ISSN 1392-6195 (print)
ISSN 2029-2058 (online)
JURISPRUDENCIJA
JURISPRUDENCE
2020, 27(2), p. 370–388.

# ASMENS DUOMENŲ TVARKYMO YPATUMAI NUOTOLINIU BŪDU TEIKIANT PASLAUGAS SVEIKATOS PRIEŽIŪROS SRITYJE[1]

**Rūta Lazauskaitė**
Mykolo Romerio universiteto Teisės mokyklos Privatinės teisės institutas
Elektroninis paštas rlazauskaite@mruni.eu

**Daiva Tamulionienė**
Valstybinė duomenų apsaugos inspekcija
Elektroninis paštas daiva.tamulioniene@ada.lt

Pateikta 2020 m. rugsėjo 8 d., parengta spaudai 2020 m. lapkričio 16 d.

DOI: 10.13165/JUR-20-27-2-07

***Santrauka.*** *Pasaulyje išplitus COVID-19 virusui nuotolinis darbas ir paslaugų teikimas tapo įprastas daugelyje veiklos sričių, įskaitant ir sveikatos priežiūros sektorių. Lietuvos Respublikos Vyriausybei nuo 2020 m. kovo 16 d. paskelbus karantiną ir įvedus judėjimo bei veiklos apribojimus, buvo patvirtintos rekomendacijos tiek viešojo, tiek privataus sektoriaus subjektams organizuoti darbą ir aptarnauti klientus nuotoliniu būdu, išskyrus atvejus, kai būtina atitinkamas funkcijas atlikti darbo vietoje. Teikiant sveikatos priežiūros paslaugas nuotoliniu būdu pagrindiniu iššūkiu tampa tinkamas duomenų subjekto (paciento) identifikavimas. Sėkmingam Bendrojo duomenų apsaugos reglamento principų, o ypač duomenų kiekio mažinimo ir skaidrumo principų, įgyvendinimui esminę reikšmę turi kokybiška teisėkūra ir kvalifikuoti duomenų apsaugos pareigūnai, nepaisant to, kokiu būdu (nuotoliniu ar*

1 Šis straipsnis finansuojamas pagal Europos Sąjungos Teisių, lygybės ir pilietiškumo programą (2014–2020 m.).

*pacientui fiziškai atvykus į sveikatos priežiūros įstaigą) teikiamos sveikatos priežiūros paslaugos.*

***Reikšminiai žodžiai:*** *sveikatos priežiūros įstaiga, asmens duomenų tvarkymo pagrindai, asmens duomenų tvarkymo principai, duomenų valdytojas, duomenų apsaugos pareigūnas.*

## Įvadas

Asmens duomenų tvarkymas teikiant sveikatos priežiūros paslaugas visuomet kėlė iššūkius, turint omenyje asmens duomenų, tvarkomų teikiant šias paslaugas, jautrumą. Klausimų, į kuriuos teks ieškoti atsakymų asmens duomenų apsaugos specialistams, matyt, kils nuolat, atsižvelgiant į tendenciją skaitmeninti teikiamų sveikatos priežiūros paslaugų procesą.

Tyrimo objektas yra asmens sveikatos duomenų tvarkymo ypatumai teikiant sveikatos priežiūros paslaugas nuotoliniu būdu. Siekiama nustatyti, ar teikiant sveikatos priežiūros paslaugas nuotoliniu būdu yra papildomų iššūkių, susijusių su asmens duomenų tvarkymo atitikties 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamente (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)[2] ir kituose teisės aktuose įtvirtintiems reikalavimams užtikrinimu.

Svarbiausi tyrimo metodai yra lyginamasis ir sisteminis. Norint nustatyti asmens sveikatos duomenų tvarkymo ypatumus teikiant sveikatos priežiūros paslaugas nuotoliniu būdu, neišvengiamai turi būti palyginti asmens duomenų tvarkymo teikiant šias paslaugas nuotoliniu būdu ir jas teikiant asmeniui atvykus į sveikatos priežiūros įstaigą reikalavimai. Sisteminis metodas taikomas tiriant asmens duomenų tvarkymui teikiant sveikatos priežiūros paslaugas nuotoliniu būdu kaip vienu iš sveikatos priežiūros paslaugų teikimo būdų keliamus reikalavimus. Analizuojant medžiagą ir darant išvadas naudoti loginis ir analizės metodai.

Tiriamos problemos aktualumas. Pasaulyje išplitus COVID-19 virusui nuotolinis darbas ir paslaugų teikimas tapo įprastas daugelyje veiklos sričių, įskaitant ir sveikatos priežiūros sektorių. Lietuvos Respublikos Vyriausybei 2020 m. kovo 14 d. nutarimu Nr. 207[3] „Dėl karantino Lietuvos Respublikoje paskelbimo“ nuo 2020 m. kovo 16 d. paskelbus karantiną ir įvedus judėjimo bei veiklos apribojimus

2 „Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. 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)“, [2016] OL L119/1, žiūrėta 2020 m. balandžio 15 d., https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=PT.

3 „Lietuvos Respublikos Vyriausybės 2002 m. kovo 14 d. nutarimas Nr. 207 „Dėl karantino Lietuvos Respublikos teritorijoje paskelbimo““, *TAR*, 2020-03-14, Nr. 5466, žiūrėta 2020 m. balandžio 15 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/deaf8694663011eaa02cacf2a861120c/asr.

buvo patvirtintos rekomendacijos tiek viešojo, tiek privataus sektoriaus subjektams organizuoti darbą ir aptarnauti klientus nuotoliniu būdu, išskyrus atvejus, kai būtina atitinkamas funkcijas atlikti darbo vietoje. Asmens sveikatos priežiūros paslaugų teikimo nuotoliniu būdu galimybė detalizuota 2020 m. kovo 16 d. Lietuvos Respublikos sveikatos apsaugos ministro-Valstybės lygio ekstremaliosios situacijos valstybės operacijų vadovo sprendimu Nr. V-387[4] „Dėl asmens sveikatos priežiūros paslaugų teikimo organizavimo paskelbus karantiną Lietuvos Respublikos teritorijoje“ (toliau – Sprendimas). Pažymėtina, kad Sprendimo 1.3.3 punktu nustatyta, jog organizuojant ambulatorines asmens sveikatos priežiūros paslaugas **prioritetas teikiamas nuotoliniam** ambulatorinių asmens sveikatos priežiūros **paslaugų teikimo būdui**, o sveikatos priežiūros paslauga, esant tiesioginiam kontaktui su pacientu, gali būti teikiama tik tuomet, kai dėl šios paslaugos specifikos jos neįmanoma suteikti nuotoliniu būdu. Taigi ši precedento neturinti COVID-19 pandemijos sukelta situacija daugelį sektorių, įskaitant ir sveikatos priežiūros, privertė prisitaikyti prie naujų veiklos sąlygų ir pereiti prie nuotolinio darbo, nepaisant praeityje buvusių abejonių ar neryžtingumo imtis telemedicinos taikymo. Kadangi teikdamos asmens sveikatos priežiūros paslaugas nuotoliniu būdu sveikatos priežiūros įstaigos susiduria su naujais iššūkiais užtikrindamos tinkamą jautrių asmens duomenų tvarkymą ir apsaugą, būtina ištirti ir išanalizuoti asmens sveikatos duomenų tvarkymo ypatumus teikiant sveikatos priežiūros paslaugas nuotoliniu būdu.

Užsienio mokslinėse publikacijose buvo nagrinėti telemedicinos teisinio reguliavimo aspektai, tačiau asmens duomenų apsaugos klausimų analizei daug dėmesio neskirta. A. Gusarova[5] 2012 m. publikacijoje Latvijos nacionalinių teisės aktų kontekste aptaria kai kuriuos duomenų apsaugos klausimus (daugiausia dėmesio skirdama paciento sutikimo klausimui) telemedicinos srityje dar iki BDAR priėmimo, t. y. Europos Parlamento ir Tarybos direktyvos (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (toliau – Direktyva 95/46/EB). V. L. Raposo[6] 2016 m. straipsnyje analizuoja telemedicinos teisinį reguliavimą (arba jo trūkumą) Europoje, tačiau tik glaustai apžvelgia kai kuriuos su sveikatos duomenų tvarkymu susijusius klausimus (pvz., paciento su-

4 „Lietuvos Respublikos sveikatos apsaugos ministro-valstybės lygio ekstremaliosios situacijos valstybės operacijų vadovo 2020 m. kovo 16 d. sprendimas Nr. V-387 „Dėl asmens sveikatos priežiūros paslaugų teikimo organizavimo paskelbus karantiną Lietuvos Respublikos teritorijoje““, *TAR*, 2020-03-17, Nr. 5561, žiūrėta 2020 m. balandžio 15 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f770372267a611eaa02cacf2a861120c/wpIAbWjrRc?jfwid=9tq147qgh.

5 Agnese Gusarova, „Data Protection in Telemedicine“ (SHS Web of Conferences. Volume 2, 2012. 3rd International Interdisciplinary Scientific Conference Society. Health. Welfare – 1st Congress of Rehabilitation Doctors of Latvia) 1–7, žiūrėta 2020 m. spalio 27 d., https://www.shs-conferences.org/articles/shsconf/pdf/2012/02/shsconf_shw2010_00013.pdf.

6 Vera Lucia Raposo, „Telemedicine: The legal framework (or the lack of it) in Europe“, *GMS Health Technology Assessment* 12 (2016): 1–12, žiūrėta 2020 m. spalio 27 d., https://www.egms.de/static/en/journals/hta/2016-12/hta000126.shtml.

tikimą kaip jo duomenų tvarkymo pagrindą, paciento kaip duomenų subjekto teises, duomenų perdavimą į trečiąsias šalis) Direktyvos 95/46/EB bei BDAR projekto kontekste. J. Vidal-Alaball, R. Acosta-Roja, N. Pastor Hernández ir kt.[7] 2020 m. publikacijoje nagrinėja telemedicinos iššūkius ir galimybes COVID-19 pandemijos metu lakoniškai aptardami galimas duomenų saugumo rizikas. Kadangi asmens sveikatos duomenų tvarkymo ypatumai teikiant sveikatos priežiūros paslaugas nuotoliniu būdu teisės doktrinoje iš esmės nėra tirti, svarbiausi tyrime naudoti šaltiniai yra Valstybinės duomenų apsaugos inspekcijos (toliau – VDAI) praktika ir metodiniai dokumentai, 29 straipsnio darbo grupės dokumentai, teismų praktika ir teisės aktai.

## 1. Sveikatos duomenų sąvoka ir šių duomenų tvarkymo pagrindai

Pagal BDAR, teikiant sveikatos priežiūros paslaugas asmens duomenys gali būti tvarkomi tik esant bent vienai iš teisėto duomenų tvarkymo sąlygų, kurios įtvirtintos BDAR 6 straipsnyje. Kadangi sveikatos priežiūros paslaugų teikimas visuomet bus susijęs su sveikatos duomenų[8], kurie laikomi specialių kategorijų asmens duomenimis, tvarkymu, sveikatos priežiūros įstaigos šiems asmens duomenims tvarkyti papildomai turi taikyti BDAR 9 straipsnio 2 dalyje įtvirtintas išimtis. Pažymėtina, kad 29 straipsnio darbo grupė 2015 m. vasario 5 d. rašte Europos Komisijai dėl *mHealth*[9] paaiškino, kad sveikatos duomenys turėtų būti suprantami daug plačiau nei mediciniai duomenys. Remiantis susiklosčiusia duomenų apsaugos teisės aktų taikymo įvairiose ES valstybėse praktika, su asmens sveikata susijusiais duomenimis laikytina net ir tokia informacija, kaip asmens intelektiniai ir emociniai gebėjimai bei savybės (pvz., intelekto koeficientas), asmens fizinės savybės (pvz., svoris, ūgis), faktas, kad asmuo susilaužė kojį (pvz., *Lindqvist* byla[10]), kad asmuo nešioja akinius ar kontaktinius lęšius, informacija apie rūkymo ir alkoholio vartojimo įpročius, duomenys apie alergijas, kurie gali būti atskleisti tiek privatiems subjektams (pvz., oro linijų bendrovei), tiek valstybinėms įstaigoms (pvz., mokyklai); asmens narystė pacientų palaikymo grupėje (pvz., paramos sergantiems vėžiu grupėje), anoniminių alkoholikų, grupinės psichoterapijos ar kitose savigalbos ir paramos grupėse, keliančiose su sveikata

7 Josep Vidal-Alaball ir kt., „Telemedicine in the face of the COVID-19 pandemic“, *Atencion Primaria* 52, 6 (2020): 418–422, žiūrėta 2020 m. spalio 27 d., https://www.elsevier.es/es-revista-atencion-primaria-27-pdf-S0212656720301268.

8 Remiantis BDAR 4 straipsnio 15 punktu, sveikatos duomenys yra „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“.

9 „29 straipsnio darbo grupės 2015 m. vasario 5 d. raštas Europos Komisijai dėl mHealth“, žiūrėta 2020 m. birželio 30 d., https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf.

10 „Byla C-101/01, *Criminal proceedings against Bodil Lindqvist* [2003]“, ECLI:EU:C:2003:596, žiūrėta 2020 m. birželio 30 d., http://curia.europa.eu/juris/documents.jsf?critereEcli=ECLI:EU:C:2003:596.

susijusius tikslus; net ir informacija (naudotina darbo santykių srityje) apie tai, kad asmuo serga, lankėsi ar nesilankė sveikatos priežiūros įstaigoje[11]. Taigi sveikatos duomenimis laikytini asmens duomenys, kurie a) aiškiai yra medicininiai duomenys; b) prietaisais ar jutikliais gauti duomenys (nors ir dar neapdoroti), kuriuos galima naudoti atskirai arba kartu su kitais duomenimis, norint padaryti išvadą apie faktinę asmens sveikatos būklę ar pavojų jo sveikatai; c) daromos išvados apie asmens sveikatos būklę ar pavojų sveikatai (nepriklausomai nuo to, ar šios išvados yra tikslios / netikslios, teisėtos / neteisėtos ir pan.).

Praktikoje pacientų sveikatos duomenų tvarkymo teisėtumui pagrįsti dažniausiai sveikatos priežiūros įstaigos remiasi vienu ar keliais BDAR 6 straipsnio 1 dalies a (paciento sutikimas), b (sutartinė prievolė), c (teisinė prievolė) arba d (gyvybiniai asmens interesai) punktais bei vienu ar keliais 9 straipsnio 2 dalies a (paciento sutikimas), c (gyvybiniai asmens interesai), h (sveikatos priežiūros paslaugų teikimas) bei i (viešasis interesas visuomenės sveikatos srityje) punktais. Šie paminėti asmens duomenų tvarkymo pagrindai taikytini ne tik teikiant sveikatos priežiūros paslaugas esant tiesioginiam kontaktui su pacientu, t. y. jam atvykus į gydymo įstaigą asmeniškai, bet ir aptarnaujant pacientą nuotoliniu būdu. „Taigi, sveikatos priežiūros įstaigos neturėtų papildomai ieškoti, kokiomis asmens duomenų tvarkymo sąlygomis galėtų būti grįstas asmens duomenų tvarkymas, teikiant paslaugas nuotoliniu būdu“[12]. Tiesa, gali būti situacijų, kai pacientas norės gauti sveikatos priežiūros paslaugas tik įprastinėmis priemonėmis, o ne nuotoliniu būdu (pvz., pacientas gali atsisakyti naudotis nuotoliniu būdu teikiamomis sveikatos priežiūros paslaugomis dėl moralinių ar religinių priežasčių)[13]. Tad tais atvejais, kai paciento duomenys tvarkomi jo sutikimo

11 Pavyzdžiui, vieno iš VDAI pateiktų skundų dėl sveikatos priežiūros įstaigos pareiškėjo darbdaviui (statutinei tarnybai) pateiktos informacijos apie pareiškėjo (ne)atvykimą į sveikatos priežiūros įstaigą tyrimo metu VDAI padarė išvadą, jog informacija, kad pareiškėjas lankėsi ar nesilankė gydymosi įstaigoje, laikytina ypatingais pareiškėjo asmens duomenimis (Asmens duomenų teisinės apsaugos įstatymo kontekste) ir konfidencialia informacija (Pacientų teisių ir žalos sveikatai atlyginimo įstatymo kontekste), o darbdavio veiksmai renkant šią informaciją iš paties pareiškėjo bei iš sveikatos priežiūros įstaigos laikytini ypatingų pareiškėjo asmens duomenų tvarkymu. Nors šiuo atveju buvo nustatyta, kad tiek darbdavys, tiek sveikatos priežiūros įstaiga pareiškėjo ypatingus asmens duomenis (informaciją apie lankymąsi (nesilankymą) sveikatos priežiūros įstaigoje) rinko bei tvarkė teisėtai, remiantis tuo metu galiojusios Asmens duomenų teisinės apsaugos įstatymo redakcijos 5 straipsnio 2 dalies 2 punktu (t. y. dėl to, kad toks tvarkymas yra būtinas darbo ar valstybės tarnybos tikslais duomenų valdytojo teisėms ir prievolėms darbo teisės srityje įgyvendinti įstatymų nustatytais atvejais), VDAI sveikatos priežiūros įstaigai pateikė nurodymą „užtikrinti, kad informacija apie pacientą valstybės institucijoms, kurioms Lietuvos Respublikos įstatymai suteikia teisę gauti konfidencialią informaciją apie pacientą, būtų suteikiama tik rašytiniu jų prašymu, kuriame nurodomas konfidencialios informacijos prašymo pagrindas, jos naudojimo tikslai ir reikalingos informacijos mastas“.

12 „Valstybinės duomenų apsaugos inspekcijos 2020 m. gegužės 18 d. Rekomendacijos dėl asmens duomenų apsaugos aspektų, teikiant sveikatos priežiūros paslaugas nuotoliniu būdu“, žiūrėta 2020 m. birželio 30 d., https://vdai.lrv.lt/uploads/vdai/documents/files/Pacientu%20konsultavimas%20nuotoliniu%20budu%202020-05-19.pdf.

13 Gusarova, *supra note*, 4, 5.

pagrindu, aiškus paciento sutikimas, kad jo duomenys būtų tvarkomi ir jam gaunant sveikatos priežiūros paslaugas nuotoliniu būdu, turi būti gaunamas iš anksto.

## 2. Duomenų tvarkymo principai

### 2.1. Duomenų kiekio mažinimo principo įgyvendinimas

Sveikatos priežiūros paslaugų teikėjas, kaip ir bet kuris kitas asmens duomenų valdytojas, tvarkydamas asmens duomenis turi laikytis BDAR 5 straipsnyje įtvirtintų principų[14]: teisėtumo, sąžiningumo ir skaidrumo, tikslo apribojimo, duomenų kiekio mažinimo, tikslumo, saugojimo trukmės apribojimo, vientisumo ir konfidencialumo bei atskaitomybės. Vis dėlto, kaip matyti iš praktikos, kai kurių iš šių principų pažeidimų sveikatos priežiūros įstaigų veikloje pasitaiko dažniau. Jeigu dėl, pavyzdžiui, saugojimo trukmės apribojimo principo laikymosi didelių problemų nekyla, nes kai kurie konkretūs asmens duomenų saugojimo terminai numatyti teisės aktuose (pavyzdžiui, Lietuvos Respublikos sveikatos ministro įsakyme „Dėl Lietuvos Respublikos sveikatos apsaugos ministro 1999 m. lapkričio 29 d. įsakymo Nr. 515 „Dėl sveikatos priežiūros įstaigų veiklos apskaitos ir atskaitomybės tvarkos“ pakeitimo“[15]), tai su duomenų kiekio mažinimo principo nesilaikymu susiduriama gana dažnai. Remiantis BDAR 5 straipsnio 1 dalies c punktu, duomenų kiekio mažinimo principas reiškia, kad asmens duomenys turi būti adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie tvarkomi, t. y. duomenų valdytojai savo veikloje turi siekti surinkti kuo mažiau duomenų apie kiekvieną asmenį ir rinkti tik tokius duomenis, kurių reikia, kad būtų tinkamai įgyvendinti jų tvarkymo tikslai. Praktikoje neretai pasitaiko, kai sveikatos priežiūros specialistai prašo pacientų pateikti informaciją, kuri nesusijusi su teikiamomis sveikatos priežiūros paslaugomis ir yra perteklinė. Pavyzdžiui, prieš teikiant burnos higienos paslaugas odontologijos klinikoje prašoma nurodyti profesiją ar darbovietę, nors teikiama sveikatos priežiūros paslauga nėra susijusi nei su profesinės ligos gydymu, nei su darbo vietos specifika. Tokios situacijos, kai sveikatos priežiūros įstaigos renka perteklinius pacientų duomenis, neretai susiklosto ir dėl to, jog kompetentingos valdžios institucijos yra patvirtinusios sveikatos priežiūros specialistams privalomas pildyti formas, kuriose būtent ir nurodyta rinkti duomenis, nelaikytinus būtinais tinkamam sveikatos priežiūros paslaugų suteikimui. Vienas iš tokių pavyzdžių yra 2016 m. spalio 7 d. Lietuvos Respublikos sveikatos apsaugos ministro įsakymu Nr. V-1149 „Dėl privalomų akušerijos,

14 Christopher F. Mondschein ir Cosimo Monda, „The EU's General Data Protection Regulation (GDPR) in a Research Context“, iš *Fundamentals of Clinical Data Science*, Kubben P., Dumontier M., Dekker A. (eds) (Cham: Springer, 2019), 51–77, žiūrėta 2020 m. birželio 30 d., https://doi.org/10.1007/978-3-319-99713-1_5.

15 „Lietuvos Respublikos sveikatos apsaugos ministro 1999 m. lapkričio 29 d. įsakymas Nr. 515 „Dėl sveikatos priežiūros įstaigų veiklos apskaitos ir atskaitomybės tvarkos““, *Valstybės žinios*, 1999, Nr. 103-2972.

ginekologijos ir neonatologijos sveikatos statistikos apskaitos formų patvirtinimo“[16] patvirtintos formos Nr. 010-1-1/a „Nėščiosios ir naujagimio kortelė“, Nr. 010-2-1/a „Nėščiosios ir negyvagimio kortelė“, Nr. 025-113/a „Nėščiosios kortelė“, Nr. 096/a „Nėštumo ir gimdymo istorija“, Nr. 097/a „Naujagimio raidos istorija“, kuriose tarp rinktinų duomenų nurodyta ne tik nėščiosios / motinos išsilavinimas bei šeiminė padėtis, bet ir jos tautybė. Ir nors informacijos apie išsilavinimą bei šeiminę padėtį rinkimą būtų galima pateisinti statistiniais tikslais, tai duomenų apie tautybę rinkimui pateisinimą rasti sunku, juo labiau kad BDAR 89 straipsnio 1 dalyje pabrėžiamas siekis užtikrinti duomenų kiekio mažinimo principo laikymąsi net ir tais atvejais, kai asmens duomenys tvarkomi archyvavimo tikslais viešojo intereso labui, mokslinių ar istorinių tyrimų arba statistiniais tikslais. Tiesa, šios publikacijos rengimo metu minėtos privalomos akušerijos, ginekologijos ir neonatologijos sveikatos statistikos apskaitos formos buvo pakeistos iš privalomų surinkti duomenų sąrašo pašalinant duomenis apie tautybę, išsilavinimą, šeiminę padėtį ir socialinį draustumą[17].

Pažymėtina, kad Europos Sąjungai nėra suteikta kompetencija visiškai suderinti asmens duomenų apsaugos reguliavimą sveikatos ir mokslinių tyrimų srityje[18], nes tai palikta reguliuoti nacionaliniams įstatymams. Vis dėlto Lietuva nėra pasinaudojusi BDAR 89 straipsnio 2 dalyje nustatyta galimybe nacionaliniuose teisės aktuose įtvirtinti nukrypti leidžiančias nuostatas, susijusias su duomenų subjektų teisėmis, nurodytomis BDAR 15 (teisė susipažinti su duomenimis), 16 (teisė reikalauti ištaisyti duomenis), 18 (teisė apriboti duomenų tvarkymą) ir 21 (teisė nesutikti) straipsniuose. Taigi, nors teisės aktai numato prievolę tvarkyti tam tikrus asmens duomenis, tačiau iš nacionalinių teisės aktų nėra aišku, kodėl būtent tokia apimtimi yra tvarkomi asmens duomenys, o esant tokiam neaiškumui kyla abejonių, ar įgyvendinamas duomenų kiekio mažinimo principas. Atkreiptinas dėmesys, kad nacionaliniais teisės aktais siekiant įtvirtinti prievolę tvarkyti asmens duomenis būtina atsižvelgti į BDAR tokiems teisės aktams keliamus reikalavimus, kaip antai nurodyti tokių asmens duomenų tvarkymo tikslą, išdėstyti konkrečias nuostatas pagal šį reglamentą taikomų taisyklių pritaikymui, įskaitant bendrąsias sąlygas, reglamentuojančias duomenų valdytojo atliekamo duomenų tvarkymo teisėtumą, tvarkytinų duomenų rūšis, atitinkamus duomenų sub-

16 „Lietuvos Respublikos sveikatos apsaugos ministro 2016 m. spalio 7 d. įsakymas Nr. V-1149 „Dėl privalomų akušerijos, ginekologijos ir neonatologijos sveikatos statistikos apskaitos formų patvirtinimo““, *TAR*, 2016-10-17, Nr. 0, žiūrėta 2020 m. balandžio 15 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/285d2e718fa511e68adcda1bb2f432d1?jfwid=8qkvwlctc.

17 „Lietuvos Respublikos sveikatos apsaugos ministro 2020 m. gegužės 5 d. įsakymas Nr. V-1065 „Dėl Lietuvos Respublikos sveikatos apsaugos ministro 2016 m. spalio 7 d. įsakymo Nr. V-1149 „Dėl privalomų akušerijos, ginekologijos ir neonatologijos sveikatos statistikos apskaitos formų patvirtinimo“ pakeitimo“, *TAR*, 2020-05-06, Nr. 9598, žiūrėta 2020 m. birželio 30 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/540d35a18f5711eaa51db668f0092944.

18 Gauthier Chassang, „The impact of the EU general data protection regulation on scientific research“, *Ecancermedicalscience* 11 (2017): 709, žiūrėta 2020 m. balandžio 15 d., https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5243137/.

jektus, subjektus, kuriems asmens duomenys gali būti atskleisti, ir tikslus, dėl kurių asmens duomenys gali būti atskleisti, tikslo apribojimo principą, saugojimo laikotarpius ir duomenų tvarkymo operacijas bei duomenų tvarkymo procedūras, įskaitant priemones, kuriomis būtų užtikrintas teisėtas ir sąžiningas duomenų tvarkymas, kaip antai tas, kurios skirtos kitiems specialiems IX skyriuje numatytiems duomenų tvarkymo atvejams (BDAR 6 straipsnio 3 dalis). Be to, toks teisės aktas turi atitikti ir specialius reikalavimus, įtvirtintus BDAR 9 straipsnio 2 dalyje atitinkamame punkte, atsižvelgiant į taikytiną išimtį, pavyzdžiui, taikant BDAR 9 straipsnio 2 dalies i punkte numatytą išimtį, teisės akte turi būti numatomos tinkamos ir konkrečios priemonės duomenų subjekto teisėms ir laisvėms apsaugoti, visų pirma profesinė paslaptis. Teisės akte įtvirtinant išimtį, leidžiančią sveikatos duomenis tvarkyti moksliniais tikslais (BDAR 9 straipsnio 2 dalies h punktas), be kita ko, pabrėžiamas būtinumas įvertinti tokio tvarkymo proporcingumą tikslui, kurio siekiama, bei imperatyvus reikalavimas nepažeisti esminių teisės į duomenų apsaugą nuostatų. Taigi teisės akto kokybė ir jo atitiktis BDAR įtvirtintiems reikalavimams galėtų prisidėti prie didesnio visuomenės užtikrintumo dėl BDAR nuostatų laikymosi ir jų privatumo gerbimo, kartu ir sveikatos priežiūros įstaigų, kaip duomenų valdytojų, darbuotojams, turintiems pareigą tvarkyti asmens duomenis, būtų kur kas lengviau paaiškinti pacientams, kodėl vienų ar kitų asmens duomenų yra prašoma. Į aspektus, kuriuos būtina įvertinti teisėkūros procese, dėmesį jau pačioje BDAR taikymo pradžioje yra atkreipusi ir VDAI[19].

Tad nacionaliniams teisės aktams esant nepakankamai aiškiems, pačios sveikatos priežiūros įstaigos, kaip duomenų valdytojai, turi ne tik tiksliai apsibrėžti, kokius pacientų duomenis joms būtina tvarkyti (pavyzdžiui, siekiant tinkamai suteikti sveikatos priežiūros paslaugas arba vykdant kompetentingų valdžios institucijų numatytą pareigą rinkti statistinę informaciją), bet ir aiškiai nustatyti, kurie duomenys kokiam tikslui yra renkami. Apie tai turi būti aiškiai informuojami ir įstaigos darbuotojai, dirbantys su pacientais, kad kiekvienu konkrečiu atveju jie galėtų pacientui paaiškinti, kokiu tikslu renkami vieni ar kiti asmens duomenys, išaiškinti teisę nesutikti su tokių duomenų tvarkymu bei atskleisti, kokios būtų tokių duomenų nepateikimo pasekmės.

Pažymėtina, kad kai kuriose Europos Sąjungos valstybėse narėse duomenų kiekio mažinimo principas aiškinamas plačiau, t. y. kaip susijęs ne tik su tam tikram tikslui surinktų ir saugomų duomenų kiekiu, bet ir su neribotos prieigos prie duomenų suteikimu per dideliam vartotojų skaičiui. Būtent tokios pozicijos laikėsi Portugalijos Nacionalinė duomenų apsaugos komisija, 2018 m. liepos 17 d. priėmusi sprendimą dėl bendros 400 000 eurų baudos skyrimo viešajai ligoninei už nustatytus asmens duomenų apsaugos pažeidimus[20]. Sprendimas dėl duomenų kiekio mažinimo principo

19 „Valstybinės duomenų apsaugos inspekcijos 2018 m. liepos 2 d. rekomendacija „Dėl reikalavimų teisės aktų projektams, kuriais reglamentuojamas asmens duomenų tvarkymas““, žiūrėta 2020 m. birželio 30 d., https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomend_teises_aktu_projektams_2018.pdf.

20 „Portugalijos Nacionalinės duomenų apsaugos komisijos 2018 m. liepos 17 d. sprendimas Nr. 984/2018“, žiūrėta 2020 m. birželio 30 d., https://www.cnpd.pt/home/decisoes/Delib/20_984_2018.pdf.

pažeidimo buvo paremtas tokiomis nustatytomis faktinėmis aplinkybėmis: ligoninė nebuvo reglamentavusi savo naudojamos informacinės sistemos vartotojų sukūrimo taisyklių, taip pat nebuvo jokio dokumento, kuriame būtų nustatyta vartotojų prieigos prie skirtingos informacijos (įskaitant informaciją apie pacientus) suteikimo tvarka priklausomai nuo jų funkcinių kompetencijų; kai kurie techniniai darbuotojai turėjo tokias pačias prieigos prie pacientų informacijos teises kaip ir medicinos personalas (t. y. tokiems darbuotojams buvo suteikta galimybė be išlygų prieiti prie visų ligoninės pacientų klinikinės informacijos); bet kuris gydytojas, nepaisant jo specializacijos, bet kuriuo metu galėjo prieiti prie bet kurio ligoninės paciento duomenų; informacinėje sistemoje buvo sukurtas ir palaikomas daugiau nei triskart didesnis vartotojų, susietų su profiliu „gydytojas“, skaičius, nei ligoninėje iš tiesų tuo metu buvo dirbančių medikų (t. y. didžioji dalis ligoninėje nebedirbančių gydytojų vartotojų paskyrų tebebuvo aktyvios). Taigi vien už BDAR 5 straipsnio 1 dalies c punkte įtvirtinto principo pažeidimą Portugalijos priežiūros institucija ligoninei skyrė 150 000 eurų baudą. Manytina, kad neribotos prieigos prie pacientų duomenų bet kokios specializacijos gydytojams suteikimas buvo prilygintas duomenų kiekio mažinimo principo, o ne konfidencialumo principo pažeidimui dėl to, kad gydytojai bet kuriuo atveju, net ir ligoninei jiems neteisėtai suteikus didesnes prieigos prie pacientų informacijos teises, yra saistomi įstatyminės konfidencialumo pareigos. Tad tikėtina, jog Portugalijos priežiūros institucija duomenų kiekio mažinimo principą šiuo atveju aiškino kaip reiškiantį, jog duomenų valdytojas (įskaitant ir atitinkamus jo darbuotojus) negali tvarkyti asmens duomenų, kurie nėra būtini atsižvelgiant į tikslus, dėl kurių šie duomenys yra tvarkomi, t. y. konkretaus paciento duomenys gali būti prieinami tik jį gydančiam medicinos personalui šio paciento gydymo tikslais. Pažymėtina, kad ligoninės veiksmuose Portugalijos Nacionalinė duomenų apsaugos komisija įžvelgė ir BDAR 32 straipsnio 1 dalies b ir d punktų pažeidimą (negebėjimą užtikrinti nuolatinį duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą bei reguliaraus techninių ir organizacinių priemonių, kuriomis užtikrinamas duomenų tvarkymo saugumas, tikrinimo, vertinimo ir veiksmingumo vertinimo proceso neužtikrinimą). Už šį pažeidimą atitinkamai buvo skirta 100 000 eurų bauda.

Nors Lietuvos sveikatos priežiūros įstaigoms sankcijos už duomenų kiekio mažinimo principo pažeidimus kol kas skirtos nebuvo[21], reikia pažymėti, kad atvejų,

21 Pažymėtina, kad vieno iš VDAI pateiktų skundų dėl sveikatos priežiūros įstaigos gydytojų konsultacinės komisijos posėdyje daryto garso įrašo tyrimo metu VDAI padarė išvadą, jog sveikatos priežiūros įstaiga, „kaip asmens duomenų valdytojas, prieš ketindamas tvarkyti duomenų subjektų asmens duomenis, t. y. daryti garso įrašus, kuriuose fiksuojami specialiųjų kategorijų asmens duomenys, turėjo įvertinti, ar toks asmens duomenų tvarkymas atitinka 5 straipsnio 1 dalies c punkte įtvirtintą asmens duomenų kiekio mažinimo principą, taip pat, vadovaujantis BDAR 35 straipsnio 1 dalies nuostatomis, atlikti duomenų poveikio asmens duomenų apsaugai vertinimą ir nustatyti duomenų tvarkymo operacijos (garso įrašo darymo) reikalingumo ir proporcingumo, palyginti su tikslais, vertinimą“. Šiuo atveju sveikatos priežiūros įstaigai buvo pareikštas papeikimas ir teiktas nurodymas sunaikinti neteisėtai tvarkomus duomenis per nurodytą terminą.

kai sveikatos priežiūros įstaigos neužtikrina, jog prieiga prie atitinkamo paciento duomenų būtų suteikiama tik tokią teisę turinčiam personalui, pasitaiko ne taip jau retai[22]. Vis dėlto, atsižvelgiant į VDAI praktiką tiriant asmens duomenų saugumo pažeidimus[23], manytina, kad Lietuvoje prieigos prie asmens duomenų kontrolės neužtikrinimas būtų kvalifikuojamas kaip konfidencialumo ir vientisumo principo, konkretizuoto BDAR 32 straipsnyje, o ne duomenų kiekio mažinimo principo, įtvirtinto BDAR 5 straipsnio 1 dalies c punkte, pažeidimas. Panašios pozicijos laikomasi ir Nyderlanduose, kur 2019 m. birželio 18 d. priežiūros institucija Hagos ligoninei skyrė 460 000 eurų baudą už pacientų bylų saugumo ligoninės viduje neužtikrinimą[24]. Nyderlandų priežiūros institucija nusprendė, kad Hagos ligoninė nesiėmė tinkamų saugumo priemonių dviejose srityse: a) ligoninė reguliariai netikrino, kas prisijungia prie atitinkamų pacientų bylų, todėl negalėjo laiku pastebėti, jei kažkas neteisėtai susipažįsta su byla, ir imtis priemonių prieš tokią veiklą; b) prisijungiant prie pacientų duomenų bazės nebuvo taikoma dviejų veiksnių autentifikavimo procedūra, kuri leistų patvirtinti vartotojo, turinčio teisėtą prieigą prie paciento bylos, tapatybę, o tada leistų vartotojui prieiti prie paciento bylos, naudojantis jam suteiktu kodu ar slaptažodžiu. Tokie ligoninės veiksmai buvo traktuojami kaip BDAR 32 straipsnio 1 dalies pažeidimas.

Iš to, kas išdėstyta aukščiau, matyti, kad nemažai problemų dėl duomenų kiekio mažinimo principo įgyvendinimo kyla pacientus aptarnaujant jiems atvykus į sveikatos priežiūros įstaigą, o papildomų neaiškumų gali atsirasti, kai sveikatos priežiūros paslaugos teikiamos nuotoliniu būdu. Pastaruoju atveju gali skirtis ne tik sveikatos priežiūros paslaugos teikimo tikslu tvarkomų asmens duomenų kiekis, bet ir duomenų,

---

22 Pavyzdžiui, asmenys iš UAB „Grožio chirurgija“ duomenų bazių įgijo privačius klinikos pacientų duomenis ir vėliau prievartavo turtą grasindami šiuos duomenis paviešinti. Iš viso pavogti daugiau kaip 22 tūkst. klinikos klientų duomenys. Nustatyta, kad į UAB „Grožio chirurgijos“ klientų duomenų bazę įsilaužta panaudojus buvusio klinikos darbuotojo prisijungimo duomenis. Plačiau žr.: „„Grožio chirurgijos“ duomenų vagystės byla grąžinta prokurorui“, *lsveikata*, 2019 m. kovo 25 d., https://lsveikata.lt/aktualijos/grozio-chirurgijos-duomenu-vagystes-byla-grazinta-prokurorui-10224.
Poliklinikoje dirbanti žmona, nebūdama vyro gydančia gydytoja, prisijungė prie poliklinikos informacinės sistemos ir peržiūrėjusi savo vyro sveikatos duomenis juos atskleidė tretiesiems asmenims skyrybų proceso metu. Plačiau žr.: Inga Saukienė, „Vyras pašiurpęs: poliklinikoje dirbanti žmona prisijungė prie jo ligos istorijos ir ją aptarė teisme“, *15min*, Vilnius, 2017 m. balandžio 30 d., https://www.15min.lt/naujiena/aktualu/lietuva/vyras-pasiurpes-poliklinikoje-dirbanti-buvusi-zmona-prisijunge-prie-jo-ligos-istorijos-ir-ja-aptare-teisme-56-790172.

23 Valstybinė duomenų apsaugos inspekcija, *„Įmonės atsakomybės neišvengs – Lietuvoje skirta ženkli bauda už Bendrojo duomenų apsaugos reglamento pažeidimus*“, 2019 m. gegužės 17 d., https://vdai.lrv.lt/lt/naujienos/imones-atsakomybes-neisvengs-lietuvoje-skirta-zenkli-bauda-uz-bendrojo-duomenu-apsaugos-reglamento-pazeidimus.

24 Nyderlandų duomenų apsaugos priežiūros institucija nustatė, jog prie ligoninės pacientės, kuri buvo žinomas žmogus Olandijoje, bylos jungėsi ir tie ligoninės darbuotojai, kurie tam neturėjo teisės, t. y. nebuvo susiję su pacientės gydymu. Žr. „Nyderlandų asmens duomenų apsaugos tarnybos 2019 m. birželio 18 d. sprendimas“, žiūrėta 2020 m. birželio 30 d., https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_haga_-_ter_openbaarmaking.pdf.

tvarkomų siekiant asmenį tinkamai identifikuoti, apimtis, taip pat paties duomenų tvarkymo apimtis, jo būdai ir priemonės. Pavyzdžiui, vienas iš nuotolinių sveikatos priežiūros paslaugų teikimo būdų yra paslaugų teikimas telefonu arba telekonferencinio ryšio priemonėmis. Kadangi šis būdas iš esmės nesiskiria nuo sveikatos priežiūros paslaugų teikimo asmeniui atvykus į sveikatos priežiūros įstaigą, todėl, VDAI nuomone[25], vien ta aplinkybė, kad jos teikiamos telefonu, savaime nereiškia, jog toks pokalbis turėtų būti įrašomas. Analogiškai turėtų būti vertinami ir atvejai, kai naudojamasi ne telefonu, o kitomis telekonferencinio ryšio priemonėmis. Darant pokalbio įrašą į jį gali patekti papildomos privačios paciento (ir jo artimųjų) informacijos, kurios duomenų valdytojas paprastai negautų, jei asmuo būtų aptarnaujamas jam asmeniškai atvykus į sveikatos priežiūros įstaigą. Ši informacija (pvz., kaip atrodo paciento gyvenamoji vieta ar su kuo jis gyvena) dažniausiai niekaip nesusijusi su sveikatos priežiūros paslaugų teikimu ir yra perteklinė. Be to, kadangi „sveikatos priežiūros paslaugų teikimo metu vertinami jautrūs paciento asmens duomenys, susiję su jo sveikata, todėl jų įrašymas ir tolesnis tvarkymas (pavyzdžiui, saugojimas) gali kelti nepagrįstą riziką paciento, kaip duomenų subjekto, teisėms ir laisvėms“[26]. Tad šiuo atveju pokalbių įrašymas, net ir esant išankstiniam asmens sutikimui, paprastai būtų laikomas nesuderinamu su BDAR įtvirtintu duomenų kiekio mažinimo principu.

Apibendrinant pabrėžtina, kad tiek teikiant sveikatos priežiūros paslaugas nuotoliniu būdu, tiek ir atvykus asmeniui į sveikatos priežiūros įstaigą duomenų valdytojas turi įsivertinti, kokius paciento asmens duomenis jam būtina tvarkyti, kad tinkamai teiktų sveikatos priežiūros paslaugas. Sveikatos priežiūros įstaigai paslaugų teikimo metu ketinant daryti pokalbio garso ir (arba) vaizdo įrašą, ji taip pat turi įvertinti, ar toks jos vykdomas asmens duomenų tvarkymas atitinka BDAR įtvirtintą asmens duomenų kiekio mažinimo principą, atlikti duomenų poveikio asmens duomenų apsaugai vertinimą ir nustatyti, ar tokia duomenų tvarkymo operacija (pokalbio įrašo darymas) yra tikrai reikalinga ir proporcinga, atsižvelgiant į siekiamus tikslus.

### 2.2. Vientisumo ir konfidencialumo principų įgyvendinimas

Valstybinė duomenų apsaugos inspekcija, vykdydama jai teisės aktais priskirtas funkcijas, *inter alia* atlieka tyrimus ir (ar) patikrinimus savo iniciatyva bei nagrinėja skundus dėl BDAR, kitų įstatymų, reglamentuojančių asmens duomenų ir (ar) privatumo apsaugą, pažeidimų. Atsižvelgdama į 2017 m. įvykusią pacientų asmens duomenų vagystę iš UAB „Grožio chirurgija“ ir šio atvejo tyrimo metu nustačiusi, kad ir pati bendrovė nebuvo tinkamai užtikrinusi asmens duomenų saugumo, VDAI 2018 m. suplanavo sveikatos priežiūros įstaigų patikrinimus, kiek tai susiję su asmens duomenų saugumo užtikrinimu, t. y. vientisumo ir konfidencialumo principų

25 „Valstybinės duomenų apsaugos inspekcijos 2020 m. gegužės 18 d. Rekomendacijos dėl asmens duomenų apsaugos aspektų, teikiant sveikatos priežiūros paslaugas nuotoliniu būdu“, *supra note*, 11.

26 *Ibid*.

įgyvendinimu. Iš VDAI savo iniciatyva atliktų sveikatos priežiūros paslaugas teikiančių subjektų tikrinimų (nuo BDAR taikymo pradžios atlikta 14 tikrinimų tiek pagal 2018 m. prevencinių tikrinimų planą, tiek pradėjus tikrinimus VDAI iniciatyva) galima išskirti pagrindines rekomendacijas sveikatos priežiūros paslaugų teikėjams, naudojantiems įvairias nuotolinio paslaugų teikimo priemones:

- sveikatos priežiūros įstaigai kaip kontaktinį elektroninio pašto adresą naudojant trečiosios šalies elektroninio pašto paslaugą (pavyzdžiui, „Google mail“) turi būti sudaryta atitinkama sutartis, dokumentuotos organizacinės ir techninės elektroninio pašto naudojimosi taisyklės, užtikrinta prieigų kontrolė bei įgyvendinama slaptažodžių politika;
- paslaugoms teikti pasitelkus duomenų tvarkytoją, su juo turi būti sudaryta sutartis, kurioje *inter alia* būtų aiškiai apibrėžta prievolė nedelsiant pranešti duomenų valdytojui apie nustatytus asmens duomenų saugumo pažeidimus;
- sveikatos priežiūros įstaigos darbuotojams jungiantis prie elektroninės sveikatos istorijų sistemos (ESIS) kompiuterinėse darbo vietose įdiegtomis naršyklėmis, ESIS turi būti aktyvuotas saugus / šifruotas ryšys (HTTPS), o ne tik HTTP;
- turi būti dokumentuotos ESIS vartotojo atliktų veiksmų auditavimo, ištrynimo, blokavimo ar deaktyvavimo procedūros, taip pat administratorių ir kitų privilegijuotų vartotojų prisijungimams taikomos saugumo priemonės, t. y. slaptažodžių politika (slaptažodžių kompleksiškumas, ilgumas, istorija, keitimo periodas, administravimas);
- ESIS duomenų bazėje turi būti vykdomas aktyvus duomenų šifravimas, įskaitant atsarginėse kopijose saugomus duomenis;
- sveikatos priežiūros įstaigoje turi būti dokumentuota tvarka, procedūros, kaip elgiamasi su duomenimis, kai kompiuterinė įranga yra likviduojama, šalinami asmens duomenys iš kietojo disko ir pan.

Pradėjus taikyti BDAR, kitaip nei iki tol, atsirado prievolė visiems duomenų valdytojams, įskaitant ir sveikatos priežiūros įstaigas, pranešti apie asmens duomenų saugumo pažeidimus. Pažymėtina, kad tokių pažeidimų atsiradimas savaime nereiškia, jog duomenų valdytojai neįgyvendina tinkamų ir pakankamų asmens duomenų saugumą užtikrinančių priemonių, nes jis gali įvykti ir, pavyzdžiui, dėl žmogiškosios klaidos. Išanalizavusi per pastaruosius metus gautus pranešimus apie asmens duomenų saugumo pažeidimus[27] VDAI būtent žmogiškąją klaidą įvardijo kaip dažniausią asmens duomenų saugumo pažeidimų priežastį. 2018 m. gegužės mėn. pradėjus taikyti BDAR, VDAI gavo ir išnagrinėjo 141 pranešimą apie asmens duomenų saugumo pažeidimą, 54 iš jų išnagrinėti nuo 2019 m. pradžios. Paveiktų fizinių asmenų skaičius sudarė daugiau nei 163 tūkstančius, o žmogiškoji klaida lėmė daugiau nei kas antrą asmens duomenų saugumo pažeidimą (71 iš 141).

27 Valstybinė duomenų apsaugos inspekcija, „Dažniausia asmens duomenų saugumo pažeidimų priežastis – žmogiškoji klaida“, 2019 m. birželio 26 d., žiūrėta 2020 m. balandžio 15 d., https://vdai.lrv.lt/lt/naujienos/dazniausia-asmens-duomenu-saugumo-pazeidimu-priezastis-zmogiskoji-klaida.

Dažniausia pažeidimo aplinkybė – neautorizuota prieiga prie duomenų ar jų atskleidimas (103 atvejai)[28].

Pažymėtina, kad analizuojant per pastaruosius dvejus metus VDAI gautus pranešimus apie įvykusius asmens duomenų saugumo pažeidimus buvo nustatyta, jog tarp 2018 m. gautų pranešimų tik 3 buvo susiję su incidentais sveikatos priežiūros paslaugų srityje, 2019 m. – 7 (iš 169), o 2020 m. I pusmetį – 5 (iš 77). Taigi per tirtą laikotarpį pranešimai, gauti iš sveikatos priežiūros įstaigų, sudarė tik 4,5 proc. visų gautų pranešimų apie įvykusius asmens duomenų saugumo pažeidimus.

Be aukščiau nurodytų pranešimų apie asmens duomenų saugumo pažeidimus, per BDAR taikymo laikotarpį gauti 37 skundai, kuriais buvo skundžiami sveikatos priežiūros paslaugas teikiantys subjektai. Tai sudarė vos 2,2 proc. visų per nurodytą laikotarpį gautų skundų. Šiuo metu išnagrinėti 32 skundai, iš kurių tik aštuoni pripažinti pagrįstais ar iš dalies pagrįstais. Dviem atvejais buvo skirti papeikimai, penkiais – nurodymai, o vienu atveju – ir nurodymas, ir papeikimas.

Nuo BDAR taikymo pradžios iki 2020 m. birželio 1 d., VDAI duomenimis, iš 1 647 asmens sveikatos priežiūros įstaigų, turinčių galiojančias licencijas[29], duomenų apsaugos pareigūnus buvo paskyrę 272 sveikatos priežiūros paslaugas teikiantys duomenų valdytojai. Iš jų maždaug ketvirtadalis (t. y. 26 proc., arba 72 asmenys) buvo išorės duomenų apsaugos pareigūnai. Taigi, atsižvelgiant į bendrą sveikatos priežiūros įstaigų, turinčių galiojančias licencijas, skaičių, tik nedidelė jų dalis yra paskyrusi duomenų apsaugos pareigūnus. Negana to, VDAI duomenimis, sveikatos priežiūros sektoriaus duomenų valdytojai duomenų apsaugos pareigūnais ne visada paskiria tinkamą kvalifikaciją turintį asmenį ir neužtikrina, kad tarp duomenų apsaugos pareigūno atliekamų kitų funkcijų ir funkcijų, kurias jis atlieka kaip duomenų apsaugos pareigūnas, nekiltų interesų konfliktas. Tokia situacija neleidžia pasiekti, kad paskirtasis duomenų apsaugos pareigūnas padės duomenų valdytojui efektyviai užtikrinti asmens duomenų tvarkymo principų, įskaitant ir šiame straipsnyje aptariamus, įgyvendinimą.

BDAR 37 straipsnio 5 dalyje numatyta, kad duomenų apsaugos pareigūnas paskiriamas remiantis profesinėmis savybėmis (įskaitant gerą supratimą apie duomenų valdytojo vykdomas duomenų tvarkymo operacijas, informacines sistemas, duomenų saugumo ir duomenų apsaugos poreikius[30]), visų pirma, duomenų apsaugos teisės ir praktikos ekspertinėmis žiniomis, taip pat gebėjimu atlikti BDAR 39 straipsnyje nurodytas užduotis. Europos Komisijos 29 straipsnio darbo grupės Duomenų ap-

28 Valstybinė duomenų apsaugos inspekcija, „Dažniausia asmens duomenų saugumo pažeidimų priežastis – žmogiškoji klaida“, 2019 m. birželio 26 d., žiūrėta 2020 m. balandžio 15 d., https://vdai.lrv.lt/lt/naujienos/dazniausia-asmens-duomenu-saugumo-pazeidimu-priezastis-zmogiskoji-klaida.

29 Valstybinė akreditavimo sveikatos priežiūros veiklai tarnyba, „Įstaigų asmens sveikatos priežiūros licencijų sąrašas, 2020“, žiūrėta 2020 m. birželio 30 d., https://www.vaspvt.gov.lt/files/Istaigu_licencijavimas/ASPI.pdf.

30 „29 straipsnio darbo grupės Duomenų apsaugos pareigūnų gairės WP 243 rev.01“, 2017 m. spalio 30 d., žiūrėta 2020 m. birželio 30 d., https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048.

saugos pareigūnų gairėse[31] pabrėžiamas itin svarbus duomenų apsaugos pareigūno vaidmuo organizacijoje skatinant duomenų apsaugos kultūrą ir padedant įgyvendinti esminius BDAR elementus, įskaitant duomenų tvarkymo principų įgyvendinimą, duomenų tvarkymo saugumo užtikrinimą naudojant tinkamas technines ir organizacines priemones, pranešimų apie duomenų saugumo pažeidimus teikimą ir kt.

BDAR 37 straipsnio 6 dalyje numatyta, kad duomenų apsaugos pareigūnas gali būti duomenų valdytojo ar duomenų tvarkytojo personalo narys arba atlikti užduotis pagal paslaugų teikimo sutartį. BDAR 38 straipsnio 6 dalyje numatyta duomenų valdytojo arba duomenų tvarkytojo pareiga užtikrinti, kad dėl bet kokių kitų duomenų apsaugos pareigūno užduočių ir pareigų nekiltų interesų konfliktas. 2018 m. atliekamų tikrinimų metu nustatyta, kad, pavyzdžiui, vienoje sveikatos priežiūros įstaigoje duomenų apsaugos pareigūnu paskirtas Ūkio skyriaus vadovas.

Europos Komisijos 29 straipsnio darbo grupės Duomenų apsaugos pareigūnų gairėse nurodoma, kad interesų konflikto nebuvimas glaudžiai susijęs su reikalavimu veikti nepriklausomai. Nors duomenų apsaugos pareigūnams nėra draudžiama atlikti kitas funkcijas, vis dėlto pavesti vykdyti kitas funkcijas jam galima tik tuomet, jeigu dėl jų vykdymo negali kilti interesų konfliktas. „Tai visų pirma reiškia, kad duomenų apsaugos pareigūnas negali organizacijoje eiti pareigų, pagal kurias jis turėtų nustatyti asmens duomenų tvarkymo tikslus ir priemones. <...> Paprastai tokios interesų konfliktą galinčios sukelti pareigybės organizacijoje, be kita ko, gali būti vyresniosios vadovybės pareigybės[32] <...>, tačiau tai gali būti ir žemesnio lygio pareigos organizacijos struktūroje, jeigu vykdant tas pareigas arba funkcijas reikia nustatyti duomenų tvarkymo tikslus ir priemones.“[33] VDAI vykdyto tikrinimo metu nustatyta, kad Ūkio skyriaus vadovo pareiginėje instrukcijoje buvo nurodyta, jog Ūkio skyriaus vadovas užtikrina IT paslaugų teikimą sveikatos priežiūros įstaigos veiklos tikslams įgyvendinti, užtikrina, kad visos teikiamos IT paslaugos atitiktų IT paslaugoms keliamus reikalavimus, taip pat užtikrina, kad IT paslaugų valdymo procesai būtų nuolatos analizuojami ir tobulinami, atsižvelgiant į veiklos tikslus, poreikius, teisinius ir standartų reikalavimus, racionaliai ir efektyviai panaudojant sveikatos priežiūros įstaigos išteklius. VDAI, atlikusi tikrinimą, priėjo prie išvados, kad Ūkio skyriaus vadovo paskyrimas duomenų apsaugos pareigūnu neatitiko BDAR 38 straipsnio 6 dalies reikalavimų.

Iš VDAI atliktų patikrinimų taip pat pastebėta, kad paskirtieji duomenų apsaugos pareigūnai ne visuomet tinkamai aiškina asmens duomenų apsaugos teisės aktus ir pataria atsakingiems duomenų valdytojo darbuotojams (pavyzdžiui, dėl garso įrašo

---

31 „29 straipsnio darbo grupės Duomenų apsaugos pareigūnų gairės WP 243 rev.01“, 2017 m. spalio 30 d., žiūrėta 2020 m. birželio 30 d., https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048.

32 Pavyzdžiui, generalinis direktorius, operacijų vadovas, vyriausiasis finansininkas, vyriausiasis gydytojas, rinkodaros padalinio vadovas, žmogiškųjų išteklių arba IT padalinio vadovas.

33 „29 straipsnio darbo grupės Duomenų apsaugos pareigūnų gairės WP 243 rev.01“, 2017 m. spalio 30 d., žiūrėta 2020 m. birželio 30 d., https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048.

darymo Gydytojų konsultacinėje komisijoje[34]). Šiuo aspektu VDAI yra atkreipusi dėmesį į didelį duomenų valdytojų (ir tvarkytojų) personalo mokymų poreikį, kadangi būtent darbuotojų (įskaitant ir duomenų apsaugos pareigūnus) mokymai yra efektyviausia priemonė siekiant išvengti žmogiškųjų klaidų, pasitaikančių atliekant duomenų tvarkymo procedūras. VDAI nuomone, „mokymai apie duomenų apsaugą ir saugumo procedūras (pvz., slaptažodžių naudojimą ir prieigą prie konkrečių IT sistemų) yra svarbūs tinkamam organizacinių ir techninių saugumo priemonių įgyvendinimui ir prevencijai dėl netyčinio duomenų sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jų (BDAR 32 straipsnio 2 dalis). Žinios apie asmens duomenų tvarkymui keliamus reikalavimus bei atsakomybes yra ypač svarbios tiems asmenims, kurie atlieka didelės rizikos asmens duomenų tvarkymo operacijas.“[35]. Pažymėtina, kad personalo mokymai reikalingi ne tik tam, kad sveikatos priežiūros sektoriaus darbuotojai patys suprastų, kaip tinkamai ir saugiai tvarkyti asmens duomenis, bet ir tam, kad šie specialistai gebėtų duomenų subjektams paaiškinti tokio duomenų tvarkymo poreikį, tikslus ir pagrindus. Tokių gebėjimų įgijimas yra ypač svarbus, atsižvelgiant į duomenų valdytojams tenkančią pareigą būti aktyviems įgyvendinant duomenų subjektų teises. Pavyzdžiui, įgyvendindamas duomenų subjekto teisę būti informuotam, kuri yra neatsiejama nuo skaidrumo principo įgyvendinimo, duomenų valdytojas turi pacientui proaktyviai pateikti visą reikalingą informaciją iš anksto nelaukdamas, kol duomenų subjektas pats jos paprašys[36].

Teikiant sveikatos priežiūros paslaugas svarbu ne tik turėti teisinį pagrindą tvarkyti asmens duomenis, bet ir nustatyti besikreipiančiojo asmens tapatybę. Jeigu tapatybės nustatymas asmeniui fiziškai atvykus į sveikatos priežiūros įstaigą dažniausiai nekelia problemų (paprastai tapatybei nustatyti prašoma parodyti asmens dokumentą), tai ši procedūra teikiant paslaugas nuotoliniu būdu gali būti rimtas iššūkis. Nors sveikatos priežiūros įstaiga besikreipiantį asmenį identifikuojantį būdą gali pasirinkti savarankiškai, ji turėtų įvertinti ne tik tokio būdo patikimumą, bet ir savo veikloje naudojamas technologijas, taip pat teikiamų paslaugų pobūdį ir pacientų, kuriems tokios sveikatos priežiūros paslaugos galėtų būti teikiamos nuotoliniu būdu, kategorijas (pavyzdžiui, pagal jų amžių). VDAI rekomenduoja priklausomai nuo konkretaus paciento ar sveikatos paslaugų pobūdžio pasirinkti ne vieną, o kelis tapatybės identifikavimo būdus (pavyzdžiui, asmens identifikavimas pagal telefono ryšio

34 Žr. 20 išnašą.

35 Valstybinė duomenų apsaugos inspekcija, *supra note*, 26.

36 Pavyzdžiui, vieno iš VDAI pateiktų skundų dėl sveikatos priežiūros įstaigos atsisakymo pateikti dokumentus / aprašus apie asmens duomenų apsaugą tyrimo metu VDAI padarė išvadą, jog įvertinant tai, kad „SPĮ Inspekcijai nurodė, kad Duomenų privatumo pranešimas buvo pateiktas pareiškėjui paprašius, darytina išvada, kad SPĮ nebuvo aktyvi siekiant įgyvendinti pareiškėjo teisę būti informuotam apie asmens duomenų tvarkymą nagrinėjamu atveju, kai buvo prašoma pateikti savo asmens duomenis jam atvykus į šią SPĮ“. Ši sveikatos priežiūros įstaiga buvo įpareigota „užtikrinti, kad aktyviais veiksmais duomenų subjektams (net ir tuo atveju, kai duomenų subjektas neprašo) būtų pateikta BDAR 13 straipsnyje numatyta informacija apie jų asmens duomenų tvarkymą asmens duomenų gavimo metu“.

numerį ir asmenį identifikuojantys klausimai ar tapatybės patvirtinimas mobiliuoju parašu) bei atkreipia dėmesį, kad kuo rimtesnės pasekmės pacientui gali kilti dėl jo netinkamo identifikavimo, tuo griežtesni tapatybės nustatymo būdai turi būti pasirenkami[37].

Nustačius besikreipiančio asmens tapatybę, nemažiau svarbu teikiant nuotolines sveikatos priežiūros paslaugas naudoti tinkamas komunikavimo bei tokios komunikacijos fiksavimo priemones. Kaip minėta, vien ta aplinkybė, kad sveikatos priežiūros paslaugos teikiamos telefonu ar naudojant telekonferencinio ryšio priemones, savaime nereiškia, jog toks pokalbis turėtų būti įrašomas. Jei visgi pokalbiai (turint teisėtą pagrindą) yra įrašomi, duomenų valdytojas turi pasirūpinti, kad prieiga prie tokių duomenų būtų ribota (prieinama tik tiems asmenims, kuriems būtina pagal jų atliekamas funkcijas), o naudojama techninė įranga ir joje esantys asmens duomenys būtų apsaugota nuo jų praradimo, sunaikinimo ar sugadinimo pavojų[38].

Renkantis techninę ar programinę įrangą, kuri būtų naudojama nuotoliniu būdu teikiant sveikatos priežiūros paslaugas, VDAI rekomenduoja atkreipti dėmesį ir įsivertinti šiuos aspektus[39]:

- ketinamo naudoti įrankio ar programinės įrangos naudojimo taisykles, privatumo politiką ir kitus dokumentus, kad būtų įvertintas jų patikimumas, saugumas ir kitos reikšmingos aplinkybės;
- pasirinktos priemonės galimybes užtikrinti tinkamą BDAR įtvirtintų duomenų subjektų teisių įgyvendinimą;
- ketinamų pasitelkti duomenų tvarkytojų galimybes užtikrinti tinkamas organizacines ir technines duomenų saugumo priemones, atitinkančias BDAR reikalavimus;
- asmens duomenų, kurie bus tvarkomi jungiantis prie nuotolinio sveikatos priežiūros paslaugų teikimo priemonės ir (ar) ja naudojantis, pobūdį bei apimtis;
- prieigų prie asmens duomenų, esančių sveikatos priežiūros įstaigos naudojamose platformose, suteikimo sąlygas, suteikiamas teises, jų apimtis ir pan.

VDAI taip pat yra ne kartą pabrėžusi, kad duomenų valdytojų darbuotojai (įskaitant ir sveikatos priežiūros specialistus), atlikdami duomenų tvarkymo operacijas, neturėtų naudoti asmeninių mobiliųjų įrenginių (telefonų, kompiuterių, planšetinių kompiuterių) jungdamiesi prie programinės įrangos, įrankių ar bendravimo platformų, taip pat naudoti šiose platformose sukurtų asmeninių paskyrų[40], kadangi toks asmens duomenų tvarkymas galėtų sukelti asmens duomenų konfidencialumo praradimo, netyčinio praradimo, sunaikinimo, ar sugadinimo pavojų.

---

37 „Valstybinės duomenų apsaugos inspekcijos 2020 m. gegužės 18 d. Rekomendacijos dėl asmens duomenų apsaugos aspektų, teikiant sveikatos priežiūros paslaugas nuotoliniu būdu“, *supra note*, 11.

38 Žr. 20 išnašą.

39 „Valstybinės duomenų apsaugos inspekcijos 2020 m. gegužės 18 d. Rekomendacijos dėl asmens duomenų apsaugos aspektų, teikiant sveikatos priežiūros paslaugas nuotoliniu būdu“, *supra note*, 11.

40 *Ibid.*

## Išvados

1. Teikiant sveikatos priežiūros paslaugas nuotoliniu būdu paprastai taikytini tie patys asmens duomenų tvarkymo pagrindai, kaip ir teikiant sveikatos priežiūros paslaugas esant tiesioginiam kontaktui su pacientu. Tiesa, tais atvejais, kai paciento duomenys tvarkomi jo sutikimo pagrindu, aiškus paciento sutikimas, kad jo duomenys būtų tvarkomi ir jam gaunant sveikatos priežiūros paslaugas nuotoliniu būdu, turi būti gaunamas iš anksto.
2. Situacijos, kai sveikatos priežiūros įstaigos netinkamai įgyvendina duomenų kiekio mažinimo principą, neretai susiklosto ir dėl to, kad perteklinius pacientų duomenis rinkti jas įpareigoja nekokybiškai parengti nacionaliniai teisės aktai. Teisės akto kokybė ir jo atitiktis BDAR įtvirtintiems reikalavimams galėtų prisidėti prie didesnio visuomenės užtikrintumo dėl BDAR nuostatų laikymosi ir jų privatumo gerbimo. Tai taip pat sudarytų sąlygas sveikatos priežiūros įstaigų, kaip duomenų valdytojų, darbuotojams kur kas lengviau paaiškinti pacientams, kodėl vienų ar kitų asmens duomenų yra prašoma.
3. Tiek teikiant sveikatos priežiūros paslaugas nuotoliniu būdu, tiek ir atvykus asmeniui į sveikatos priežiūros įstaigą, asmens duomenų tvarkymo apimtis tvarkant juos sveikatos priežiūros paslaugos teikimo tikslu gali skirtis, pavyzdžiui, jeigu daromas telefoninio pokalbio ar telekonferencinio ryšio įrašas. Visgi pokalbių įrašymas, net ir esant išankstiniam paciento sutikimui, paprastai būtų laikomas nesuderinamu su BDAR įtvirtintu duomenų kiekio mažinimo principu.
4. Teikiant sveikatos priežiūros paslaugas nuotoliniu būdu pagrindiniu iššūkiu tampa tinkamas duomenų subjekto (paciento) identifikavimas. Atsižvelgiant į tai, kad sveikatos priežiūros paslaugų teikimas visuomet susijęs su jautrių asmens duomenų tvarkymu, pritartina VDAI nuomonei, kad ketinamo pasirinkti tapatybės nustatymo būdo griežtumas turėtų būti nulemtas pacientui dėl jo netinkamo identifikavimo galinčių kilti pasekmių rimtumo.
5. Sėkmingam BDAR principų, o ypač duomenų kiekio mažinimo ir skaidrumo principų, įgyvendinimui esminę reikšmę turi kokybiška teisėkūra ir kvalifikuoti duomenų apsaugos pareigūnai, nepaisant to, kokiu būdu (nuotoliniu ar pacientui fiziškai atvykus į sveikatos priežiūros įstaigą) teikiamos sveikatos priežiūros paslaugos.
6. Remiantis VDAI duomenimis, tik nedidelė sveikatos priežiūros įstaigų, turinčių galiojančias licencijas, dalis yra paskyrusi duomenų apsaugos pareigūnus. Be to, sveikatos priežiūros sektoriaus duomenų valdytojai duomenų apsaugos pareigūnais ne visada paskiria tinkamą kvalifikaciją turintį asmenį ir neužtikrina, kad tarp duomenų apsaugos pareigūno atliekamų kitų funkcijų ir funkcijų, kurias jis atlieka kaip duomenų apsaugos pareigūnas, nekiltų interesų konfliktas. Kvalifikuoto duomenų apsaugos pareigūno paskyrimas sveikatos priežiūros įstaigoms padėtų ne tik skatinti ir palaikyti asmens duomenų

apsaugos kultūrą jų viduje, bet ir tinkamai įgyvendinti duomenų tvarkymo, įskaitant vientisumo ir konfidencialumo, principus, užtikrinti duomenų tvarkymo saugumą naudojant tinkamas technines ir organizacines priemones.

7. Darbuotojų švietimas ir nuolatinis mokymas gali padėti sveikatos priežiūros įstaigoms išvengti asmens duomenų saugumo pažeidimų, taip pat ir vientisumo bei konfidencialumo principo pažeidimo, ypač teikiant paslaugas nuotoliniu būdu.

# PROVIDING SERVICES REMOTELY: PECULIARITIES OF PERSONAL DATA PROCESSING IN THE HEALTHCARE SECTOR

**Rūta Lazauskaitė**
Mykolas Romeris University, Lithuania

**Daiva Tamulionienė**
State Data Protection Inspectorate, Lithuania

**Abstract.** *With the global spread of COVID-19, remote work and provision of services remotely have become the norm in many areas of activity, including the provision of healthcare services. Following the decision of the government of the Republic of Lithuania to declare quarantine and introduce restrictions to limit movement and activities, recommendations were adopted for public and private sector entities to organize work and provide remote services for customers. The only exception made was in the case of certain functions that could only be physically performed in the actual workplace. Priority for remote provision of services was established in the healthcare sector. Hence, the unprecedented situation presented by COVID-19 has obliged healthcare (and many other sectors) to adapt, and even switch, to remote work, despite doubts or a reluctance to adopt telemedicine.*

*A key challenge in providing distance healthcare is the proper identification of a data subject (patient). Given that the provision of healthcare services is linked to the processing of sensitive personal data, the intended method of identification of a data subject must adhere to strict protocols. These are determined by the potential severity of the consequences that may arise for a patient (and also the healthcare provider) due to misidentification. Qualified data protection officers, supported by appropriate legislation, are essential for the successful implementation of the principles established in the General Data Protection Regulation, and in particular the principle of data minimisation and the principle of transparency, regardless of the way in which the healthcare services are provided (remotely or in person upon arrival to the healthcare institution). Ensuring the education and continuous training of the personnel can help to prevent*

*healthcare institutions from violating the security of personal data, as well as ensure they maintain principles of integrity and confidentiality, especially when and where services are provided remotely.*

**Keywords:** *Healthcare Institution, Basis for Data Processing Personal Data, Principles of Personal Data Processing, Data Controller, Data Protection Officer.*

---

**Rūta Lazauskaitė**, Mykolo Romerio universiteto Teisės mokyklos Privatinės teisės instituto docentė. Mokslinių tyrimų kryptys: asmens duomenų apsauga, sutarčių teisė, intelektinės nuosavybės teisė.

**Rūta Lazauskaitė**, associate professor at the Institute of Private Law at the Mykolas Romeris University Law School. Research interests: data protection, contract law, intellectual property law.

---

**Daiva Tamulionienė**, Valstybinės duomenų apsaugos inspekcijos Priežiūros skyriaus vedėja. Mokslinių tyrimų kryptys: asmens duomenų apsauga.

**Daiva Tamulionienė**, head of the Supervisory Division at the State Data Protection Inspectorate. Research interests: data protection.