



VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

SPRENDIMAS

2026 m. balandžio 8 d. Nr. 3R-592 (2.13-1.E)

Vilnius

Valstybinė duomenų apsaugos inspekcija (toliau – Inspekcija) 2024-05-13 gavo [DUOMENYS NESKELBTINI] (toliau – Pareiškėja) skundą (Inspekcijos reg. Nr. 1R-3180 (2.13.Mr)) ir 2024-05-20 skundo papildymą (Inspekcijos reg. Nr. 1R-3316 (2.13.Mr)) (toliau kartu – skundas) dėl galimai neteisėto jos sveikatos duomenų tvarkymo VŠĮ Šakių pirminės asmens sveikatos priežiūros centre (toliau – Įstaiga, Skundžiamas asmuo).

Pareiškėja nurodo, kad informacinėje sistemoje Foxus (toliau – Sistema) pastebėjo, jog prie jos paciento kortelės jungėsi su gydymo paslaugų teikimu nesusijusios Įstaigos darbuotojos – [DUOMENYS NESKELBTINI] (toliau – Darbuotoja1)¹ ir [DUOMENYS NESKELBTINI] (toliau – Darbuotoja2)² (toliau kartu – Darbuotojos). Pareiškėja taip pat nurodo, kad šiuo laikotarpiu ji dirbo Įstaigoje (gydytoja) ir kartu buvo Įstaigos pacientė. Pareiškėjos teigimu, Darbuotojos neturėjo sveikatos priežiūros specialisto kvalifikacijos ir neatliko funkcijų, susijusių su medicininės informacijos tvarkymu, neteisėtai jungėsi prie jos paciento kortelės ir turėjo galimybę susipažinti su jos sveikatos duomenimis (prisijungimai suteikė galimybę matyti diagnozes, tyrimų ir gydymo duomenis, nedarbingumo istoriją).

Pareiškėjos teigimu, pagal Įstaigoje nustatytą prieigos prie Sistemos tvarką, prie paciento sveikatos duomenų gali jungtis tik sveikatos priežiūros specialistai, teikiantys sveikatos priežiūros paslaugas paciento atžvilgiu. Pareiškėja prašo pripažinti, kad jos sveikatos duomenys buvo tvarkomi neteisėtai.

Inspekcija, išnagrinėjusi Pareiškėjos skundą pagal savo kompetenciją,

n u s t a t ė,

Skundžiamas asmuo 2024-06-13 atsakyme (Inspekcijos reg. Nr. 1R-3947 (2.13 Mr)) nurodė, kad Įstaiga su UAB „SOFTDENT“ yra sudariusi Sutartį³ dėl teisės naudoti Sistemą. Kartu su Sutartimi pasirašyta ir Asmens duomenų tvarkymo 2023-10-10 sutartis Nr. 2023_09/399DA. Sistema Įstaigoje naudojama tiek darbuotojų, tiek pacientų asmens duomenų tvarkymui. Sistemos administratore yra paskirta Darbuotoja1. Sistemos administratorius, kaip ir kiti su Sistema dirbantys darbuotojai (taip pat ir Darbuotoja2) yra pasirašę Sistemos naudotojo konfidencialumo pasižadėjimus, Sistema naudojama laikantis Nuostatų⁴, Asmens duomenų tvarkymo taisyklių⁵. Skundžiamas asmuo pažymėjo, kad Sistema yra sukonfigūruota taip, kad užėjus į asmens kortelę atsivėrusiame lange be

¹ Darbuotoja 1 jungėsi laikotarpiu - 2024-03-06; 2024-03-07; 2024-03-08; 2024-03-18.

² Darbuotoja 2 jungėsi laikotarpiu - 2024-03-07 ir 2024-03-22.

³ Skundžiamo asmens ir UAB „SOFTDENT“ 2023-10-10 sutartis Nr. 2023_10/339FX (toliau – Sutartis).

⁴ Informacinės sistemos Foxus duomenų saugos nuostatai, patvirtinti VŠĮ Šakių sveikatos priežiūros centro vyriausiojo gydytojo 2021 m. birželio 23 d. įsakymu Nr. V-66 (toliau – Nuostatai).

⁵ VŠĮ Šakių pirminės asmens sveikatos priežiūros centro asmens duomenų tvarkymo IS Foxus taisyklės, patvirtintos VŠĮ Šakių pirminės asmens sveikatos priežiūros centro vyriausiojo gydytojo 2021 m. birželio 21 d. įsakymu Nr. V-67 (toliau – Asmens duomenų tvarkymo Taisyklės).

asmens duomenų, tokių kaip vardas, pavardė, priskyrimas konkrečiam gydytojui ir pan., taip pat matomi įkelti dokumentai, receptai, prevencinės programos, kuriose pacientas dalyvauja, ir pan. Kai Įstaigos darbuotojas yra ir Įstaigos pacientas ar atlieka tam tikrus tyrimus Įstaigoje, darbuotojui taip pat suformuojami šie sveikatos duomenis atspindintys laukai. Užėjus į asmens kortelę iš karto pažymima, kad kortelėje buvo apsilankyta, tačiau Sistema neišskiria, kuri konkrečiai kortelės skiltis buvo peržiūrėta. Taip pat Sistemoje fiksuojami duomenų įvedimo, keitimo ir šalinimo veiksmai. Vien tai, kad buvo apsilankyta Sistemoje esančioje Pareiškėjos kortelėje, nereiškia, jog Darbuotojos susipažino su Pareiškėjos sveikatos duomenimis. Skundžiamas asmuo paaiškino, kad prieigos prie Sistemos darbuotojams yra suteikiamos pagal jų pareigas, t. y. prie Sistemos jungiasi tie darbuotojai, kuriems Sistema reikalinga tiesioginių darbo funkcijų vykdymo tikslais. Darbuotojos, vykdydamos joms pareiginiuose nuostatuose priskirtas darbo funkcijas, naudoja Sistemą tiesioginių darbo funkcijų vykdymo tikslu – Įstaigos kasos aparato, kuris susietas su Sistema, operacijų tikrinimui su informacija apie mokėjimus, darbuotojų grafikų sudarymui ir keitimui, užklausų atitinkamiems gydytojams persiuntimui ir kt. Darbuotojos į Pareiškėjos kortelę Sistemoje jungėsi tiesioginių darbo funkcijų vykdymo tikslais – nedarbingumo pažymėjimo galiojimo datos patikrinimui ir darbo grafikų sudarymui, darbuotojų informavimui, kasos operacijų sutikrinimui. Darbuotojos neturėjo jokio tikslo susipažinti su Pareiškėjos sveikatos duomenimis, o prisijungimas prie Sistemoje esančių Įstaigos darbuotojų ir (ar) pacientų kortelių yra būtinas įgyvendinant tiesiogines darbo funkcijas. Įstaigoje asmens duomenų tvarkymas griežtai reglamentuotas Asmens duomenų tvarkymo taisyklėse, visi Sistemą naudojančius darbuotojai supažindinti su Nuostatais, vedami veiklos įrašai. Darbuotojai supažindinti su jų darbo funkcijoms priskirtų asmens duomenų kategorijomis bei saugumo reikalavimais.

Kartu su atsakymu Skundžiamas asmuo pateikė Darbuotojų paaiškinimus.

Darbuotoja1 paaiškino, jog Sistemoje esančius duomenis (susijusius ne tik su pacientų sveikata, bet ir sveikatos priežiūros specialistų darbo grafikais, personalo duomenimis, mokėjimų bei kainyno informacija) tvarko kaip Sistemos administratorius. Pareiškėjos paciento kortelėje lankėsi, nes: 1) 2024-03-06 galimai ieškojo kito paciento su panašiu vardu ar pavarde; 2) 2024-03-07 norėjo pasitikslinti, ar Pareiškėjai nėra išduotas nedarbingumo pažymėjimas (Pareiškėja buvo užsiminusi, kad turės nedarbingumą), peržiūrėjo Pareiškėjos kortelės 025 formą. Jos (Darbuotojos1) viena iš funkcijų yra tvarkyti sveikatos priežiūros specialistų darbo grafikus ir reikėjo pasitikslinti informaciją apie nedarbingumą, kad gydytoja nebūtų registruojama grafike; 3) 2024-03-08 tikslinosi, ar Pareiškėja neprasitęsė nedarbingumo kitai savaitei; 4) 2024-03-18 reikėjo sutikrinti neatitikimus mokėjimuose (2024-03-14 buvo atliktas Pareiškėjos mokėjimas kortele už paslaugas).

Darbuotoja2 paaiškino, kad Pareiškėjos paciento kortelėje lankėsi, nes: 1) 2024-03-07 tikslinosi, kuriam laikui yra išduotas nedarbingumas, šią informaciją tikslinosi Sistemoje, nes joje jau tikrino kasos mokėjimus; 2) 2024-03-22 ieškojo nesutapimų tarp suformuotų mokėjimo ataskaitos duomenų ir kasos aparato duomenų.

Pareiškėja 2024-07-29 papildomai pateiktuose paaiškinimuose (Inspekcijos reg. Nr. 1R-4950 (2.13.Mr)) nurodė, kad 2022–2024 m. ji nebuvo supažindinta su Asmens duomenų tvarkymo taisyklėmis, tik po jos (Pareiškėjos) skundo Įstaiga ėmėsi priemonių įgyvendinti reikalavimus. Pareiškėja pateikė Sistemos ekrano kopijas, patvirtinančias, kad pagal įvestas pirmąsias vardo ir pavardės raides Sistema pateikia tik vieną rezultatą – Pareiškėją, todėl, Pareiškėjos teigimu, Darbuotojos1 argumentas dėl „galimai ieškojo kito paciento“, nepagrįstas. Pareiškėja pažymėjo, jog Darbuotojai1 buvo žinoma apie planuojamą nedarbingumą, todėl nebuvo būtina jungtis prie Pareiškėjos kortelės Sistemoje. Nors Darbuotojos nurodo, kad prie Pareiškėjos sveikatos duomenų jungėsi dėl mokėjimų sutikrinimo, tačiau ji (Pareiškėja) jokių mokėjimų 2024-03-18 neatliko, 2024-03-14 mokėjo už sūnui suteiktas paslaugas, tačiau sūnaus kortelėje nei

mokėjimo, nei kitą dieną apsilankyta nebuvo. Pareiškėja pažymi, kad Sistemoje prisijungus prie paciento kortelės iš karto yra matomi paciento demografiniai duomenys, visų diagnozių sąrašas, o po jomis, jei yra aktyvus, nedarbingumo pažymėjimas su aiškiu TLK-10-AM kodu. Pareiškėja pabrėžia, kad Įstaiga, palikdama galimybę [DUOMENYS NESKELBTINI] ir [DUOMENYS NESKELBTINI] tikrinti darbuotojo ligos diagnozes ir duomenis apie sveikatą, neįgyvendino tinkamos prieigos kontrolės.

Dėl sveikatos duomenų tvarkymo teisėtumo

Asmens duomenų tvarkymą reglamentuoja BDAR⁶ ir ADTAI⁷. Pagal šiuos teisės aktus asmens duomenų tvarkymas laikomas teisėtu tik jei jis atitinka BDAR 5 straipsnyje nustatytus su asmens duomenų tvarkymu susijusius principus bei yra pagrįstas bent viena teisėto asmens duomenų tvarkymo sąlyga, numatyta BDAR 6 straipsnyje, ir BDAR 6 ir 9 straipsniuose, kai tvarkomi specialiu kategorijų asmens duomenys.

BDAR 4 straipsnio 2 punkte nustatyta, kad duomenų tvarkymas – 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 15 punkte nustatyta, kad sveikatos duomenys – 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.

Skundo nagrinėjimo metu iš Pareiškėjos pateiktų Sistemos momentinių ekrano nuotraukų ir Darbuotojų paaiškinimų nustatyta, jog Įstaiga (Įstaigos Darbuotojos) laikotarpiu nuo 2024-03-06 iki 2024-03-22 šešis kartus prisijungė prie Pareiškėjos kortelės Sistemoje, kurių metu buvo peržiūrėta Pareiškėjos ambulatorinio gydymo statistinė kortelė (forma Nr. 025/a⁸) (kurioje, be kita ko, nurodoma informacija apie asmens diagnozes, gydytojų įrašus, apsilankymus gydymo įstaigoje, intervencijas, paskirtus vaistus), informacija apie išduotą nedarbingumą ir kt., taigi prisijungimų metu buvo tvarkomi Pareiškėjos sveikatos duomenys – su jais buvo susipažinta.

Taip pat, nors Įstaiga nurodo, kad vien tai, jog buvo apsilankyta Sistemoje esančioje Pareiškėjos kortelėje nereiškia, kad Darbuotojos susipažino su Pareiškėjos sveikatos duomenimis, tačiau, Inspekcija pažymi, kad atsižvelgiant į aukščiau nurodytus Darbuotojų pateiktus paaiškinimus neabejotinai nustatyta, kad buvo ne tik prisijungta prie Pareiškėjos kortelės, tačiau ir susipažinta su joje esančiais sveikatos duomenimis. Šioje vietoje pažymėtina ir tai, kad net jeigu Darbuotojos nebūtų susipažinę su konkrečiais Pareiškėjos sveikatos duomenimis (ambulatorinio gydymo statistine kortele ir kt.), Sistemoje atlikus Pareiškėjos duomenų paiešką buvo gauti rezultatai, kuriuose, be kita ko, yra ir Pareiškėjos sveikatos duomenys, taigi, pagal BDAR 4 straipsnio 2 punkte pateiktą duomenų tvarkymo apibrėžtį, atlikti paieškos pagal Pareiškėją veiksmai laikyti Pareiškėjos sveikatos duomenų išgava, t. y. sveikatos duomenų tvarkymu.

BDAR 6 straipsnio 1 dalyje nustatyta, kad duomenų tvarkymas yra teisėtas tik tuo atveju, jeigu taikoma bent viena iš a–f punktuose nurodytų sąlygų.

⁶ 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).

⁷ Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (toliau – ADTAI) .

⁸ Forma Nr. 025/a-LK, patvirtinta Lietuvos Respublikos sveikatos apsaugos ministro 1998 m. lapkričio 26 d. įsakymu Nr. 687 (Lietuvos Respublikos sveikatos apsaugos ministro 2023 m. birželio 13 d. įsakymo Nr. V-671 redakcija).

BDAR 9 straipsnio 1 dalyje nustatyta, kad draudžiama tvarkyti asmens duomenis, atskleidžiančius rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus ar narysę profesinėse sąjungose, taip pat tvarkyti genetinius duomenis, biometrinius duomenis, siekiant konkrečiai nustatyti fizinio asmens tapatybę, sveikatos duomenis arba duomenis apie fizinio asmens lytinį gyvenimą ir lytinę orientaciją. Šio straipsnio 2 dalyje nustatyti atvejai, kada BDAR 9 straipsnio 1 dalyje nustatytas draudimas netaikomas.

Skundžiamas asmuo Pareiškėjos asmens duomenų tvarkymą (prisijungimą prie kortelės Sistemoje) grindžia tuo, kad Darbuotojoms buvo būtina prisijungti prie Pareiškėjos duomenų Sistemoje atliekant tiesiogines darbo funkcijas – Įstaigos kasos aparato, kuris susietas su Sistema, operacijų tikrinimui apie mokėjimus, nedarbingumo pažymėjimo galiojimo datos patikrinimui ir darbuotojų grafikų sudarymui. Konkrečių BDAR 6 straipsnio 1 dalies ir 9 straipsnio 2 dalies nuostatų, kuriomis remiantis buvo tvarkomi (tikrinami Sistemoje esančioje paciento kortelėje) Pareiškėjos asmens duomenys, Skundžiamas asmuo nenurodė.

Nors Skundžiamas asmuo nurodo, kad buvo būtina prisijungti prie Pareiškėjos kortelės Sistemoje tam, kad patikrinti išduoto nedarbingumo galiojimo datą, tačiau, Inspekcijos vertinimu, tam, kad darbdavys (šiuo atveju Skundžiamas asmuo) gautų informaciją apie Pareiškėjai išduotą nedarbingumą, kad galėtų planuoti darbo grafiką, nebuvo būtina jungtis prie Sistemoje esančios Pareiškėjos kortelės. Šią informaciją Skundžiamas asmuo, pirmiausia, galėjo gauti iš pačios Pareiškėjos (Pareiškėjos teigimu, ji ir buvo informavusi apie planuojamą nedarbingumą), taip pat informaciją apie darbuotojui išduotą nedarbingumą darbdaviui teikia Valstybinio socialinio draudimo fondo valdyba prie Socialinės apsaugos ir darbo ministerijos. Atkreiptinas dėmesys, kad Darbuotoja2 paaiškinime nurodė, jog informaciją apie Pareiškėjai išduotą nedarbingumą pasirinko tikrinti Sistemoje dėl darbo optimizavimo, kadangi joje jau tikrino kasos mokėjimus, kas patvirtina, jog Pareiškėjos duomenų (informacijos apie nedarbingumą) tvarkymas Sistemoje, kurioje yra tvarkomi itin jautrūs Pareiškėjos duomenys, buvo Darbuotojos2 pasirinkimas ir tokio būtinumo priežastys buvo susijusios tik su Skundžiamo asmens Darbuotojos2 patogumu.

Taip pat, Inspekcijos vertinimu, Skundžiamas asmuo neįrodė, kad buvo būtina jungtis prie Pareiškėjos kortelės sistemoje, siekiant sutikrinti kasos operacijas. Skundžiamas asmuo nepateikė jokios informacijos ir įrodymų, patvirtinančių, kad Įstaigoje buvo nustatyti nesutapimai, susiję su Pareiškėjos mokėjimais, tik Darbuotoja1 savo paaiškinime nurodė, jog Pareiškėja 2024-03-14 atliko mokėjimą kortele ir dėl to galimai buvo tikrinama informacija. Pažymėtina, kad Pareiškėja Inspekcijai nurodė, jog 2024-03-14 ji mokėjo už sūnui suteiktas paslaugas, tačiau sūnaus kortelėje lankomasi nebuvo, kas, Inspekcijos vertinimu, paneigia Skundžiamo asmens paaiškinimus dėl Pareiškėjos duomenų tvarkymo sistemoje, siekiant sutikrinti operacijas.

Be to, nors Skundžiamo asmens pateiktame Darbuotojos1 paaiškinime nurodyta, kad Sistemoje esančius duomenis (susijusius ne tik su pacientų sveikata, bet ir sveikatos priežiūros specialistų darbo grafikais, personalo duomenimis, mokėjimų bei kainyno informacija) ji (Darbuotoja1) tvarko kaip Sistemos administratorius, tačiau iš Nuostatų matyti, kad Sistemos administratoriaus funkcijos ir atsakomybė yra tinkamas Sistemos funkcionavimas, naudotojų pasirengimo dirbti su Sistema vertinimas ir teisių naudotis Sistema suteikimas, vartotojų registravimosi prie Sistemos posistemės E.pacientas.lt priežiūra, pasiūlymų dėl Sistemos palaikymo ir priežiūros teikimas, Sistemą sudarančių komponentų administravimas, saugos įgaliojinių informavimas apie saugos incidentus (Nuostatų 8 punktą). Nors Darbuotoja1 yra paskirta Sistemos administratore ir dėl to turi prieigą prie visų Sistemoje esančių duomenų, tačiau tai nereiškia, kad šiuos (visus) duomenis tvarkyti (su jais susipažinti) turi teisę vykdydama kitas savo, ne kaip Sistemos administratoriaus, funkcijas (sudarant darbuotojų grafikus, tikrinant mokėjimus).

Atsižvelgiant į tai, kas nurodyta, Skundžiamo asmens teiginiai, jog buvo būtina 2024-03-06–2024-03-22 jungtis prie Sistemoje esančios Pareiškėjos kortelės ir tvarkyti joje esančius sveikatos duomenis Darbuotojoms atliekant tiesiogines darbo funkcijas, vertinti kaip deklaratyvūs ir neįrodyti,

Inspekcija sprendžia, jog Skundžiamas asmuo neįrodė, kad nagrinėjamu atveju Pareiškėjos asmens duomenys buvo tvarkomi (tikrinami Sistemoje esančioje paciento kortelėje) egzistuojant teisėto asmens duomenų tvarkymo sąlygoms, įtvirtintoms BDAR 6 straipsnio 1 dalyje ir BDAR 9 straipsnio 2 dalyje, taigi duomenys buvo tvarkomi neteisėtai ir Skundžiamas asmuo pažeidė BDAR 5 straipsnio 1 dalies a punkte įtvirtintą teisėtumo principą, BDAR 6 straipsnio 1 dalį ir 9 straipsnio 2 dalį.

Dėl techninių ir organizacinių priemonių taikymo

BDAR 24 straipsnio 1 dalyje nustatyta, kad 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.

BDAR 32 straipsnio 4 dalyje nustatyta, kad duomenų valdytojas ir duomenų tvarkytojas imasi priemonių, siekdami užtikrinti, kad bet kuris duomenų valdytojui arba duomenų tvarkytojui pavaldus fizinis asmuo, galintis susipažinti su asmens duomenimis, jų netvarkytų, išskyrus atvejus, kai duomenų valdytojas duoda nurodymus juos tvarkyti, nebent tas asmuo privalo tai daryti pagal Sąjungos arba valstybės narės teisę.

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“, LST ISO/IEC 27002:2022 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo kontrolės priemonės“ 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 (toliau – VDAI gairės)⁹ duomenų valdytojams ir duomenų tvarkytojams.

Pagal LST EN ISO/IEC 27002:2023¹⁰ 5.15 punktą įstaiga turi dokumentuoti tvarką, skirtą kontroliuoti fizinę ir loginę prieigą prie asmens duomenų ar kito susijusio turto.

Pagal VDAI gaires kiekvienam vaidmeniui, susijusiam su asmens duomenų tvarkymu, turi būti priskirtos konkrečios prieigos kontrolės teisės, vadovaujantis principu „būtina žinoti“ (angl. *need to know*). Prieigų valdymo politikoje organizacija turėtų nustatyti atitinkamas prieigos kontrolės taisykles, prieigos teises ir apribojimus pagal konkrečias naudotojų pareigas, susijusias su asmens duomenų tvarkymo procesais ir procedūromis.

Skundžiamas asmuo atsakyme Inspekcijai nurodė, kad prieigos prie Sistemos darbuotojams suteikiamos pagal jų pareigas, Darbuotojos Pareiškėjos kortelėje Sistemoje lankėsi tiesioginių darbo funkcijų tikslais, pateikė [DUOMENYS NESKELBTINI] pareiginius nuostatus¹¹, [DUOMENYS

⁹ Prie VDAI gairėse nurodytų priemonių yra pateikiamos nuorodos į susijusį informacijos saugumo valdymo standarto LST ISO/IEC 27001:2017 reikalavimą ir jį papildantį privatumo užtikrinimo reikalavimą pagal ISO/IEC 27701:2019.

¹⁰ Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo kontrolės priemonės (ISO/IEC 27002:2023) (toliau – ISO/IEC 27002:2023).

¹¹ Šakių pirminės asmens sveikatos priežiūros centro [DUOMENYS NESKELBTINI] pareiginiai nuostatai, patvirtinti VŠĮ Šakių pirminės asmens sveikatos priežiūros centro direktoriaus 2024 m. birželio 3 d. įsakymu Nr. V-54 (toliau – [DUOMENYS NESKELBTINI] pareiginiai nuostatai).

NESKELBTINI] pareiginius nuostatus¹², Darbuotojų pasirašytus Sistemos naudotojo konfidencialumo pasižadėjimus. Inspekcija pažymi, kad nors [DUOMENYS NESKELBTINI] pareiginiai nuostatai numato, jog [DUOMENYS NESKELBTINI] funkcijos yra sudaryti darbuotojų darbo grafikus, informuoti personalą apie nedarbingumą ir kt., o [DUOMENYS NESKELBTINI] pareiginiai nuostatai numato, kad [DUOMENYS NESKELBTINI] funkcijos yra tikrinti kasos aparato (mokėjimų) duomenis per Sistemą ir kt., tačiau tai nereiškia, kad šioms funkcijoms atlikti Darbuotojoms turi būti suteikta prieiga prie pacientų sveikatos duomenų. Taip pat Skundžiamo asmens nurodyta aplinkybė, kad Darbuotojos yra pasirašiusios konfidencialumo pasižadėjimus, savaime nesuteikia teisės tvarkyti sveikatos duomenų, minėti pasižadėjimai nustato pareigą saugoti duomenis, bet nėra pagrindas tvarkyti Sistemoje esančius sveikatos duomenis.

Skundo nagrinėjimo metu nustatyta, kad Darbuotojos Pareiškėjos asmens duomenis Sistemoje tvarkė (tikrino) neteisėtai (žr. šio sprendimo dalį „Dėl sveikatos duomenų tvarkymo teisėtumo“), Skundžiamas asmuo nepateikė informacijos ir įrodymų, patvirtinančių, kad Įstaigos administracinėms funkcijoms atlikti būtina tvarkyti Sistemoje esančius pacientų (Pareiškėjos) sveikatos duomenis, priešingai, iš Skundžiamo asmens Pareiškėjai pateikto 2024-05-13 rašto Nr. S-(4.10)-152 matyti, kad Skundžiamas asmuo pats nurodė, jog atliekant Pareiškėjos tarnybinio pranešimo tyrimą pastebėta, jog kai kurios darbuotojų funkcijos Sistemoje dubliuojasi (paslaugų ir mokėjimų sutikrinimas) ir prisijungimai prie Sistemos nėra būtini ir prisijungimas Darbuotojai² bus panaikintas.

Skundžiamas asmuo kartu su atsakymu pateikė Nuostatus, iš kurių matyti, kad Įstaigoje yra apibrėžti su asmens duomenų tvarkymu Sistemoje susiję vaidmenys ir atsakomybės, taip pat, kad naudotojams – Skundžiamo asmens darbuotojams yra priskiriamos tik tos Sistemos sritys, kurios priklauso pagal darbo sritį (Nuostatų 9 punktą), tačiau nepateikė jokių įrodymų, patvirtinančių, kad Įstaigoje yra konkrečiai apibrėžta, kokios konkrečios prieigos yra būtinos kiekvienam vaidmeniui, susijusiam su asmens duomenų tvarkymu.

Atsižvelgiant į tai, kas nurodyta, Inspekcija sprendžia, kad Skundžiamas asmuo suteikė prieigą Darbuotojoms prie pacientų sveikatos duomenų, kurie nėra būtini jų funkcijoms (darbuotų grafikų sudarymui, nedarbingumo, kasos aparatų duomenų tikrinimui ir kt.) atlikti, t. y. neužtikrino, kad jam pavaldus fizinis asmuo, galintis susipažinti su asmens duomenimis, jų netvarkytų, ir tokiu būdu netinkamai įgyvendino BDAR 24 straipsnio 1 dalies ir 32 straipsnio 4 dalies reikalavimus ir Pareiškėjos skundas šioje dalyje pripažįstamas pagrįstu.

Dėl poveikio priemonių

BDAR preambulės 129 punkte numatyta, jog kiekviena priežiūros institucijos taikoma priemonė turi būti tinkama, būtina ir proporcinga siekiant užtikrinti šio reglamento laikymąsi, atsižvelgiant į kiekvieno konkretaus atvejo aplinkybes.

Sprendžiant dėl poveikio priemonių skyrimo Skundžiamam asmeniui Inspekcija atsižvelgia į tai, jog Inspekcija neturi duomenų, kad Skundžiamas asmuo ne pirmą kartą pažeidė BDAR 5 straipsnio 1 dalies a punkto, BDAR 6 straipsnio 1 dalies, 9 straipsnio 2 dalies, 24 straipsnio 1 dalies ir 32 straipsnio 4 dalies nuostatas. Atsižvelgiant į tai, kas nurodyta, Skundžiamam asmeniui, vadovaujantis BDAR 58 straipsnio 2 dalies b punktu, už BDAR 5 straipsnio 1 dalies a punkto, 6 straipsnio 1 dalies, 9 straipsnio 2 dalies nuostatų pažeidimus pareiškiamas papeikimas, o už BDAR 24 straipsnio 1 dalies ir 32 straipsnio 1 dalies 4 dalies nuostatų pažeidimus teikiama nurodymai apibrėžti / reglamentuoti su asmens duomenų tvarkymu susijusius vaidmenis ir atsakomybes bei

¹² Šakių pirminės asmens sveikatos priežiūros centro [DUOMENYS NESKELBTINI]pareiginiai nuostatai, patvirtinti VŠĮ Šakių pirminės asmens sveikatos priežiūros centro direktoriaus 2024 m. birželio 3 d. įsakymu Nr. V-54 (toliau – [DUOMENYS NESKELBTINI] pareiginiai nuostatai).

prieigų valdymo politiką ir užtikrinti, kad prieiga prie Sistemoje esančių asmens duomenų būtų suteikta tik tiems darbuotojams, kuriems tokia prieiga būtina jų darbo funkcijoms vykdyti.

Inspekcija, vadovaudamasi ADTAJ 31 straipsnio 1 dalies 1 punktu, 2 dalies 1 punktu, BDAR 58 straipsnio 2 dalies b ir d punktais,

n u s p r e n d ž i a:

1. Pareiškėjos skundą pripažinti pagrįstu.
2. Skundžiamam asmeniui už BDAR 5 straipsnio 1 dalies a punkto, 6 straipsnio 1 dalies, 9 straipsnio 2 dalies nuostatų pažeidimus pareikšti papeikimą.
3. Skundžiamam asmeniui už BDAR 24 straipsnio 1 dalies ir 32 straipsnio 1 dalies 4 dalies nuostatų pažeidimus teikti nurodymus:
 - 3.1. apibrėžti / reglamentuoti su asmens duomenų tvarkymu susijusius vaidmenis ir atsakomybes bei prieigų valdymo politiką;
 - 3.2. užtikrinti, kad prieiga prie Sistemoje esančių asmens duomenų būtų suteikta tik tiems darbuotojams, kuriems tokia prieiga būtina jų darbo funkcijoms vykdyti;
 - 3.3. apie nurodymų įvykdymą raštu informuoti Inspekciją iki 2026-05-18¹³;
4. Apie priimtą sprendimą informuoti Pareiškėją ir Skundžiamą 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).

Direktorė

Dijana Šinkūnienė

¹³ Inspekcija paaiškina, kad jeigu bus nustatyta, kad nurodymas nebuvo įgyvendintas, tuomet tai bus laikoma Inspekcijos nurodymo nevykdymu ir atitinkamai už tai bus taikoma atsakomybė.