atskyrimo yra nepagrįsta.

Taigi, nors Tikrinamas asmuo paaiškinimuose nurodo, kad praktikoje buvo taikoma daugelis organizacinių ir techninių priemonių siekiant užtikrinti valdomos infrastruktūros saugumą, Inspekcijos vertinimu, šios priemonės, atsižvelgiant į duomenų tvarkymo pobūdį, apimtį ir su juo susijusią riziką, nebuvo pakankamos BDAR 32 straipsnio 1 dalies b punkto prasme. Nors BDAR 32 straipsnis nėra skirtas absoliučiai eliminuoti asmens duomenų saugumo pažeidimų riziką, tačiau jis įpareigoja įgyvendinti tokias technines ir organizacines priemones, kurios būtų tinkamos konkrečiomis aplinkybėmis ir užtikrintų adekvatų apsaugos lygį. Incidentas kilo pasinaudojus tipinėmis ir plačiai žinomomis pažeidžiamumo prielaidomis – [DUOMENYS NESKELBTINI] – kurios, atsižvelgiant į viešosios debesijos paslaugų teikimo pobūdį, turėjo būti vertinamos kaip reikšminga ir reali rizika nustatant taikytinas organizacines ir technines priemones. Šiame kontekste taip pat atkreiptinas dėmesys, kad Inspekcijos Išvadoje nurodomos techninės ir organizacinės priemonės

[DUOMENYS NESKELBTINI], kurioms esant ADSP būtų neįvykęs arba būtų mažesnio masto, nelaikytinos išskirtinėmis ar nejprastomis. Inspekcijos vertinimu, atsižvelgiant į tai, kas nurodyta, aplinkybė, kad trečiajam asmeniui pakako [DUOMENYS NESKELBTINI], kad būtų galima pasiekti skirtingas infrastruktūros dalis bei jose saugomus duomenis, rodo, jog įdiegtos techninės ir organizacinės priemonės nebuvo pakankamos.

7.5. Dėl Tikrinamo asmens bendradarbiavimo su NKSC

Papildomuose paaiškinimuose Inspekcijai Tikrinamas asmuo nurodo, kad papildomos peržiūros metu nustatyta, kad NKSC UAB „Rakrėjus“ IP adresų ruožų stebėseną vykdo bent jau nuo 2015 metų. Anot Tikrinamo asmens, tai patvirtina nuolatinį ir sistemingą bendradarbiavimą su kompetentinga nacionaline institucija kibernetinio saugumo srityje. Tikrinamas asmuo pažymėjo, kad atlikus papildomą patikrinimą nenustatyta, jog iki Inspekcijos nagrinėjamo ADSP NKSC būtų pateikęs informaciją apie konkrečius pažeidžiamumus, kuriuos savo rašte nustatė Inspekcija.

Inspekcijos vertinimu, aplinkybė, jog NSKC vykdė Tikrinamo asmens IP adresų stebėseną ar kad tarp šalių egzistavo tam tikras bendradarbiavimas kibernetinio saugumo srityje, nepakeičia Tikrinamo asmens, kaip duomenų tvarkytojo, pareigos užtikrinti tinkamą techninių ir organizacinių priemonių įgyvendinimą, o tai, kad iki nagrinėjamo ADSP NKSC nepateikė informacijos apie konkrečius pažeidžiamumus, nereiškia, jog tokių pažeidžiamumų nebuvo. Pažymėtina, kad atsakomybė už asmens duomenų saugumo užtikrinimą negali būti perkeliama nacionalinei kibernetinio saugumo institucijai, kurios funkcijos yra susijusios su bendro pobūdžio kibernetinių grėsmių stebėseną ir informacijos teikimu, tačiau neapima individualaus kiekvieno ūkio subjekto informacinių sistemų saugumo užtikrinimo. Atsižvelgiant į tai, nėra pagrindo sutikti su Tikrinamo asmens argumentais, kad bendradarbiavimas su ar konkrečių įspėjimų nebuvimas iš šios institucijos pusės galėtų būti laikomas aplinkybe, mažinančia ar apskritai pašalinančia Tikrinamo asmens atsakomybę pagal BDAR.

8. Sprendimo skirti / neskirti administracinę baudą motyvai

Pagal BDAR 83 straipsnio 1 dalį, priežiūros institucija užtikrina, kad pagal šį BDAR straipsnį skiriamos administracinės baudos už 4, 5 ir 6 dalyse nurodytus šio reglamento pažeidimus kiekvienu konkrečiu atveju būtų veiksmingos, proporcingos ir atgrasomos. Pagal BDAR 83 straipsnio 2 dalį, administracinės baudos, atsižvelgiant į kiekvieno konkretaus atvejo aplinkybes, skiriamos kartu su BDAR 58 straipsnio 2 dalies a–h punktuose ir j punkte nurodytomis priemonėmis arba vietoje jų.

Sprendžiant dėl to, ar skirti administracinę baudą, ir sprendžiant dėl administracinės baudos dydžio kiekvienu konkrečiu atveju deramai atsižvelgiama į šiuos dalykus: a) pažeidimo pobūdį, sunkumą ir trukmę, atsižvelgiant į atitinkamo duomenų tvarkymo pobūdį, aprėptį ar tikslą, taip pat į nukentėjusių duomenų subjektų skaičių ir jų patirtos žalos dydį; b) tai, ar pažeidimas padarytas tyčia, ar dėl aplaidumo; c) bet kuriuos veiksmus, kurių duomenų valdytojas arba duomenų tvarkytojas ėmėsi, kad sumažintų duomenų subjektų patirtą žalą; d) duomenų valdytojo arba duomenų tvarkytojo atsakomybės dydį, atsižvelgiant į jų pagal 25 ir 32 straipsnius įgyvendintas technines ir organizacines priemones; e) bet kuriuos to duomenų valdytojo arba duomenų tvarkytojo svarbius ankstesnius pažeidimus; f) bendradarbiavimo su priežiūros institucija siekiant atitaisyti pažeidimą ir sumažinti galimą neigiamą jo poveikį laipsnį; g) asmens duomenų, kuriems pažeidimas turi poveikį, kategorijas; h) tai, koku būdu priežiūros institucija sužinojo apie pažeidimą, visų pirma tai, ar duomenų valdytojas arba duomenų tvarkytojas pranešė apie pažeidimą (jei taip – koku mastu); i) jei atitinkamam duomenų valdytojui arba duomenų tvarkytojui dėl to paties dalyko anksčiau buvo taikytos 58 straipsnio 2 dalyje nurodytos priemonės – ar laikytasi tų priemonių; j) ar laikomasi patvirtintų elgesio kodeksų pagal 40 straipsnį arba patvirtintų sertifikavimo mechanizmų pagal 42

straipsnį; k) kitus sunkinančius ar švelninančius veiksnius, susijusius su konkretaus atvejo aplinkybėmis, pavyzdžiui, finansinę naudą, kuri buvo gauta, arba nuostolius, kurių buvo išvengta, tiesiogiai ar netiesiogiai dėl pažeidimo.

Pagal BDAR preambulės 129 punktą, priežiūros institucijos skiriama poveikio priemonė turėtų būti tinkama, būtina ir proporcinga, siekiant užtikrinti BDAR laikymąsi, atsižvelgiant į kiekvieno konkreto atvejo aplinkybes, ja turėtų būti gerbiama kiekvieno asmens teisė būti išklausytam prieš imantis konkrečios priemonės, kuri jam padarytų neigiamą poveikį, ir taikoma taip, kad atitinkami asmenys nepatirtų bereikalingų išlaidų ir pernelyg didelių nepatogumų.

BDAR preambulės 129 punkte taip pat nustatyta, kad siekiant užtikrinti nuoseklią šio reglamento taikymo stebėseną ir jo vykdymą visoje Europos Sąjungoje, priežiūros institucijos kiekvienoje valstybėje narėje turėtų vykdyti tas pačias užduotis ir naudotis tais pačiais veiksmingais įgaliojimais, įskaitant tyrimo įgaliojimus, įgaliojimus imtis taisyklių veiksmų ir skirti sankcijas, taip pat leidimų išdavimo ir patariamuosius įgaliojimus, visų pirma tais atvejais, kai gaunami skundai iš fizinių asmenų, ir, nedarant poveikio baudžiamojo persekiojimo institucijų įgaliojimams pagal valstybės narės teisę, atkreipti teisminių institucijų dėmesį į šio reglamento pažeidimus ir (arba) būti teismo proceso šalimi. Priežiūros institucijų įgaliojimais turėtų būti naudojamosi laikantis atitinkamų procedūrinių apsaugos priemonių, nustatytų Sąjungos ir valstybės narės teisėje, nešališkai, sąžiningai ir per pagrįstą laikotarpį. Visų pirma kiekviena priemonė turėtų būti tinkama, būtina ir proporcinga siekiant užtikrinti šio reglamento laikymąsi, atsižvelgiant į kiekvieno konkreto atvejo aplinkybes, ja turėtų būti gerbiama kiekvieno asmens teisė būti išklausytam prieš imantis konkrečios priemonės, kuri jam padarytų neigiamą poveikį, ir taikoma taip, kad atitinkami asmenys nepatirtų bereikalingų išlaidų ir pernelyg didelių nepatogumų.

Europos duomenų apsaugos valdyba (toliau – EDAV), siekdama užtikrinti nuoseklų požiūrį į administracinių baudų skyrimą, priėmė Gairės dėl administracinių baudų apskaičiavimo⁴, kuriose pažymima, kad skiriamos administracinės baudos turėtų atitikti pažeidimo pobūdį, sunkumą ir padarinius. Minėtose gairėse nurodoma, kad kiekvienas atvejis turi būti vertinamas individualiai, o BDAR 83 straipsnio 2 dalis yra tokio individualaus vertinimo pradžios taškas. Šiose gairėse pateikiamas BDAR 83 straipsnio 2 dalyje nustatytų vertinimo kriterijų aiškinimas, kuriuo remiamasi žemiau šiame sprendime. Be to, minėtose gairėse nustatyta baudų apskaičiavimo metodika ir pažymima, kad skiriant baudas, turi būti atsižvelgiama į šiuos tris elementus: pažeidimų kvalifikavimą pagal pobūdį, pažeidimo sunkumą ir įmonės apyvartą, taip pat nurodoma, kad duomenų apsaugos institucijos turi atsižvelgti ir į sunkinančias arba lengvinančias aplinkybes, dėl kurių bauda gali padidėti arba sumažėti ir kurių nuoseklų išaiškinimą teikia EDAV.

Vertinant patikrinimo metu surinktą ir šiame sprendime pateikiamą informaciją, sprendžiant skirti ar neskirti Tikrinamam asmeniui administracinę baudą bei sprendžiant dėl administracinės baudos dydžio, Inspekcija atsižvelgia į šiuos žemiau BDAR 83 straipsnio 2 dalyje pateikiamus aspektus.

i) BDAR 83 straipsnio 2 dalies a punktas – pažeidimo pobūdis, sunkumas ir trukmė

Tikrinamo asmens atžvilgiu nustatytas BDAR 32 straipsnio 1 dalies b punkto pažeidimas atitinka BDAR 83 straipsnio 4 dalies a punkto nuostatas (BDAR 83 straipsnio 4 dalies pažeidimai priskiriami lengvesnių pažeidimų kategorijai).

Gairėse dėl administracinių baudų apskaičiavimo nurodoma, kad atliekant šio kriterijaus vertinimą reikėtų atsižvelgti į toliau aprašytus konkrečius veiksnius: 1) pažeidimo pobūdį; 2) pažeidimo sunkumą; 3) pažeidimo trukmę. Šiose gairėse EDAV taip pat pažymi, kad priežiūros institucija gali nustatyti pirmiau minėtų veiksnių svarbą priklausomai nuo konkreto atvejo aplinkybių.

⁴ Europos duomenų apsaugos valdybos 2023-05-24 Gairės Nr. 04/2022 dėl administracinių baudų apskaičiavimo pagal BDAR (toliau – Gairės dėl administracinių baudų apskaičiavimo)

29 straipsnio darbo grupės gairėse dėl pranešimo apie ADSP⁵ nurodyta, jog pažeidimas gali turėti poveikio tik vienam ar keliems asmenims arba net keliems tūkstančiams ar dar daugiau asmenų. Paprastai galioja taisyklė, kad kuo daugiau yra asmenų, kuriems pažeidimas turi poveikio, tuo didesnį poveikį tas pažeidimas gali padaryti.

Gairėse dėl pranešimo apie ADSP yra nurodyta, kad galimo pavojaus dydis priklauso ir nuo to, ar duomenų valdytojas žino, jog asmens duomenys yra žmonių, kurių ketinimai yra nežinomi arba galbūt piktavališki, rankose. Pavyzdžiui, jei asmens duomenys atsitiktinai atskleidžiami trečiajai šaliai, kurią duomenų valdytojas laiko patikima (pvz., su ja nuolat bendradarbiauja, yra susipažinęs su šios šalies procedūromis, kita svarbia informacija), galima pagrįstai tikėtis, kad toji šalis nežiūrės per klaidą nusiųstų duomenų ar nepasinaudos prieiga prie jų ir laikysis duomenų valdytojo nurodymų dėl tų duomenų grąžinimo. Net jei bus pasinaudota prieiga prie duomenų, duomenų valdytojas vis vien galės tikėtis, kad duomenų gavėjas nesiims jokių papildomų veiksmų ir skubiai grąžins duomenis duomenų valdytojui, taip pat bendradarbiaus juos susigrąžinant. Tokiais atvejais į tai gali būti atsižvelgta per pavojų vertinimą. Gairėse dėl pranešimo apie ADSP taip pat pažymima, kad reikėtų atsižvelgti į pasekmių asmenims ilgalaikiškumą: jei pažeidimo pasekmės yra ilgalaikės, tai ir jo poveikis veikiausiai bus didesnis.

BDAR preambulės 75 punkte paaiškinta, kad įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms gali kilti ir dėl tokio duomenų tvarkymo, kai duomenų subjektai gali netekti galimybės naudotis savo teisėmis ir laisvėmis ir jiems užkertamas kelias kontroliuoti savo asmens duomenis.

Vertindama pažeidimo pobūdį Inspekcija pažymi, kad BDAR 32 straipsnio nuostatomis siekiama užtikrinti asmens duomenų saugumą ir apsaugą nuo neteisėtos prieigos, praradimo ar sunaikinimo. Atsižvelgiant į tai, kad pagrindinis BDAR tikslas yra užtikrinti vienodo ir aukšto lygio fizinių asmenų apsaugą visoje Europos Sąjungoje, asmens duomenų saugos pažeidimai, kurių metu dėl neteisėtos prieigos paveikiamas didelis skaičius duomenų subjektų, yra laikytini reikšmingo pobūdžio BDAR pažeidimais.

Vertindama pažeidimo sunkumą Inspekcija nagrinėjamu atveju reikšmingais veiksniais laiko paveiktų duomenų subjektų skaičių ir jų patirtą žalą.

Inspekcija nustatė, kad pažeidimai yra susiję su dideliu skaičiumi duomenų subjektų (mažiausiai 2 689 duomenų subjektų⁶) asmens duomenimis ir didelės apimties jų duomenimis. Taigi, dėl įvykusio ADSP buvo pažeistas didelio skaičiaus duomenų subjektų asmens duomenų saugumas. Be to, pagal [DUOMENYS NESKELBTINI] Inspekcijai pateiktą 2025-04-22 asmens duomenų saugumo pažeidimo ataskaitą Nr. [DUOMENYS NESKELBTINI], atšifravimo metu nepavyko atkurti: 1) terminuotų indėlių sutarčių PDF formato failų (apie 1 436 failai); 2) mokėjimų nurodymų PDF formato failų.

Pagal [DUOMENYS NESKELBTINI] pateiktą informaciją, laikotarpiu nuo 2025-03-03 iki 2025-03-05 buvo sutrikusi šio duomenų valdytojo teikiamos (kaip licencijuoto banko) paslaugos, dėl ko duomenų subjektai negalėjo laikinai naudotis teikiamomis finansinėmis paslaugomis.

Pagal [DUOMENYS NESKELBTINI] ir [DUOMENYS NESKELBTINI] pateiktą informaciją dėl asmens duomenų prieinamumo pažeidimo šie duomenų valdytojai taip pat laikinai negalėjo teikti paslaugų.

Pasisakydama dėl trukmės Inspekcija pažymi, kad nagrinėjamu atveju nėra pagrindo šį veiksnį laikyti reikšmingu. Nustatytas pažeidimas yra susijęs su nepakankamų techninių ir organizacinių priemonių įgyvendinimu, t. y. su Inspekcijos nustatytomis saugumo spragomis Tikrinamo asmens valdomoje infrastruktūroje. Kadangi šios spragos materializavosi trečiajam asmeniui konkrečiu momentu neteisėtai įgijus prieigą prie Tikrinamo asmens IT infrastruktūros, nėra poreikio vertinti pažeidimo trukmės kaip reikšmingo veiksnio.

⁵ 29 straipsnio darbo grupės 2017-02-06 Gairės dėl pranešimo apie asmens duomenų saugumo pažeidimą pagal Reglamentą (ES) 2016/679 (toliau – Gairės dėl pranešimo apie ADSP)

⁶ Pagal [DUOMENYS NESKELBTINI] Inspekcijai pateiktą informaciją.

Atsižvelgdama į tai, kad 1) buvo paveiktas didelis duomenų subjektų skaičius ir jų duomenų kiekis bei sutrikdytas paslaugų teikimas, įskaitant finansinių (banko) paslaugų⁷, kurių prieinamumas yra reikšminga sąlyga duomenų subjektams disponuoti savo lėšomis, vykdyti mokėjimus ir naudotis kitomis finansinėmis paslaugomis, 2) dalis duomenų buvo negrįžtamai prarasta, Inspekcijos vertinimu nagrinėjamas pažeidimas kvalifikuotinas kaip vidutinio sunkumo.

Inspekcija taip pat neturi pagrindo sutikti su Tikrinamo asmens argumentais, jog nagrinėjamu atveju nebuvo pažeistas duomenų konfidencialumas. Pažymėtina, kad duomenų konfidencialumas yra pažeidžiamas ne tik tada kai duomenys yra neteisėtai pasisavinami ar eksfiltruojami, tačiau ir tada kai prie jų apskritai įgaunama neleistina prieiga. EDAV 2021-12-14 gairėse Nr. 01/2021 dėl pranešimo apie asmens duomenų saugumo pažeidimą pavyzdžių, yra pateikiamas pavyzdys (žr. 2.1 atvejį), kai išpirkos reikalavimo programinės įrangos atakos metu duomenys buvo užšifruoti, tačiau neeksfiltruoti, o įsilaužėlis įgijo prieigą tik prie užšifruotų duomenų. Nepaisant to, EDAV tokį incidentą vertina kaip apimantį ne tik duomenų prieinamumo sutrikimą, bet ir neleistiną prieigą prie asmens duomenų.

ii) BDAR 83 straipsnio 2 dalies b punktas – tai, ar pažeidimas padarytas tyčia, ar dėl aplaidumo

Gairėse dėl administracinių baudų apskaičiavimo nurodoma, kad kalbant apie pažeidimo požymius, „tyčia“ apima ir žinojimą, ir sąmoningą darymą, o „netyčia“ reiškia, kad nebuvo ketinimo padaryti pažeidimą, nors duomenų valdytojas ir (arba) duomenų tvarkytojas pažeidė teisės aktuose nustatytą rūpestingumo pareigą. Minėtose gairėse nurodoma, jog tyčinis ar aplaidumo nulemtas pažeidimo pobūdis (BDAR 83 straipsnio 2 dalies b punktas) turėtų būti vertinamas atsižvelgiant į objektyvius elgesio elementus, nustatytus vertinant faktines atvejo aplinkybes. Atsižvelgdama į atvejo aplinkybes, priežiūros institucija taip pat gali suteikti svarbos aplaidumo laipsniui. Geriausiu atveju aplaidumas galėtų būti laikomas neutraliu.

Inspekcija, vertindama patikrinimo metu nustatytas aplinkybes, konstatuoja, kad Tikrinamo asmens veiksmuose tyčios nebuvo. Inspekcijos vertinimu, Tikrinamas asmuo tinkamai neįgyvendindamas aukščiau šiame sprendime įvardintų techninių organizacinių saugumo priemonių pažeidė teisės aktuose nustatytą rūpestingumo pareigą.

Atsižvelgiant į tai, kas nurodyta, Inspekcija Tikrinamo asmens veiksmus pagal BDAR 83 straipsnio 2 dalies b punktą laiko neutraliu veiksmu.

iii) BDAR 83 straipsnio 2 dalies c punktas – veiksmai, kurių buvo imtasi, kad būtų sumažinta duomenų subjektų patiriama žala

Gairėse dėl administracinių baudų apskaičiavimo nurodoma, jog tinkamos priemonės, skirtos duomenų subjektų patirtai žalai sumažinti, turi būti įvertintos visų pirma atsižvelgiant į savalaikiškumo elementą, t. y. laiką, kada duomenų valdytojas arba duomenų tvarkytojas jas įgyvendina, ir jų veiksmingumą. EDAV pabrėžia, jog labiau tikėtina, kad lengvinančia aplinkybe bus laikomos tos priemonės, kurios buvo įgyvendintos spontaniškai prieš priežiūros institucijai pradedant tyrimą ir duomenų valdytojui arba duomenų tvarkytojui apie jį sužinant, nei tos, kurios buvo įgyvendintos po to momento.

Tikrinamas asmuo įvykus ADSP ėmėsi šių veiksmų [DUOMENYS NESKELBTINI].

Inspekcija pažymi, kad nurodytų priemonių Tikrinamas asmuo ėmėsi nedelsiant po ADSP ir nežinodamas apie tai, kad bus pradėtas Inspekcijos tikrinimas (tikrinimas pradėtas 2025-03-25). Atsižvelgiant į tai, Inspekcija šį veiksnį vertina kaip švelninančią aplinkybę.

⁷ Pažymėtina, jog tokių paslaugų prieinamumas yra kritiškai svarbus duomenų subjektams, nes jų sutrikdymas gali apriboti galimybę disponuoti lėšomis, vykdyti atsiskaitymus ar vykdyti kitus finansinius įsipareigojimus. Todėl net ir laikinas tokių paslaugų neprieinamumas laikytinas reikšmingu poveikiu duomenų subjektų teisėms ir laisvėms.

iv) BDAR 83 straipsnio 2 dalies d punktas – atsakomybės dydis, atsižvelgiant į duomenų tvarkytojo pagal 25 ir 32 straipsnius įgyvendintas technines ir organizacines priemones

BDAR 25 ir 32 straipsniai reglamentuoja duomenų tvarkytojo pareigą įgyvendinti tinkamas technines ir organizacines priemones, kad būtų užtikrintas pavojų atitinkančio lygio saugumas, tvarkant asmens duomenis. Gairėse dėl administracinių baudų apskaičiavimo pažymima, kad atsižvelgiant į padidėjusį atskaitomybės lygį pagal BDAR, tikėtina, kad duomenų valdytojo arba duomenų tvarkytojo atsakomybės laipsnis bus laikomas sunkinančiu arba neutraliu veiksmu ir tik išskirtinėmis aplinkybėmis, kai duomenų valdytojas arba duomenų tvarkytojas viršys jiems nustatytas pareigas pagal BDAR 25 ir 32 straipsnius, tai bus laikoma atsakomybę lengvinančia aplinkybe.

Inspekcija ADSP tyrimo metu nustatė, kad Tikrinamas asmuo neįgyvendino atitinkamų techninių ir organizacinių priemonių, kurių trūkumas sąlygojo ADSP, tačiau, atsižvelgiant į tai, jog nustatyti pažeidimai yra susiję su techninių ir organizacinių priemonių netinkamu įgyvendinimu / neįgyvendinimu, šie Tikrinamo asmens veiksmai / neveikimas kaip jo atsakomybę švelninantis ar sunkinantis veiksnys nevertinami.

v) BDAR 83 straipsnio 2 dalies e punktas – Tikrinamo asmens ankstesni pažeidimai

Šis kriterijus skirtas pažeidimą padariusio subjekto reputacijai įvertinti. Gairėse dėl administracinių baudų apskaičiavimo nurodoma, kad ankstesnių pažeidimų buvimas apskaičiuojant baudą gali būti laikomas sunkinančia aplinkybe. Šio veiksnio svarba turi būti nustatoma atsižvelgiant į ankstesnių pažeidimų pobūdį ir dažnumą. Minėtose gairėse taip pat pažymima, kad ankstesnių pažeidimų buvimas gali būti laikomas sunkinančiu veiksmu, apskaičiuojant administracinę baudą. Atsižvelgiama į ankstesnių pažeidimų pobūdį ir dažnumą. Tačiau pabrėžiama, kad ankstesnių pažeidimų nebuvimas negalėtų būti laikomas švelninančiu veiksmu, nes atitikimas BDAR yra norma ir ta aplinkybė, kad nėra ankstesnių pažeidimų, galėtų būti vertinama kaip neutrali.

Inspekcija neturi informacijos, kad Tikrinamas asmuo anksčiau būtų pažeidęs BDAR nuostatas, todėl BDAR 83 straipsnio 2 dalies e punkte nustatytą veiksnį laiko neutraliu.

vi) BDAR 83 straipsnio 2 dalies f punktas – bendradarbiavimas su Inspekcija, siekiant atitaisyti pažeidimą ir sumažinti galimą neigiamą jo poveikio laipsnį

BDAR 83 straipsnio 2 dalies f punkte numatyta, kad sprendžiant, ar skirti administracinę baudą, ir nustatant baudos dydį gali būti „deramai atsižvelgiama“ į bendradarbiavimą su priežiūros institucija.

Gairėse dėl administracinių baudų apskaičiavimo nurodoma, jog pagal BDAR 31 straipsnį duomenų valdytojui ir duomenų tvarkytojui tenka bendra pareiga bendradarbiauti ir kad dėl nepakankamo bendradarbiavimo gali būti skirta BDAR 83 straipsnio 4 dalies a punkte numatyta bauda. Todėl reikėtų manyti, kad įprasta bendradarbiavimo pareiga yra privaloma ir todėl turėtų būti laikoma neutralia (o ne lengvinančia aplinkybe).

Paaiškinimuose Tikrinamas asmuo nurodo, kad kaip atsakingas duomenų tvarkytojas, darė viską, ką gali, kad sumažintų ADSP galimas neigiamas pasekmes, t.y. laikantis nustatytų terminų apie incidentą pranešė visiems paveiktiems duomenų valdytojams, įdiegė papildomas technines ir organizacines priemones, apie įvykusį kibernetinį incidentą pranešė NKSC, atsakinėjo į kiekvieną duomenų valdytojų paklausimą; glaudžiai bendradarbiavo siekiant atstatyti paveiktus duomenis; noriai ir sklandžiai teikė informaciją Inspekcijai vykdant ADSP tyrimą. Tikrinamo asmens vertinimu, įdėtos pastangos viršija teisės aktų numatomą bendradarbiavimo su institucijomis minimumą.

Tikrinamas asmuo Inspekcijai tiek atliekant patį tikrinimą, tiek nusprendus inicijuoti administracinės baudos skyrimo procedūrą, iš esmės teikė prašomą informaciją. Visgi, tiek BDAR, tiek ir ADTAĮ nustato prievolę (pareigą) duomenų tvarkytojui vykdyti priežiūros institucijos reikalavimus, todėl laiku pateikti atsakymai į Inspekcijos klausimus ar nurodymus pateikti informaciją, nėra vertinami kaip atsakomybę švelninantis veiksnys.

Be to, pagal BDAR 83 straipsnio 2 dalies f punktą yra vertinamas bendradarbiavimas tik su pačia priežiūros institucija, o ne su absoliučiai visais suinteresuotais subjektais, todėl vien tai, kad Tikrinamas asmuo aktyviai bendradarbiavo su duomenų valdytojais ir NKSC valdant ADSP, nesudaro pagrindo vertinti Tikrinamo asmens veiksmų BDAR 83 straipsnio 2 dalies f punkto prasme kaip švelninančios aplinkybės.

Inspekcija, įvertinusi tai, kas nurodyta, Tikrinamo asmens privalomo bendradarbiavimo su Inspekcija, reglamentuoto pagal teisės aktus, nei atsakomybę švelninančiu, nei sunkinančiu veiksmu nelaiko, t. y. laiko neutraliu veiksmu.

vii) BDAR 83 straipsnio 2 dalies g punktas – asmens duomenų, kuriems pažeidimas turi poveikį, kategorijos

Gairėse dėl baudų apskaičiavimo pažymima, jog BDAR aiškiai nurodytos duomenų rūšys, kurioms reikia ypatingos apsaugos, taigi ir griežtesnio atsako skiriant baudas. Tai susiję bent su BDAR 9 ir 10 straipsniuose nurodytų rūšių duomenimis ir duomenimis, nepatenkančiais į šių straipsnių taikymo sritį, dėl kurių platinimo duomenų subjektas patiria tiesioginę žalą arba įtampą (tai, pvz., vietos nustatymo duomenys, privačių pokalbių duomenys, nacionaliniai identifikavimo numeriai arba finansiniai duomenys, pvz., sandorių apžvalga arba kredito kortelių numeriai). Apskritai kuo daugiau tokių duomenų kategorijų arba kuo jautresni duomenys, tuo daugiau svarbos priežiūros institucija gali suteikti šiam veiksmui. Be to, svarbu nustatyti su kiekvienu duomenų subjektu susijusių duomenų kiekį, atsižvelgiant į tai, kad didėjant kiekvieno duomenų subjekto duomenų kiekiui, didėja teisės į privatų gyvenimą ir asmens duomenų apsaugą pažeidimas.

Tikrinimo metu nustatyta, kad dėl įvykusio ADSP buvo paveikti duomenų subjektų asmens duomenys: (vardai, pavardės, elektroniniai paštai, telefono numeriai, asmens tapatybės dokumentų duomenys, nuotraukos, IP adresai, interneto banko prisijungimo duomenys, naršymo informacija (kada ir iš kur buvo prisijungta prie banko sistemų), mokesčių mokėtojo identifikaciniai numeriai, duomenys apie klientų sandorius su banku ir sudarytas sutartis (banko sąskaitų numeriai, indėliai, mokėjimo nurodymai ir kitos mokėjimo operacijos, naudojamos mokėjimo priemonės ir jų naudojimo duomenys, piniginių lėšų įnešimo, išėmimo operacijų duomenys), duomenys, susiję su kredituojamu ar lizinguojamu turtu ir jo savininkais (turto adresas, unikalūs numeris, automobilio VIN, savininko duomenys, lizingo objekto (turto) pardavėjo duomenys), klientų duomenys, susiję su duomenų subjekto patikimumu ir veiklos vertinimu (finansinės operacijos, duomenys apie žalą, padarytą bankui, informacija, reikalinga pinigų plovimo ir teroristų finansavimo prevencijai, informacija apie tarptautinių sankcijų vykdymą, verslo veikla ir turto kilmės šaltinis, sandorių šalys, galutiniai naudos gavėjai), klientų finansiniai duomenys (informacija apie esamą ar buvusią darbovietę, vykdomą ūkinę komercinę veiklą, sąskaitų numeriai, turimas/turėtas turtas, sandoriai, paskolos, pajamos (įskaitant prognozuojamas pajamas ir jų stabilumą), išlaidos, įsipareigojimai, finansinė patirtis, kredito istorija ir kreditingumas, duomenys apie draudimą, sudarytos vartojimo kredito sutartys).

Pažymėtina, kad dėl įvykusio ADSP laikotarpiu nuo 2025-03-03 iki 2025-03-05 buvo sutrikusi [DUOMENYS NESKELBTINI] teikiamų bankinių paslaugų veikla, dėl ko, kaip jau minėta, duomenų subjektai galėjo patirti tiek materialinę, tiek nematerialinę žalą. Be to, paveikti duomenys sudarė itin jautrius asmens duomenis, susijusius su duomenų subjektų finansine informacija.

Atsižvelgiant į tai, kas nurodyta, Inspekcija Tikrinamo asmens veiksmus pagal BDAR 83 straipsnio 2 dalies g punktą laiko sunkinančiu veiksmu.

viii) BDAR 83 straipsnio 2 dalies h punktas – Inspekcijos sužinojimas apie pažeidimą

Priežiūros institucija gali sužinoti apie pažeidimą atlikdama tyrimą, gavusi skundų, iš visuomenės informavimo priemonių, anoniminių pranešimų arba duomenų valdytojo pranešimo. Gairėse dėl administracinių baudų apskaičiavimo nurodyta, kad ypatingas dėmesys gali būti skiriamas klausimui, ar duomenų valdytojas arba duomenų tvarkytojas savo iniciatyva pranešė apie pažeidimą prieš tai, kai priežiūros institucija sužinojo apie pažeidimą, pavyzdžiui, gavusi skundą arba atlikusi tyrimą. Ši aplinkybė nėra svarbi, kai duomenų valdytojui taikomos konkrečios pareigos pranešti (pvz., ADSP pagal BDAR 33 straipsnį atveju). Tokiais atvejais šis pranešimas turėtų būti laikomas neutraliu.

Nagrinėjamu atveju įvykusį ADSP pastebėjo ir apie jį Inspekcijai pranešė ne Tikrinamas asmuo, o duomenų valdytojai, kurie saugojo asmens duomenis naudodamiesi Tikrinamo asmens teikiamomis paslaugomis. Inspekcija pažymi, kad pagal sutartinius santykius su duomenų valdytojais, Tikrinamas asmuo neturėjo pareigos tiesiogiai pranešti Inspekcijai apie įvykusį ADSP, todėl tokią pareigą turėjo būtent duomenų valdytojai. Atsižvelgiant į tai, ši aplinkybė laikoma neutraliu veiksmu.

ix) BDAR 83 straipsnio 2 dalies i punktas – BDAR 58 straipsnio 2 dalyje nurodytų priemonių taikymas tikrinamam asmeniui

BDAR 83 straipsnio 2 dalies i punktas yra siejamas su aplinkybe įvertinti, ar duomenų valdytojas laikėsi BDAR 58 straipsnio 2 dalyje nurodytų priemonių, jei duomenų valdytojui dėl to paties dalyko anksčiau buvo taikytos šios priemonės.

Atsižvelgiant į tai, jog Tikrinamam asmeniui anksčiau taisomosios priemonės nebuvo taikytos, Inspekcija BDAR 83 straipsnio 2 dalies i punkte nurodyto veiksmo nevertina.

x) BDAR 83 straipsnio 2 dalies j punktas – tikrinamam asmeniui taikomi elgesio kodeksai ar sertifikavimo mechanizmai

Atsižvelgiant į tai, kad Tikrinamam asmeniui nebuvo taikomi elgesio kodeksai ar sertifikavimo mechanizmai pagal BDAR nuostatas, šis veiksnys nevertinamas.

xi) BDAR 83 straipsnio 2 dalies k punktas – kiti lengvinantys ar sunkinantys veiksniai

Paaikškinimuose Tikrinamas asmuo akcentuoja, kad jo vertinimu baudos skyrimas šiuo atveju nebūtų nei veiksmingas, nei proporcingas, nei atgrasomas pagal BDAR 83 straipsnio 1 dalį, o priešingai galėtų būti vertinamas kaip perteklinė ir neadekvati priemonė. Nurodo, kad ADSP kilo laikotarpiu, kai paslaugas teikė ne UAB DELSKA Lithuania, bet UAB „Rakrėjus“, t.y. juridinis asmuo, kuris po ADSP buvo prijungtas prie UAB DELSKA Lithuania ir šiuo metu nebeegzistuoja kaip atskiras subjektas. Nors UAB DELSKA Lithuania perėmė UAB „Rakrėjus“ teises ir pareigas, UAB DELSKA Lithuania nėra vien tik „Rakrėjus“ teisinis tęsinys ar formalus pertvarkymas, bet veikia kaip atskiras juridinis asmuo, turintis kitokią organizacinę struktūrą, kitokią techninę ir informacijos saugumo valdymo komandą, procesus ir rizikos profilį. Pažymi, kad UAB DELSKA Lithuania yra ir nepriekaištingą reputaciją turinčios buvusios UAB „Duomenų logistikos centras“ tąsa, perėmusi būtent šio juridinio asmens kodą, o prijungus UAB „Rakrėjus“ prie UAB DELSKA Lithuania, UAB „Rakrėjus“ nustojo egzistuoti kaip toks. Tikrinamo asmens įsitikinimu, reikšmingos administracinės baudos skyrimas UAB DELSKA Lithuania už veiksmus ir aplinkybes, susijusias su subjektu, kuris faktiškai jau nebevykdo veiklos, neatitiktų veiksmingumo,

proporcingumo ir atgrasomumo kriterijų, nes baudos poveikis būtų nukreiptas į kitą subjektą, o ne į tą, kurio veiklos metu kilo ADSP.

Vertindama šią Tikrinamo asmens nurodomą aplinkybę Inspekcija pažymi, kad nei BDAR nei ADTAĮ nenumato duomenų tvarkytojo atleidimo nuo atsakomybės už nustatytus pažeidimus ar šios atsakomybės švelninimo tuo atveju, jeigu priežiūros institucijos atliekamo tyrimo metu tikrinamo asmens teisės ir pareigos perima kitas juridinis asmuo, t.y. įvyksta reorganizavimas prijungimo būdu.

Lietuvos Respublikos civilinio kodekso (toliau – CK) 2.95 straipsnio 1 dalis numato, kad juridiniai asmenys pasibaigia likvidavimo arba reorganizavimo būdu. 2 šio straipsnio dalis numato, kad reorganizavimas – tai juridinio asmens pabaiga be likvidavimo procedūros. CK 2.97 straipsnio 3 dalis numato, kad prijungimas – tai vieno ar daugiau juridinių asmenų prijungimas prie kito juridinio asmens, kuriam pereina visos reorganizuojamo juridinio asmens teisės ir pareigos.

Tikrinimo metu nustatyta, kad nors nustatytus pažeidimus atliko UAB „Rakrėjus“, šis juridinis asmuo prijungimo būdu buvo prijungtas prie UAB DELSKA Lithuania, kuri perėmė jos teises ir pareigas. Taigi, nors teisine prasme UAB „Rakrėjus“ iš tiesų pasibaigė, jos teisės ir pareigos (įskaitant galimą administracinę atsakomybę už BDAR pažeidimus) perėjo kitam juridiniam asmeniui (UAB DELSKA Lithuania).

Remiantis nurodytais argumentais, ši aplinkybė vertinama kaip neutrali.

Kitų aplinkybių, kurios BDAR 83 straipsnio 2 dalies k punkto prasme galėtų būti vertinamos kaip lengvinančios arba sunkinančios Tikrinamo asmens atsakomybę, Inspekcija nenustatė.

Atsižvelgiant į aukščiau išdėstytus Inspekcijos argumentus, Inspekcija nusprendžia Tikrinamam asmeniui skirti administracinę baudą.

10. Administracinės baudos dydžio nustatymas

Gairėse dėl administracinių baudų apskaičiavimo nustatyta, kad skiriant administracinę baudą, būtina atsižvelgti į tris elementus, kurie yra administracinės baudos apskaičiavimo pagrindas: pažeidimų suskirstymą į kategorijas pagal pobūdį pagal BDAR 83 straipsnio 4–6 dalis, pažeidimo sunkumą ir įmonės apyvartą kaip vieną iš svarbių elementų, į kuriuos reikia atsižvelgti siekiant pagal BDAR 83 straipsnio 1 dalį skirti veiksmingą, atgrasomą ir proporcingą baudą.

Gairėse dėl administracinių baudų apskaičiavimo nurodyta, kad įvertinus pažeidimą, pažeidimas gali būti priskiriamas mažo, vidutinio arba didelio sunkumo lygio pažeidimui. Atitinkamai pagal tai nustatomas pradinis baudos dydis: už mažo sunkumo lygio pažeidimus 0–10 proc. teisės aktais nustatytos didžiausios sumos; už vidutinio sunkumo lygio pažeidimus 10–20 proc. teisės aktais nustatytos didžiausios sumos; už didelio sunkumo lygio pažeidimus 20–100 proc. teisės aktais nustatytos didžiausios sumos.

Minėtose gairėse paaiškinta, kad pažeidimo sunkumas yra nustatomas, atsižvelgiant į BDAR 83 straipsnio 2 dalies a, b ir g punktus, t. y. viso pažeidimo sunkumas nustatomas įvertinus pažeidimo pobūdį, sunkumą ir trukmę (BDAR 83 straipsnio 2 dalies a punktas); tai, ar pažeidimas padarytas tyčia, ar dėl aplaidumo (BDAR 83 straipsnio 2 dalies b punktas) ir asmens duomenų, kuriems pažeidimas turi poveikį, kategorijas (BDAR 83 straipsnio 2 dalies g punktas).

Inspekcija nenustatė, kad Tikrinamo asmens padaryti pažeidimai būtų padaryti tyčia, tačiau nustatyta, kad pažeidimai susiję su dideliu duomenų subjektų skaičiumi ir dideliu kiekiu duomenų, taip pat su itin jautriais finansiniais duomenimis, taip pat tai, kad dėl paveiktų asmens duomenų kategorijų šie duomenų subjektai patyrė nors ir laikinus, tačiau Inspekcijos vertinimu, reikšmingus padarinius negalėdami naudotis finansinėmis paslaugomis, todėl spręstina, kad Tikrinamo asmens padaryti pažeidimai yra priskiriami vidutinio sunkumo lygio pažeidimams ir tokiu atveju nustatomas pradinis minimalios baudos dydis atitinka nuo 10 iki 20 proc. taikomos maksimalios baudos sumos.

Inspekcija, atsižvelgdama ir į tai, kad iš pagal BDAR 83 straipsnio 2 dalį Tikrinamam asmeniui taikytų aštuonių veiksnų, pagal vieną nustatyti Tikrinamo asmens atsakomybę sunkinantis veiksnys, pagal vieną nustatytas švelninantis veiksnys, o pagal šešis – neutralūs, sprendžia, kad Tikrinamam asmeniui turėtų būti skiriama 15 proc. bauda nuo taikomos maksimalios sumos (10 000 000 EUR sumos), t. y. 1 500 000 EUR (pradinis minimalios baudos dydis).

Gairėse dėl administracinių baudų taip pat yra nurodyta, kad priežiūros institucija gali apsvarstyti galimybę pakoreguoti pradinę baudos sumą pagal pažeidimo sunkumą tais atvejais, kai šį pažeidimą padaro įmonė, kurios metinė apyvarta neviršija 2 mln. eurų, 10 mln. eurų arba 50 mln. eurų:

a) įmonėms, kurių metinė apyvarta ≤ 2 mln. eurų, priežiūros institucijos gali apsvarstyti galimybę atlikti skaičiavimus remiantis suma, patenkančia į 0,2–0,4 proc. nustatytos pradinės baudos sumos intervalą;

b) įmonėms, kurių metinė apyvarta 2–10 mln. eurų, priežiūros institucijos gali apsvarstyti galimybę atlikti skaičiavimus remiantis suma, patenkančia į 0,3–2 proc. nustatytos pradinės baudos sumos intervalą;

c) įmonėms, kurių metinė apyvarta 10–50 mln. eurų, priežiūros institucijos gali apsvarstyti galimybę atlikti skaičiavimus remiantis suma, patenkančia į 1,5–10 proc. nustatytos pradinės baudos sumos intervalą.

Nagrinėjamu atveju, pažymėtina, kad bauda skiriama Tikrinamam asmeniui, kurio 2024 finansinių metų metinė pasaulinė apyvarta sudarė 5 904 909 EUR. Atsižvelgiant į šias nustatytas aplinkybes bei vadovaujantis Gairių dėl administracinių baudų išaiškinimais, nustatytam pradiniam minimalios baudos dydžiui (1 500 000 EUR) pritaikius 0,3 proc. koeficientą, minimali administracinė bauda yra 4 500 EUR. Inspekcijos vertinimu, tokio dydžio bauda nagrinėjamu atveju laikytina proporcinga, veiksminga ir atgrasančia poveikio priemone.

Inspekcija, atsižvelgusi į tai, kas išdėstyta šiame sprendime bei vadovaudamasi BDAR 58 straipsnio 2 dalies i punktu, 83 straipsnio 1, 2 dalimis, 83 straipsnio 4 dalies a punktu, ADTAJ 34 straipsnio 10 dalimi,

n u s p r e n d ž i a:

1. Už šiame sprendime nustatytus BDAR 32 straipsnio 1 dalies b punkto pažeidimus Tikrinamam asmeniui skirti 4 500 Eur (keturių tūkstančių penkių šimtų eurų) baudą.
2. Apie priimtą sprendimą informuoti Tikrinamą asmenį.

Šis sprendimas Lietuvos Respublikos administracinių bylų teisenos įstatymo nustatyta tvarka per vieną mėnesį nuo jo įteikimo dienos gali būti skundžiamas Regionų administraciniam teismui (adresas: Žygimantų g. 2, Vilnius).

Vadovaujantis ADTAJ 35 straipsnio 1 dalimi, paskirta bauda ne vėliau kaip per tris mėnesius nuo baudos paskyrimo priėmimo dienos turi būti sumokėta į biudžeto pajamų surenkamąją sąskaitą⁸ (įmokos kodas 6803, lėšų gavėjas Valstybinė mokesčių inspekcija prie Lietuvos Respublikos finansų ministerijos, juridinio asmens kodas 188659752).

Direktorė

Dijana Šinkūnienė

⁸ Nr. LT78729000000130151 (AB „Citadele“ bankas); Nr. LT744010051001324763 ir Nr. LT122140030002680220 (Luminor Bank AS Lietuvos skyrius); Nr. LT057044060007887175 (AB SEB bankas); Nr. LT327180000000141038 (AB Šiaulių bankas); Nr. LT247300010112394300 (AB „Swedbank“); LT427230000000120025 (UAB Medicinos bankas).