Elektroninio dokumento išrašas

VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

SPRENDIMAS

2026 m. birželio 19 d. Nr. 3R-1143 (2.13-1 E)
Vilnius

Valstybinė duomenų apsaugos inspekcija (toliau ir – Inspekcija) žodinės procedūros tvarka 2026-06-02 vykusiame posėdyje [DUOMENYS NESKELBTINI] išnagrinėjo bylą dėl administracinės baudos skyrimo UAB InMedica (toliau ir – Bendrovė arba Klinika), juridinio asmens kodas 300011170.

Inspekcijos patikrinimų inicijavimo aplinkybės

Inspekcija, atsižvelgdama į 2024 m. rugsėjo mėn. viešoje erdvėje prieinamą informaciją[1] apie asmens duomenų saugumo pažeidimą (toliau - ADSP 1), kurioje nurodoma, kad trečiasis asmuo prisijungė prie UAB „Kardiolita“ (toliau ir – Bendrovė 1) vidinės duomenų valdymo sistemos, kurioje matomi duomenų subjektų asmens duomenys, bei vadovaudamasi Valstybinės duomenų apsaugos inspekcijos vykdomos stebėsenos atlikimo taisyklių[2] 5.1 papunkčiu bei BDAR[3] 57 straipsnio 1 dalies a punktu, atliko BDAR taikymo stebėseną Bendrovės 1 atžvilgiu. Atsižvelgdama į stebėsenos metu gautą informaciją ir vadovaudamasi ADTAĮ[4] 20 straipsnio 1 ir 2 dalimis, Valstybinės duomenų apsaugos inspekcijos vykdomų tyrimų ir (ar) patikrinimų atlikimo taisyklių[5] (toliau – Taisyklės) 4.4 ir 16.1 papunkčiais, Valstybinės duomenų apsaugos inspekcijos direktoriaus 2025-01-24 įsakymu Nr. 1T-16 (1.12.E) „Dėl UAB „Kardiolita“ tikrinimo Valstybinės duomenų apsaugos inspekcijos iniciatyva“ nusprendė savo iniciatyva pradėti tikrinimą, susijusį su galimu BDAR nuostatų pažeidimu, Bendrovės 1 atžvilgiu (toliau – Patikrinimas 1).

Inspekcija 2025-10-31 gavusi Bendrovės pateiktą pranešimą apie asmens duomenų saugumo pažeidimą (toliau – ADSP 2) (Inspekcijoje gauta 2025-11-03, reg. Nr. 1R-7533 (2.23 Mr)) (toliau – Pranešimas 2) ir vadovaudamasi ADTAĮ 20 straipsnio 1 ir 2 dalimis, Taisyklių 4.2, 4.4 ir 16.1 papunkčiais Valstybinės duomenų apsaugos inspekcijos direktoriaus 2025-11-03 įsakymu Nr. 1T-81 (1.12 E) „Dėl UAB InMedica tikrinimo Valstybinės duomenų apsaugos inspekcijos iniciatyva“, inicijavo tyrimą dėl galimo BDAR nuostatų pažeidimo Bendrovės atžvilgiu (toliau – Patikrinimas 2).

1. Teisinis reglamentavimas[6]

[1] https://www.youtube.com/watch?v=uqRnL6iNYq8

[2] Valstybinės duomenų apsaugos inspekcijos vykdomos stebėsenos atlikimo taisyklės, patvirtintos Valstybinės duomenų apsaugos inspekcijos direktoriaus 2023 m. lapkričio 8 d. įsakymu Nr. 1T-91 (1.12.E.) „Dėl Valstybinės duomenų apsaugos inspekcijos vykdomos stebėsenos atlikimo taisyklių patvirtinimo“

[3] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (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)

[4] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo (toliau – ADTAĮ)

[5] Valstybinės duomenų apsaugos inspekcijos vykdomų tyrimų ir (ar) patikrinimų atlikimo taisyklės, patvirtintos Valstybinės duomenų apsaugos inspekcijos direktoriaus 2019 m. liepos 17 d. įsakymu Nr. 1T-92 (1.12.E) „Dėl Valstybinės duomenų apsaugos inspekcijos vykdomų tyrimų ir (ar) patikrinimų atlikimo taisyklių patvirtinimo“

[6] Tiek Patikrinimo 1, tiek Patikrinimo 2 atvejais taikomas analogiškas teisinis reglamentavimas

BDAR 4 straipsnio 1 dalies 15 punkte sveikatos duomenys yra apibrėžiami kaip asmens duomenys, susiję su fizine ar psichine fizinio asmens sveikata, įskaitant duomenis apie sveikatos priežiūros paslaugų teikimą, atskleidžiantys informaciją apie to fizinio asmens sveikatos būklę.

Asmens duomenų tvarkymas laikomas teisėtu, jei jis yra pagrįstas bent viena iš BDAR 6 straipsnio 1 dalyje nustatytų teisėto asmens duomenų tvarkymo sąlygų ir atitinka bent vieną BDAR 9 straipsnio 2 dalyje numatytą išimtį (tvarkant specialiųjų kategorijų asmens duomenis) bei atitinka BDAR 5 straipsnyje nustatytus su asmens duomenų tvarkymu susijusius principus. Pagal BDAR 5 straipsnio 2 dalį, duomenų valdytojas yra atsakingas už tai, kad būtų laikomasi BDAR 5 straipsnio 1 dalies, ir turi sugebėti įrodyti, kad jos laikomasi (atskaitomybės principas).

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

Vientisumo ir konfidencialumo principas neatskiriamai susijęs su BDAR 24 ir 32 straipsniuose numatytomis prievolėmis duomenų valdytojui įgyvendinti tinkamas technines ir organizacines priemones, kad būtų užtikrintas tvarkomų asmens duomenų saugumas.

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

Vadovaujantis BDAR 32 straipsnio 1 dalies b punktu, 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. Pagal BDAR 32 straipsnio 2 dalį, nustatant tinkamo lygio saugumą visų pirma atsižvelgiama į pavojus, kurie kyla dėl duomenų tvarkymo, visų pirma dėl netyčinio arba neteisėto persiųstų, saugomų ar kitaip tvarkomų duomenų sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jų.

Nustatant asmens duomenims kylantį pavojų ir rizikas bei vertinant, ar duomenų valdytojas įgyvendina tinkamas technines ir organizacines saugumo priemones, yra atsižvelgiama į metodines rekomendacijas pateiktas ISO/IEC 27002:2022 standarte „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“ (toliau – ISO standartas).

Pranešimą priežiūros institucijai apie asmens duomenų saugumo pažeidimą (toliau ši sąvoka – ADSP) reglamentuoja BDAR 33 ir 34 straipsniai.

Pažymėtina, kad pagal BDAR 5 straipsnio 2 dalį pareiga užtikrinti tinkamas technines ir organizacines priemones bei įrodyti, kad asmens duomenys tvarkomi laikantis BDAR, taikoma duomenų valdytojui (Patikrinimo 1 atveju – Bendrovei 1, vėliau[7] - Bendrovei).

2. Patikrinimo 1 rezultatai

2.1. ADSP 1 aplinkybės ir pobūdis

Bendrovės 1 pranešime apie ADSP 1 (Inspekcijoje gauta 2024-09-13, reg. Nr. 1R-5836 (2.23 E)) ir papildomoje informacijoje (Inspekcijoje gauta 2024-09-18, reg. Nr. 1R-5962 (2.29 Mr), Inspekcijoje gauta 2024-09-24, reg. Nr. 1R-6105 (2.29 Mr), Inspekcijoje gauta 2024-10-01, reg. Nr. 1R-6304 (2.29 Mr), Inspekcijoje gauta 2024-02-17, reg. Nr. 1R-1032 (2.29 Mr)) (toliau kartu – Pranešimas 1)

[7] Nuo 2025-06-25

nurodoma, kad 2024-09-08 Bendrovė 1 gavo informaciją, kad trečiasis asmuo pasinaudojęs viešai prieinamais prisijungimo duomenimis, galimai neteisėtai prisijungė prie Bendrovės 1 naudojamos pacientų informacinės sistemos. Atsižvelgdama į tai, Bendrovė 1 nedelsiant pradėjo incidento tyrimą ir jį pabaigusi Inspekcijai pateikė tyrimo ataskaitą (toliau – Ataskaita 1). Ataskaitoje 1 Bendrovė 1 nurodė, kad ADSP 1 galimai įvyko kai trečiasis asmuo, pasinaudojęs Bendrovės 1 darbuotojos prisijungimo duomenimis, prisijungė prie informacinės sistemos „Foxus“ (toliau – Foxus). Bendrovė 1 mano, kad darbuotojos prisijungimo duomenys į tamsiajame internete nutekintų duomenų bazę (angl. *Dark web*) pateko jai anksčiau pakliuvus į socialinės inžinerijos metodais paremtą ataką (angl. *phishing attack*) ir tapus jos auka.

Sistemos teikėjas UAB „Softdent“ pateikė žurnalinius įrašus (angl. *logs*), kuriuos išanalizavusi Bendrovė 1 nustatė, kad laikotarpiu nuo 2024-08-27 iki 2024-09-07 pasinaudojus darbuotojos prisijungimo duomenimis buvo prisijungta prie 63 Bendrovės 1 pacientų informacijos. Pranešime 1 papildomai pažymėta, kad prie dalies jų galėjo jungtis ir pati darbuotoja, vykdydama darbo funkcijas. Bendrovė 1 nustatė, kad neteisėtos prieigos metu buvo atliekama pacientų paieška, atidaroma ir iškart uždaroma paciento kortelė. Duomenų pasisavinimas, eksfiltravimas ir atsisiuntimas iš Foxus nebuvo fiksuotas.

Bendrovė 1 Ataskaitoje 1 nurodė, kad ADSP 1 metu, trečiasis asmuo galėjo susipažinti su šiais 63 pacientų asmens duomenimis:

1) Anketiniai duomenys: Bendrovės 1 klientų (pacientų) kontaktiniai duomenys bei informacijos suvestinė: vardas, pavardė, tautybė, gimimo data, adresas, telefono numeris, įskaitant asmens kodus.

2) Specialių kategorijų asmens duomenys: Bendrovės 1 klientų (pacientų) sveikatos duomenys (Bendrovėje 1 klientams (pacientams) suteiktų sveikatos priežiūros paslaugų suvestinė, atliktų tyrimų pavadinimai, receptai, skiepai ir pan.).

Papildomai pažymėtina, kad Bendrovė 1 Ataskaitoje 1 aprašydama incidento seką, nurodė, kad: *„<...> pasinaudojus Bendrovės darbuotojos (Gydytojos) Prisijungimo duomenimis, laikotarpiu nuo 2024.08.27 iki 2024.09.07 buvo įvykdyta trumpalaikė, epizodinė neteisėta prieiga prie Informacinės sistemos „Foxus“, kelis kartus siekiant (i) patikrinti, ar yra įmanomas prisijungimas prie Sistemos su minėtais Prisijungimo duomenimis; (ii) patikrinti, prie kiek ir kokių duomenų galima prieiti prisijungus prie Sistemos ir (iii) padaryti kelias Sistemoje esančių duomenų (pacientų kortelių) ekrano nuotraukas (angl. print screen, screen shots*)“ (tekstas nekoreguotas).

Bendrovė 1 Ataskaitoje 1 nurodė, kad Foxus sinchronizuojasi su išorinėmis duomenų bazėmis ar informacinėmis sistemomis (pvz., ESPBI IS[8]). Sinchronizavimas yra atliekamas pacientą registravus vizitui Bendrovės 1 klinikoje ar kitais atvejais, kai atliekami veiksmai susiję su paslaugų suteikimu pacientui, todėl Foxus yra kaupiami pacientų duomenys iki jų paskutinio apsilankymo Bendrovėje 1.

Atsižvelgiant į tai, kas išdėstyta, darytina išvada, kad ADSP 1 galimai įvyko – kai trečiasis asmuo, pasinaudojęs tamsiajame internete nutekintų duomenų bazėje (angl. *Dark web*) rastais Bendrovės 1 darbuotojos prisijungimais, prisijungė prie Foxus ir peržiūrėjo duomenų subjektų informaciją.

2.2. Bendrovės 1 pateiktų paaiškinimų bei tyrimo metu nustatytų aplinkybių vertinimas dėl gebėjimo užtikrinti nuolatinį duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą (BDAR 32 straipsnio 1 dalies b punktas)

Atlikus ADSP 1 tyrimą pagal Bendrovės 1 pateiktą Pranešimą 1 bei pagal Inspekcijos kompetenciją įvertinus įvykusio ADSP 1 aplinkybes bei surinktus įrodymus, parengta Valstybinės duomenų apsaugos inspekcijos Informacinių technologijų skyriaus 2025-09-17 ataskaita Nr. 4R-474 (2.14.E) dėl UAB „Kardiolita“ asmens duomenų saugumo pažeidimo (toliau – Tikrinimo ataskaita 1).

Prieigų kontrolė ir autentifikavimas

Prieigų kontrolė ir autentifikavimas yra esminiai saugos reikalavimai, siekiant apsisaugoti nuo neautorizuotos prieigos prie IT sistemos, kurioje yra tvarkomi asmens duomenys.

[8] Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinė sistema (toliau – ESPBI IS)

Remiantis Gairių[9] 86 punktu, *„Turi būti veikiantis autentifikavimo mechanizmas, leidžiantis prieigą prie IT sistemos (paremtas Prieigų kontrolės politika). Minimalus reikalavimas naudotojui prisijungti prie IT sistemos – naudotojo prisijungimo vardas ir slaptažodis. Slaptažodis sudaromas atsižvelgiant į tam tikrą kompleksiškumo lygį“*. ISO standarto 5.17 papunktyje „Autentiškumo patvirtinimo informacija“ nurodoma, kad *„Autentiškumo patvirtinimo informacijos priskyrimas ir valdymas turėtų būti kontroliuojamas pagal valdymo procesą, įskaitant personalo konsultavimą dėl tinkamo autentiškumo patvirtinimo informacijos tvarkymo“*. Duomenų valdytojas techninėmis ir organizacinėmis priemonėmis turi užtikrinti, jog sistemų naudotojų naudojami prisijungimo slaptažodžiai atitiktų reikiamą saugumo lygį ir tam tikrą kompleksiškumo lygį. Atsižvelgiant į tai, kad Bendrovės 1 darbuotojai, jungdamiesi prie Foxus, gauna prieigą prie pacientų asmens duomenų, įskaitant ir sveikatos duomenis, prisijungimų slaptažodžiams turi būti taikomi griežtesni reikalavimai. Papildomai atkreipiamas dėmesys, kad remiantis Inspekcijos rekomendacija dėl saugių ir stiprių slaptažodžių naudojimo svarbos[10], slaptažodis, atitinkantis tam tikrą kompleksiškumo lygį, turi būti sudarytas iš ne mažiau nei 12 simbolių, naudojamos didžiosios ir mažosios raidės, skaičiai ir specialieji simboliai.

Remiantis Gairių 91 punktu, *„<...> Kai į tokias sistemas jungiamasi ne iš vidinio kompiuterių tinklo, turi būti naudojamos ir papildomos saugumo priemonės, tokios kaip IP adreso kontrolė <...>“*, ISO standarto 8.3 papunkčiu „Prieigos prie informacijos ribojimas“, turi būti užkertamas kelias neleistinai prieigai, atsižvelgiant į prieigos leidimų suteikimą pagal tapatybę, įtaisą, vietą ar taikomąją programą. Taip pat ISO standarto 8.5 papunktyje „Saugus autentiškumo patvirtinimas“ nurodoma, kad turėtų būti pasirinktas tinkamas autentiškumo patvirtinimo metodas. Atsižvelgiant į tai, duomenų valdytojas, siekdamas užtikrinti asmens duomenų saugumą, privalo pasirinkti tinkamus autentiškumo patvirtinimo metodus (pvz. kelių faktorių autentifikaciją (angl. *Multi-factor authentification)* (toliau - MFA) ir / ar leidimą jungtis prie sistemų tik iš žinomų IP adresų, iš tam tikrų LAN tinklų, iš tam tikros teritorijos ar kitą.

Tikrinimo ataskaitoje 1 nurodoma, kad atliekant tyrimą Bendrovės 1 atžvilgiu buvo vertinama, ar Bendrovė 1 prieš įvykstant ADSP 1 ėmėsi tinkamų techninių ir organizacinių priemonių, kad tokie ADSP neįvyktų, ir buvo nustatyta, kad:

1. Darbuotojai prie Foxus jungėsi su slaptažodžiais, kurie buvo sudaryti iš ne mažiau kaip 8 simbolių, susidedantys iš raidžių ir skaičių[11], nenaudojant asmeninės informacijos;
2. Foxus buvo pasiekiama per išorinį tinklą (internetu);
3. Išoriniams prisijungimams nebuvo taikomas dviejų faktorių autentifikavimas (angl. *2FA – Two-factor authentication*);
4. Jungimuisi prie Foxus nebuvo taikomas prieigos ribojimas tik įgaliotiems asmenims, t. y. nebuvo vykdomas IP adresų filtravimas, todėl Bendrovės 1 darbuotojai galėjo jungtis prie Foxus iš nežinomų bei ne Lietuvoje esančių IP adresų.

Atsižvelgiant į tai, kad ADSP 1 galėjo įvykti dėl to, kad trečiasis asmuo iš anksto žinojo darbuotojos prisijungimo vardą ir slaptažodį, pažymėtina, kad jei darbuotojams, kurie prie Foxus jungėsi per išorinį tinklą (internetu), būtų taikoma *MFA* ar būtų įdiegtas prieigos ribojimas tik įgaliotiems asmenims (pavyzdžiui, pagal iš anksto nurodytus IP adresus ar tik iš tam tikrų LAN tinklų), trečiasis asmuo nebūtų neteisėtai prisijungęs prie Foxus ir ADSP 1 būtų neįvykęs. Kadangi jungiantis prie Foxus su kelių veiksnių autentifikacija, kai pirmas žingsnis yra atliktas, prisijungimo vardas ir slaptažodis yra suvesti, yra inicijuojamas autentifikavimas išsiunčiant prisijungimo kodą į iš anksto nustatytą el. paštą ar telefoną, todėl antras žingsnis autentifikacijos nebūtų atliktas ir net trečiajam asmeniui iš anksto žinant prisijungimo vardą ir slaptažodį. Analogiškai su Foxus pasiekimo ribojimu

[9] Valstybinės duomenų inspekcijos 2024 m. rugpjūčio 13 d. gairės Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams (toliau – Gairės)

[10] https://vdai.lrv.lt/public/canonical/1734937137/678/Rekomendacija_del_slaptazodziu_2024.pdf

[11] Nenaudojant specialiųjų simbolių

pagal IP adresus ar iš vidinio Bendrovės 1 tinklo, t. y. net ir žinant prisijungimo vardą ir slaptažodį nebūtų galima prisijungti, kadangi pati Foxus nebūtų pasiekiama, trečiasis asmuo dar papildomai turėtų patekti į vidinį Bendrovės 1 tinklą arba gauti prieigą pagal IP adresą. Atsižvelgiant į nustatytas aplinkybes, darytina išvada, kad ADSP 1 metu Bendrovės 1 naudojamoje Foxus nebuvo užtikrinamas tinkamas asmens duomenų saugumo lygis.

Apibendrinant šioje rašto dalyje pateiktą informaciją ir atsižvelgiant į rašte jau pateiktą BDAR nustatytą teisinį reglamentavimą bei Gairėse bei ISO standarte pateiktus išaiškinimus (rekomendacijas) ir nustatytas ADSP 1 aplinkybes, darytina išvada, kad ADSP 1 įvyko dėl Bendrovėje 1 nepakankamai užtikrinamos prieigų kontrolės ir netinkamo autentifikavimo jungiantis prie Foxus, kai Bendrovės 1 darbuotojams jungiantis per išorinį tinklą (internetu) nebuvo taikomas kelių veiksnių autentifikavimas ir nebuvo įdiegtas prieigos apribojimas tik įgaliotiems asmenims, taip pat darbuotojų prisijungimų prie Foxus slaptažodžiai neatitiko tam tikro kompleksiškumo lygio. Inspekcija sprendžia, kad Bendrovė 1, neužtikrindama ISO standarto 5.17, 8.3 ir 8.5 papunkčiuose nustatytų reikalavimų, pažeidė BDAR 24 straipsnio 1 dalies, BDAR 32 straipsnio 1 dalies b punkto reikalavimus bei BDAR 5 straipsnio 1 dalies f punkte įtvirtintą konfidencialumo principą.

3. Patikrinimo 2 rezultatai

3.1. ADSP 2 aplinkybės ir pobūdis

Pranešime 2 nurodyta, kad 2025-10-29 tarp 12-13 val. Bendrovės darbuotojams pradėjus fiksuoti informacinių sistemų sutrikimus, IT departamentas nustatė, kad įvyko incidentas, kurio metu buvo užšifruoti duomenys, tvarkomi 4 Bendrovės naudojamose sistemose (toliau bendrai – Sistemos):

- stacionaro pacientų valdymo sistema, naudojama pacientų sveikatos duomenims tvarkyti dviejose Bendrovės klinikose (toliau – Med.I.S);
- radiologijos vaizdų sistema, naudojama radiologinių tyrimų saugojimui ir peržiūrai (toliau – PACS);
- personalo valdymo sistema, kurioje saugomi darbuotojų duomenys (toliau – Edrana);
- bendras failų serveris, kuriame saugomi administraciniai dokumentai ir kiti darbo failai (toliau – File Share).

Bendrovė Pranešime 2 nurodė, kad visos šios Sistemos veikė atskiruose virtualiuose „Windows Servers“ serveriuose, toje pačioje virtualizacijos aplinkoje.

Bendrovė Pranešime 2 nurodė, kad ADSP metu buvo paveiktos keturios Bendrovės Sistemos, kuriose tvarkomi pacientų bei darbuotojų asmens duomenys (darbuotojai – apie 10 tūkst., pacientai – 383 tūkst.) .

Taip pat nurodė, kad buvo paveikti:

1) darbuotojų – vardai, pavardės, pareigos, padaliniai, el. pašto adresai, kontaktiniai telefonų numeriai, vartotojų ID, asmens kodai, darbuotojų administraciniai duomenys (darbo sutarties informacija, atlyginimo dydis, atostogų prašymai, darbo grafikai, kiti su darbo santykiais susiję dokumentai ir juose esantys asmens duomenys);

2) pacientų – vardai, pavardės, gimimo datos, amžius, asmens kodai, telefono numeriai, el. pašto adresai, sveikatos duomenys (medicininiai įrašai, diagnozės, gydymo istorija, atliktų tyrimų ir procedūrų duomenys, laboratorinių tyrimų atsakymai, radiologiniai vaizdai (MRT, KT, rentgeno ir kt.), su tyrimais susijusios ataskaitos), identifikatoriai medicininių įrašų sistemoje (ID numeriai, medicininės kortelės numeriai).

Pranešime 2 nurodyta, kad Bendrovė nedelsiant pradėjo incidento valdymo veiksmus, t. y. sustabdė paveiktų serverių veiklą ir pradėjo duomenų atkūrimą iš atsarginių kopijų. Tą pačią dieną apie 17 – 18 val. Sistemų veikimas buvo pilnai atkurtas duomenis atstačius iš atsarginių kopijų.

Tirdama ADSP 2 valdymo veiksmus, Inspekcija Bendrovei uždavė papildomus klausimus, į kuriuos Bendrovė pateikė atsakymus (Inspekcijos reg. data 2025-11-11, reg. Nr. 1R-7829 (2.14 K);

2025-11-21, reg. Nr. 1R-8073 (2.23 Mr); 2025-11-11, reg. Nr. 1R-7829 (2.14 K) ir 2026-01-06, reg. Nr. 1R-62 (2.14 E).

Bendrovė atliko kibernetinį incidento tyrimą, kurio ataskaitą 2025-12-04 pateikė Inspekcijai (Inspekcijos reg. data 2025-12-05, reg. Nr. 1R-8529 (2.14 K) (toliau – Ataskaita 2). Ataskaitoje 2 nurodyta, kad 2025-10-29 12 val. 24 min. 32 sek. į serverį [DUOMENYS NESKELBTINI] (toliau – Serveris) buvo sėkmingai prisijungta iš kenkėjiško IP adreso su [DUOMENYS NESKELBTINI] vartotoju. Prisijungimui buvo panaudota administratoriaus teises turėjusi domeno paskyra, o tai suteikė galimybę toliau pasiekti kitas vidines sistemas ir inicijuoti duomenų šifravimo veiksmus. Bendrovė patyrė išpirkos reikalaujančią ataką (angl. Ransomware), kai trečioji šalis, prisijungusi per nuotolinio darbalaukio protokolo (angl. Remote Desktop Protocol) (toliau ir - RDP) paslaugą ir pasinaudojusi šoniniu judėjimu (angl. lateral movement)[12], užšifravo keturių Sistemų duomenis.

Bendrovė nurodė, kad nesankcionuota prieiga tęsėsi iki 2025-10-29 13 val. 34 min. 58 sek., kai Bendrovės IT departamento komanda nutraukė aktyvią sesiją, blokavo RDP prieigą ir izoliuodama paveiktus Serverius nedelsiant sustabdė tolesnius trečiojo asmens veiksmus. Bendra trečiojo asmens neteisėta prieiga truko 70 minučių ir 30 sekundžių.

Taip pat Bendrovė nurodė, kad visos paveiktos Sistemos buvo pilnai atkurtos ir įprastinis paslaugų teikimas buvo pilnai atnaujintas 2025-10-29 apie 17 valandą. Bendrovė pažymėjo, kad įvykio metu paslaugų teikimas nenutrūko, nes gydytojai galėjo naudotis ESPBI IS esančiais medicininiais įrašais ir asmens duomenimis, kurie buvo perduoti iš vietinių sistemų anksčiau. Taip pat naudotasi medicininių dokumentų įrašais, kurie saugomi fizinėse (popierinėse) pacientų kortelėse.

Atsižvelgiant į tai, kas išdėstyta šioje dalyje, darytina išvada, kad Bendrovė patyrė duomenų šifravimo ir išpirkos reikalaujančią ataką (angl. Ransomware), kai trečioji šalis, prisijungusi per RDP paslaugą ir pasinaudojusi šoniniu judėjimu (angl. lateral movement), užšifravo keturių Sistemų duomenis.

3.2. Bendrovės pateiktų paaiškinimų bei tyrimo metu nustatytų aplinkybių vertinimas dėl gebėjimo užtikrinti nuolatinį duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą (BDAR 32 str. 1 dalies b punktas)

Atlikus ADSP 2 tyrimą pagal Bendrovės pateiktą Pranešimą 2 bei pagal Inspekcijos kompetenciją įvertinus įvykusio ADSP 2 aplinkybes bei surinktus įrodymus, parengta Valstybinės duomenų apsaugos inspekcijos Informacinių technologijų skyriaus 2026-03-10 ataskaita Nr. 4R-145 (2.14.E) dėl UAB INMEDICA asmens duomenų saugumo pažeidimo (toliau – Tikrinimo ataskaita 2).

Bendrovė Ataskaitoje 2 nurodė, kad ADSP 2 įvyko trečiajam asmeniui gavus RDP prieigą prie Serverio. Trečiasis asmuo prie Serverio prisijungė su [DUOMENYS NESKELBTINI] domeno paskyra (t. y. turėdamas privilegijuotas prieigos teises), todėl pasiekė visas 4 paveiktas Sistemas.

Lietuvos Respublikos Vyriausybės nutarimu 2018 m. rugpjūčio 13 d. Nr. 818[13] „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ patvirtintame Kibernetinio saugumo reikalavimų apraše (toliau – Aprašas) nustatyti reikalavimai yra taikomi kibernetinio saugumo subjektams, kurie yra įtraukti į kibernetinio saugumo subjektų sąrašą. Apraše nustatytos techninės ir organizacinės priemonės šiame sprendime vertinamos kaip visuotinai pripažįstama geroji praktika kibernetinio saugumo srityje. Atsižvelgiant į BDAR duomenų valdytojams nustatytą pareigą įgyvendinti tinkamas technines ir organizacines priemones, siekiant užtikrinti aukštesnį asmens duomenų apsaugos lygį ir veiksmingesnį kibernetinių grėsmių valdymą, laikytina, kad Apraše nustatytos priemonės turi būti žinomos ir taikomos, nepriklausomai nuo to, ar duomenų valdytojai yra įtraukti į kibernetinio saugumo subjektų sąrašą ar ne.

[12] Šoninis judėjimas (angl. lateral movement) – tai etapas, kai trečiasis asmuo, jau patekęs į vieną sistemą, pradeda judėti tinklo viduje, ieškodamas, kur dar turi galimybę prisijungti.

[13] https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr

Atliekant tyrimą Bendrovės atžvilgiu, buvo vertinama, ar Bendrovė prieš įvykstant ADSP 2 ėmėsi tinkamų techninių ir organizacinių priemonių, kad tokie ADSP neįvyktų. Inspekcija nustatė, kad:

1. Trečiasis asmuo prisijungė prie privilegijuotas prieigos teises turinčios paskyros.
2. Paveiktas Serveris buvo pasiekiamas per išorinį tinklą (internetu).
3. Naudotojams, turintiems privilegijuotas prieigos teises, jungiantis per išorinį tinklą nebuvo taikoma *MFA*.
4. Jungimuisi prie Serverio per RDP nebuvo taikomas IP adresų filtravimas.

Aprašo XII skirsnyje „Prieigos valdymas ir kelių veiksnių tapatumo nustatymo priemonės“ 7 lentelės 61 punkte nurodyta, kad: „Naudotojas ir administratorius turi patvirtinti savo tapatybę slaptažodžiu ir papildoma tapatumo nustatymo priemone (kelių veiksnių tapatumo nustatymo priemonės).“, ISO standarto 8.5 papunktyje „Saugus autentiškumo patvirtinimas“ nurodyta, kad turėtų būti pasirinktas tinkamas autentiškumo patvirtinimo metodas. Gairių 91 punkte nurodyta, kad privilegijuotiems naudotojams (pvz., sistemų administratoriams) prisijungimui prie asmens duomenų tvarkymo sistemų turi būti taikomas kelių veiksnių autentifikavimas.

Pažymėtina, kad remiantis Gairių 91 punktu, „<...> Kai į tokias sistemas jungiamasi ne iš vidinio kompiuterių tinklo, turi būti naudojamos ir papildomos saugumo priemonės, tokios kaip IP adreso kontrolė <...>“ ir ISO standarto 8.3 papunkčiu „Prieigos prie informacijos ribojimas“, kuriame nurodoma, kad turi būti užkertamas kelias neleistinai prieigai, atsižvelgiant į prieigos leidimų suteikimą pagal tapatybę, įtaisą, vietą ar taikomąją programą. Atsižvelgiant į tai, duomenų valdytojas, siekdamas užtikrinti asmens duomenų saugumą, privalo pasirinkti tinkamus autentiškumo patvirtinimo metodus (MFA ir / ar leidimą jungtis prie sistemų tik iš žinomų IP adresų, iš tam tikrų LAN tinklų, iš tam tikros teritorijos ar kitą).

Atsižvelgiant į tai, kad Bendrovė nurodė, jog ADSP 2 galėjo įvykti dėl to, kad trečiasis asmuo iš anksto žinojo naudotojo, turinčio privilegijuotas prieigos teises, prisijungimo vardą ir slaptažodį, pažymėtina, kad jei jungiantis prie Serverio per išorinį tinklą (internetu) būtų taikoma *MFA* ar būtų įdiegtas prieigos ribojimas tik įgaliotiems asmenims (pavyzdžiui, pagal iš anksto nurodytus IP adresus ar tik iš tam tikrų LAN tinklų), trečiasis asmuo nebūtų neteisėtai prisijungęs prie Serverio ir ADSP 2 būtų neįvykęs. Pažymėtina, kad jungiantis prie Serverio su kelių veiksnių autentifikacija, atlikus pirmą žingsnį (įvedus prisijungimo vardą ir slaptažodį), toliau yra inicijuojamas antras žingsnis (autentifikavimas) į iš anksto nustatytą el. paštą ar telefoną išsiunčiant prisijungimo kodą ir vartotojui jį suvedus. Atitinkamai nagrinėjamu atveju, antras žingsnis nebūtų atliktas, net trečiajam asmeniui iš anksto žinant prisijungimo vardą ir slaptažodį. Analogiškai su Serverio pasiekimo ribojimu pagal IP adresus ar iš vidinio Bendrovės tinklo, t. y. net ir žinant prisijungimo vardą ir slaptažodį, nebūtų galima prisijungti, kadangi Serveris nebūtų pasiekiamas, nes trečiasis asmuo dar papildomai turėtų patekti į vidinį Bendrovės tinklą arba gauti prieigą pagal IP adresą. Atsižvelgiant į pateiktus argumentus, darytina išvada, kad ADSP 2 metu Bendrovės paveiktose Sistemose nebuvo užtikrinamas tinkamas asmens duomenų saugumo lygis.

Papildomai vertinant Bendrovės argumentus, kad incidento metu neįvyko asmens duomenų konfidencialumo praradimas ir nustačius, kad Bendrovė prieš įvykstant ADSP 2 netaikė dviejų lygių autentifikavimo, papildomai pažymėtina, kad Bendrovė netaikė ir kitų techninių priemonių, kuriomis būtų užtikrinama, kad asmeniui, neturinčiam leidimo susipažinti su asmens duomenimis, jie būtų nesuprantami, pavyzdžiui, taikant pažangų šifravimą ar naudojant prieigos raktus. Tačiau šiuo atveju, prieš įvykstant ADSP 2 tokios priemonės nebuvo taikytos, todėl vertinant ADSP 2 aplinkybes turi būti atsižvelgiama į tai, kad nors duomenys ir nebuvo tiesiogiai eksfiltruoti, tačiau trečiasis neįgaliotas asmuo gavo prieigą prie asmens duomenų, įskaitant ir specialios kategorijos (sveikatos) asmens duomenis, todėl vertinama, kad incidento metu buvo prarastas asmens duomenų konfidencialumas.

Be to, atsižvelgiant į tai, kad buvo užšifruotos keturios Bendrovės Sistemos ir darbuotojai tam tikrą laiką, kol duomenys nebuvo pilnai atstatyti iš atsarginių kopijų, negalėjo pasiekti duomenų, buvusių paveiktose Sistemose, darytina išvada, kad buvo pažeistas ir nuolatinis duomenų tvarkymo sistemų ir paslaugų prieinamumas.

Atsižvelgiant į tai, kas išdėstyta, darytina išvada, kad ADSP 2 metu buvo paveiktos keturios Bendrovės Sistemos, kuriose tvarkomi pacientų bei darbuotojų asmens duomenys (darbuotojai – apie 10 tūkst., pacientai – 383 tūkst.). ADSP 2 įvyko dėl Bendrovėje nepakankamai užtikrinamos prieigų kontrolės ir autentifikavimo, jungiantis prie paveikto Serverio, kai privilegijuotiems naudotojams jungiantis per išorinį tinklą (internetu) nėra taikomas kelių veiksnių autentifikavimas ir nebuvo įdiegtas prieigos apribojimas tik įgaliotiems asmenims. Todėl Bendrovė, neužtikrindama ISO standarto 5.17, 8.3 ir 8.5 papunkčiuose nustatytų reikalavimų, pažeidė BDAR 24 straipsnio 1 dalies, BDAR 32 straipsnio 1 dalies b punkto reikalavimus bei BDAR 5 straipsnio 1 dalies f punkte įtvirtintą konfidencialumo principą.

4. Po siūlymo skirti baudą Bendrovės pateikti rašytiniai paaiškinimai

Bendrovė 2026-05-08 Inspekcijai pateikė savo paaiškinimus (Inspekcijos reg. Nr. 1R-3709 (2.13 Mr)).

4.1. Dėl ADSP 1

Bendrovė papildomai pažymi, kad nuo ADSP 1 nustatymo momento (2024 m. rugsėjo mėn.) iki 2026-05-08, t. y. per daugiau nei 1 (vienerius) metus ir 8 (aštuonis) mėnesius, Bendrovė nėra sulaukusi nė vieno duomenų subjekto skundo, pretenzijos ar pranešimo apie bet kokį realų neigiamą poveikį, susijusį su ADSP 1.

Taip pat nurodoma, kad vadovaudamasi BDAR 24 ir 32 straipsnių reikalavimais, Bendrovė nuosekliai vykdo savo informacinių sistemų, duomenų bazių ir duomenų tvarkymo operacijų rizikų vertinimą. Bendrovė sistemingai vertina IT sistemų ir kitų IT išteklių (įskaitant asmens duomenis) saugumą, atsparumą ir apsaugą, parenka adekvačias ir proporcingai rizikai atitinkančias saugumo priemones bei sprendinius ir atitinkamai juos diegia bei palaiko. Paaiškinama, kad IT sistemų saugumo ir susijusių rizikų vertinimas yra nuolatinis, dinaminis ir kompleksinis procesas, apimantis nuolat kintančių ir naujai atsirandančių technologijų, procesų bei jų sąlygojamų grėsmių analizę. Pažymima, kad atlikdama rizikos vertinimą, Bendrovė vadovaujasi Inspekcijos rekomendacijomis, gerąja sektoriaus praktika, taip pat ENISA gairėmis, parengtomis remiantis tarptautiniais standartais (LST ISO/IEC 27001:2017, ISO/IEC 27002:2017, ISO/IEC 27701:2019 ir kt.).

Bendrovė pripažįsta, kad ADSP 1 metu Foxus neturėjo įdiegtos MFA autentifikacijos išorinei prieigai, kartu pažymint, kad šis faktas turėtų būti vertinamas visų tyrimo metu nustatytų aplinkybių kontekste:

1) Bendrovės teigimu, MFA taikymas prieigai prie trečiųjų šalių informacinių sistemų sveikatos priežiūros įstaigose 2024 m. nebuvo visuotinė praktika – priešingai, Inspekcijos atlikta 2025 m. planinė sveikatos priežiūros įstaigų saugumo priemonių stebėsena[14] patvirtina, kad 2025 m. tik 11 proc. sveikatos priežiūros įstaigų šią priemonę taikė. Bendrovės nuomone, tai rodo, kad MFA nebuvimas nėra išimtinis Bendrovės aplaidumo požymis, o sisteminis visos sveikatos priežiūros sektoriaus brandos klausimas.

2) Pažymima, kad Bendrovė šį trūkumą ištaisė operatyviai, savo iniciatyva – aktyviai koordinuodama procesą su Foxus tiekėju UAB „Softdent“, teikdama jam konkrečius nurodymus bei teisinę ir techninę pagalbą, užtikrino MFA įdiegimą per kelias dienas nuo ADSP 1 nustatymo. Atsižvelgiant į tai, kad Inspekcijos stebėsenos duomenimis, tik 1 iš 10 stebėtų sveikatos priežiūros įstaigų taiko MFA, Bendrovė daro prielaidą, kad ta viena įstaiga yra Bendrovė, kurios iniciatyva MFA buvo įdiegta dar 2024 m. rugsėjo mėnesį – gerokai anksčiau nei buvo atlikta minėta stebėsena.

[14] https://vdai.lrv.lt/lt/naujienos/vdai-atlikusi-sveikatos-prieziuros-istaigu-stebesena-teikia rekomendacijas-9Qv/

3) Paaiškinama, kad MFA įdiegimo Foxus procesas objektyviai užtruko, nes reikalavo reikšmingo techninio pasirengimo iš Foxus tiekėjo UAB „Softdent“ pusės – MFA funkcionalumas šioje sistemoje iki tol nebuvo įdiegtas apskritai, todėl tiekėjas turėjo suprojektuoti, sukurti ir integruoti visiškai naują autentifikacijos modulį. Kartu pažymima, kad Bendrovė buvo pirmoji iš visų UAB „Softdent“ klientų, pareikalavusi MFA įdiegimo Foxus, nors UAB „Softdent“ teikia informacinės sistemos paslaugas daugeliui sveikatos priežiūros įstaigų Lietuvoje. Pasak Bendrovės, tai reiškia, kad ji ne tik operatyviai reagavo į nustatytą pažeidžiamumą, bet ir faktiškai inicijavo bei paskatino naujo saugumo standarto sukūrimą visai Foxus naudotojų bendruomenei – veikdama proaktyviai ir viršydama tuo metu (ir, tikėtina, netgi šiuo metu) sektoriuje vyravusią praktiką. Pažymima, kad UAB „Softdent“ yra po aptartų įvykių linkęs šį MFA sprendimą siūlyti ir kitiems Foxus naudotojams, tačiau Bendrovės žiniomis iki šios dienos nė vienas kitas duomenų valdytojas šio sprendimo nėra įdiegęs. Atitinkamai, Bendrovė mano išliekanti vienintelė (tiek tarp Inspekcijos stebėtų sveikatos priežiūros įstaigų, tiek tarp visų Foxus naudotojų) realiai įgyvendinusi šią priemonę savo iniciatyva.

4) Pažymima, kad sprendimas įdiegti MFA nebuvo techniškai trivialus ir nepriklausė vien nuo Bendrovės valios – Foxus yra trečiosios šalies (UAB „Softdent“) kuriamas ir administruojamas produktas, todėl MFA funkcionalumo sukūrimas ir integravimas buvo išimtinai Foxus tiekėjo kompetencijos ir techninių pajėgumų klausimas. Jo įgyvendinimas reikalavo aktyvaus koordinavimo su sistemos tiekėju, techninių modifikacijų tiekėjo pusėje ir organizacinių pokyčių Bendrovės darbo procesuose. Nepaisant šios priklausomybės nuo trečiosios šalies, Bendrovė nurodo, jog šį žingsnį inicijavo ryžtingai ir operatyviai.

Bendrovė taip pat nurodo, kad po ADSP 1 slaptažodžių reikalavimai buvo sugriežtinti – slaptažodis, be kita ko, privalo būti ne trumpesnis nei 12 simbolių (iki ADSP 1 Foxus buvo įdiegtas funkcionalumas, pagal kurį reikalauta ne mažiau kaip 6 simbolių kombinacijos).

4.2. Dėl ADSP 2

Bendrovė pabrėžė, kad teorinė paveiktų duomenų subjektų riba (skaičiai) atspindi tik bendrą visų paveiktose sistemose tvarkomų duomenų subjektų skaičių ir jokiu būdu neatspindi faktinio poveikio apimties.

Vertindama ADSP 2 pobūdį, apimtį ir poveikį duomenų subjektams Bendrovė padarė išvadą, kad galimos neigiamos pasekmės duomenų subjektams išlieka išimtinai hipotetinės: pažeidimas buvo greitai suvaldytas, konfidencialumo ir vientisumo pažeidimo nenustatyta, nėra jokių indikacijų, kad asmens duomenys būtų buvę peržiūrėti, kopijuoti ar eksfiltruoti, paslaugos pacientams buvo teikiamos be pertrūkio naudojant alternatyvius šaltinius, o duomenų prieinamumas atkurtas tą pačią dieną. Bendrovė taip pat negavo jokių skundų ar kitų signalų iš pacientų, kurie reikštų realų poveikį jų teisėms ar laisvėms. Tai pat, kad Bendrovės pasirengimas reaguoti į ADSP ir turėtos techninės bei organizacinės priemonės leido ADSP 2 suvaldyti operatyviai ir veiksmingai apriboti jo pasekmes, todėl faktinis poveikis duomenų subjektams yra minimalus, o galimų neigiamų pasekmių rizika – žema.

Nepaisant to, Bendrovė pripažino, kad ADSP 2 metu privilegijuotų naudotojų prisijungimui per RDP nebuvo taikoma MFA, tačiau atkreipė dėmesį, kad po ADSP 1 Bendrovė įdiegė MFA Foxus išorinei prieigai – tai buvo tikslinė, operatyvi reakcija į ADSP 1. Bendrovė pažymėjo, kad sprendimas dėl MFA įdiegimo buvo planuotas organizacinis veiksmas, kurio Bendrovė iki ADSP 1 nespėjo įgyvendinti, tačiau ADSP 1 aplinkybės lėmė jo neatidėliotiną realizavimą. Tuo tarpu RDP infrastruktūra yra techniškai atskira sistema, kuriai MFA sprendimas nebuvo tiesiogiai taikomas.

Bendrovė pabrėžė, kad po ADSP 1 šią spragą pašalino radikaliai ir visapusiškai: MFA aktyvuota visoje organizacijos aplinkoje, apimant visus naudotojus; lygiagrečiai vykdomas strateginis perėjimas prie vieno prisijungimo sistemos (SSO)[15] architektūros.

[15] angl. Single Sign-On

Bendrovė taip pat pripažino, kad ADSP 2 metu nesankcionuotas veikėjas turėjo techninę galimybę pasiekti Sistemose saugomus asmens duomenis, tačiau šio fakto reikšmė turi būti vertinama atsižvelgiant į faktinę prieigos trukmę ir fizinę galimybę susipažinti su duomenimis. Visa nesankcionuota prieiga truko 70 minučių ir 30 sekundžių, tačiau šis laikotarpis apima visus veiksmus: pirminį prisijungimą, šoninį judėjimą tinkle, šifravimo įrankių įkėlimą ir jų vykdymą. Atsižvelgiant į tai, kad didžiąją šio laiko dalį užėmė šifravimo proceso vykdymas, o ne duomenų peržiūra, faktinis laikotarpis, per kurį nesankcionuotas veikėjas galėjo aktyviai susipažinti su asmens duomenimis, yra itin ribotas. Bendrovė padarė išvadą, kad per tokį trumpą laikotarpį fiziškai ir techniškai įmanoma susipažinti tik su itin riboto skaičiaus duomenų subjektų duomenimis. Net ir turint prieigą prie Sistemos, žmogus per kelias minutes gali peržiūrėti tik fragmentišką ir atsitiktinę duomenų dalį – tai reiškia, kad faktinis poveikio mastas yra nepalyginamai mažesnis nei maksimali teorinė riba, kurią atspindi bendras Sistemose saugomų duomenų subjektų skaičius.

Bendrovė taip pat kaip nereikšmingą įvertino prieinamumo praradimą, kadangi paslaugų teikimas pacientams nenutrūko ir nebuvo sulaukta nei vieno paciento ar kito duomenų subjekto skundo.

Reaguodama į Tikrinimo ataskaitoje 2 Inspekcijos padarytas išvadas, Bendrovė pastebėjo, kad Inspekcija negali konstatuoti BDAR 32 straipsnio pažeidimo vien remdamasi tuo, kad nebuvo laikytasi ISO/IEC 27002:2017 standarto atskirų papunkčių, nes ISO standarto laikymasis ar jo nesilaikymas pats savaime nereiškia BDAR pažeidimo. BDAR 32 straipsnis reikalauja tinkamų priemonių atsižvelgiant į riziką – tai yra lankstus, kontekstinis vertinimas, o ne mechaniškas ISO punktų taikymas.

5. Žodinio bylos nagrinėjimo metu gauti paaiškinimai

Žodinio bylos nagrinėjimo metu Bendrovė pateikė ADSP 1 chronologiją, atkreipė dėmesį, kokiame kontekste jis įvyko, kokios yra ADSP 1 platesnės aplinkybės, akcentuojant, kad:

1) Bendrovė mano (kokybiški *log* neišlikę), jog apie 80 proc. kortelių atvertė pati gydytoja (nes incidentas vyko darbo metu), t. y. nurodo, kad 63 yra maksimalus subjektų skaičius;

2) Bendrovė sureagavo itin greitai – MFA buvo įdiegtas per kelias dienas (2 d.) nuo sužinojimo apie ADSP 1, kas Bendrovės teigimu, rodo, jog su Foxus tiekėju apie tai (įdiegimą) jau buvo kalbėta kurį laiką, tačiau nespėta įgyvendinti laike;

3) Pažymima, kad incidentas įvyko išimtinai duomenų tvarkytojo infrastruktūroje, tačiau Bendrovės žiniomis, UAB „Softdent“ nebuvo įtrauktas, apklaustas, tyrimas jo atžvilgiu nebuvo pradėtas (nors duomenų tvarkytojui irgi taikomos pareigos pagal BDAR 32 straipsnį);

4) Bendrovė pažymi, kad produktas yra praktiškai vienintelis, sunkiai pakeičiamas rinkoje, todėl Bendrovė siekia, kad jis būtų saugus visam sveikatos priežiūros sektoriui.

Bendrovė pakartojo jau iki žodinio posėdžio pateiktą informaciją tiek dėl ADSP 1, tiek dėl ADSP 2, pabrėždama, kad nėra jokių įrodymų, kad paveikti duomenys būtų atskleisti kitiems nenustatytiems asmenims; taip pat akcentuodama savo aktyvumą diegiant naujas papildomas saugumo priemones po ADSP.

6. Bendrovės pateiktų papildomų[16] paaiškinimų vertinimas

Atkreiptinas dėmesys, kad Bendrovė po siūlymo skirti baudą pateikė papildomą informaciją, kurios nebuvo pateikusi iki jau minėtų Tikrinimo ataskaitų parengimo.

Papildoma informacija buvo įvertinta 2026-06-08 Inspekcijos Informacinių technologijų skyriaus tikrinimo Išvadoje dėl pateiktos informacijos (Inspekcijos reg. Nr. 4R-353 (2.14 E)) (toliau – Išvada).

6.1. Dėl Bendrovės iki ADSP 1 taikytos slaptažodžių politikos

[16] Po siūlymo skirti baudą ir žodinio posėdžio

Inspekcija Tikrinimo ataskaitoje 1 nurodė, kad darbuotojai prie Foxus jungėsi su slaptažodžiais, kurie buvo sudaryti iš ne mažiau kaip 8 simbolių, susidedantys iš raidžių ir skaičių, nenaudojant asmeninės informacijos.

Bendrovė papildomai nurodė, kad iki ADSP 1 buvo taikoma dokumentuota slaptažodžių politika, kurioje naudotojų slaptažodžiams buvo taikomas reikalavimas, kad slaptažodžiai būtų ne trumpesni nei 6 simboliai, turėtų bent po vieną skaičių, mažą ir didžiąją raides, specialų simbolį, o faktiškai buvo taikoma taisyklė dėl netrumpesnių kaip 8 simbolių slaptažodžių, kurie turėtų bent vieną raidę ir vieną skaičių.

Išvadoje pažymima, kad remiantis Gairių 86 punktu „Turi būti veikiantis autentifikavimo mechanizmas, leidžiantis prieigą prie IT sistemos (paremtas Prieigų kontrolės politika). Minimalus reikalavimas naudotojui prisijungti prie IT sistemos – naudotojo prisijungimo vardas ir slaptažodis. Slaptažodis sudaromas atsižvelgiant į tam tikrą kompleksiškumo lygį“ ir ISO standarto 5.17 papunkčiu „Autentiškumo patvirtinimo informacija“, kuriame nurodoma, kad „Autentiškumo patvirtinimo informacijos priskyrimas ir valdymas turėtų būti kontroliuojamas pagal valdymo procesą, įskaitant personalo konsultavimą dėl tinkamo autentiškumo patvirtinimo informacijos tvarkymo“. Duomenų valdytojas techninėmis ir organizacinėmis priemonėmis turi užtikrinti, jog sistemų naudotojų naudojami prisijungimo slaptažodžiai atitiktų reikiamą saugumo lygį ir tam tikrą kompleksiškumo lygį. Papildomai atkreipiamas dėmesys, kad remiantis Inspekcijos rekomendacija dėl saugių ir stiprių slaptažodžių naudojimo svarbos[17] slaptažodis atitinkantis tam tikrą kompleksiškumo lygį turi būti sudarytas iš ne mažiau nei 12 simbolių, naudojamos didžiosios ir mažosios raidės, skaičiai ir specialieji simboliai.

Atsižvelgiant į tai, kad Bendrovė dar kartą patvirtino ir neneigė, kad iki ADSP 1 buvo taikomi nepakankamo kompleksiškumo slaptažodžiai, Inspekcija daro išvadą, kad iki ADSP 1 darbuotojų prisijungimų prie Foxus slaptažodžiai neatitiko tinkamo kompleksiškumo lygio.

6.2. Dėl ADSP 2 trečiojo asmens neteisėto prisijungimo prie nenaudojamos administratoriaus paskyros

Inspekcija Tikrinimo ataskaitoje 2, remdamasi Bendrovės pateikta informacija, nurodė, kad prisijungimui buvo panaudota administratoriaus teises turėjusi domeno paskyra, o tai suteikė galimybę toliau pasiekti kitas vidines sistemas ir inicijuoti duomenų šifravimo veiksmus.

Bendrovė Rašte nurodė, kad *„Tyrimo analizė patvirtino, kad nesankcionuotas veikėjas pasinaudojo serverio [DUOMENYS NESKELBTINI] pasiekiama RDP paslauga ir prisijungė naudodamas domeno vartotojo [DUOMENYS NESKELBTINI] paskyrą. Ši paskyra buvo sukurta 2023 m. birželio 22 d., tačiau Klinikos IT komanda jos nenaudojo ir nepriskyrė teisėtų veikimo funkcijų. Kitaip tariant, atakos vektorius buvo neaktyvios administracinės paskyros išnaudojimas – tai aplinkybė, dėl kurios tokios paskyros egzistavimas iš esmės galėjo likti nepastebėtas taikant įprastines prieigos stebėsenos priemones.“* (tekstas nekoreguotas).

Atkreiptinas dėmesys, kad Aprašo XII skirsnyje „Prieigos valdymas ir kelių veiksnių tapatumo nustatymo priemonės“ 7 lentelės 65 punkte nurodyta, kad: „Nereikalingos ar nenaudojamos tinklų ir informacinių sistemų paskyros turi būti blokuojamos nedelsiant, bet ne vėliau kaip per kibernetinio saugumo subjekto nustatytą terminą ir ištrinamos praėjus žurnalinių įrašų saugojimo terminui (ne trumpiau kaip 90 kalendorinių dienų)“, taip pat 7 lentelės 73 punkte nurodyta, kad turi būti vykdoma administratorių paskyrų kontrolė: svarbiems kibernetinio saugumo subjektams privalo būti taikomas 73.1 papunktis „reguliariai, ne rečiau kaip kartą per metus, tikrinama, ar administratoriaus paskyros atitinka šiame skyriuje nustatytus reikalavimus, ir pranešama įgaliotam atsakingam asmeniui apie administratorių paskyras, kurios neatitinka šiame skirsnyje nustatytų reikalavimų.“, o esminiams – 73.2 papunktis „naudojamos administratorių paskyrų kontrolės priemonės, kurios periodiškai tikrina administratoriaus paskyras. Apie administratoriaus paskyras,

[17] https://vdai.lrv.lt/public/canonical/1734937137/678/Rekomendacija_del_slaptazodziu_2024.pdf

kurios neatitinka šiame skirsnyje nustatytų reikalavimų, turi būti pranešama įgaliotam asmeniui.“ ISO standarto 5.18 papunktyje „Prieigos teisės“ nurodyta, kad turi būti užtikrinama, kad prieigos teisės būtų panaikintos, kai jos tampa nebereikalingomis, taip pat ISO standarto 8.2 papunktyje „Privilegijuotos prieigos teisės“ nurodyta, kad reguliariai arba po tam tikrų pokyčių turi būti peržiūrimi naudotojai dirbantys su privilegijuotomis prieigos teisėmis. Gairių 18 punkte nurodyta, kad „Prieigos teisės turi būti panaikinamos kai nebereikia prieigos (pasikeitė veikla, pareigos) prie asmens duomenų“. Taip pat Gairių 20 punkte nurodyta, kad „Prieigos teisės (ypač privilegijuotosios prieigos teisės) turi būti peržiūrimos ne rečiau kaip kartą per metus.“ Atsižvelgiant į tai duomenų valdytojas privalo užtikrinti, kad nenaudojamos paskyros būtų nedelsiant blokuojamos, o visos, įskaitant ir privilegijuotos prieigos teisės būtų reguliariai, ne rečiau kaip kartą per metus, peržiūrimos.

Inspekcija pažymi, kad paskyra, prie kurios ADSP 2 metu neteisėtai prisijungė trečiasis asmuo, buvo sukurta 2023-06-22, o incidentas įvyko 2025-10-29, t. y. praėjus daugiau nei 2 metams nuo paskyros, turinčios privilegijuotas teises, sukūrimo, todėl darytina išvada, kad ADSP 2 būtų neįvykęs jei Bendrovė iki ADSP 2 būtų taikiusi MFA ar būtų įdiegusi prieigos ribojimus tik įgaliotiems asmenims (pavyzdžiui, pagal iš anksto nurodytus IP adresus ar tik iš tam tikrų LAN tinklų). Taip pat jei būtų tinkamai užtikrinusi prieigos kontrolę ir nedelsiant būtų blokavusi nenaudojamą Admin paskyrą ir vykdžiusi reguliarias prieigos teisių peržiūras, Bendrovė būtų galėjusi nustatyti, kad yra nenaudojama paskyra, turinti privilegijuotas prieigos teises, ir ją nedelsiant užblokuoti, o trečiasis asmuo nebūtų galėjęs neteisėtai prisijungti prie nenaudojamos administratoriaus paskyros ir įsilaužti į Bendrovės ADSP 2 metu paveiktas Sistemas.

Apibendrinant šios dalies 6.1 ir 6.2 papunkčiuose pateiktą informaciją, Išvadoje nustatyta, kad:

- Bendrovės papildomai pateikti paaiškinimai nepaneigė Tikrinimo ataskaitoje 1 ir Tikrinimo ataskaitoje 2 nustatytų BDAR 32 straipsnio 1 dalies b punkte nustatyto reikalavimo pažeidimų ADSP 1 ir ADSP 2 atžvilgiu ir nenaudotų techninių ir organizacinių priemonių, užtikrinančių pavojų atitinkančio lygio saugumo.
- Bendrovė iki ADSP 2 papildomai neužtikrino nenaudojamų paskyrų blokavimo ir reguliarių, ne rečiau kaip kartą per metus, vykdomų prieigos teisių peržiūrų, tuo pažeidė BDAR 32 straipsnio 1 dalies b punktą, Aprašo 7 lentelės 65 ir 73 punktų reikalavimus ir ISO standarto 5.18 ir 8.2 papunkčiuose nustatytų reikalavimų.
- Bent vienos iš Tikrinimo ataskaitoje 1 išvardintų priemonių[18] naudojimas būtų užkirtęs kelią įsilaužimui į Bendrovės ADSP 1 metu paveiktą sistemą.
- Bent vienos iš šioje Išvadoje ir Tikrinimo ataskaitoje 2 išvardintų priemonių[19] naudojimas, būtų užkirtęs kelią trečiojo asmens neteisėtam prisijungimui prie nenaudojamos paskyros ir įsilaužimui į Bendrovės ADSP 2 metu paveiktas Sistemas.

6.3. Vertinimo apibendrinimas

Inspekcija pažymi, kad Bendrovės argumentai dėl visuotinai taikomos praktikos nepaneigia Bendrovės, kaip savarankiško duomenų valdytojo, atsakomybės. Kitų rinkos dalyvių neveikimas ar žema sektoriaus branda neatleidžia konkretaus duomenų valdytojo nuo pareigos užtikrinti jo tvarkomų duomenų saugumą, ypač tvarkant sveikatos duomenis, kuriems taikomas aukščiausias apsaugos standartas.

Pagal BDAR 24 straipsnio 1 dalį, pareiga įgyvendinti tinkamas technines ir organizacines priemones yra numatyta būtent duomenų valdytojui, atitinkamai, duomenų valdytojas privalo

[18] Jei būtų naudojama MFA ar būtų įdiegtas prieigos ribojimas tik įgaliotiems asmenims (pavyzdžiui, pagal iš anksto nurodytus IP adresus ar tik iš tam tikrų LAN tinklų).

[19] Jei būtų naudojama MFA ar būtų įdiegtas prieigos ribojimas tik įgaliotiems asmenims (pavyzdžiui, pagal iš anksto nurodytus IP adresus ar tik iš tam tikrų LAN tinklų) arba būtų užtikrinama prieigos kontrolė, nedelsiant blokuojant nenaudojamas paskyras ir vykdant reguliarias prieigos teisių peržiūras.

kontroliuoti, kad priemonės būtų ne tik numatytos, bet ir realiai taikomos (įgyvendintos). Kartu pažymėtina, kad pagal BDAR 28 straipsnį, duomenų valdytojas pasitelkia tik tuos duomenų tvarkytojus, kurie pakankamai užtikrina, kad tinkamos techninės ir organizacinės priemonės bus įgyvendintos tokiu būdu, kad duomenų tvarkymas atitiktų šio reglamento reikalavimus ir būtų užtikrinta duomenų subjekto teisių apsauga.

Nagrinėjamu atveju, pagal Bendrovės paaiškinimus matyti, kad Bendrovei buvo žinoma, kad MFA Foxus nebuvo taikomas, tačiau ryžtingų veiksmų buvo imtasi tik po ADSP 1, t. y. per 2 dienas atliktas MFA įdiegimas (ir tik Bendrovei) rodo, kad techninių kliūčių nebuvo arba jos nebuvo esminės, o MFA galėjo būti įdiegtas atskirai tik Bendrovei (nepaisant kitų rinkos dalyvių, naudojančių Foxus, pasyvumo / nepritarimo), tačiau realus impulsas imtis priemonių atsirado tik įvykus incidentui.

Kartu pažymėtina, kad Bendrovės pažeidimų konstatavimas siejamas ne su konkrečiai MFA netaikymu, o su tinkamų saugumo priemonių (atsižvelgiant ir į kitas galimas alternatyvias priemones) netaikymu. Atkreiptinas dėmesys, kad net ir netaikant MFA, Bendrovė galėjo taikyti kitas saugumo priemones, pvz. įdiegti Foxus pasiekimo ribojimą pagal IP adresus ar iš vidinio Bendrovės tinklo, tačiau jo netaikė, taip pat slaptažodžiai neatitiko tinkamo kompleksiškumo lygio. Šių aplinkybių visuma parodo, kad duomenų valdytojas (Bendrovė), atsižvelgiant į Foxus tvarkomų asmens duomenų jautrumą, neužtikrino tinkamo šių duomenų saugumo (tą patvirtina ir įvykęs ADSP 1).

Bendrovė nurodė, kad Inspekcija negali konstatuoti BDAR 32 straipsnio pažeidimo vien remdamasi tuo, kad nebuvo laikytasi ISO/IEC 27002:2017 standarto atskirų papunkčių, nes ISO standarto laikymasis ar jo nesilaikymas pats savaime nereiškia BDAR pažeidimo. BDAR 32 straipsnis reikalauja tinkamų priemonių atsižvelgiant į riziką – tai yra lankstus, kontekstinis vertinimas, o ne mechaniškas ISO punktų taikymas.

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 valdytojas ir (ar) tvarkytojas, tai nereiškia, kad Inspekcijos Informacinių technologijų skyrius rengdamas Išvadą, taip pat Inspekcija, siūlydama 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 valdytojai ir tvarkytojai faktiškai negalėtų būti traukiami atsakomybėn už nepakankamų ar netinkamų saugumo priemonių taikymą, nors būtent BDAR 32 straipsnis aiškiai įtvirtina pareigą užtikrinti tinkamo 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.

Tikrinimų metu Bendrovė nepaneigė, kad:

(1) ADSP 1 įvyko dėl Bendrovėje 1 nepakankamai užtikrinamos prieigų kontrolės ir netinkamo autentifikavimo jungiantis prie Foxus, kai Bendrovės 1 darbuotojams jungiantis per išorinį tinklą (internetu) nebuvo taikomas kelių veiksnių autentifikavimas ir nebuvo įdiegtas prieigos apribojimas tik įgaliotiems asmenims, taip pat darbuotojų prisijungimų prie Foxus slaptažodžiai neatitiko tinkamo kompleksiškumo lygio.

(2) ADSP 2 įvyko dėl Bendrovėje nepakankamai užtikrinamos prieigų kontrolės ir netinkamo autentifikavimo, jungiantis prie paveikto Serverio, kai privilegijuotiems naudotojams jungiantis per išorinį tinklą (internetu) nėra taikomas kelių veiksnių autentifikavimas ir nebuvo įdiegtas prieigos apribojimas tik įgaliotiems asmenims.

7. Sprendimo skirti / neskirti administracinę baudą motyvai

Pagal BDAR 83 straipsnio 1 dalį, kiekviena 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, kokiu būdu priežiūros institucija sužinojo apie pažeidimą, visų pirma tai, ar duomenų valdytojas arba duomenų tvarkytojas pranešė apie pažeidimą (jei taip – kokiu 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.

BDAR konstatuojamosios dalies 129 punkte 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 taisomųjų 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 naudojamasi 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 konkretaus 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 konstatuojamosios dalies 148 punkte nurodyta, kad siekiant užtikrinti, kad šio reglamento taisyklės būtų geriau įgyvendinamos, už šio reglamento pažeidimus kartu su atitinkamomis priemonėmis, kurias priežiūros institucija nustatė pagal šį reglamentą, arba vietoj jų turėtų būti skiriamos sankcijos, įskaitant administracines baudas. Nedidelio pažeidimo atveju arba jeigu bauda, kuri gali būti skirta, sudarytų neproporcingą naštą fiziniam asmeniui, vietoj baudos gali būti pareikštas papeikimas. Vis dėlto reikėtų tinkamai atsižvelgti į pažeidimo pobūdį, sunkumą ir trukmę, tai, ar pažeidimas buvo tyčinis, veiksmus, kurių imtasi patirtai žalai sumažinti, atsakomybės

mastą arba į bet kokius svarbius ankstesnius pažeidimus, tai, kaip apie pažeidimą sužinojo priežiūros institucija, ar buvo laikomasi tam duomenų valdytojui arba duomenų tvarkytojui taikytų priemonių, ar buvo laikomasi elgesio kodekso, ir visus kitus sunkinančius ar švelninančius veiksnius. Sankcijos, įskaitant administracines baudas, turėtų būti skiriamos atsižvelgiant į atitinkamas procedūrines apsaugos priemones ir laikantis Sąjungos teisės ir Chartijos bendrųjų principų, įskaitant veiksmingą teisminę apsaugą ir tinkamą procesą.

Europos duomenų apsaugos valdyba (toliau – EDAV) 2023-05-24 yra priėmusi gaires 04/2022 dėl administracinių baudų apskaičiavimo pagal BDAR (toliau – Gairės dėl baudų), kuriose 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 atsakomybę sunkinančius arba švelninančius veiksnius, dėl kurių bauda gali padidėti arba sumažėti ir kurių nuoseklų išaiškinimą teikia EDAV.

Vertindama administracinės baudos skyrimo procedūros metu surinktą ir šiame sprendime pateiktą informaciją, sprendžiant skirti ar neskirti administracinę baudą Bendrovei bei sprendžiant dėl administracinės baudos dydžio, Inspekcija atsižvelgia į aktualius 83 straipsnio 2 dalyje pateikiamus aspektus.

7.1. BDAR 83 straipsnio 2 dalies a punktas – pažeidimo pobūdis, sunkumas ir trukmė, atsižvelgiant į atitinkamo duomenų tvarkymo pobūdį, aprėptį ar tikslą, taip pat į nukentėjusių duomenų subjektų skaičių ir jų patirtos žalos dydį

7.1.1. Bendrovės paaiškinimai

Bendrovė, teikdama paaiškinimus, BDAR 83 straipsnio 2 dalies a punkte nustatytą dalyką dar suskaidė į dvi dalis ir savo vertinimą pateikė pagal kiekvieną incidentą atskirai:

7.1.1.1. Pažeidimo pobūdis, sunkumas ir trukmė, atsižvelgiant į atitinkamo duomenų tvarkymo pobūdį, aprėptį ar tikslą:

(a) ADSP 1 - neteisėta prieiga truko nuo 2024-08-27 iki 2024-09-07 (12 dienų), tačiau faktinis nesankcionuotos prieigos mastas yra ženkliai mažesnis nei teorinis – prieiga vyko darbo valandomis, kai darbuotoja tuo pačiu metu teisėtai naudojosi sistema; duomenų eksfiltracija nenustatyta; prieita prie ribotos apimties pacientų vizitų duomenų;

(b) ADSP 2 - nesankcionuota prieiga truko 70 minučių ir 30 sekundžių; sistemos atkurtos per apytiksliai 5 val.; duomenų eksfiltracija nenustatyta; paslaugų teikimas nenutrūko; prieita prie ribotos apimties vizitų duomenų.

7.1.1.2. Nukentėjusių duomenų subjektų skaičius ir jų patirtos žalos dydis:

(a) ADSP 1 - paveiktų duomenų subjektų skaičius – 63 pacientai, yra maksimali teorinė riba, o ne faktinis nesankcionuotos prieigos mastas; šis skaičius apima tiek teisėtus, tiek neteisėtus prieigos epizodus, nes neteisėta prieiga vyko darbo valandomis, kai darbuotoja tuo pačiu metu teisėtai naudojosi sistema vykdydama įprastas profesines funkcijas; duomenų eksfiltracija, perdavimas ar platinimas nenustatyti; realios neigiamos pasekmės duomenų subjektams – finansinė žala, tapatybės vagystė ar kitas apčiuopiamas poveikis, tyrimo metu nenustatytos; Bendrovė nesulaukė nė vieno duomenų subjekto skundo ar pretenzijos, susijusios su šiuo incidentu;

(b) ADSP 2 - maksimalus teorinis paveiktų duomenų subjektų skaičius – apie 383 tūkst. pacientų ir apie 10 tūkst. darbuotojų, atspindi bendrą visų sistemose saugomų duomenų subjektų skaičių, o ne faktinį nesankcionuotos prieigos mastą. Šio skaičiaus negalima tapatinti su realiai paveiktų asmenų skaičiumi; duomenų eksfiltracija, perdavimas ar platinimas nenustatyti; realios neigiamos pasekmės duomenų subjektams – finansinė, moralinė ar kitokia apčiuopiama žala, nenustatytos; Klinika nei incidento metu, nei po jo nesulaukė nė vieno duomenų subjekto skundo, pretenzijos ar neigiamo atsiliepimo.

7.1.2. Inspekcijos vertinimas

*Pažeidimo pobūdis***.** Nustačius, kad Bendrovė įvykus abiem ADSP pažeidė ne tik BDAR 32 straipsnio 1 dalies b punktą, bet ir BDAR 5 straipsnio 1 dalies f punkte nustatytą konfidencialumo principą, už kurį gali būti skiriama maksimali bauda pagal BDAR 83 straipsnio 5 dalį, Bendrovės veiksmai pagal savo pobūdį priskirtini sunkesnių pažeidimų kategorijai.

Pažeidimo sunkumas ir trukmė. Gairėse dėl baudų nurodoma, kad pažeidimo sunkumas vertinamas pagal konkrečias aplinkybes ir tai apima tvarkymo pobūdį, taip pat aprėptį, tvarkymo tikslą, paveiktų duomenų subjektų skaičių ir žalos dydį.

Neteisėtu asmens duomenų tvarkymu sukelta žala nebūtinai turi būti materialinė. 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. Šiuo konkrečiu atveju Inspekcija neturi informacijos apie duomenų subjektų (pacientų ir Bendrovės darbuotojų) patirtą materialinę žalą, tačiau atsižvelgdama į tai, kad duomenų subjektų sveikatos duomenis galėjo peržiūrėti neteisėtai prisijungę tretieji asmenys, darytina išvada, kad duomenų subjektams (įskaitant pacientus) buvo užkirstas kelias kontroliuoti savo duomenis ir tai vertintina kaip nematerialinė žala.

Atsižvelgdama į aukščiau padarytą išvadą bei į tai, kad dėl ADSP 1 galėjo nukentėti dešimtys, o dėl ADSP 2 šimtai tūkstančių asmenų, Inspekcija sprendžia, kad tokia žala negali būti vertinama kaip mažareikšmė.

Nepaisant to, kad Patikrinimo 1 ir Patikrinimo 2 metu Bendrovė pateikė argumentus, kad Bendrovės pacientų ir darbuotojų asmens duomenys nebuvo atskleisti didesniam duomenų gavėjų skaičiui, Inspekcija sprendžia, kad atsižvelgiant į šiame papunktyje nustatytas aplinkybes, BDAR 83 straipsnio 2 dalies a punkte nurodytas veiksnys vertintinas kaip atsakomybę sunkinantis.

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

7.2.1. Bendrovės paaiškinimai

Bendrovė nurodė, kad abiem atvejais tyčios nebuvo. Kad abu ADSP kilo dėl išorinių, piktavališkų trečiųjų asmenų veiksmų – tikslinės *phishing* atakos (ADSP 1) ir *ransomware* atakos per RDP (ADSP 2). Klinikos veiksmai neturi sisteminio, pakartotinio ar organizacinio aplaidumo požymių. Iki incidentų Klinika taikė dokumentuotas technines ir organizacines priemones, vykdė periodinius darbuotojų mokymus, turėjo incidentų valdymo procedūras.

7.2.2. Inspekcijos vertinimas

Gairių dėl baudų 55 punkte nurodyta, kad „apskritai „tyčia“ reiškia, kad pažeidimas daromas apie jį žinant ir norint jį padaryti, o „netyčinis“ reiškia, kad nors duomenų valdytojas ar tvarkytojas pažeidė teisėje nustatytą rūpestingumo pareigą, jis pažeidimo padaryti neketino“.

Pagal Gaires dėl baudų, 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. EDAV pabrėžė, kad iš esmės pripažįstama, jog tyčiniai pažeidimai, „rodantys nepagarbą teisės aktų nuostatoms, yra sunkesni nei netyčiniai“. Tyčinio pažeidimo atveju tikėtina, kad priežiūros institucija šiam veiksniui suteiks daugiau svarbos. Atsižvelgdama į atvejo aplinkybes, priežiūros institucija taip pat gali suteikti svarbos aplaidumo laipsniui. Geriausiu atveju aplaidumas galėtų būti laikomas neutraliu veiksniu.

Nagrinėjamu atveju Bendrovės veiksmai vertintini kaip neutralūs, kadangi Inspekcija neturi pagrindo spręsti, kad abu ADSP įvyko dėl tyčios, tačiau daro išvadą, kad ADSP 2 įvyko dėl Bendrovės aplaidumo, kadangi nuo ADSP 1 iki ADSP 2 praėjo pakankamas laiko tarpas, kad Bendrovė sugebėtų (suspėtų) pašalinti ADSP 1 metu nustatytus pažeidimus.

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

7.3.1. Bendrovės paaiškinimai

Klinikos veiksmai suvaldant ADSP, teikiant pagalbą ir informaciją pacientams, duomenų subjektams, institucijoms buvo aktyvūs, konstruktyvūs, efektyvūs ir savalaikiai.

7.3.2. Inspekcijos vertinimas

Pagal BDAR nuostatas duomenų valdytojai privalo įgyvendinti technines ir organizacines priemones, kad užtikrintų pavojų atitinkantį saugumo lygį, tačiau to tinkamai nepadarius, atsakinga šalis turėtų imtis visų priemonių, kad sumažintų pažeidimo padarinius atitinkamam (-iems) asmeniui (ims). Pasirinkdama taisomąją priemonę ir apskaičiuodama skiriamą sankciją, priežiūros institucija turėtų atsižvelgti į duomenų valdytojo atsakingą elgesį (arba jo nebuvimą). Ši nuostata padeda įvertinti duomenų valdytojo atsakomybės dydį po to, kai įvyksta pažeidimas, ji gali būti taikoma tais atvejais, kai duomenų valdytojas akivaizdžiai būdamas neatsargus ir (arba) aplaidus, bet, sužinojęs apie pažeidimą, ėmėsi visų priemonių savo veiksmams ištaisyti.

Gairėse dėl baudų nurodyta, kad pažeidimo atveju duomenų valdytojas arba duomenų tvarkytojas turėtų „daryti viską, ką gali, kad sumažintų pažeidimo pasekmes atitinkamam (-iems) asmeniui (-ims)“. Tinkamų priemonių, skirtų duomenų subjektų patirtai žalai sumažinti, priėmimas gali būti laikomas švelninančiu veiksniu, dėl kurios baudos suma būtų sumažinta. Priimtos priemonės turi būti įvertintos visų pirma atsižvelgiant į savalaikiškumo elementą, t. y. laiką, kada duomenų valdytojas arba duomenų tvarkytojas jas įgyvendina, ir jų veiksmingumą. Šiuo požiūriu, labiau tikėtina, kad švelninančiu veiksniu 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.

Nagrinėjamu atveju Bendrovė, sužinojusi apie ADSP abiem atvejais ėmėsi aktyvių savalaikių veiksmų, kad duomenų subjektai nepatirtų arba patirtų kuo mažesnę žalą, todėl šis veiksnys vertintinas kaip švelninantis atsakomybę.

7.4. BDAR 83 straipsnio 2 dalies d punktas – duomenų valdytojo arba duomenų tvarkytojo atsakomybės dydį, atsižvelgiant į jų pagal 25 ir 32 straipsnius įgyvendintas technines ir organizacines priemones

7.4.1. Bendrovės paaiškinimai

Klinika nuo BDAR taikymo pradžios nuosekliai, nuolatos ir sistemingai įgyvendina BDAR 24, 25, 28, 32 ir kitus BDAR reikalavimus, nuosekliai investuoja į saugumo didinimą, pacientų duomenų saugumo didinimą, kt.

7.4.2. Inspekcijos vertinimas

BDAR 25 ir 32 straipsniai reglamentuoja duomenų valdytojo pareigą įgyvendinti tinkamas technines ir organizacines priemones, kad būtų užtikrintas pavojų atitinkančio lygio saugumas, tvarkant asmens duomenis.

Gairėse dėl baudų pažymima, kad atsižvelgiant į padidėjusį atskaitomybės lygį pagal BDAR, tikėtina, kad duomenų valdytojo arba duomenų tvarkytojo atsakomybės laipsnis bus laikomas sunkinančiu arba neutraliu veiksniu ir tik išskirtinėmis aplinkybėmis, kai duomenų valdytojas arba duomenų tvarkytojas viršys jiems nustatytas pareigas pagal BDAR 25 ir 32 straipsnius, tai bus laikoma atsakomybę švelninančiu veiksniu.

Inspekcija pažymi, kad, atsižvelgiant į Gairėse dėl baudų pateiktą išaiškinimą, taip pat ir į BDAR 25 ir 32 straipsnių reglamentavimą, duomenų valdytojas įgyvendinti tinkamas organizacines ir technines duomenų saugumo priemones privalo tiek prieš pradėdamas asmens duomenų tvarkymo veiksmus, tiek jau paties duomenų tvarkymo metu (atsižvelgdamas į techninių galimybių išsivystymo lygį, duomenų tvarkymo pobūdį, aprėptį, tikslus, nustatytą – išryškėjusią problematiką ir kt.).

Atsižvelgdama į tai, kad Tikrinimo metu nustatyti būtent BDAR 32 straipsnio pažeidimai, Inspekcija šio aspekto papildomai nevertina.

7.5. BDAR 83 straipsnio 2 dalies e punktas – ankstesni Bendrovės pažeidimai

7.5.1. Bendrovės paaiškinimai

Nebuvo tokių, kurie būtų susiję su vertinamais ADSP.

7.5.2. Inspekcijos vertinimas

Šis kriterijus skirtas pažeidimą padariusio subjekto reputacijai įvertinti. Gairėse dėl baudų nurodoma, kad ankstesnių pažeidimų buvimas gali būti laikomas sunkinančiu veiksniu, apskaičiuojant administracinę baudą. Atsižvelgiama į ankstesnių pažeidimų pobūdį ir dažnumą. Tačiau taip pat pažymima, kad ankstesnių pažeidimų nebuvimas negalėtų būti laikomas švelninančiu veiksniu, nes atitikimas BDAR yra norma ir ta aplinkybė, kad nėra ankstesnių pažeidimų, galėtų būti vertinama kaip neutrali.

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

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

7.6.1. Bendrovės paaiškinimai

Klinika, vykdydama BDAR nustatytas pareigas, apie ADSP informavo Inspekciją greičiau nei per 72 val., vėliau Inspekcijai teikė papildytą pranešimą, papildomus paaiškinimus, atsakymus ir informaciją. Klinika dėjo ir deda labai daug pastangų bendradarbiauti su Inspekcija, NKSC, o taip pat kitomis kompetentingomis institucijomis. Klinika ėmėsi būtinų ir pakankamų priemonių ADSP suvaldyti bei jų padariniams maksimaliai sušvelninti.

7.6.2. Inspekcijos vertinimas

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

Gairėse dėl baudų pažymima, kad įprastos bendradarbiavimo pareigos vykdymas turėtų būti laikomas kaip neutralus, o ne švelninantis, veiksnys.

Pažymėtina, kad ADSP tyrimų ir tikrinimų metu Bendrovė bendradarbiavo su Inspekcija, teikė prašomą informaciją, kaip tai numato BDAR, ir tokie Klinikos veiksmai vertintini kaip neutralus veiksnys.

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

7.7.1. Bendrovė paaiškinimų nepateikė

7.7.2. Inspekcijos vertinimas

Gairėse dėl baudų kaip vienas iš faktorių, apibūdinančių pažeidimo rimtumą, nurodomas reikalavimas atsižvelgti į asmens duomenų, kuriems pažeidimas turi poveikį, kategorijas (BDAR 83 straipsnio 2 dalies g punktas). Šių gairių 57 punkte yra paaiškinta, kad 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 veiksniui. 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.

Atsižvelgiant į tai, kad abu ADSP susiję su sveikatos duomenų tvarkymu, Inspekcija sprendžia, kad ši aplinkybė laikytina sunkinančiu veiksniu.

7.8. BDAR 83 straipsnio 2 dalies h punktas – Inspekcijos sužinojimas apie pažeidimą.

7.8.1. Bendrovės paaiškinimai

Klinikos pranešimai, pateikti laikantis BDAR 33 straipsnio reikalavimų ir sąlygų**.**

7.8.2. Inspekcijos vertinimas

Priežiūros institucija gali sužinoti apie pažeidimą atlikdama tyrimą, gavusi skundų, iš visuomenės informavimo priemonių, anoniminių pranešimų arba duomenų valdytojo pranešimo.

Gairėse dėl baudų 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 veiksniu.

Nagrinėjamu atveju įvykusį ADSP 1 pastebėjo ir apie jį visuomenės informavimo priemonėse pranešė žiniasklaidos atstovas, apie ADSP 2 - jau pranešė pati Bendrovė. Šį veiksnį Inspekcija vertina kaip neutralų.

7.9. BDAR 83 straipsnio 2 dalies i punktas – BDAR 58 straipsnio 2 dalyje nurodytų priemonių taikymas

7.9.1. Bendrovės paaiškinimai

Taikytos nebuvo.

7.9.2. Inspekcijos vertinimas

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 Bendrovei anksčiau taisomosios priemonės nebuvo taikytos, Inspekcija BDAR 83 straipsnio 2 dalies i punkte nurodyto veiksnio nevertina.

7.10. BDAR 83 straipsnio 2 dalies j punktas – taikomi elgesio kodeksai ar sertifikavimo mechanizmai

7.10.1. Bendrovė paaiškinimai

Nėra patvirtintų elgesio kodeksų, tačiau Klinika laikosi geryjų praktikų.

7.10.2. Inspekcijos vertinimas

Atsižvelgiant į tai, kad Bendrovės veiksmams nėra taikomi jokie elgesio kodeksai ar sertifikavimo mechanizmai, šis punktas nebus vertinamas.

7.11. BDAR 83 straipsnio 2 dalies k punktas – kiti atsakomybę švelninantys ar sunkinantys veiksniai

Kitų atsakomybę švelninančių ar sunkinančių veiksnių Bendrovė nenurodė ir Inspekcija nenustatė.

Apibendrindama šio sprendimo 4, 5, 6 ir 7 dalyse atliktą ADSP vertinimą, Inspekcija nusprendžia Bendrovei skirti administracinę baudą.

8. Dėl administracinės baudos dydžio

Gairių dėl baudų 48 punkte 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.

Atsižvelgdama į tai, jog Bendrovės padarytas pažeidimas pagal jo pobūdį priskirtinas BDAR 83 straipsnio 5 dalyje įtvirtintai pažeidimų kategorijai, už tokį pažeidimą skiriamos administracinės baudos iki 20 000 000 EUR arba, įmonės atveju – iki 4 % jos ankstesnių finansinių metų bendros metinės pasaulinės apyvartos, atsižvelgiant į tai, kuri suma yra didesnė.

Nagrinėjamu atveju Bendrovė pateikė UAB „Kardiolita“ 2024 finansinių metų bendrąją pasaulinę metinę apyvartą bei UAB „Inmedica“ 2025 finansinių metų bendrąją pasaulinę metinę apyvartą. Remiantis VĮ „Registrų centras“ duomenimis, Bendrovės teisių ir pareigų perėmėjas nuo 2025-06-25 yra UAB „InMedica“. Atitinkamai administracinė bauda bus skaičiuojama nuo UAB „InMedica“. 2025 finansinių metų bendrosios pasaulinės metinės apyvartos.

Gairėse dėl baudų 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). Remiantis veiksnių vertinimu, laikoma, kad pažeidimas yra i) mažo, ii) vidutinio arba iii) didelio sunkumo lygio. Šios kategorijos nedaro poveikio klausimui, ar galima skirti baudą.

Inspekcija nustatė, kad Bendrovės padaryti pažeidimai susiję su dideliu duomenų subjektų skaičiumi, dideliu kiekiu duomenų, įskaitant ir sveikatos duomenis, duomenų subjektams padaryta nematerialine žala, tačiau nenustatė, kad Bendrovė būtų veikusi tyčia, todėl sprendžia, kad Bendrovės padaryti pažeidimai yra priskiriami vidutinio sunkumo lygio pažeidimams ir tokiu atveju nustatomas pradinis baudos dydis atitinka nuo 10 iki 20 proc. taikomos maksimalios baudos sumos, t. y. nuo 20 000 000 EUR. Inspekcija, atsižvelgdama į šiame sprendime nustatytas aplinkybes, sprendžia, kad Bendrovei nustatomas 15 proc. pradinis baudos dydis nuo taikomos maksimalios 20 000 000 EUR sumos, t. y. 3 000 000 EUR (pradinis baudos dydis).

Gairėse dėl 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 100 mln. eurų, 250 mln. eurų ir 500 mln. eurų.

- Įmonėms, kurių metinė apyvarta 50–100 mln. EUR, priežiūros institucijos gali apsvarstyti galimybę atlikti skaičiavimus remiantis suma, patenkančia į 8–20 proc. nustatytos pradinės baudos sumos intervalą.

- Įmonėms, kurių metinė apyvarta 100–250 mln. EUR, priežiūros institucijos gali apsvarstyti galimybę atlikti skaičiavimus remiantis suma, patenkančia į 15–50 proc. nustatytos pradinės baudos sumos intervalą.

- Įmonėms, kurių metinė apyvarta 250–500 mln. EUR, priežiūros institucijos gali apsvarstyti galimybę atlikti skaičiavimus remiantis suma, patenkančia į 40–100 proc. nustatytos pradinės baudos sumos intervalą.

Nagrinėjamu atveju, pažymėtina, kad bauda skiriama Bendrovei, kurios 2025 finansinių metų metinė pasaulinė apyvarta sudarė 147 459 349 EUR, t. y. viršijo 100 000 000 EUR. Atsižvelgiant į šias nustatytas aplinkybes bei vadovaujantis Gairių dėl baudų išaiškinimais, nustatytam pradiniam baudos dydžiui (3 000 000 EUR) pritaikius 15 % koeficientą, minimali administracinė bauda yra 450 000 EUR.

Atsižvelgdama į šiame sprendime pateiktą informaciją bei teisinį reglamentavimą, Inspekcija sprendžia, kad Bendrovei skirtina administracinė bauda - 450 000 EUR - laikytina efektyvia, proporcinga ir atgrasančia.

Inspekcija, atsižvelgusi į tai, kas išdėstyta šiame sprendime bei vadovaudamasi BDAR 58 straipsnio 2 dalies i punktu, 83 straipsnio 1 ir 2 dalimis, 83 straipsnio 5 dalimi, ADTAĮ 34 straipsnio 10 dalimi,

n u s p r e n d ž i a:

1. Už šiame sprendime nustatytus BDAR 24 straipsnio 1 dalies, BDAR 32 straipsnio 1 dalies b punkto bei BDAR 5 straipsnio 1 dalies f punkto nuostatų pažeidimus Bendrovei skirti 450 000 EUR (keturi šimtai penkiasdešimt tūkstančių eurų) baudą.

2. Apie priimtą sprendimą informuoti Bendrovę.

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

Vadovaujantis ADTAĮ 35 straipsnio 1 dalimi, paskirta bauda ne vėliau kaip per tris mėnesius nuo baudos paskyrimo priėmimo dienos turi būti sumokėta į biudžeto pajamų surenkamąją sąskaitą[20] (įmokos kodas 6803, lėšų gavėjas Valstybinė mokesčių inspekcija prie Lietuvos Respublikos finansų ministerijos, juridinio asmens kodas 188659752).

Direktoriaus pavaduotoja,
pavaduojanti direktorių Danguolė Morkūnienė

[20] Nr. LT787290000000130151 (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)