Vilniaus universiteto Teisės fakulteto

Viešosios teisės katedra

Elzės Markauskaitės,

V kurso, tarptautinės ir Europos Sąjungos teisės

studijų šakos studentės

Magistro darbas

Išmaniųjų sveikatos aplikacijų ir prietaisų problematika pagal ES duomenų apsaugos teisę

Issues of Smart Health Applications and Devices under the EU Data Protection Law

Vadovas: asist. dr. Julius Zaleskis

Recenzentė: doc. dr. Vygantė Milašiūtė

Vilnius

2023

ANOTACIJA IR PAGRINDINIAI ŽODŽIAI

Siekiant atskleisti išmaniųjų sveikatos aplikacijų ir prietaisų teisinį reglamentavimą asmens duomenų apsaugos kontekste, šiame darbe analizuojami pagrindiniai šios technologijos sampratos elementai, tokie kaip sąvoka, privalumai, naudojimo iššūkiai bei atskirtis nuo kitų technologijų rūšių. Taip pat nagrinėjami išmaniųjų sveikatos aplikacijų ir prietaisų reguliavimo ypatumai, problematika, alternatyvūs reguliavimo būdai ir naujovės Europos Sąjungos duomenų apsaugos teisėje.

Pagrindiniai žodžiai: išmaniosios sveikatos aplikacijos ir prietaisai, sveikatos duomenys, BDAR, kūrėjai, naudotojai, ESDER, aplikacijų parduotuvės.

In order to understand the legal framework of smart health applications and devices in the context of the protection of personal data, this thesis analyses the key elements of the concept of this technology, such as its definition, advantages, challenges of use and distinction from other types of technologies. It also examines the regulatory specificities, challenges, alternative regulatory approaches and innovations of smart health applications and devices in European Union data protection law.

Keywords: smart health applications and devices, health data, GDPR, developers, users, EHDSR, app stores.

TURINYS

ĮŽANGA 2
1. IŠMANIŲJŲ SVEIKATOS APLIKACIJŲ IR PRIETAISŲ SAMPRATA....5
1.1 Išmaniųjų sveikatos aplikacijų ir prietaisų sąvoka, panaudojimas ir privalumai....5
1.2 Privatumo ir saugumo iššūkiai....6
1.3 Išmaniųjų sveikatos aplikacijų ir prietaisų atskyrimas nuo medicinos prietaisų....7
2. REGULIAVIMO YPATUMAI IR PROBLEMATIKA BDAR KONTEKSTE....11
2.1 Pagrindiniai asmens duomenų tvarkymo principai....12
2.2 Sveikatos duomenys kaip specialių kategorijų duomenys....14
2.3 Sutikimo išimtis sveikatos duomenų tvarkymui....21
2.4 Duomenų subjektų teisės....23
2.5 Poveikio duomenų apsaugai vertinimas....25
2.6 BDAR netinkamo įgyvendinimo apsaugant sveikatos duomenis problematika....26
3. SAVIREGULIACIJA ES DUOMENŲ APSAUGOS TEISĖS POŽIŪRIU....28
3.1 Aplikacijų parduotuvių savireguliacija kaip būdas sveikatos duomenų apsaugai tobulinti....28
4. TEISINIO REGLAMENTAVIMO NAUJOVĖS PAGAL EUROPOS SVEIKATOS DUOMENŲ ERDVĖS REGLAMENTĄ....33
4.1 Samprata ir siekiamos išspręsti problemos....33
4.2 Pirminis sveikatos duomenų panaudojimas....35
4.3 Antrinis sveikatos duomenų panaudojimas....36
4.4 Išmaniųjų sveikatos aplikacijų ir prietaisų ženklinimas....38
4.5 ESDER pasiūlymo problematika bei įtaka išmaniųjų sveikatos aplikacijų ir prietaisų kūrėjams....39
IŠVADOS....41
ŠALTINIŲ SĄRAŠAS....43
SANTRAUKA....50
SUMMARY....51

ĮŽANGA

Nagrinėjamos temos aktualumas. Mūsų kūnai nuolatos skleidžia duomenų srautus: viską – nuo fizinio aktyvumo, suvartojamų kalorijų, miego ir laikysenos iki lytinių santykių, menstruacijų ciklo, vaisingumo ir kvėpavimo įpročių – galima sekti, matuoti, registruoti ir analizuoti, siekiant stebėti sveikatos pokyčius bei pažinti save. Nuo 2008 m., kai buvo atidaryta Apple App Store aplikacijų parduotuvė, mobiliųjų aplikacijų skaičius išaugo ypač dideliu mastu. Šiuo metu rinkoje yra daugiau kaip 250 000 sveikatos aplikacijų (Tzanou, 2020, p. 5) (pvz., aplikacija Flo, kurioje galima stebėti ir prognozuoti menstruacijų ciklą) ir su jomis susietų dėvimųjų bei nešiojamų prietaisų (tokių kaip: išmanieji laikrodžiai; kūno rengybos (angl. *fitness*) sekimo įrenginiai pvz., Fitbit bevielis matuoklis, išmanieji drabužiai pvz., išmaniosios vaikų sauskelnės ar kojinė kuri matuoja kūdikio temperatūrą, širdies ritmą, deguonies prisotinimą ir judėjimą, tai pat išmanieji juvelyriniai dirbiniai bei implantai). Lietuvoje šių sveikatos technologijų sektorius taip pat auga. Pavyzdžiui, Lietuvos įmonė UAB „Kilo grupė“, veikianti Kilo.Health prekės ženklo vardu, kuria išmaniąsias sveikatos aplikacijas ir prietaisus bei kitus sveikatos technologijų produktus. Tai viena iš Europoje pirmaujančių skaitmeninės sveikatos ir sveikatingumo bendrovių.

Šioms minėtoms technologijoms taikomi bendrieji duomenų apsaugos, intelektinės nuosavybės apsaugos bei kiti Europos Sąjungos lygmens ir nacionaliniai teisės aktai. Visgi išmaniųjų sveikatos aplikacijų ir prietaisų naudojimo teisinis reglamentavimas nėra pakankamai plačiai išplėtotas praktikoje, todėl susiduriama su įvairiais iššūkiais ir atitikties problemomis.

Kūno stebėjimas pasitelkiant technologijas tapo daugelio kasdienio gyvenimo dalimi, o gauti duomenys naudojami produktų vystymui ir naujų kūrimui. Todėl ypatingai svarbu užtikrinti kiekvieno individualaus asmens teisių apsaugą, kartu suteikiant galimybę verslui vystyti modernius technologinius sprendimus. Siekiant didinti visuomenės informuotumą apie sveikatos technologijų tvarkomus asmens duomenis ir kuriamų produktų atitiktį galiojančiam reglamentavimui yra ypač aktuali ir reikalinga išsami išmaniųjų sveikatos aplikacijų ir prietaisų sampratos ir reguliavimo analizė.

Darbo tikslas. Šio darbo tikslas yra atskleisti išmaniųjų sveikatos aplikacijų ir prietaisų teisinį reglamentavimą asmens duomenų apsaugos kontekste.

Darbo uždaviniai. Siekiant darbo tikslo būtų aktualūs šie uždaviniai:

1. Išnagrinėti išmaniųjų sveikatos aplikacijų ir prietaisų sampratos ypatybes, atskleidžiant jų sąvoką, privalumus, naudojimo iššūkius ir atskyrimą nuo medicinos prietaisų.
2. Identifikuoti išmaniųjų sveikatos aplikacijų ir prietaisų reguliavimo ypatumus ES Bendrojo duomenų apsaugos reglamento taikymo srityje;
3. Išskirti išmaniųjų aplikacijų ir prietaisų reguliavimo problematiką bei aptarti alternatyvius reguliavimo būdus;
4. Išnagrinėti reikšmingas teisines naujoves išmaniosioms sveikatos aplikacijoms ir prietaisams Europos sveikatos duomenų erdvės reglamento prasme bei įvertinti jų problematiką ir įtaką kūrėjams.

Objektas. Šiame darbe analizuojami išmaniųjų sveikatos aplikacijų ir prietaisų reglamentavimo principai ir normos Europos Sąjungos duomenų apsaugos teisės kontekste.

Tyrimo metodai. Analizuojant darbo objektą yra pasitelkiami sisteminis, lingvistinis ir teleologinis metodai. Sisteminis metodas naudojamas vertinant įvairių *soft law* šaltinių bei naujojo Europos sveikatos duomenų erdvės reguliavimo nuostatas neatsiejamai nuo visos Bendrojo duomenų apsaugos reglamento sistemos. Lingvistinis metodas pasitelkiamas aiškinant esmines darbe minimas sąvokas, tokias kaip išmaniosios sveikatos aplikacijos ir prietaisai, sveikatos duomenys, pirminis ir antrinis duomenų naudojimas ir t.t. Naudojant teleologinį metodą, siekiama ištirti kokie yra Europos Sąjungos įstatymų leidėjo tikslai kuriant naująjį Europos sveikatos erdvės reglamentą.

Darbo originalumas. Ši tema tarptautinėje literatūroje daugiausiai tirta moksliniuose straipsniuose. C. B. Olsen straipsnyje „To track or not to track? Employees' data privacy in the age of corporate wellness, mobile health, and GDPR“ nagrinėjamas sveikatos prietaisų ir aplikacijų naudojimo teisėtumas įmonių sveikatingumo programose, konkrečiai atsižvelgiant į darbuotojų teises į duomenų apsaugą pagal Europos Sąjungos teisę, ypač Bendrąjį duomenų apsaugos reglamentą, Europos žmogaus teisių konvenciją ir susijusią teismų praktiką. H. van Kolfschooten straipsnyje „The mHealth Power Paradox“ apžvelgia su sveikatos aplikacijomis ir prietaisais susijusius iššūkius. M. Tzanou „Health Data Privacy under the GDPR: Big Data Challenges and Regulatory Responses” skyriuje

„Privacy issues in eHealth and mHealth apps" aptariant išmaniąsias sveikatos aplikacijas ir prietaisus nagrinėjami sveikatos privatumo klausimai atsižvelgiant į Bendrąjį duomenų apsaugos reglamentą ir bendrą Europos Sąjungos duomenų privatumo teisinę sistemą.
Šis magistro darbas yra unikalus tuo, jog jame pateikiama išsami visų svarbiausių aspektų susijusių su išmaniosiomis sveikatos aplikacijomis ir prietaisais analizė, suteikianti galimybę skaitytojui tinkamai susipažinti su nagrinėjama tema, kuri šiuo metu yra tirta pavieniuose užsienio autorių straipsniuose, apžvelgiančiuose tik tam tikrus atskyrus su tema susijusius elementus. Darbo autorės žiniomis, Lietuvoje ši tema mokslinėje literatūroje nebuvo nagrinėta, taip pat panašia tema nebuvo rašyti magistro darbai.

Svarbiausi šaltiniai. Turint omenyje tai, jog ES Bendrasis duomenų apsaugos reglamentas šiuo metu yra vienas svarbiausių privalomo pobūdžio duomenų apsaugos teisės aktų taikomų išmaniųjų sveikatos aplikacijų ir prietaisų kontekste, būtent šio šaltinio nuostatos, aktualios nagrinėjamai temai, darbe analizuojamos daugiausiai. Taip pat, daug dėmesio skiriama naujojo Europos sveikatos duomenų erdvės reglamento pasiūlyme numatomų naujovių tyrimui. Be to, siekiant aptarti išmaniųjų sveikatos aplikacijų ir prietaisų atskyrimą nuo medicinos prietaisų, nagrinėjami Europos Sąjungos medicinos prietaisų direktyvos ir ją pakeitusio Europos Sąjungos medicinos priemonių reglamento pagrindiniai aspektai bei Europos Sąjungos Teisingumo Teismo praktika.
Darbe taip pat daug remiamasi 29 straipsnio darbo grupės ir ją pakeitusios Europos duomenų apsaugos valdybos bei Europos Komisijos parengtais *soft law* šaltiniais. Nagrinėjant alternatyvius reguliavimo mechanizmus darbe atliekama dviejų didžiausių aplikacijų parduotuvių (Apple App Store ir Google Play) duomenų apsaugos nuostatų analizė.

1. IŠMANIŲJŲ SVEIKATOS APLIKACIJŲ IR PRIETAISŲ SAMPRATA

1.1 Išmaniųjų sveikatos aplikacijų ir prietaisų sąvoka, panaudojimas ir privalumai

Pasaulio sveikatos organizacija mobilias sveikatos technologijas apibrėžia kaip visuomenės sveikatos praktiką, paremtą mobiliaisiais įrenginiais, pvz., mobiliaisiais telefonais, pacientų stebėsenos prietaisais ir kitais belaidžiais įrenginiais (WHO Global Observatory for eHealth…, 2011, p. 6). Tai į mobilius įrenginius instaliuotos išmaniosios sveikatos aplikacijos, į kurių sąvoką patenka vadinamos sveikatos ar sveikatingumo, kūno rengybos ir gyvenimo būdo aplikacijos, bei dėvimieji ar nešiojami prietaisai, kurie yra susieti su šiomis aplikacijomis ir yra jų kaip technologijos neatsiejama dalis. Pavyzdžiui, įmonė Natural Cycles sukūrė išmaniąją aplikaciją, skirtą padėti moterims stebėti savo vaisingumą. Ji numato, kuriomis dienomis moteris yra vaisinga matuojant jos temperatūrą specialiu termometru, kuris yra susietas su aplikacija ir perduoda į ją gautus duomenis. Taigi, dėvimieji ar nešiojamieji prietaisai gali būti įvairių formų, pvz., laikrodžiai, kūno rengybos stebėjimo prietaisai, akiniai, žiedai ir pan. Kaip minėta, jų esminis technologinis bruožas yra tai, jog šie prietaisai turi išmaniuosius jutiklius, kurie seka judesius bei biometrinius duomenis ir perduoda juos į aplikacijas, kur naudotojai gali susipažinti su duomenimis ir juos apžvelgti (What is Wearable Tech? Everything…, 2019). Šios sveikatos technologijos gali padėti siekti tokių tikslų, kaip palaikyti gerą fizinę formą, numesti svorio bei stebėti psichinę ar fizinę sveikatą. Pavyzdžiui, Apple Watch išmanus laikrodis gali aptikti nereguliarų širdies plakimą. Tokie prietaisai taip pat gali padėti stebėti cukraus kiekį kraujyje, kraujospūdį ar pan. Svarbu paminėti, kad pastaraisiais metais šios aplikacijos ir prietaisai reikšmingai prisidėjo prie visuomenės sveikatos rodiklių gerinimo. (What is Wearable Tech? Everything…, 2019). Pažymėtina, jog šiuo metu minėtų technologijų rinka ypač sparčiai auga, todėl aktualu apžvelgti pagrindinius išmaniųjų sveikatos aplikacijų ir prietaisų privalumus:

1. sveikatos savarankiška stebėsena: kai sveikatos aplikacijoje įdiegiamos tinkamos priemonės, pacientai gali prisiimti atsakomybę už savo sveikatos stebėseną ir taip sumažinti krūvį sveikatos priežiūros įstaigoms (Shad, 2022);
2. lengvas duomenų pasiekiamumas: duomenys sveikatos aplikacijoje pasiekiami akimirksniu bei saugiai, dėl šios priežasties galima laiku imtis reikalingų veiksmų (Shad, 2022);
3. efektyvus lėtinių ligų valdymas: skirtingai nuo to kaip buvo ankstesniais laikais, kai asmenys buvo tikrinami tik periodiškai, dabar sveikatos aplikacijos leidžia nuosekliai ir reguliariai stebėti pacientų sveikatos būklę (Shad, 2022);

4. reguliarūs priminimai apie vaistus: dažnai pacientų sveikata pablogėja dėl nereguliaraus vaistų vartojimo. Todėl priminimai apie juos gali padėti išspręsti šią problemą (Shad, 2022);
5. gydytojų darbo efektyvumo didinimas: gydytojai dažnai yra pervargę dėl klinikinių užduočių ir priežiūros teikimo. Dėl to mažėja jų produktyvumas ir darbo efektyvumas. Tačiau sveikatos aplikacijos gali išspręsti šią problemą, suteikdamos gydytojams reikšmingų įžvalgų, padedančių pagerinti pacientų priežiūrą (Shad, 2022).
Taigi, galima teigti, jog išmaniosios sveikatos aplikacijos ir prietaisai yra daug žadanti technologija.
Svarbu paminėti, jog šio darbo kontekste pavadinimai: **išmaniosios sveikatos aplikacijos ir prietaisai** arba tiesiog **sveikatos aplikacijos** reikš visas prieš tai išvardintas, į sveikatos aplikacijos sąvoką patenkančias sveikatos aplikacijų bei nuo jų neatsiejamų prietaisų, rūšis.

1.2 Privatumo ir saugumo iššūkiai

Kaip ir kiekviena šiuolaikinė technologija, išmaniosios sveikatos aplikacijos bei prietaisai turi savų iššūkių. Europos Komisijos Žaliojoje knygoje dėl mobilios sveikatos jau 2014 m. buvo pripažinta, jog sparti išmaniųjų sveikatos aplikacijų bei prietaisų plėtra kelia susirūpinimą dėl tinkamo surinktų duomenų tvarkymo pasitelkiant šią technologiją (Europos Komisija. Žalioji knyga dėl..., 2014, p. 8). Svarbu paminėti, jog išmaniosios sveikatos aplikacijos ir prietaisai renka ir apdoroja gan didelį kiekį duomenų, todėl šios technologijos naudotojai pagrįstai gali nerimauti dėl jų duomenims kylančių pavojų. Pavyzdžiui, dėl duomenų vagystės ar nepageidaujamo dalijimosi su trečiosiomis šalimis – daugeliu atvejų šią informaciją sudaro asmens duomenys, susiję su asmeniu, kurio tapatybė tiesiogiai ar netiesiogiai nustatyta arba kurio tapatybę galima nustatyti (Europos Komisija. Žalioji knyga dėl..., 2014, p. 8). Netinkamas sveikatos duomenų tvarkymas gali turėti ilgalaikį neigiamą poveikį asmenų gyvenimui ir socialinei aplinkai, todėl išmaniųjų sveikatos aplikacijų bei prietaisų naudotojų teisių pažeidimo rizika yra didelė.
Svarbu pažymėti, kad sveikatos duomenys yra vertinga prekė: didžiųjų duomenų (angl. *big data*) bendrovės vis labiau domisi sveikatos duomenimis. Būtent šios kategorijos duomenų trūkumas yra ypač jaučiamas dėl brangaus jų rinkimo proceso (van Kolfschooten, 2022). Todėl išmaniosios sveikatos aplikacijos gali skatinti naudotojus pateikti vis didesnį kiekį sveikatos duomenų, siekiant gauti daugiau pelno ir vis geresnių rezultatų. Be to, susirūpinimą kelia tai, ar naudotojai gali tinkamai kontroliuoti prieigą prie savo sveikatos duomenų. Turint omeny tai, jog dauguma išmaniųjų sveikatos aplikacijų numato galimybę

atskleisti informaciją neapibrėžtai (būsimai) auditorijai pvz., parduoti sveikatos duomenis trečiosioms šalims, tarkim, reklamuotojams ar draudimo bendrovėms (van Kolfschooten, 2022).

Apibendrinant galima daryti išvadą, kad dėl sveikatos aplikacijų vykdomo didelio masto sveikatos duomenų tvarkymo ir dalijimosi jais su trečiosiomis šalimis kyla pavojus naudotojų sveikatos duomenų kontrolei, todėl atitinkamai kyla grėsmė jų teisėms, susijusioms su duomenų apsauga.

1.3 Išmaniųjų sveikatos aplikacijų ir prietaisų atskyrimas nuo medicinos prietaisų

Tiek išmaniosios sveikatos aplikacijos ir prietaisai, tiek medicinos prietaisai renka arba gali rinkti asmens duomenis. Dėl šios priežasties kuriant abi technologijų rūšis yra svarbu atsižvelgti į duomenų apsaugos reglamentavimą. Tačiau medicinos prietaisams priskiriamai technologijai taikoma dar platesnė teisinio reglamentavimo sistema. Todėl įgyvendinami duomenų apsaugos reikalavimai turėtų praktiškai derėti su papildomai taikomais konkrečiais ir griežtais medicinos prietaisų teisės aktuose nustatytais saugos ir veiksmingumo standartais.

Šie reikalavimai, pvz., specialaus ženklinimo ar saugumo reikalavimas, daro nemažą įtaką produkto kainai, jo kūrimo, registravimo laikui ir atitinkamų nacionalinių institucijų vykdomai jo kontrolei, todėl yra ypač reikšminga atskirti išmaniąsias sveikatos aplikacijas ir prietaisus nuo medicinos prietaisų (Monegier, 2020).

Kalbant apie medicinos prietaisų reguliavimą, konkreti atskira, autonominė programinė įranga (angl. *software*) pripažįstama medicinos prietaisu. Aktualu tai, jog į programinės įrangos apibrėžimą patektų ir tokie skaitmeniniai sveikatos produktai kaip išmaniosios sveikatos aplikacijos ir prietaisai.

Medicinos prietaisų direktyvoje (toliau – **MPD**) teigiama, kad: „medicinos prietaisas – bet kuris instrumentas, aparatas, įtaisas, **programinė įranga**, medžiaga arba kitas gaminys, naudojamas atskirai arba kartu su kitais reikmenimis, įskaitant programinę įrangą, jos gamintojo specialiai numatytą naudoti diagnostikos ir (arba) gydymo tikslais ir reikalingą tinkamai jam taikyti <...>“ (Europos Parlamento ir Tarybos 2007 m. rugsėjo 5 d. direktyva 2007/47/EB..., 1 str., a p.). Nors ši direktyva nustojo galioti 2021 m., tačiau didžioji dalis jos nuostatų buvo perkeltos į ją pakeitusį naująjį Medicinos priemonių reglamentą (toliau – **MPR**). Todėl šios direktyvos nagrinėjimas ir nuostatų aiškinimas nepraranda aktualumo ir yra reikšmingas. Pagal MPR, taikomą nuo 2020 m. gegužės 26 d., medicinos prietaiso ir programinės įrangos ryšio vertinimas ypač reikšmingai nepasikeitė.

Didžiausia teisinė problema yra tai, kad teisiškai atskirti medicinos prietaisą nuo išmaniosios sveikatos aplikacijos ar prietaiso nėra lengva. MPD apibrėžiant programinę įrangą kaip medicinos prietaisą, pabrėžiami du aspektai (Europos Parlamento ir Tarybos 2007 m. rugsėjo 5 d. direktyva 2007/47/EB..., 2 str., 1 d., a p.), kurių iš esmės laikomasi ir MPR (Europos Parlamento ir Tarybos 2017 m. balandžio 5 d. reglamentas (ES) 2017/745 dėl medicinos priemonių..., 2 str., 1 d.). Pagal abu reguliavimus programinė įranga, t. y. sveikatos technologija, turi būti gamintojo skirta naudoti konkrečiai diagnostikos ir (arba) gydymo tikslais, o jos tinkamam taikymui būtina, kad gamintojas ją numatytų naudoti žmonėms vienu ar keliais iš šių tikslų: „diagnozuoti, vykdyti profilaktiką, stebėti, numatyti, prognozuoti, gydyti ar palengvinti ligą; diagnozuoti, stebėti, gydyti traumą ar negalią, jas palengvinti arba kompensuoti; tirti, visiškai pakeisti arba modifikuoti anatomiją arba fiziologinį ar patologinį procesą ar būklę <...>“, ir kuria nepasiekiamas pagrindinis numatytas veikimas – ji neveikia žmogaus organizmo iš vidaus ar išorės farmakologinėmis, imunologinėmis ar metabolinėmis priemonėmis, tačiau pastarosios gali būti naudojamos kaip pagalbinės priemonės jos veikimui užtikrinti“ (Europos Parlamento ir Tarybos 2017 m. balandžio 5 d. reglamentas (ES) 2017/745 dėl medicinos priemonių..., 2 str., 1 d.). MPR išplečiama apibrėžtis, įtraukiant prognozavimą ir numatymą, todėl kai kurios sveikatos technologijos, galinčios prognozuoti tam tikrų ligų tikimybę ar prognozę, galimai pateks į medicinos prietaiso apibrėžtį.

MPR teigiama, kad: „ <...> pati programinė įranga, kai ji gamintojo yra specialiai skirta naudoti vienu ar keliais medicinos tikslais, išdėstytais medicinos priemonės apibrėžtyje, yra laikoma medicinos priemone, o bendrosios paskirties programinė įranga, net kai ji naudojama sveikatos priežiūros sistemoje, arba gyvenimo būdo ir gerovės tikslais naudoti skirta programinė įranga nėra medicinos priemonė. <...>“ (Europos Parlamento ir Tarybos 2017 m. balandžio 5 d. reglamentas (ES) 2017/745 dėl medicinos priemonių..., 19 konstatuojamoji dalis.).

Taigi, autonominės programinės įrangos, kaip medicinos prietaiso, apibrėžimas turi du esminius elementus, t. y., **objektyvų** medicininės paskirties, kurią turi atitikti prietaisas, elementą ir **subjektyvų** gamintojo ketinimo pagaminti medicininės paskirties prietaisą elementą. Vadinasi, bet kokia programinė įranga, neatitinkanti šių dviejų elementų, būtų klasifikuojama kaip paprastas vartojimo produktas, o ne medicinos prietaisas.

Vertinant **objektyvų** medicininės paskirties elementą, programine įranga turi būti siekiama gan didelis skaičius medicininių tikslų.

Europos Komisijos Gairėse dėl sveikatos apsaugos sektoriuje naudojamos autonominės programinės įrangos priskyrimo ir klasifikacijos medicinos priemonių reglamentavimo

sistemai, pateikiama keletas programinės įrangos, kuri galėtų būti laikoma medicinos prietaisu, pavyzdžių, t. y. programinė įranga, skirta kurti ar keisti medicininę informaciją arba, jei atliekami kokie nors medicininės informacijos pakeitimai, palengvinti sveikatos priežiūros specialisto atliekamas suvokimo ir (arba) interpretavimo užduotis (Europos Komisijos Gairėse dėl sveikatos apsaugos sektoriuje naudojamos autonominės programinės įrangos..., 2016, p. 11).

Vertinant antrąjį – **subjektyvųjį** elementą (sveikatos technologijos kūrėjo ketinimą), galima remtis Europos Sąjungos Teisingumo Teismo (toliau – **ESTT**) 2012 m. lapkričio 22 d., sprendimu Brain Products GmbH prieš BioSemi VOF ir kt. (C-219/11).

Byla buvo susijusi su bendrovės BioSemi gaminamu produktu – sistema ActiveTwo, kuria galima registruoti žmogaus smegenų veiklą t. y. registruojami iš žmogaus kūno sklindantys smegenų, širdies ir raumenų elektriniai signalai. BioSemi teigimu, jų gaminys nebuvo skirtas naudoti medicininei diagnostikai ar gydymui, tačiau jis buvo naudojamas mokslininkų, atliekančių klinikinius tyrimus, ypač kognityvinių mokslų srityje (Generalinio advokato Paolo Mengozzi išvada, para 16.). „Bendrovės Brain Products teigimu, kadangi ActiveTwo yra medicinos prietaisas, o BioSemi neturi tokiems prietaisams skirto CE ženklo, toks pardavimas turi būti uždraustas“ (Byla Brain Products GmbH prieš BioSemi VOF ir kt., para 6). BrainProducts klinikiniais tikslais prekiavo panašiu produktu, kuris buvo pažymėtas CE ženklu pagal MPD. Jie teigė, kad, nepriklausomai nuo numatomo naudojimo būdo, BioSemi pagaminta sistema pagal šią direktyvą turi būti laikoma medicinos prietaisu ir atitinkamai turi būti ženklinama (Generalinio advokato Paolo Mengozzi išvada, para 18) .

Tačiau „BioSemi teigė, kad ActiveTwo nėra medicininės paskirties, todėl ji negali būti laikoma medicinos prietaisu, kaip jis suprantamas pagal MPD. Be to, tai, kad ši sistema gali būti perdaryta į diagnostikos aparatą, nereiškia, kad ją galima priskirti prie medicinos prietaisų“ (Byla Brain Products GmbH prieš BioSemi VOF ir kt., para 7). ESTT nustatė, kad tai, jog prietaisas, kuris nėra aiškiai suprojektuotas kaip medicininis, gali būti naudojamas medicininiais tikslais, nėra pakankamas pagrindas suteikti prietaisui medicinos prietaiso statusą, nes aiškus gamintojo ketinimas išlieka pagrindiniu veiksniu (Byla Brain Products GmbH prieš BioSemi VOF ir kt., para 33). Taigi, nors ActiveTwo sistema galėjo įrašyti žmogaus kūno skleidžiamus elektrinius signalus, o tokio tipo matavimai sveikatos srityje yra dažni (elektrokardiograma, elektroencefalograma ir t. t.), tačiau nagrinėjamas gaminys nebuvo sukurtas naudoti medicinos sektoriuje (Generalinio advokato Paolo Mengozzi išvada, para 16.).

Reikėtų pabrėžti, kad ESTT sprendimas prieštarauja ankstesnei generalinio advokato nuomonei, kuris teigė, kad net jei gamintojo pateikta informacija yra pagrindinis veiksnys nustatant, ar gaminys skirtas naudoti medicininiais tikslais, bet koks gaminys, kuris dėl savo pobūdžio yra aiškiai skirtas naudoti tik medicininio pobūdžio tikslais, turėtų būti laikomas medicinos prietaisu, net jeigu gamintojas to nenurodė (Generalinio advokato Paolo Mengozzi išvada, para 63). Galima būtų interpretuoti, kad generalinis advokatas turėjo omenyje tai, kad kitu atveju nesąžiningi sveikatos technologijų produktų kūrėjai, galėtų lengvai nurodyti, kad jų produktai nėra skirti naudoti medicininiams tikslams, nepaisant jų akivaizdžios medicininės paskirties ir taip išvengti griežtesnio jų produktų reglamentavimo pagal MPD bei didelių išlaidų kylančių iš medicinos prietaisų specialaus ženklinimo.

Atsižvelgiant į išdėstytą reglamentavimą ir ESTT praktiką, akivaizdu jog išmaniųjų sveikatos aplikacijų ir medicinos prietaisų atskyrimas yra itin svarbus sprendžiant dėl teisinių reikalavimų atitikties. Todėl prieš pateikiant produktą į rinką, išmaniųjų sveikatos aplikacijų ir prietaisų kūrėjai turi įvertinti savo produktą ir įsitikinti ar jis nėra priskiriamas medicinos prietaisų kategorijai. Kitu atveju, tokiai technologijai bus taikomas platesnis ir griežtesnis reguliavimo mechanizmas.

2. REGULIAVIMO YPATUMAI IR PROBLEMATIKA BDAR KONTEKSTE

Šiai dienai yra sukurta keletas reikšmingų gairių ir aiškinamųjų dokumentų skirtų padėti užtikrinti išmaniųjų sveikatos aplikacijų ir prietaisų tinkamą kūrimą, naudojimą ir reguliavimo įgyvendinimą. Pavyzdžiui, Sveikatos aplikacijų privatumo elgesio kodekso projektas ar Europos Komisijos Žalioji knyga dėl mobiliosios sveikatos, tačiau visi šie dokumentai nėra privalomo pobūdžio. Šiuo metu vienas pagrindinių teisiškai privalomų aktų, reglamentuojančių išmaniąsias sveikatos aplikacijas ir prietaisus duomenų apsaugos srityje, yra Europos Sąjungos Bendrasis duomenų apsaugos reglamentas (toliau – **BDAR**). Todėl šio dokumento analizei sveikatos aplikacijų ir prietaisų kontekste skiriama daugiausiai dėmesio. Prieš pradedant detalesnį aptarimą, prasminga apžvelgti aktualias BDAR įtvirtintas nuostatas ir sąvokas.

BDAR yra pagrindinis Europos Sąjungos duomenų privatumo teisės aktas. Tai gana didelės apimties, abstrakčių nuostatų rinkinys. BDAR taikymo sritis apibrėžiama 2 straipsnyje. Jis netaikomas kai: 1. duomenų tvarkymas yra susijęs su nacionalinio saugumo politika; 2. kai fizinis asmuo duomenis tvarko išimtinai asmeniniais ar namų ūkio tikslais; 3. kai duomenys yra tvarkomi siekiant nusikalstamų veikų prevencijos ar atsakomybės už jas; 4. ir kitoms BDAR numatytoms specialioms aplinkybėms (BDAR, 2 str.). Iš esmės BDAR yra bendras reglamentas, apimantis asmens duomenų tvarkymą tiek privačiose, tiek viešosiose įstaigose ir skirtas didžiuliam galimų informacinių problemų kiekiui spręsti (Tzanou, 2020, p. 9).

Pažymėtina, kad BDAR reglamentavimas iš esmės remiasi į du kertinius elementus: duomenų subjektus ir duomenų valdytojus bei jų teises ir pareigas. Duomenų subjektai yra fiziniai asmenys, kurių asmens duomenys yra tvarkomi, todėl šio darbo kontekste duomenų subjektais bus laikomi išmaniųjų sveikatos aplikacijų ir prietaisų naudotojai. Duomenų valdytojais yra laikomi fiziniai ar juridiniai asmenys, valdžios institucijos ar kitos įstaigos, kurios „vienos arba kartu su kitais nustato asmens duomenų tvarkymo tikslus ir priemones“ (BDAR, 4 str., 7 p.). Atitinkamai šiame darbe duomenų valdytojais bus laikomi išmaniųjų sveikatos aplikacijų ir prietaisų kūrėjai, gamintojai bei tiekėjai.

Toliau nagrinėjami pagrindiniai BDAR principai išmaniųjų sveikatos aplikacijų bei prietaisų veikimo analizės prasme.

2.1 Pagrindiniai asmens duomenų tvarkymo principai

BDAR yra principais grindžiamas reglamentas. Jame numatyti 7 principai, kuriais remiantis turi būti tvarkomi asmens duomenys: teisėtumo, sąžiningumo ir skaidrumo, tikslo apribojimo, duomenų kiekio mažinimo, tikslumo, saugojimo trukmės apribojimo, vientisumo ir konfidencialumo bei atskaitomybės principai (BDAR, 5 str.). Šių pagrindinių duomenų apsaugos principų laikymasis yra pirmas duomenų valdytojų žingsnis siekiant užtikrinti, kad jie vykdo savo prievoles pagal BDAR. Toliau kiekvienas iš principų aptariami detaliau.

Pirma, teisėtumo, sąžiningumo ir skaidrumo principas (BDAR, 5 str., 1 d., a p.) reiškia, kad bet koks asmens duomenų tvarkymas turi būti teisėtas ir sąžiningas. Asmenims turėtų būti aišku, kad su jais susiję asmens duomenys yra renkami, naudojami, kaip su jais konsultuojamasi ir kokia apimtimi asmens duomenys yra ar bus tvarkomi. Pagal skaidrumo principą reikalaujama, kad bet kokia informacija ir pranešimai, susiję su šių asmens duomenų tvarkymu, būtų lengvai prieinami ir suprantami, taip pat, kad vartojama kalba būtų aiški ir paprasta (The Data Protection Commission of Ireland. Principles of Data …). Kalbant konkrečiai apie teisėtumą, šis principas yra susijęs su tuo, kad tvarkydami asmens duomenis, duomenų valdytojai privalo turėti rimtą pagrindą tai daryti (Onetrust. Understanding the 7 Principles…). Kaip bus aiškinama vėliau, sveikatos aplikacijų bei prietaisų vykdomam duomenų tvarkymui labiausiai tinkantis pagrindas dažniausiai yra aiškus duomenų subjekto sutikimas.

BDAR įtvirtinta sąžiningumo sąvoka neatsiejama nuo teisėtumo. Tai reiškia, kad sveikatos aplikacijų ir prietaisų kūrėjai neturėtų sąmoningai nuslėpti informacijos apie tai, kokius ir kodėl duomenis jie renka. Kitaip tariant, turi būti siekiama, kad naudotojai nenustebtų, jei sužinotų, kaip valdytojai tvarko jų duomenis. Taigi, sąžiningumas reiškia, kad valdytojai nesielgs netinkamai su surinktais duomenimis ir jų nenaudos netinkamu būdu (Onetrust. Understanding the 7 Principles…).

Skaidrumas yra neatsiejamas nuo sąžiningumo: skaidrumas tai aiškus, atviras ir sąžiningas elgesys su duomenų subjektais, kai jiems duomenų valdytojai aiškiai atskleidžia, kas jie yra, kodėl ir kaip tvarko jų asmens duomenis. Laikydamiesi jo, duomenų valdytojai elgiasi sąžiningai savo duomenų subjektų atžvilgiu (Onetrust. Understanding the 7 Principles…).

Antruoju BDAR principu nustatomos duomenų naudojimo tik konkrečiai veiklai ribos. Šis tikslo apribojimo principas reiškia, kad duomenys turi būti „renkami nustatytais, aiškiai apibrėžtais bei teisėtais tikslais ir toliau netvarkomi su tais tikslais nesuderinamu būdu“ (BDAR, 5 str., 1 d., b p.). Konkretūs asmens duomenų tvarkymo tikslai turėtų būti aiškūs,

teisėti ir nustatyti prieš renkant asmens duomenis. Be to, apie juos taip pat reikia aiškiai informuoti asmenis, pateikiant privatumo pranešimą. Galiausiai, duomenų valdytojai privalo griežtai šių tikslų laikytis, apribodami duomenų tvarkymą tik nurodytais tikslais (Onetrust. Understanding the 7 Principles…). Taigi, nusprendus dėl savo tikslų ir aiškiai apie juos pranešus naudotojui, sveikatos aplikacijų ir prietaisų kūrėjai gali tvarkyti duomenis tik suderintais tikslais t. y., su naudotojo sutikimu ir tiek, kiek reikia aplikacijų ir prietaisų funkcionalumui užtikrinti (European Commission. Draft Code of…, p. 7).

Trečia, duomenų kiekio mažinimo principas reiškia, kad asmens duomenys turi būti „adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie tvarkomi“ (BDAR, 5 str., 1 d., c p.). Asmens duomenys turėtų būti tvarkomi tik tuo atveju, jei jų tvarkymo tikslo negalima pagrįstai pasiekti kitomis priemonėmis. (The Data Protection Commission of Ireland. Principles of Data …). Kitaip tariant, yra svarbu rinkti tik mažiausią kiekį duomenų, kuris yra reikalingas atitinkamiems tikslams pasiekti. Pavyzdžiui, jei būtų norima pritraukti asmenis, kurie prenumeruotų naujienlaškį, reiktų prašyti tik tos informacijos, kuri reikalinga naujienlaiškiams siųsti. Duomenų valdytojai negali rinkti asmeninių duomenų,, kurie nėra tiesiogiai susiję su rinkimo tikslu, pvz., telefono numerių ar namų adreso, kurie nėra būtini naujienlaiškio siuntimui(Onetrust. Understanding the 7 Principles…).

Ketvirta, tikslumo principas reikalauja, kad išmaniųjų sveikatos aplikacijų ir prietaisų kūrėjai užtikrintų, kad asmens duomenys būtų „tikslūs ir prireikus atnaujinami; turi būti imamasi visų pagrįstų priemonių užtikrinti, kad asmens duomenys, kurie nėra tikslūs, atsižvelgiant į jų tvarkymo tikslus, būtų nedelsiant ištrinami arba ištaisomi“ (BDAR, 5 str., 1 d., d p.). Ypač duomenų valdytojai turėtų tiksliai registruoti renkamą ar gaunamą informaciją ir tos informacijos šaltinį (The Data Protection Commission of Ireland. Principles of Data …). Taip pat, svarbu, kad išmaniųjų sveikatos aplikacijų ir prietaisų kūrėjai nustatytų reguliarius patikrinimus, kad būtų galima ištaisyti, atnaujinti arba ištrinti gautus neteisingus arba neišsamius duomenis (Onetrust. Understanding the 7 Principles…).

Penkta, saugojimo trukmės apribojimo principas turi būti aiškinamas kaip reikalaujantis, kad asmens duomenys būtų „laikomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, nei tai yra būtina tais tikslais, kuriais asmens duomenys yra tvarkomi“ (BDAR, 5 str., 1 d., e p.). Be to, siekdami užtikrinti, kad asmens duomenys nebūtų saugomi ilgiau nei būtina, duomenų valdytojai turėtų nustatyti asmens duomenų ištrynimo arba periodinės peržiūros terminus (The Data Protection Commission of Ireland. Principles of Data …).

Šešta, pagal BDAR reikalaujama, kad būtų išlaikytas surinktų duomenų vientisumas ir konfidencialumas (BDAR, 5 str., 1 d., f p.), t. y. duomenys būtų saugomi nuo vidinių ir išorinių grėsmių. Siekiant tai užtikrinti yra reikalingas efektyvus planavimas ir aktyvus reagavimas. Išmaniųjų sveikatos aplikacijų ir prietaisų kūrėjai turi apsaugoti duomenis nuo neleistino ar neteisėto tvarkymo ir atsitiktinio praradimo, sunaikinimo ar sugadinimo (Onetrust. Understanding the 7 Principles…).

Galiausiai duomenų valdytojas yra atsakingas už visų pirmiau išvardytų duomenų apsaugos principų laikymąsi ir turi sugebėti tai įrodyti (BDAR, 5 str. 2 d.). Išmaniųjų sveikatos aplikacijų ir prietaisų kūrėjai privalo turėti tinkamas priemones ir įrašus, įrodančius, kad yra laikomasi duomenų tvarkymo principų, turint omeny, jog priežiūros institucijos gali bet kada paprašyti pateikti šiuos įrodymus (Onetrust. Understanding the 7 Principles…). Atitinkamai, paskutinysis – atskaitomybės principas – yra vienas svarbiausių, apimantis visus aukščiau išvardintus.

Taip pat svarbu paminėti BDAR 25 straipsnyje įtvirtintą pritaikytosios duomenų apsaugos ir standartizuotosios duomenų apsaugos (angl. *data protection by design and default*) principą, kuris veikia kaip prieš tai minėtų principų įgyvendinimo būdas. Šis principas turi ypatingai didelę reikšmę technologijų kūrėjams, įskaitant ir išmaniųjų sveikatos aplikacijų bei prietaisų kūrėjus. Jis reikalauja, kad duomenų apsauga būtų įtraukta į visą technologijos gyvavimo ciklą – nuo ankstyvojo projektavimo etapo iki galutinio įdiegimo, naudojimo ir galutinio sunaikinimo. Taip pat svarbu, kad kūrėjai užtikrintų, jog technologija būtų sukurta taip, kad būtų išvengta nereikalingų asmens duomenų tvarkymo (Article 29 data protection working party. Opinion on Privacy and..., 2015).

2.2 Sveikatos duomenys kaip specialių kategorijų duomenys

BDAR taikomas visų tipų aplikacijoms, tvarkančioms asmens duomenis, neatsižvelgiant į tai, ar aplikacijoje yra nuoroda į sveikatos ar kitų tipų asmens duomenis. Tačiau svarbu atkreipti dėmesį, jog pagal BDAR 9 straipsnį draudžiama tvarkyti specialių kategorijų duomenis, įskaitant „<...> genetinius duomenis, biometrinius duomenis, siekiant konkrečiai nustatyti fizinio asmens tapatybę, **sveikatos duomenis** arba duomenis apie fizinio asmens lytinį gyvenimą ir lytinę orientaciją“ (BDAR, 9 str. 1 d.). BDAR 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“ (BDAR, 4 str. 15 d.). BDAR 35 konstatuojamojoje dalyje dar labiau patikslinama apibrėžtis, pateikiant

pavyzdžių, kas patenka į su sveikata susijusių duomenų kategoriją: „prie asmens sveikatos duomenų turėtų būti priskirti visi duomenys apie duomenų subjekto sveikatos būklę, kurie atskleidžia informaciją apie duomenų subjekto buvusią, esamą ar būsimą fizinę ar psichinę sveikatą. Tai apima informaciją apie fizinį asmenį, surinktą registruojantis sveikatos priežiūros paslaugoms gauti ar jas teikiant tam fiziniam asmeniui, <...>; fiziniam asmeniui priskirtą numerį, simbolį ar žymę, pagal kurią galima konkrečiai nustatyti fizinio asmens tapatybę sveikatos priežiūros tikslais; informaciją, gautą atliekant kūno dalies ar medžiagos tyrimus ar analizę, įskaitant genetinius duomenis ir biologinius mėginius; ir bet kurią informaciją apie, pavyzdžiui, ligą, negalią, riziką susirgti, sveikatos istoriją, klinikinį gydymą arba duomenų subjekto fiziologinę ar biomedicininę būklę, neatsižvelgiant į informacijos šaltinį, pavyzdžiui, ar ji būtų gauta iš gydytojo, ar iš kito sveikatos priežiūros specialisto, ligoninės, in vitro diagnostinio tyrimo, medicinos priemonės" (BDAR, 35 konstatuojamoji dalis). Taigi, sveikatos duomenys apima tiek medicininio pobūdžio duomenis pvz., medicininių / instrumentinių tyrimų rezultatus, tiek duomenis, susijusius su duomenų subjekto sveikatos būkle, neatsižvelgiant į jų rinkimo tikslą ir kontekstą. Pastaroji kategorija yra plati ir, svarbiausia, apima duomenis apie ligų susirgimo riziką.

29 straipsnio darbo grupė (toliau – **Darbo grupė**)[1] vienoje iš savo nuomonių šiek tiek patikslino su sveikata susijusių duomenų apimtį (Article 29 data protection working party. Letter to Paul…, 2015). Pasak Darbo grupės, informacija, pavyzdžiui, kad asmuo susilaužė koją, kad jis nešioja akinius ar kontaktinius lęšius, duomenys apie asmens intelektinius ir emocinius gebėjimus pvz., IQ, informacija apie rūkymo ir alkoholio vartojimo įpročius, duomenys apie alergijas, atskleidžiami privatiems subjektams pvz., avialinijoms arba viešosioms įstaigoms pvz., mokykloms; duomenys apie sveikatos būklę, kurie turi būti naudojami skubios pagalbos atveju pvz., informacija, kad vasaros stovykloje ar panašiame renginyje dalyvaujantis vaikas serga astma; asmens narystė pacientų paramos grupėje pvz. pagalbos sergant vėžiu grupėje, anoniminių alkoholikų ar kitų savitarpio pagalbos ir paramos grupėse, kurių tikslas yra susijęs su sveikata; ar vien tik paminėjimas, kad asmuo serga darbo aplinkoje, yra duomenys apie atskirų duomenų subjektų sveikatą (Article 29 data protection working party. Letter to Paul…, 2015). Šiai kategorijai taip pat priskiriami duomenys apie medicinos produktų, prietaisų ir paslaugų pirkimą, kai iš duomenų galima spręsti apie sveikatos būklę, arba informacija apie dalyvavimą tam tikruose pasirinktinai

[1] Tai nepriklausoma institucija, turinti konsultacinį statusą. Ši institucija skelbė nuomones ir siekė suderinti duomenų apsaugos taisyklių taikymą Europos Sąjungoje. Įsigaliojus BDAR, ji nustojo veikti ir ją pakeitė Europos duomenų apsaugos valdyba. Nepaisant BDAR priėmimo ir išformavus Darbo grupę, daugelis jos priimtų gairių ir nuomonių tebėra aktualios, kadangi jos yra grindžiamos principais ir straipsniais, kurie tebegalioja BDAR.

atliekamuose atrankinės patikros tyrimuose pvz., atrankinės patikros dėl AIDS ar kitų lytiškai plintančių ligų arba retų ligų (Article 29 data protection working party. Letter to Paul…, 2015). Apibendrindama Darbo grupė nurodė, kad asmens duomenys yra sveikatos duomenys, kai: 1. duomenys iš prigimties yra medicininiai duomenys, 2. kai duomenys gali būti naudojami vieni arba kartu su kitais duomenimis, kad būtų galima padaryti išvadą apie faktinę asmens sveikatos būklę arba riziką sveikatai, 3. daromos išvados apie asmens sveikatos būklę ar riziką sveikatai (Article 29 data protection working party. Letter to Paul…, 2015). Taip pat nuomonėje buvo išsamiai aptarta informacijos apie ligos susirgimo riziką apimtis. Darbo grupės teigimu, informacija apie susirgimo liga riziką apima informaciją apie asmens nutukimą, aukštą ar žemą kraujospūdį, paveldimą ar genetinį polinkį, besaikį alkoholio vartojimą, tabako vartojimą, narkotikų vartojimą arba bet kokią kitą informaciją, kai yra moksliškai įrodyta arba visuotinai suvokiama ligos rizika ateityje (Article 29 data protection working party. Letter to Paul…, 2015). Taigi, sveikatos duomenų apimtis yra gana plati ir dauguma sveikatos aplikacijų surinktų duomenų patenka į šią kategoriją. Be to, sveikatos aplikacijos taip pat gali generuoti biometrinius duomenis remiantis naudotojo elgsena. Pagal BDAR biometriniai duomenys apibrėžiami kaip „po specialaus techninio apdorojimo gauti asmens duomenys, susiję su fizinio asmens fizinėmis, fiziologinėmis arba elgesio savybėmis, pagal kurias galima konkrečiai nustatyti arba patvirtinti to fizinio asmens tapatybę, kaip antai veido atvaizdai arba daktiloskopiniai duomenys“ (BDAR, 4 str., 4 d.). Vadinasi, dauguma sveikatos aplikacijų renkamų duomenų patenka į BDAR 9 straipsnyje pateiktą sveikatos, biometrinių ar genetinių duomenų apibrėžtį, todėl jiems taikomi griežtesni tvarkymo reikalavimai.

2016 m. ES paskelbė Sveikatos aplikacijų privatumo elgesio kodekso projektą (toliau – **Kodekso projektas**), kuriame nurodoma, kaip sveikatos aplikacijų gamintojai gali apsaugoti naudotojų privatumą (European Commission. Draft Code of…, 2016). Kodekso projektą parengė mobilios sveikatos t. y. sveikatos aplikacijų ir prietaisų kūrėjų bei gamintojų organizacijos, o jį parengti padėjo Europos Komisija. Kodekso projektu siekiama skatinti mobiliųjų aplikacijų, kuriose tvarkomi asmens duomenys, įskaitant duomenis apie sveikatą, naudotojų pasitikėjimą (European Commission. Draft Code of…, 2016). Taip pat, siekiama skatinti sveikatos aplikacijų ir prietaisų plėtrą, kartu užtikrinant aukšto lygio naudotojų sveikatos duomenų apsaugą pagal BDAR. Nors Kodeksas aplikacijų kūrėjams būtų savanoriškas ir neprivalomas, tačiau jo turinys padeda dar labiau suprasti sveikatos duomenų kaip specialių kategorijų duomenų reikšmę. Šiek tiek vėliau po jo paskelbimo, projektas buvo pateiktas tvirtinti Darbo grupei. Tačiau Darbo grupė kodekso projektui nepritarė, todėl šiuo metu kodekso projektas rengiamas iš naujo, kad atitiktų

Darbo grupės pastabas (European Commission. Shaping Europe's digital…, 2018). Visgi šis dokumentas išlieka aktualus nagrinėjamos temos prasme. Toliau Kodekso projektas bus nagrinėjamas atsižvelgiant į Darbo grupės pastabas.

Kaip buvo minėta anksčiau, šio darbo kontekste į sąvoką sveikatos aplikacija patenka vadinamos gyvenimo būdo aplikacijos ir nuo jų neatsiejami prietaisai (kurie nėra laikomi medicinos prietaisais). Svarbu aptarti būtent šią sąvokos dalį, kadangi dėl šių aplikacijų bei prietaisų renkamų duomenų pobūdžio kyla nemažai taikymo trūkumų. Neaiškumai atsiranda todėl, kad gyvenimo būdo duomenys, kurie didžiąja dalimi nėra susiję su asmens sveikata, ne visada galėtų būti priskiriami prie sveikatos duomenų kategorijos. Taigi, gali kilti interpretavimo iššūkių, kadangi duomenys apie gyvenimo būdą bus laikomi sveikatos duomenimis tik tuomet, kai jie yra aiškiai ir glaudžiai susiję su asmens sveikatos būkle (European Commission. Draft Code of…, 2016). Pažymėtina, jog Kodekso projekte atskiriami sveikatos duomenys ir gyvenimo būdo duomenys. BDAR tokio atskyrimo nėra, nes jame pateikiama tik pozityvi sveikatos duomenų apibrėžtis, tačiau neapibrėžiama, kas nepatenka į šios apibrėžties taikymo sritį (BDAR, 4 str., 15 d., 35 konstatuojamoji dalis). Vienas iš Kodekso projekto tikslų yra užpildyti tokią spragą ir paaiškinti informacijos apie gyvenimo būdą pobūdį. Taigi, Kodekso projekte sveikatos duomenys apibrėžiami kaip bet kokie asmens duomenys, susiję su fizine ar psichine asmens sveikata, įskaitant sveikatos priežiūros paslaugų teikimą, kurie atskleidžia informaciją apie asmens sveikatos būklę (European Commission. Draft Code of…, 2016, p. 2), toks apibrėžimas atspindi BDAR 4 straipsnyje pateiktą apibrėžtį. Tačiau taip pat pateikiama ir gyvenimo būdo duomenų sąvoka. Teigiama, kad neapdoroti duomenys apie asmens įpročius ir elgseną, kurie iš esmės nėra susiję su asmens sveikata, nebūtinai bus laikomi sveikatos duomenimis (European Commission. Draft Code of…, 2016, p. 2). Taip pat, Kodekso projekte pabrėžiama, kad abiejų kategorijų duomenims (sveikatos ir gyvenimo būdo) taikoma duomenų apsaugos teisė (European Commission. Draft Code of…, 2016, p. 2–3). Tačiau sveikatos duomenys pripažįstami jautresniais, todėl jiems taikomas aukštesnis apsaugos lygis, t. y. BDAR 9 straipsnyje nustatytas draudimas tvarkyti specialių kategorijų duomenis.

Kodekso projekte pateikiamas naudotojo žingsnius sekančios aplikacijos pavyzdys. Jei vienintelis aplikacijos tikslas – matuoti ir stebėti naudotojo fizinį aktyvumą, šie duomenys yra tik gyvenimo būdo duomenys (European Commission. Draft Code of…, 2016, p. 2). Tačiau tie patys duomenys priskiriami sveikatos duomenims, jei žingsnių sekimo tikslas yra matuoti ar prognozuoti riziką sveikatai (pvz., riziką susižeisti ar patirti infarktą) ir (arba) saugoti duomenis siekiant analizuoti ir vertinti naudotojo sveikatą (European Commission. Draft Code of…, 2016, p. 2). Toks sveikatos duomenų aiškinimas atspindi jau minėtą

Darbo grupės nuomonę, kurioje teigiama, kad tai, ar duomenys patenka į sveikatos duomenų apimtį, nustatoma pagal numatomą duomenų naudojimą. Šioje nuomonėje gyvenimo būdo duomenys apibrėžiami kaip duomenys iš kurių negalima daryti pagrįstų išvadų apie duomenų subjekto sveikatos būklę. Teigiama, kad ne visi per aplikaciją surinkti neapdoroti duomenys (matavimai) gali būti laikomi informacija, iš kurios galima daryti išvadas apie asmens sveikatos būklę (Article 29 data protection working party. Letter to Paul…, 2015). Pavyzdžiui, jei aplikacija skaičiuotų tik žingsnių skaičių vieno pasivaikščiojimo metu ir negalėtų šių duomenų sujungti su kitais apie tą patį duomenų subjektą gautais duomenimis, ir jei nėra konkretaus medicininio konteksto, kuriame bus naudojami aplikacijos duomenys, tikėtina, kad surinkti duomenys neturės reikšmingo poveikio duomenų subjekto privatumui ir jiems nereikės papildomos specialios sveikatos duomenų kategorijos apsaugos (Article 29 data protection working party. Letter to Paul…, 2015). Tai tik neapdoroti (palyginti nedidelį poveikį gyvenimo būdui darantys) asmens duomenys (jei aplikacija netvarko buvimo vietos duomenų), o ne informacija, iš kurios būtų galima spręsti apie asmens sveikatą. Nuomonėje taip pat teigiama, kad su sveikatos duomenų tvarkymu susijęs pavojus privatumui turi būti vertinamas atsižvelgiant į sparčią mobiliųjų ir dėvimųjų technologijų raidą, leidžiančią žmonėms registruoti įvairius aspektus apie savo asmenybę, protą, kūną, elgesio modelius ir buvimo vietą. (Article 29 data protection working party. Letter to Paul…, 2015). Kartu su kitais duomenimis šie duomenys gali būti naudojami išvadoms apie aplikacijomis ir prietaisais besinaudojančių duomenų subjektų sveikatą daryti bei taip pat gali tapti piktybinių veiksmų objektu. Tokio duomenų tvarkymo pavyzdys – socialinės medijos analizė siekiant nustatyti, ar žmonės galimai neserga depresija. Nors naudotojų siunčiamų liūdnų žinučių socialiniai tinklai apskritai neturi laikyti sveikatos duomenimis, sisteminga tokių žinučių analizė diagnozavimo ir (arba) sveikatos rizikos prevencijos ar medicininių tyrimų tikslais neabejotinai laikytina sveikatos duomenų tvarkymu (Article 29 data protection working party. Letter to Paul…, 2015). Kalbant apie aplikacijas, reikšminga suprasti, kad duomenis apie save renka ne tik naudotojas t. y., jie taip pat yra tvarkomi duomenų valdytojo. Labai svarbu, kad naudotojai galėtų sąmoningai nuspręsti, ar jie sutinka, ar ne su bet kokiu duomenų, iš kurių galima daryti išvadas apie jų sveikatą, tvarkymu (Article 29 data protection working party. Letter to Paul…, 2015). Pavyzdžiui, yra daugybė aplikacijų, kuriomis naudodamiesi duomenų subjektai gali pateikti savo svorį ir ūgį, kad būtų galima apskaičiuoti kūno masės indeksą. Kai duomenys sujungiami su žingsnių matuokliu, duomenų valdytojas gali naudoti šiuos duomenis, norėdamas nustatyti, ar asmens gyvenimo būdas yra sėslus, ar ne. Sujungęs šiuos duomenis, duomenų valdytojas kai

kuriuos naudotojus gali priskirti populiacijai, kuriai kyla didesnė rizika sveikatai. Jei duomenų valdytojas aiškiai neinformuoja aplikacijos naudotojų apie duomenų tvarkymo tikslus, naudotojai gali nepagrįstai manyti, kad visi jų duomenys lieka jų pačių įrenginyje ir yra skirti tik jų pačių naudojimui (Article 29 data protection working party. Letter to Paul…, 2015). Atsižvelgiant į tai, kad tokį duomenų tvarkymą nėra lengva pripažinti sveikatos duomenų tvarkymu, tačiau kartu jis kelia realią riziką privatumui, svarbu nustatyti kriterijus, kurie padėtų nuspręsti, kokiais atvejais gyvenimo būdo duomenys turėtų būti laikomi sveikatos duomenimis. Nuomonėje taip pat pateikiami pavyzdžiai galimų rodiklių, leidžiančių nustatyti, kad sveikatos duomenys yra tvarkomi. Taigi, neapdoroti, palyginti nedidelį poveikį privatumui darantys asmens duomenys gali greitai virsti sveikatos duomenimis, kai juos galima naudoti asmens sveikatos būklei nustatyti. Norint tai įvertinti, nepakanka pažvelgti į patį duomenų pobūdį. Taip pat reikia atsižvelgti į jų paskirtį, atskirai arba kartu su kita informacija (Article 29 data protection working party. Letter to Paul…, 2015). Pavyzdžiui, vien tik užregistravus asmens svorį, kraujospūdį arba pulsą ir (arba) širdies ritmą, bent jau be jokios papildomos informacijos apie amžių ar lytį, negalima daryti išvados apie faktinę ar tikėtiną būsimą to asmens sveikatos būklę. Tačiau šie nustatyti faktai, laikui bėgant, ypač kartu su amžiumi ir lytimi, gali būti naudojami svarbiam asmens sveikatos aspektui nustatyti, pavyzdžiui, su nutukimu ar liga, dėl kurios labai sumažėja svoris, aukštu ir (arba) žemu kraujospūdžiu, aritmija ir t. t., susijusiai sveikatos rizikai nustatyti. Žymus svorio sumažėjimas gali būti susijęs su keliomis priežastimis, kai kuriomis teigiamomis (dieta), kai kuriomis neigiamomis (sunkaus gydymo poveikis, depresija ir kt.) (Article 29 data protection working party. Letter to Paul…, 2015). Labai svarbu pabrėžti, kad tokio pobūdžio informacija nėra neutrali. Kai daromos išvados apie kieno nors sveikatą, neatsižvelgiant į jų patikimumą, šios išvados turi būti laikomos sveikatos duomenimis. Taip pat nuomonėje teigiama, kad turi būti akivaizdus ryšys tarp neapdorotų duomenų ir gebėjimo nustatyti asmens sveikatos būklę. Pavyzdžiui, jei mitybos aplikacijoje skaičiuojamos tik kalorijos, apskaičiuotos pagal duomenų subjekto pateiktus duomenis, o informacija apie konkrečius suvalgytus maisto produktus nesaugoma, vargu ar būtų galima daryti kokias nors reikšmingas išvadas apie to asmens sveikatą (nebent per dieną suvartojamų kalorijų kiekis būtų per didelis) (Article 29 data protection working party. Letter to Paul…, 2015). Tačiau jei dietos aplikacijos, širdies ritmo matuoklio ar miego dienoraščio aplikacijos duomenys sujungiami su duomenų subjekto pateikta informacija (tiesiogiai ar netiesiogiai, pavyzdžiui, remiantis informacija, surinkta iš to asmens socialinio tinklo profilio), gali būti daromos išvados (tikslios ar netikslios) apie to asmens sveikatos būklę, pvz., medicininę riziką ar diabetą, tokiais

atvejais tikėtina, kad tai bus laikoma sveikatos duomenimis (Article 29 data protection working party. Letter to Paul…, 2015).

Taigi, sveikatos duomenų ir gyvenimo būdo duomenų atskyrimas yra svarbus, nes atitinkamai šioms dviems duomenų kategorijoms bus taikomi skirtingi reikalavimai. Iš tiesų, jei tam tikra sveikatos aplikacijų ir prietaisų informacija būtų laikoma gyvenimo būdo duomenimis, šiai informacijai BDAR 9 straipsnio 1 dalis (draudimas tvarkyti duomenis) nebūtų taikoma. Tokiu atveju duomenų valdytojai ir (arba) duomenų tvarkytojai galėtų tvarkyti tokią informaciją tik gavę naudotojo sutikimą pagal BDAR 6 straipsnio 1 dalį. Suprantama, kad šių kategorijų duomenų atskyrimas BDAR kontekste turi daug pasekmių, o kadangi šiuo metu nėra aiškių atskyrimo gairių, atsiranda tam tikro subjektyvumo ir galimų tinkamos duomenų apsaugos trūkumų. Visgi, būtų tikslinga laikytis plačios sveikatos duomenų apibrėžties pagal BDAR ir vengti skirtumų, ypač atsižvelgiant į sąžiningumo ir proporcingumo principus, taip pat į tai, kad naujosios technologijos suteikia vis daugiau stebėjimo galimybių (Article 29 data protection working party. Letter to Paul…, 2015).

Svarbu atkreipti dėmesį, kad kai kurie gyvenimo būdo duomenys patenka į biometrinių duomenų, kurie pagal 9 BDAR straipsnį pripažįstami kaip speciali duomenų kategorija, taikymo sritį. Kaip minėta anksčiau, BDAR biometriniai duomenys apibūdinami kaip „po specialaus techninio apdorojimo gauti asmens duomenys, susiję su fizinio asmens fizinėmis, fiziologinėmis arba elgesio savybėmis <...>“ (BDAR 4 str., 4 d.). Įtraukus elgesio savybes, BDAR priimta plati biometrinių duomenų apibrėžtis. Kol kas neaišku, ką apima elgsenos savybės, tačiau šis terminas gali būti aiškinamas kaip apimantis tam tikrus asmens veiksmus ir įpročius, taigi apimantis didelę dalį gyvenimo būdo duomenų (Article 29 data protection working party. Letter to Paul…, 2015).

Apibendrinant nurodytų BDAR straipsnių aiškinimą ir teisės doktrinoje pateikiamus pavyzdžius, galima rasti daugiau argumentų, pagrindžiančių gyvenimo būdo duomenų priskyrimą specialių kategorijų asmens duomenims. Toks vertinimas taip pat užtikrintų šių jautrių duomenų specialią apsaugą ir paliktų mažai vietos spragoms bei savivalei. Todėl šio darbo kontekste aplikacijų bei prietaisų tvarkomi gyvenimo būdo duomenys bus laikomi sveikatos duomenimis.

2.3 Sutikimo išimtis sveikatos duomenų tvarkymui

Atsižvelgiant į prieš tai padarytą išvadą, kad visų rūšių sveikatos aplikacijos tvarko sveikatos duomenis, aktualu nagrinėti būtent specialių kategorijų duomenų teisėto tvarkymo pagrindus.

Kaip minėta anksčiau, pagal BDAR yra draudžiama tvarkyti specialių kategorijų asmens duomenis, išskyrus atvejus, kai taikoma viena iš 9 straipsnyje nurodytų išimčių (BDAR, 9 str. 1 d.). Šiuo atžvilgiu, kalbant apie išmaniąsias sveikatos aplikacijas ir prietaisus, aktualiausia išimtis, kurioje minima būtinybė gauti aiškų duomenų subjekto sutikimą tvarkyti jo asmens duomenis (BDAR 9 str., 2 d., a p).

Visų pirma kalbant apie duomenų subjekto sutikimą, svarbu paminėti, jog jis turi būti konkretus ir duodamas laisva valia (BDAR, 4 str., 11 p.). Remiantis Europos duomenų apsaugos valdybos (toliau – **EDAV**) gairėmis dėl sutikimo: „sutikimo sąvokos elementas „laisvas“ reiškia, kad duomenų subjektai turi realų pasirinkimą ir kontrolę. Pagal BDAR įtvirtintą bendrą taisyklę, jei duomenų subjektas neturi realaus pasirinkimo, jaučiasi priverstas sutikti arba patirtų neigiamų pasekmių, jei sutikimo neduotų, toks sutikimas negalioja. Jei sutikimas yra neatskiriamai sujungtas su sąlygomis kaip jų dalis, dėl kurios nesiderama, jis laikomas ne laisva valia duotu sutikimu. Taigi, sutikimas nebus laikomas laisvu sutikimu, jei duomenų subjektas negalės atsisakyti sutikti arba duoto sutikimo atšaukti, nepatirdamas žalos“ (Europos duomenų apsaugos valdyba. Gairės dėl sutikimo..., 2020, p. 7).

Taip pat, aplikacijų kūrėjai turi užtikrinti, kad sutikimas būtų duodamas vienu ar keliais konkrečiais, aiškiais ir teisėtais tikslais. Prieš tai minėtose gairėse teigiama, kad: „reikalavimu, kad sutikimas būtų konkretus, siekiama duomenų subjektui užtikrinti tam tikrą vartotojo turimą kontrolę ir skaidrumą“ (Europos duomenų apsaugos valdyba. Gairės dėl sutikimo..., 2020, p. 14). Be to, turi būti užtikrinta, kad duomenų subjektai turėtų teisę bet kada atšaukti duotą sutikimą (BDAR, 7 str., 3d.). Taip pat, prašymas duoti sutikimą turi būti glaustas, skaidrus, suprantamas ir lengvai prieinamos formos, vartojant aiškią ir paprastą kalbą: „tai reiškia, kad toks prašymas turėtų būti lengvai suprantamas ne tik teisininkams, bet ir paprastam žmogui. Duomenų valdytojai negali naudoti ilgų, sunkiai suprantamų privatumo politikos tekstų ar pareiškimų, kuriuose gausu teisės terminų. Sutikimas turi būti aiškus ir atskiriamas nuo kitų dalykų bei pateikiamas suprantama ir lengvai prieinama forma. Šis reikalavimas iš esmės reiškia, kad priimant informacija grindžiamus sprendimus duoti sutikimą ar jo neduoti, svarbi informacija negali būti

„paslėpta“ bendrosiose sąlygose“ (Europos duomenų apsaugos valdyba. Gairės dėl sutikimo..., 2020, p. 14).

Aiškinant aiškaus sutikimo specifiką gairėse teigiama, kad „aiškus sutikimas yra reikalingas tam tikromis aplinkybėmis, kai kyla rimta su duomenų apsauga susijusi rizika, todėl manoma, kad reikia griežtos individualios asmens duomenų kontrolės“ (Europos duomenų apsaugos valdyba. Gairės dėl sutikimo..., 2020, p. 21). Taip pat, teigiama, kad: „terminas „aiškus“ reiškia tai, kaip duomenų subjektas išreiškia sutikimą. Tai reiškia, kad duomenų subjektas turi pateikti aiškų sutikimo pareiškimą. Akivaizdžiai tinkamas būdas užtikrinti sutikimo aiškumą būtų aiškiai patvirtinti sutikimą rašytiniu pareiškimu“ (Europos duomenų apsaugos valdyba. Gairės dėl sutikimo..., 2020, p. 21). Tačiau, kalbant apie skaitmeninę erdvę ir sveikatos aplikacijas, būtų pakankama jei duomenų subjektas užpildytų sutikimo elektroninę formą (Europos duomenų apsaugos valdyba. Gairės dėl sutikimo..., 2020, p. 21).

Taigi, tais atvejais, kai reikalingas duomenų subjekto aiškus sutikimas, aplikacijos kūrėjai taip pat turi atsižvelgti į BDAR straipsnius, susijusius su sutikimu, įskaitant principus, susijusius su asmens duomenų tvarkymu (5 straipsnis), sąlygas, kuriomis duomenų tvarkymas yra teisėtas (6 straipsnis), ir sutikimo sąlygas (7 straipsnis). Taip pat, 12 ir 13 straipsniai taikomi dėl informacijos, kurią duomenų valdytojas turi pateikti duomenų subjektui, rūšies (13 straipsnis) ir dėl informacijos apie duomenų subjekto teises kokybės (12 straipsnis). Gairėse taip pat minima, kad: „BDAR yra sugriežtintas reikalavimas, kad sutikimas turi būti pagrįstas informacija. <...> Suteikti duomenų subjektams informaciją prieš gaunant jų sutikimą yra labai svarbu, kad jie galėtų priimti informacija pagrįstus sprendimus, suprastų, su kuo sutinka, ir, pavyzdžiui, naudotųsi savo teise atšaukti duotą sutikimą. Jei duomenų valdytojas neteikia prieinamos informacijos, vartotojas tokiu atveju turi tik tariamą kontrolę, ir sutikimas nėra tinkamas duomenų tvarkymo pagrindas. Jei nebus laikomasi reikalavimų gauti informacija pagrįstą sutikimą, to pasekmės bus tokios, kad sutikimas negalios ir duomenų valdytojas galimai pažeis BDAR“ (Europos duomenų apsaugos valdyba. Gairės dėl sutikimo..., 2020, p. 15). Be to, teigiama, kad: „norint gauti galiojantį sutikimą, būtina pateikti nors šią informaciją: 1. Duomenų valdytojo tapatybę; 2. Kiekvienos iš duomenų tvarkymo operacijų, kurioms prašoma sutikimo, tikslą; 3. Kokie (kokios rūšies) duomenys bus renkami ir naudojami; 4. Informaciją apie turimą teisę atšaukti sutikimą; <…>” (Europos duomenų apsaugos valdyba. Gairės dėl sutikimo..., 2020, p. 15). Kalbant apie tai kaip informacija turi būti pateikta, teigiama, kad: „BDAR nenurodyta, kokia forma ar pavidalu turi būti teikiama informacija vykdant reikalavimą gauti informacija pagrįstą sutikimą. Tai reiškia, kad tinkama informacija gali būti

pateikiama įvairiais būdais, kaip antai, rašytiniais ar žodiniais pareiškimais, garso arba vaizdo pranešimais <...>“ (Europos duomenų apsaugos valdyba. Gairės dėl sutikimo..., 2020, p. 16).

Apibendrinant galima teigti, kad norint tinkamai tvarkyti specialių kategorijų duomenis (sveikatos duomenis) išmaniųjų sveikatos aplikacijų ir prietaisų kontekste, būtina gauti aiškų duomenų subjektų sutikimą bei įgyvendinti kitus sutikimui BDAR numatytus reikalavimus. Tik įgyvendinus šias pareigas duomenų valdytojai galės pagrįsti, jog sveikatos duomenys yra tvarkomi teisėtu būdu.

2.4 Duomenų subjektų teisės

Įsigaliojus BDAR, asmenims buvo suteiktos 7 duomenų subjekto teisės, kurių bendras tikslas – suteikti asmenims galimybę kontroliuoti savo asmens duomenis. Šios teisės yra: teisė būti informuotam apie duomenų tvarkymą, teisė susipažinti su asmens duomenimis, juos ištaisyti, teisė būti pamirštam, teisė į duomenų perkeliamumą, teisė apriboti duomenų tvarkymą ir nesutikti su juo. Toliau kiekviena iš šių teisių bus aptariama detaliau.

Pirma, duomenų subjektas turi teisę gauti informaciją, kai tvarkomi jo asmens duomenys (teisė būti informuotam apie duomenų tvarkymą). Informaciją apie asmens duomenų tvarkymą duomenų valdytojas turi pateikti ir tada, kai duomenys yra renkami, ir tada, kai duomenų subjektas pats to paprašo. Kitaip sakant, ši teisė leidžia išmaniųjų sveikatos aplikacijų ir prietaisų naudotojams žinoti, kokie asmens duomenys apie juos yra renkami, kodėl, kas juos renka, kiek laiko jie bus saugomi, kaip jie gali pateikti skundą ir su kuo bus dalijamasi duomenimis. Tiksliau, sveikatos aplikacijų ir prietaisų kūrėjai privalo atitikti bendruosius reikalavimus ir pateikti informaciją numatytą BDAR 13 – 14 str. Svarbu, kad visa ši informacija turi būti pateikiama paprasta ir aiškia kalba.

Antra, išmaniųjų sveikatos aplikacijų ir prietaisų naudotojai turi teisę pateikti prašymus ir gauti iš duomenų valdytojų informaciją apie tai, ar yra tvarkomi jų asmens duomenys (teisė susipažinti su asmens duomenimis). Tuomet išmaniųjų sveikatos aplikacijų ir prietaisų kūrėjai privalo pateikti turimų asmens duomenų apie asmenį kopiją ir papildomą informaciją numatytą BDAR 15 str. Be to, duomenų subjektai turi teisę kreiptis į išmaniųjų sveikatos aplikacijų ir prietaisų kūrėjus, kurie tvarko asmens duomenis, ir prašyti ištaisyti netikslią informaciją (teisė ištaisyti duomenis). Tai taip pat reiškia, kad asmuo turi teisę papildyti trūkstamus asmens duomenis, kurie yra svarbūs atsižvelgiant į asmens duomenų tvarkymo tikslą (BDAR, 16 str.).

Trečia, išmaniųjų sveikatos aplikacijų ir prietaisų naudotojai turi teisę kreiptis į duomenų valdytojus, kurie tvarko jų asmens duomenis, ir prašyti ištrinti su jais susijusius duomenis (teisė būti pamirštam). Pagal šią teisę duomenų subjektai gali prašyti, kad jų asmens duomenys būtų ištrinti, jei: asmens duomenys yra nebereikalingi; duomenų subjektas atšaukia savo sutikimą, asmens duomenys buvo tvarkomi neteisėtai; duomenų subjektas prieštarauja duomenų tvarkymui, o duomenų valdytojas neturi pagrindo tęsti duomenų tvarkymo; duomenų ištrynimas yra būtinas, kad būtų įvykdyta teisinė prievolė (BDAR, 17 str., 1 d.). Tačiau yra atvejų, kai duomenų valdytojai gali atsisakyti tenkinti prašymą ištrinti duomenis. Pavyzdžiui, dėl priežasčių, susijusių su viešuoju interesu arba teisinių įsipareigojimų laikymusi (BDAR, 17 str., 2 d.).

Ketvirta, kiekvienas duomenų subjektas, pateikęs savo asmens duomenis, tam tikrais atvejais turi teisę gauti, persikelti ir naudoti savo asmens duomenis kitur, pvz., kitoje socialinės medijos paskyroje (teisė į duomenų perkeliamumą) (BDAR, 20 str.). Duomenų valdytojai gavę asmens duomenis privalo sudaryti sąlygas tokiam asmens duomenų perdavimui. Tačiau jis gali būti taikomas tik tiems duomenims, kuriuos asmuo pateikė duomenų valdytojui sutikimo arba sutarties pagrindu, ir tik tuo atveju, jei duomenys tvarkomi automatizuotomis priemonėmis (BDAR, 20 str.).

Penkta, išmaniųjų sveikatos aplikacijų ir prietaisų naudotojai gali prašyti, kad duomenų valdytojai apribotų jų asmens duomenų tvarkymą (teisė apriboti duomenų tvarkymą) (BDAR, 18 str.). Duomenų valdytojai neprivalo automatiškai ištrinti duomenų. Tačiau tam tikrais atvejais jie turi susilaikyti nuo jų tvarkymo: jei duomenys yra netikslūs (tikslumo tikrinimo proceso metu) (BDAR, 18 str., 1 d., a p.); jei duomenų tvarkymas yra neteisėtas, tačiau duomenų subjektas nepageidauja, kad duomenys būtų ištrinti, ir prašo juos apriboti (BDAR, 18 str., 1 d., b p.); duomenų valdytojui duomenys nebereikalingi, tačiau duomenų subjektas nori, kad duomenys būtų išsaugoti, kad būtų galima įgyvendinti teisinį reikalavimą (BDAR, 18 str., 1 d., c p.); kai duomenų valdytojas imasi priemonių duomenų ištrynimo prašymui patikrinti (BDAR, 18 str., 1 d., d p.). Apribojus duomenų tvarkymą, duomenų valdytojams draudžiama juos tvarkyti, išskyrus atvejus, kai jie turi duomenų subjekto sutikimą, kai duomenys reikalingi teisiniams reikalavimams arba kitų asmenų teisėms apsaugoti (BDAR, 18 str., 2 d.).

Galiausiai, duomenų subjektas turi teisę nesutikti su asmens duomenų tvarkymu (BDAR, 21 str.). Ši teisė leidžia duomenų subjektams tam tikrais atvejais, bet kuriuo metu nesutikti, kad jų asmens duomenys būtų naudojami. Ji priklauso nuo duomenų tvarkymo tikslo ir teisinio duomenų tvarkymo pagrindo. Duomenų subjektai turi absoliučią teisę sustabdyti savo asmens duomenų tvarkymą tiesioginės rinkodaros tikslais (BDAR, 21 str., 2 d.).

Tačiau jie taip pat gali nesutikti, kad duomenys būtų tvarkomi remiantis teisėtu interesu arba viešojo intereso užduotimis (BDAR, 21 str., 6 d.).

Taigi, išmaniųjų sveikatos aplikacijų ir prietaisų kūrėjams siekiant atitikti BDAR keliamus reikalavimus yra privalų paisyti ir gerbti šias duomenų subjektų teises savo kuriamuose produktuose. Kartu tai reiškia, kad jau produkto kūrimo stadijoje turėtų būti įvertinta, kaip bus užtikrintas šių teisių įgyvendinimas ne tik teoriškai, bet ir praktiškai.

2.5 Poveikio duomenų apsaugai vertinimas

Remiantis tuo, kad ankstesnėje darbo dalyje buvo prieita prie išvados, jog išmaniosios sveikatos aplikacijos ir prietaisai tvarko specialių kategorijų – sveikatos duomenis, aktualu aptarti poveikio duomenų apsaugai vertinimo (toliau – **PDAV**) procesą. Kai duomenų valdytojai renka, saugo ar naudoja asmens duomenis, asmenims, kurių duomenis yra tvarkomi, kyla nemažai pavojų. Šie pavojai gali būti įvairūs, nuo asmens duomenų vagystės ar netyčinio paviešinimo iki asmenų nerimo, kad jų duomenis bus panaudoti nežinomais tikslais.

PDAV apibūdinamas kaip procesas, „skirtas duomenų tvarkymui aprašyti ir tokio tvarkymo reikalingumui ir proporcingumui įvertinti, padedantis valdyti pavojų, kuris fizinių asmenų teisėms ir laisvėms kyla dėl asmens duomenų tvarkymo, jį įvertinant ir nustatant šio pavojaus pašalinimo priemones“ (29 straipsnio duomenų apsaugos darbo grupė. Poveikio duomenų apsaugai..., 2017, p. 4). Šis procesas yra svarbi priemonė, padedanti paneigti riziką ir įrodyti atitiktį BDAR reikalavimams. Pagrindiniai PDAV privalumai yra tai, jog jis gali tapti būdu gerinti duomenų valdytojų informuotumą apie siejamą su jų produktais pavojų duomenų apsaugai. Be to, šis procesas gali padėti didinti visuomenės pasitikėjimą duomenų valdytoju, tobulinant komunikaciją duomenų apsaugos klausimais. PDAV dėka taip pat gali mažėti duomenų apsaugos priemonių sąnaudos, skatinant įdiegti šias priemones į produkto mechanizmą ankstyvajame jo kūrimo etape (The Data Protection Commission of Ireland. Data Protection…).

Pagal BDAR, PDAV yra privalomas, kai tvarkant asmens duomenis „fizinių asmenų teisėms bei laisvėms gali kilti didelis pavojus“ (BDAR 35 str. 1d.). Tai ypač aktualu, kai yra diegiama nauja duomenų tvarkymo technologija kaip išmaniosios sveikatos aplikacijos ir prietaisai. BDAR pateikiama keletas pavyzdžių, kada duomenų tvarkymas gali kelti didelį pavojų. Vienas iš jų, aktualus būtent nagrinėjamos temos kontekste, yra „9 straipsnio 1 dalyje nurodytų specialių kategorijų duomenų <...> tvarkymas dideliu mastu“ t. y., šiuo atveju sveikatos duomenų tvarkymas (BDAR 35 str., 2 d., b p.).

Svarbu paminėti, jog Darbo grupės Gairėse dėl PDAV yra nustatyti kriterijai į kuriuos reiktų atsižvelgti vertinant ar duomenų tvarkymas gali kelti didelį pavojų. Vienas iš šių kriterijų yra „vertinimas arba balų skyrimas, įskaitant profiliavimą ir prognozavimą, remiantis aspektais, susijusiais su duomenų subjekto <...> sveikatos būkle, <...>“. (29 straipsnio duomenų apsaugos darbo grupė. Poveikio duomenų apsaugai..., 2017, p. 10). Pavyzdžiui, „biotechnologijų bendrovę, kuri tiesiogiai vartotojams siūlo atlikti genetinius tyrimus, siekiant įvertinti ir prognozuoti su liga susijusį ir (arba) sveikatai gresiantį pavojų“ (29 straipsnio duomenų apsaugos darbo grupė. Poveikio duomenų apsaugai..., 2017, p. 10). Taip pat, atkreiptinas dėmesys į tai, kad PDAV turėtų būti atliekamas prieš pradedant tvarkyti duomenis (BDAR 35 str. 1d.).

PDAV atlikimas kuo anksčiau yra vertinamas kaip gera praktika, planuojant atlikti duomenų tvarkymo operacijas (The Data Protection Commission of Ireland. Data Protection…). Bet kokiu atveju, PDAV atliekamas prieš asmens duomenų tvarkymo pradžią. BDAR nenustatytas tikslus PDAV atlikimo procesas ar forma, todėl, atsižvelgiant į duomenų valdytojų poreikius, jį galima taikyti lanksčiai – atsižvelgiant į konkrečią situaciją. Nors nėra vieno nustatyto būdo, kuriuo reikėtų vadovautis, duomenų valdytojai galėtų remtis toliau nurodytais veiksmais atliekant PDAV: produkto savybių apibrėžimas, kad būtų galima atlikti rizikos vertinimą; duomenų apsaugos ir susijusios rizikos nustatymas; duomenų apsaugos sprendimų, skirtų rizikai sumažinti arba pašalinti, nustatymas bei duomenų apsaugos sprendimų integravimas į produkto mechanizmą (The Data Protection Commission of Ireland. Data Protection…). Svarbu paminėti ir tai, kad tais atvejais, kai nėra aišku, ar PDAV yra griežtai privalomas, duomenų valdytojams reikia turėti omenyje, jog šis procesas yra laikomas gera praktika ir naudinga priemone, kuri jiems gali padėti laikytis duomenų apsaugos teisės aktų reikalavimų (The Data Protection Commission of Ireland. Data Protection…).

Apibendrinant būtų galima teigti, kad išmaniųjų sveikatos aplikacijų bei prietaisų kūrėjams kaip duomenų valdytojams tvarkantiems specialiųjų kategorijų – sveikatos duomenis dideliu mastu, yra privalu atlikti PDAV prieš pateikiant savo produktą į rinką.

2.6 BDAR netinkamo įgyvendinimo apsaugant sveikatos duomenis problematika

BDAR numatyta plati teisių apsauga kartu su griežta sveikatos duomenų apsaugos tvarka suteikia galimybę pakankamai apsaugoti išmaniųjų sveikatos aplikacijų ir prietaisų naudotojų sveikatos duomenis. Tačiau iš kelių tyrimų matyti, kad daugelis sveikatos aplikacijų neužtikrina atitikties tam tikroms ypač svarbioms BDAR nuostatoms,

susijusioms su sveikatos duomenimis. Pavyzdžiui, atlikus 20–ties Europos Sąjungoje prieinamų sveikatos aplikacijų tyrimą nustatyta, kad dauguma sveikatos aplikacijų neatitinka nuostatų dėl duomenų subjekto sutikimo: tik 55 proc. analizuotų aplikacijų prieš registraciją pateikia informaciją apie aplikacijos teikėjo privatumo politiką, tik 5 proc. aplikacijų prašo sutikimo kiekvieną kartą, kai naudotojas dalijasi papildoma asmenine informacija bei nė viena aplikacija neatitinka reikalavimo išreikšti aiškų sutikimą konkrečiais klausimais, ir tik 35 proc. aplikacijų suteikia galimybę atšaukti sutikimą ir taip ištrinti savo sveikatos duomenis (van Kolfschooten, 2022). Kita ES sveikatos aplikacijų privatumo politikos analizė, kurioje buvo analizuojama 31–na aplikacija rodo, kad nė viena iš jų neatitiko teisės į informaciją reikalavimo: tik 42 proc. aplikacijų paminėta teisė nesutikti ir tik 58 proc. aplikacijų paminėta teisė į duomenų ištaisymą ir prieigą (Mulder, 2019). Atlikus dar vieną sveikatos aplikacijų tyrimą, kuriame buvo analizuojamos 24–ios aplikacijos, paaiškėjo, kad 79 proc. jų neskaidriai siunčia naudotojų sveikatos duomenis trečiosioms šalims (Grundy. *et al*., 2019).

Taigi, iš minėtų pavyzdžių galima teigti, kad praktikoje daugelis sveikatos aplikacijų neįgyvendina tam tikrų joms taikomų BDAR reikalavimų. To priežastys gali atsirasti tiek kuriant produktą pvz., dėl nepakankamų aplikacijų kūrėjų žinių apie BDAR reikalavimus (Fong, 2017), tiek dėl neužtektinos reguliavimo priežiūros ir kontrolės.

3. SAVIREGULIACIJA ES DUOMENŲ APSAUGOS TEISĖS POŽIŪRIU

Kai įprastinis teisinis reguliavimas neduoda norimo rezultato, sprendimu gali būti papildomos alternatyvios reguliavimo formos, pavyzdžiui, savireguliacija. Sektoriaus savireguliacija gali būti apibrėžiama kaip reguliavimo procesas, kurio metu sektoriaus lygmens organizacija ar įmonė, nustato ir įgyvendina taisykles ir standartus, susijusius su sektoriaus įmonių elgesiu (Gupta, Lad, 1983, p. 417). Dažnai minimi tokie savireguliacijos privalumai: lankstumas pritaikant taisykles prie technologinių pokyčių ir didesnis įsipareigojimas laikytis taisyklių (van Kolfschooten, 2022). Duomenų apsaugos srityje vis dažniau pasitaiko sektoriaus savireguliacijos atvejų. Siekdamos apsaugoti vartotojų interesus, padidinti visuomenės pasitikėjimą ir reputaciją bei kovoti su neigiama visuomenės nuomone, įmonės dažnai nusprendžia papildyti galiojančius teisės aktus savireguliacijos priemonėmis (van Kolfschooten, 2022). Be to, savireguliacijai skiriama daug dėmesio duomenų apsaugos srityje Europos Sąjungos lygmeniu: BDAR remiama ir skatinama įmonių savireguliacija rengiant elgesio kodeksus ir privalomas įmonių taisykles (BDAR, str. 40, 47). Elgesio kodeksai pagal BDAR – tai savanoriški taisyklių rinkiniai, padedantys užtikrinti duomenų apsaugos reikalavimų laikymąsi ir atskaitomybę konkrečiuose sektoriuose. Kodeksai gali padėti įmonėms užtikrinti, kad jos laikytųsi geriausios praktikos ir taisyklių, sukurtų konkrečiai jų sektoriui ar duomenų tvarkymo operacijoms, taip sustiprinant atitiktį duomenų apsaugos teisės aktams. Kodeksus rengia ir valdo asociacija ar kita įstaiga, atstovaujanti tam tikram sektoriui, turinti ekspertinių ir sektorinių žinių, kaip gerinti duomenų apsaugą savo srityje. Šie kodeksai tai daugiau nei gairės, juose turi būti iš esmės patikslintas ar patobulintas duomenų apsaugos teisės taikymas tam tikram sektoriui ar duomenų tvarkymo veiklai, o ne tik pakartotas BDAR (The Data Protection Commission of Ireland. Codes of…).

3.1 Aplikacijų parduotuvių savireguliacija kaip būdas sveikatos duomenų apsaugai tobulinti

Kalbant apie sveikatos aplikacijų sektoriaus savireguliaciją Europos Sąjungoje, matoma, kad aplikacijų parduotuvės (angl. *app store*) jau šiuo metu atlieka svarbų vaidmenį, reguliuodamos sveikatos aplikacijas, platinamas jų platformose, taikant aplikacijų peržiūros procedūras (App Store Review Guidelines, Google Play Developer Distribution Agreement, 2022). Aplikacijų sistema veikia tokiu būdu: kad aplikacijų kūrėjai galėtų platinti savo aplikacijas plačiajai visuomenei, jie turi paskelbti savo aplikacijas aplikacijų parduotuvėse, kad vartotojai jas galėtų atsisiųsti į savo mobiliuosius

įrenginius (App Store Review Guidelines, Google Play Developer Distribution Agreement, 2022). Aplikacijų parduotuvės reikalauja, kad aplikacijų kūrėjai laikytųsi tam tikrų taisyklių, kurios yra išankstinio patvirtinimo proceso dalis, taip pat parduotuvės pašalina reikalavimų neatitinkančias aplikacijas (App Store Review Guidelines, Google Play Developer Distribution Agreement, 2022). Ši priežiūros funkcija suteikia aplikacijų parduotuvėms galimybę daryti įtaką aplikacijų kūrėjų elgesiui. Todėl aplikacijų parduotuvės yra pagrindiniai aplikacijų sistemos koordinatoriai bei turi didelę vartotojų kontrolę (van Kolfschooten, 2022).

Aplikacijų parduotuvės suteikia platformą aplikacijų teikėjams siūlyti savo aplikacijas ir netvarko aplikacijų naudotojų duomenų surinktų jas naudojant. Tačiau, aplikacijų parduotuvės gali daryti įtaką tam, kaip aplikacijos, užtikrina naudotojų duomenų apsaugą (European Union Agency for Cybersecurity, 2018, p. 16). Be to, pagal BDAR jos skatinamos atlikti šį vaidmenį (BDAR, 78 konstatuojamoji dalis). Šiuo atžvilgiu aplikacijų parduotuvės vykdo tam tikrą sektoriaus savireguliaciją.

Siekiant ištirti šių aplikacijų parduotuvių elgseną, susijusią su sveikatos aplikacijų privatumu, ir įvertinti esamos sveikatos aplikacijų sveikatos duomenų apsaugos praktikos veiksmingumą, toliau bus kalbama apie Apple App Store ir Google Play, šiandien didžiausių ir populiariausių aplikacijų parduotuvių analizę.

Kalbant apie Apple aplikacijų parduotuvę, tam, kad aplikacijų kūrėjai galėtų pateikti aplikacijas į šią parduotuvę, jie turi užsiregistruoti Apple kūrėjų programoje, kuriai taikoma Apple kūrėjų programos licencijos sutartis (Apple Developer Program License Agreement, 2022). Be to, Apple aplikacijų parduotuvė peržiūri visas pateiktas aplikacijas ir aplikacijų atnaujinimus pagal šios aplikacijų parduotuvės peržiūros gaires (App Store Review Guidelines, 2022). Šiose gairėse pateikiamos konkrečios sveikatos aplikacijų taisyklės ir nurodoma, kad šios aplikacijos gali būti tikrinamos atidžiau (App Store Review Guidelines, 2022, 5.1.3 d.). Gairėse taip pat pateikiamos bendrosios nuostatos dėl asmens duomenų tvarkymo ir privatumo. Pirma, aplikacijose turi būti privatumo politika, kurioje būtų paaiškinta, kaip naudotojai gali pasinaudoti savo teisėmis dėl duomenų saugojimo, ištrynimo ir sutikimo atšaukimo (App Store Review Guidelines, 2022, 5.1.1 d., 1 p.). Antra, duomenų rinkimas turi būti grindžiamas duomenų subjekto sutikimu, o naudotojams turi būti suteikta lengvai prieinama ir suprantama galimybė atšaukti sutikimą (App Store Review Guidelines, 2022, 5.1.1 d., 2 p.). Trečia, aplikacijose duomenų rinkimas turėtų būti kuo mažesnės apimties (App Store Review Guidelines, 2022, 5.1.1 d., 3 p.). Taip pat, norint dalytis duomenimis su trečiosiomis šalimis, reikalingas naudotojo (duomenų subjekto) sutikimas (App Store Review Guidelines, 2022, 5.1.2 d., 1, 2 p.). Tačiau svarbu, kad

aplikacijos neturėtų bandyti sudaryti naudotojo profilio pagal surinktus duomenis (App Store Review Guidelines, 2022, 5.1.2 d., 3 p.). Apple kūrėjų programos licencijos sutartyje taip pat teigiama, kad aplikacijų kūrėjai privalo atsižvelgti į naudotojų privatumą ir laikytis privatumą reglamentuojančių teisės aktų (Apple Developer Program License Agreement, 2022, 3.3.7–3.3.11 d.).

Be to, gairėse pateikiamos aiškios taisyklės dėl sveikatos aplikacijų tvarkomų sveikatos duomenų (App Store Review Guidelines, 2022, 5.1.3 d.). Pirma, aplikacijos negali naudoti ar atskleisti surinktų sveikatos duomenų trečiosioms šalims reklamos, rinkodaros ar kitais duomenų gavybos tikslais (App Store Review Guidelines, 2022, 5.1.3 d., 1 p.). Tačiau aplikacijos gali naudoti arba atskleisti sveikatos duomenis sveikatos valdymo gerinimo ir sveikatos tyrimų tikslais, tačiau tik gavę duomenų subjekto sutikimą (App Store Review Guidelines, 2022, 5.1.3 d.). Antra, aplikacijų kūrėjai negali į sveikatos aplikacijas įrašyti netikslių duomenų (App Store Review Guidelines, 2022, 5.1.3 d., 2 p.). Trečia, sveikatos aplikacijos negali saugoti sveikatos informacijos iCloud aplinkoje (App Store Review Guidelines, 2022, 5.1.3 d., 2 p.).

Kalbant apie Google Play, peržiūros kriterijai nurodyti kūrėjų platinimo sutartyje ir kūrėjų programos taisyklėse (Google Play Developer Distribution Agreement, 2022). Sutartis yra teisiškai įpareigojantis susitarimas tarp aplikacijos kūrėjo ir Google (Google Play Developer Distribution Agreement, 2022, 2.1 p.). Kalbant apie asmens duomenų tvarkymą, susitarime teigiama, kad aplikacijos turėtų atitikti taikomus duomenų apsaugos įstatymus (Google Play Developer Distribution Agreement, 2022, 4.6 p). Tiksliau, aplikacijos turi informuoti naudotojus apie tai, kokie asmens duomenys tvarkomi, pateikti privatumo pranešimą ir užtikrinti tinkamą duomenų apsaugą. Be to, aplikacijose asmens duomenys gali būti naudojami tik tais tikslais, kuriems naudotojas davė sutikimą (Google Play Developer Distribution Agreement, 2022, 4.8 p). Sutartyje konkrečiai neminimos sveikatos aplikacijos ar sveikatos duomenys.

Kūrėjų programos taisyklėse pateikiama daugiau gairių dėl asmens duomenų tvarkymo. Taisyklėse teigiama, kad griežtai draudžiama naudoti aplikacijas, kuriomis siekiama piktnaudžiauti ar netinkamai naudoti asmens duomenis (Google Play Developer Program Policies, 2022). Be to, aplikacijos turi laikytis skaidrumo principo, naudojant ir dalijantis asmens duomenimis (Google Play Developer Program Policies, 2022). Kalbant apie jautrius asmens duomenis, kurie tikriausiai apima ir sveikatos duomenis, taisyklėse teigiama, kad juos rinkti ir naudoti reikėtų tik tais tikslais, kurie tiesiogiai susiję su aplikacijos funkcionalumu. Taip pat pačioje aplikacijoje turi būti paskelbta prieinama privatumo politika. Be kitos pateikiamos informacijos, ji taip pat turi atskleisti, su kokiomis

šalimis dalijamasi neskelbtinais duomenimis (Google Play Developer Program Policies, 2022). Be to, atskleidžiant informaciją aplikacijoje turi būti prašoma naudotojų sutikimo prieš pradedant tvarkyti duomenis, todėl svarbu, kad naudotojas atliktų aktyvius veiksmus. Šiuose prašymuose dėl sutikimo turi būti aiškiai nurodyti duomenų tvarkymo ar perdavimo tikslai. Be to, asmens duomenys gali būti naudojami tik tais tikslais, kuriems naudotojas davė sutikimą (Google Play Developer Program Policies, 2022). Taisyklėse nėra aiškių konkrečių nuostatų dėl sveikatos aplikacijų, išskyrus draudimą teikti melagingus ar klaidinančius teiginius apie sveikatą (Google Play Developer Program Policies, 2022).

Iš pirmiau pateiktos aplikacijų parduotuvių sutarčių, taisyklių ir gairių apžvalgos galima daryti išvadą, kad aplikacijų parduotuvėms yra svarbūs ir aktualūs duomenų apsaugos klausimai. Tačiau abejotina, ar dėl to yra užtikrinama geresnė išmaniųjų sveikatos aplikacijų ir prietaisų naudotojų sveikatos duomenų apsauga. Abiejų aplikacijų parduotuvių gairėse nurodyta, kad aplikacijos turi atitikti privatumą reglamentuojančius teisės aktus bei turėti privatumo politiką. Tačiau šių parduotuvių privatumo nuostatų išsamumo lygis labai skiriasi. Nors Apple aplikacijų parduotuvė konkrečiai remiasi BDAR duomenų apsaugos principais ir duomenų subjektų teisėmis, Google Play aplikacijų parduotuvės privatumo gairės suformuluotos gan miglotai. Konkrečiai, Google Play aplikacijų parduotuvės gairėse kūrėjams nepateikiama reikiamų nurodymų, kaip apsaugoti asmens duomenis, ypač atsižvelgiant į duomenų subjektų teises. Dėl to kyla didelė rizika, jog tinkama privatumo apsauga nebus užtikrinta. Be to, Apple aplikacijų parduotuvė turi konkrečias sveikatos duomenų tvarkymo gaires, o Google Play aplikacijų parduotuvės taisyklėse minimi tik jautrūs asmens duomenys. Pažymėtina, kad abiejose gairėse trūksta nuostatos dėl aiškaus sutikimo tvarkyti sveikatos duomenis, kurio pagal BDAR reikalaujama iš aplikacijų kūrėjų. Nors abiejose gairėse pateikiamos nuostatos dėl naudotojo sutikimo, įprastas ir aiškus sutikimai neskiriami bei atitinkamai nepaaiškinama, kaip gauti būtent aiškų sutikimą.

Taigi, galima daryti išvadą, kad dabartinė savireguliacijos praktika, ypač Google Play aplikacijų parduotuvės, nepateisina savo galimybių ir pakankamai neužtikrina, kad sveikatos aplikacijų naudotojai galėtų tinkamai kontroliuoti savo sveikatos duomenis. Tačiau dėl labai svarbios aplikacijų parduotuvių padėties t. y., buvimo vienintele erdve kur naudotojai gali įsigyti aplikacijas, šių parduotuvių savireguliacija vis tiek turi daugiausiai galimybių padėti užtikrinti aukštesnį sveikatos duomenų apsaugos lygį, jei būtų padaryti tam tikri jų taisyklių turinio ir formos pakeitimai.

Dabartinę aplikacijų parduotuvių savireguliacijos praktiką būtų galima patobulinti daugeliu aspektų. Pirma, aplikacijų parduotuvės galėtų pateikti aplikacijų kūrėjams aiškesnes gaires dėl duomenų tvarkymo pareigų ir duomenų subjektų teisių. Jose galėtų būti nurodytos visos

pagal BDAR taikytinos pareigos ir teisės bei pateiktos praktinės rekomendacijos, kaip tai tinkamai įgyvendinti aplikacijose (van Kolfschooten, 2022). Antra, galėtų būti įtrauktos konkrečios nuostatos dėl sveikatos duomenų apsaugos, kad būtų atkreiptas dėmesys į šios kategorijos svarbą ir padidėjusią riziką privatumui. Į šias nuostatas turėtų būti įtrauktas bent jau reikalavimas gauti aiškų sutikimą dėl sveikatos duomenų tvarkymo ir pateiktos techninės gairės, kaip tai įgyvendinti (van Kolfschooten, 2022). Taip pat galėtų būti numatytos konkrečios nuostatos dėl dalijimosi sveikatos duomenimis su trečiosiomis šalimis apribojimo ir galimo komercinio naudojimo. Be to, aplikacijų parduotuvės gali dar labiau sustiprinti naudotojų kontrolę reikalaudamos, kad į aplikacijas būtų įtrauktos naudotojų pranešimų apie duomenų apsaugos pažeidimus priemonės (van Kolfschooten, 2022). Nors nėra jokių garantijų, kad aplikacijų parduotuvės įdiegs tokius pakeitimus, paskatinimu gali būti tai, jog dėl didesnio teisinio tikrumo aplikacijų parduotuvės įgyja didesnį naudotojų pasitikėjimą ir atitinkamai pranašumą tarp konkurentų.

Apibendrinant, nors teoriškai BDAR siūlo tvirtus sprendimo būdus, kaip apsaugoti sveikatos aplikacijų naudotojų duomenis, kaip minėta anksčiau jis nėra pakankamai veiksmingas praktiškai. Išmaniųjų sveikatos aplikacijų reguliavimas aplikacijų parduotuvėse taikant peržiūros procedūras galėtų padėti užpildyti spragas ir taip prisidėti prie sveikatos duomenų apsaugos lygio kėlimo Europos Sąjungoje. Tačiau atlikta dviejų didžiųjų aplikacijų parduotuvių analizė rodo, kad dabartinis savireguliacijos mechanizmas taip pat turi trūkumų. Vis dėlto, atsižvelgiant į svarbią aplikacijų parduotuvių padėtį šiame technologijų sektoriuje, papildomas sveikatos aplikacijų reguliavimas aplikacijų parduotuvėse vis dar gali būti perspektyviausia priemonė sveikatos aplikacijų naudotojų duomenų apsaugos lygiui gerinti.

4. TEISINIO REGLAMENTAVIMO NAUJOVĖS PAGAL EUROPOS SVEIKATOS DUOMENŲ ERDVĖS REGLAMENTĄ

4.1 Samprata ir siekiamos išspręsti problemos

Mokslininkai, vaistininkai, įvairūs sveikatos priežiūros specialistai, įstaigos bei institucijos iš visos Europos Sąjungos nuolatos sukuria ir tvarko ypač didelį kiekį sveikatos duomenų, kurie tampa labai svarbūs šių subjektų veiklai rūpinantis asmenų sveikata bei gyvybėmis (Europos Komisija. Klausimai ir…, 2022). COVID-19 pandemija patvirtino, kad sveikatos duomenys yra itin reikšmingi norint taikyti išsamiai pagrįstas visuomenės sveikatos priemones ir tinkamai reaguoti į įvairias krizines situacijas (Europos Komisija. Klausimai ir…, 2022). Pandemija taip pat lėmė spartesnį naudojimąsi įvairiomis skaitmeninėmis priemonėmis pvz., išmaniosiomis sveikatos aplikacijomis ir prietaisais. Tačiau kol kas vis dar esama sunkiai pašalinamų kliūčių, trukdančių pasinaudoti visomis sveikatos duomenų teikiamomis galimybėmis (Europos Komisija. Klausimai ir…, 2022). Viena iš šių kliūčių yra tai, jog reikalingi bei svarbūs sveikatos duomenys yra prarandami ar nepasiekiami. Dėl šios priežasties, dažnai be pagrindo kartojami įvairūs diagnostiniai tyrimai arba taikomi keli tarpusavyje nesuderinami gydymo režimai, tokiu būdu asmenims užkertant kelią gauti veiksmingą ar naujovišką gydymą (Europos Komisija. Klausimai ir…, 2022). Taip pat, asmenys ne visada gali lengvai pasiekti savo sveikatos duomenis elektroniniu būdu, o jei jie pageidautų konsultuotis su gydytojais daugiau nei vienoje ligoninėje ar kitoje sveikatos priežiūros įstaigoje, dažnai šiems asmenims nėra suteikiama galimybė dalytis duomenimis su kitais sveikatos priežiūros specialistais (Europos Komisija. Klausimai ir…, 2022). Be to, šiandien asmens sveikatos duomenys dažnu atveju vis dar įrašomi popieriniuose dokumentuose, kurie pasklinda po skirtingas sveikatos priežiūros įstaigas, todėl šių dokumentų paprasčiausia neįmanoma atsekti. Situacija tampa dar sudėtingesnė tuomet, kai yra kertamos valstybių sienos. Jei asmuo apsilanko pas gydytoją kitoje šalyje, jo sveikatos duomenys dažnai yra neprieinami, todėl diagnozė ar gydymas gali vėluoti ir būti klaidingas. Daugumoje atvejų gydytojai negali matyti paciento sveikatos duomenų, jei jam buvo atliktos sveikatos procedūros kitoje šalyje (Europos Komisija. Klausimai ir…, 2022). Kita kliūtis yra susijusi su duomenų gavimu moksliniams tyrimams atlikti ir inovacijoms kurti. Prieigos prie sveikatos duomenų nebuvimas yra pagrindinė sveikatos technologijų produktus kuriančių įmonių ir mokslinius tyrimus atliekančių subjektų problema (Europos Komisija. Klausimai ir…, 2022). Taip pat, naujų skaitmeninių technologijų, pvz., dirbtinio intelekto ar išmaniųjų sveikatos aplikacijų bei prietaisu gamintojams, duomenų trūkumas yra didelė kliūtis siekiant kurti naujus produktus

ir technologijas. Tai yra ypač aktualu, nes būtent šios technologijos turės ypatinga reikšmę sprendžiant dabartines sveikatos priežiūros sistemų problemas, nuo gydytojų trūkumo tam tikruose regionuose iki individualizuotos medicinos ir įvairių su senėjančia visuomene susijusių iššūkių (Europos Komisija. Klausimai ir…, 2022).

Būtent dėl šių kliūčių, 2022 m. gegužės 3 d. Europos Komisija paskelbė pasiūlymą dėl reglamento (toliau – **Pasiūlymas dėl ESDER**) dėl Europos bendros sveikatos duomenų erdvės (toliau – **ESDER**) sukūrimo. Šis reglamentas yra vienas iš pagrindinių elementų padedančių kurti Europos sveikatos sąjungą. ESDER tai su sveikata susijusi ekosistema, kurią sudaro taisyklės, bendri standartai ir praktika, infrastruktūra bei valdymo sistema. Pagrindinis reglamento tikslas yra palengvinti ir pagerinti asmenų, sveikatos priežiūros specialistų, mokslininkų bei įmonių kuriančių sveikatos technologijų produktus, prieigą prie sveikatos duomenų ir jų naudojimą visoje Europos Sąjungoje (Europos Komisija. Klausimai ir…, 2022). Taigi, Pasiūlymu dėl ESDER siekiama trijų konkrečių tikslų: 1. įgalinti asmenis, suteikiant jiems daugiau skaitmeninės prieigos prie jų elektroninių asmens sveikatos duomenų; 2. skatinti bendrą elektroninių sveikatos įrašų sistemų, išmaniųjų sveikatos aplikacijų ir prietaisų, medicinos prietaisų ir didelės rizikos dirbtinio intelekto sistemų rinką; 3. užtikrinti patikimą ir veiksmingą sveikatos duomenų naudojimą moksliniams tyrimams, inovacijoms, naujų sveikatos technologijų produktų kūrimui, politikos formavimui ir reguliavimo veiklai (Europos Komisija. Klausimai ir…, 2022).

Trumpai tariant, siūlomu reglamentu sukuriama bendra sveikatos duomenų erdvė, kurioje fiziniai asmenys gali kontroliuoti savo elektroninius sveikatos duomenis (pirminis naudojimas), o tyrėjai, inovacijų kūrėjai ir politikos formuotojai gali naudotis šiais elektroniniais sveikatos duomenimis patikimu ir saugiu būdu, išsaugant asmens duomenis (antrinis naudojimas). Be to, duomenų turėtojams (pvz., sveikatos priežiūros paslaugų teikėjams ar išmaniųjų sveikatos aplikacijų bei prietaisų kūrėjams) bus taikomi nauji įpareigojimai teikti savo duomenis antriniam naudojimui per ESDER (Europos Komisija. Klausimai ir…, 2022). Vėliau visi šie elementai bus nagrinėjami detaliau. Taigi, apibendrinant, tikimasi, kad kai ESDER bus įgyvendintas, asmenys galės greitai, lengvai ir nemokamai gauti duomenis elektronine forma. Jie galės lengvai dalytis šiais duomenimis su kitais sveikatos priežiūros specialistais valstybėse narėse, taip gerinant sveikatos priežiūros paslaugų teikimą. (Europos Komisija. Klausimai ir…, 2022) Be to, asmenys galės visiškai kontroliuoti savo duomenis bei galės papildyti informaciją, ištaisyti neteisingus duomenis, apriboti prieigą kitiems asmenims ir gauti informaciją apie tai, kaip ir kokiais tikslais jų duomenys naudojami (Europos Komisija. Klausimai ir…, 2022). Taip pat, esant griežtoms sąlygoms, mokslininkai, novatoriai, viešosios institucijos ar įmonės

kuriančios sveikatos technologijų produktus, tokius išmaniosios sveikatos aplikacijos ir prietaisai (ESDER 1 str., 3 d., a p.), galės naudotis dideliu kiekiu aukštos kokybės sveikatos duomenimis, kurie yra labai svarbūs kuriant gyvybę gelbstinčius gydymo būdus, sveikatą palaikančias ir savistebėsenos programas, vakcinas ir pan., tokiu būdu užtikrinant geresnį sveikatos priežiūros paslaugų prieinamumą bei atsparesnes sveikatos sistemas (Europos Komisija. Klausimai ir…, 2022).

4.2 Pirminis sveikatos duomenų panaudojimas

Kaip minėta anksčiau, pirmasis pasiūlymo dėl ESDER tikslas yra sustiprinti fizinių asmenų teises, susijusias su jų elektroninių sveikatos duomenų prieinamumu ir kontrole (Pasiūlymas dėl ESDER 1 str., 2 d., a p). Taigi, domenų subjektų teisės, susijusios su elektroninių sveikatos duomenų pirminiu naudojimu, yra įtvirtintos pasiūlyme dėl ESDER, nustatant, kad: „pirminis elektroninių sveikatos duomenų naudojimas, tai asmens elektroninių sveikatos duomenų tvarkymas sveikatos priežiūros paslaugoms teikti siekiant įvertinti, palaikyti ar atkurti fizinio asmens, su kuriuo tie duomenys yra susiję, sveikatos būklę, įskaitant vaistų ir medicinos priemonių (receptų) išrašymą, išdavimą ir tiekimą, taip pat atitinkamoms socialinės apsaugos, administracinėms ar išlaidų kompensavimo paslaugoms teikti“ (Pasiūlymas dėl ESDER 1 str., 2 d., d p). Atitinkamai, pasiūlyme yra numatyta, kad: „fiziniai asmenys turi teisę nedelsdami, nemokamai ir lengvai įskaitoma, suvestine ir prieinama forma susipažinti su savo asmens elektroniniais sveikatos duomenimis, tvarkomais pirminio elektroninių sveikatos duomenų naudojimo tikslu“ (Pasiūlymas dėl ESDER 3 str., 1 d), tokiu būdu užtikrinant, kad fiziniams asmenims bus suteikta galimybė kontroliuoti savo elektroninius sveikatos duomenis ir dalytis jais su pasirinktu sveikatos priežiūros paslaugų teikėju. Taip pat yra numatyta, kad sveikatos priežiūros specialistai turi teisę susipažinti su jų gydomų asmenų elektroniniais sveikatos duomenimis (visų pirma su paciento ligos istorija, receptais, vaistų išrašais, medicininiais vaizdais ir vaizdų ataskaitomis, laboratorinių tyrimų rezultatais ir išrašų ataskaitomis, t. y. prioritetinėmis asmens elektroninių sveikatos duomenų kategorijomis) (Pasiūlymas dėl ESDER 4 str., 1 d., a p). Kartu jie būtų įpareigoti užtikrinti, kad elektroniniai sveikatos duomenys būtų atnaujinami Europos sveikatos įrašų (toliau – **ESĮ**) sistemoje, įtraukiant informaciją apie jų suteiktas sveikatos priežiūros paslaugas (Pasiūlymas dėl ESDER 4 str., 1 d., b p). Tuo tarpu Valstybės narės turės užtikrinti, kad prioritetinių kategorijų duomenys būtų prieinami bendru Europos elektroninių sveikatos įrašų keitimosi formatu (Pasiūlymas dėl ESDER 3 str., 8 d.). Jos taip pat privalės dalyvauti tarpvalstybinėje skaitmeninėje

infrastruktūroje, skirtoje keistis sveikatos duomenimis teikiant sveikatos priežiūros paslaugas (MyHealth@EU) (Pasiūlymas dėl ESDER, 24 konstatuojamoji dalis). Vienas iš pavydžių kaip pirminis naudojimas galėtų atrodyti praktikoje, būtų situacija, kai Valstybėje narėje A gyvenantis asmuo vyksta atostogauti į Valstybę narę B. Valstybėje B jis suserga, todėl jam reikia apsilankyti pas vietos gydytoją. Naudodamasis ESDER ir MyHealth@EU, gydytojas valstybėje B savo kompiuteryje pamatys šio asmens ligos istoriją valstybės B kalba. Gydytojas, atsižvelgdamas į asmens ligos duomenis, galės paskirti reikiamus vaistus, išvengiant tų, kurie asmeniui nėra tinkami (Europos Komisija. Klausimai ir…, 2022). Taigi, tikimasi, kad įgyvendinus ESDER bus užtikrinta galimybė fiziniams asmenims tinkamai ir efektyviai naudotis savo teisėmis susijusiomis su sveikatos duomenimis bei veiksmingai šiuos duomenis kontroliuoti.

4.3 Antrinis sveikatos duomenų panaudojimas

Kitas iš ESDER elementų, kuris, tikėtina, turės didelį poveikį skaitmeninės sveikatos technologijų sektoriui, yra pasiūlymas išplėsti sveikatos duomenų prieinamumą antriniam naudojimui. Kaip minėta anksčiau, daugeliui įmonių prieigos prie kokybiškų sveikatos duomenų trūkumas yra pagrindinė kliūtis, trukdanti kurti vertę pasitelkiant skaitmenines inovacijas. Todėl nauja sistema, kuri išsprendžia šią problemą, pateikiant aukščiausius etikos standartus atitinkantį sprendimą, yra ypatingai reikšminga. Tai pirmas kartas, kai teisės aktų leidėjai nustato antrinio sveikatos duomenų naudojimo reguliavimo koncepciją (Fromel, 2022).

Antrinis elektroninių sveikatos duomenų naudojimas tai sveikatos duomenų tvarkymas kitais tikslais, nei pirminiai tikslai, dėl kurių duomenys buvo surinkti. Pavyzdžiui, kai tyrėjai pakartotinai apdoroja klinikinius ir sveikatos draudimo duomenis, kad ištirtų paslaugos ar produkto ekonominį efektyvumą (World Health Organization. Meeting..., 2022). Dar vienas pavyzdys galėtų būti, kai sveikatos technologijų įmonė diegia nauja sveikatos aplikaciją, kuri padės naudojams stebėti jų miego ritmą ir pagerinti jų miego kokybę. Tam, kad aplikacija galėtų tinkamai funkcionuoti, ją kuriant yra reikalinga įvertinti didelio kiekio asmenų turinčių miego sutrikimus sveikatos duomenis. Naudodamasi ESDER, įmonė galės efektyviai ir saugiai naudotis dideliu kiekiu sveikatos duomenų, kuriuos pateikė kiti sveikatos duomenų naudotojai, siekiant apmokyti aplikacijos algoritmą ir patobulinti efektyvumą prieš pateikiant produktą į rinką (Europos Komisija. Klausimai ir…, 2022). Pačiame Pasiūlyme dėl ESDER numatyta, kad antrinis naudojimas tai

„elektroninių sveikatos duomenų tvarkymas šiame pasiūlyme nustatytais tikslais“ (Pasiūlymas dėl ESDER, 2 str., 2 d., e p.).

Taigi, ESDER nustatoma tvarka, pagal kurią numatoma kokiais tikslais yra leidžiamas elektroninių sveikatos duomenų antrinis naudojimas, pavyzdžiui, produktų ar paslaugų, kuriais prisidedama prie visuomenės sveikatos ar socialinės apsaugos, kūrimo, tai pat individualiems poreikiams pritaikytų sveikatos priežiūros paslaugų teikimo ir inovacijų diegimo veiklos arba algoritmų mokymo, testavimo ir vertinimo tikslais (Pasiūlymas dėl ESDER, 34 str.). Atitinkamai, asmens sukurti elektroniniai sveikatos duomenys, įskaitant medicinos prietaisų, išmaniųjų sveikatos aplikacijų bei prietaisų ir kitų skaitmeninių sveikatos aplikacijų duomenis, patenka į būtiniausių kategorijų duomenų, kuriuos duomenų turėtojai turi pareigą pateikti antriniam naudojimui, taikymo sritį (Pasiūlymas dėl ESDER, 33 str., 1 d., f p.). Duomenų turėtojo apibrėžtis yra plati ir apima subjektą, veikiantį sveikatos priežiūros sektoriuje arba atliekantį su šiuo sektoriumi susijusius mokslinius tyrimus, turintį teisę, pareigą ar galimybę teikti tam tikrus duomenis (Pasiūlymas dėl ESDER, 2 str., 2 d., y p). Pasiūlyme dėl ESDER aiškiai nurodyta, kad privatūs subjektai patenka į duomenų turėtojų taikymo sritį, todėl ši sąvoka galėtų būti taikoma sveikatos technologijų įmonėms, jei jos laikomos priklausančiomis sveikatos priežiūros sektoriui. Taip pat, ESDER pateikiama keletas konkrečių draudžiamų duomenų naudojimo būdų, įskaitant reklamą ar rinkodarą, skirtą sveikatos priežiūros specialistams, arba duomenų naudojimą siekiant pritaikyti draudimo įmokas (Pasiūlymas dėl ESDER, 35 str.).

Taigi, tie subjektai, kurie pageidautų antriniu naudojimo būdu (pakartotinai) naudoti duomenis, privalės pateikti prašymą dėl prieigos, kurį turėtų įvertinti kompetentinga sveikatos duomenų prieigos įstaiga, atsakinga už leidimo naudotis duomenimis išdavimą. Leidime naudoti duomenis reikės nurodyti, kaip ir kokiu tikslu duomenys gali būti naudojami (Pasiūlymas dėl ESDER, 36 str.). Svarbu paminėti, kad duomenys galės būti prieinami ir tvarkomi tik uždaroje saugioje aplinkoje, kurią užtikrins sveikatos duomenų prieigos įstaigos, taikančios aiškius kibernetinio saugumo standartus. Be to, iš saugios duomenų apdorojimo aplinkos leidimo prašantis naudotojas gali gauti anoniminius duomenis. Tačiau, jei tyrėjams, įmonėms ar valstybės institucijoms reikia prieigos prie asmeninių elektroninių sveikatos duomenų, jie gali juos gauti tik pseudonimizuota forma, t. y. duomenis, kuriuose pateikiama informacija apie ligą, simptomus ir vaistus, neatskleidžiant naudotojui asmens tapatybės. Naudotojui draudžiama bandyti iš naujo nustatyti duomenų subjektų tapatybę (Pasiūlymas dėl ESDER, 44 str.).

Taip pat, pažymėtina, kad visos valstybės narės privalės dalyvauti ES antrinio naudojimo infrastruktūroje (HealthData@EU), kad būtų sudarytos palankesnės sąlygos tarpvalstybiniams tyrimams vystyti (Pasiūlymas dėl ESDER, 52 str.).

4.4 Išmaniųjų sveikatos aplikacijų ir prietaisų ženklinimas

Dar viena su sveikatos aplikacijomis susijusių naujovių pateiktų Pasiūlyme dėl ESDER yra savanoriškas sveikatos aplikacijų ženklinimas. Pasiūlymo dėl ESDER 31 str., teigiama, kad sveikatos aplikacijų, teigiančių, kad jos yra sąveikios su ESĮ sistema ir todėl atitinka esminius reikalavimus, gamintojai gali savanoriškai pageidauti, kad prie jų aplikacijų būtų pridėtas ženklas, nurodantis, kad jos atitinka šiuos reikalavimus (Pasiūlymas dėl ESDER, 31 str., 1 d.).

Savo bendroje Nuomonėje dėl pasiūlymo dėl ESDER (toliau – **Nuomonė)**, EDAV ir Europos duomenų apsaugos priežiūros pareigūnas (toliau – **EDAPP**) iš esmės pritaria savanoriškam sveikatos aplikacijų ženklinimui, kadangi tai gali užtikrinti skaidrumą sveikatos aplikacijų naudotojams, atsižvelgiant į aplikacijų pagrindines savybes, ir taip padėti naudotojams pasirinkti patikimas sveikatos aplikacijas (European Data Protection Board. EDPB-EDPS Joint..., p. 21). Tačiau Nuomonėje pažymima, kad pasiūlymo dėl ESDER 31 ir 32 str., aptariama tik sveikatos aplikacijų sąveika su ESĮ sistemomis ir nustatomas savanoriško atitikimo mechanizmas, apsiribojantis pasiūlymo dėl ESDER II priede nustatytais sąveikos ir saugumo reikalavimais, siekiant užtikrinti, kad sveikatos aplikacijos galėtų perduoti elektroninius sveikatos duomenis ESĮ sistemoms (European Data Protection Board. EDPB-EDPS Joint..., p. 21). Šiuo atžvilgiu EDAV ir EDAPP pabrėžia, kad prie sveikatos aplikacijų pridedamas ženklas pagal pasiūlymo dėl ESDER 31 str., nebūtinai reiškia, kad duomenų tvarkymo operacijos, kuriomis grindžiamas tų aplikacijų veikimas, savaime yra teisėtos ir naudotojas jas gali naudoti. Duomenų valdytojas taip pat turi laikytis kitų reikalavimų, nustatytų ES duomenų apsaugos teisės aktuose. EDAV ir EDAPP rekomenduoja, kad tai būtų paaiškinta pačiame Pasiūlyme dėl ESDER (European Data Protection Board. EDPB-EDPS Joint..., p. 21). Pasiūlymo dėl ESDER 35 konstatuojamojoje dalyje teigiama, kad: „sveikatos aplikacijų, tokių kaip mobiliosios aplikacijos, naudotojai turėtų būti informuojami apie tokių aplikacijų prijungimo prie ESĮ sistemų arba nacionalinių elektroninės sveikatos sprendimų ir duomenų tiekimo į jas galimybes tais atvejais, kai sveikatos aplikacijų teikiami duomenys yra naudingi sveikatos priežiūros tikslais <...>“ (Pasiūlymas dėl ESDER, 35 konstatuojamoji dalis). Tačiau sąlygos, kuriomis tokios sveikatos aplikacijos gali būti

teisėtai prijungtos ir teikti asmens duomenis ESĮ sistemoms (arba nacionaliniams elektroninės sveikatos sprendimams) pagal duomenų apsaugos teisės aktus, pasiūlyme dėl ESDER nenurodytos (European Data Protection Board. EDPB-EDPS Joint..., p. 21).
Taigi, nors ši reguliavimo naujovė yra vertinama teigiamai, tačiau visgi yra reikalingi atitinkami jos patobulinimai siekiant visapusiškai išnaudoti šios naujovės potencialą.

4.5 ESDER pasiūlymo problematika bei įtaka išmaniųjų sveikatos aplikacijų ir prietaisų kūrėjams

Kalbant apie ESDER pasiūlymo problematika išmaniųjų sveikatos aplikacijų ir prietaisų kontekste, pažymėtina jog EDAV ir EDAPP savo Nuomonėje teigia, kad privalomas antriniam naudojimui skirtų elektroninių sveikatos duomenų, gautų naudojant sveikatos aplikacijas ir prietaisus, prieinamumas turi būti vertinamas atsižvelgiant į sparčią mobiliųjų ir dėvimųjų technologijų vystymosi raidą ir vis labiau populiarėjančias aplikacijas ir prietaisus, kurie leidžia asmenims registruoti įvairius aspektus apie savo asmenybę, protą, kūną, elgesio modelius ir buvimo vietą (European Data Protection Board. EDPB-EDPS Joint..., p. 21–22). Nuomonėje minima, kad tokiam duomenų tvarkymui reikia skirti daug dėmesio, nes dažnu atveju duomenų subjektai nelengvai atpažįsta, kad yra tvarkomi būtent jų sveikatos duomenys. Svarbu dar kartą užsiminti, jog toks tvarkymas kelia realią riziką privatumui, ypač tuo atveju, kai sveikatos duomenys tvarkomi papildomais tikslais ir (arba) sujungiami su kitais duomenimis arba perduodami trečiosioms šalims. Taigi, sveikatos duomenų tvarkymas gali sukelti nemažai pavojų, įskaitant nevienodo ar nesąžiningo elgesio riziką, pagrįstą duomenimis apie numanomą ar faktinę asmens sveikatos būklę, gautais, pavyzdžiui, profiliavimo būdu, neatsižvelgiant į tai, ar šios išvados apie asmens sveikatos būklę yra tikslios, ar ne (European Data Protection Board. EDPB-EDPS Joint..., p. 21–22). Teigiama, kad iš tiesų ši rizika taip pat gali būti susijusi su sveikatos aplikacijų generuojamų duomenų patikimumu ir tikslumu. Šiuo atžvilgiu EDAV ir EDAPP rekomenduoja į pasiūlymo IV skyriaus (antrinis elektroninių sveikatos duomenų naudojimas) taikymo sritį neįtraukti sveikatos aplikacijų. Tačiau jei šie duomenys visgi ateityje ir toliau pateks į IV skyriaus taikymo sritį, EDAV ir EDAPP pabrėžia, kad naudotojai turi turėti teisę laisvai nuspręsti, ar ir kokie jų asmens duomenys, gauti naudojant sveikatos aplikacijas, neatsižvelgiant į tai, kad jie buvo įkelti į jų pačių ESĮ, bus perduoti kitiems gavėjams ir toliau tvarkomi antrinio naudojimo tikslais (European Data Protection Board. EDPB-EDPS Joint..., p. 21–22). Todėl EDAV ir EDAPP rekomenduoja iš dalies pakeisti Pasiūlymą dėl ESDER, kad būtų užtikrinta, jog duomenų subjektai būtų tinkamai informuoti apie jų galimus pasirinkimus, susijusius su tolesniu jų

elektroninių sveikatos duomenų, sukurtų naudojant sveikatos aplikacijas, naudojimu. Be to, pagal duomenų apsaugos teisės aktus turi būti aiškiai nustatytos konkrečios tolesnio tokių asmens duomenų tvarkymo sąlygos bei nustatyti tinkami mechanizmai, kuriais būtų užtikrinta, kad duomenų subjektų valios dėl tolesnio jų asmens sveikatos duomenų, gautų naudojant sveikatos aplikacijas, tvarkymo būtų paisoma (European Data Protection Board. EDPB-EDPS Joint..., p. 21–22).

Taigi, jei Pasiūlymas dėl ESDER nebus pakeistas atsižvelgiant į Nuomonėje pateiktą rekomendaciją neįtraukti sveikatos aplikacijų į pasiūlymo IV skyriaus taikymo sritį, išmaniųjų sveikatos aplikacijų ir prietaisų kūrėjams tai reikš galimybę naudotis antrinio duomenų naudojimo mechanizmu kuriant naujus produktus. Tačiau tuo pačiu metu aplikacijų kūrėjai atitinkamai turės laikytis reikalavimo pateikti savo tvarkomus duomenis antrinio duomenų naudojimo reikmėms (Pasiūlymas dėl ESDER, 41 str.).

Šiuo metu ESDER yra tik pasiūlymas sukurti konkrečiai sričiai skirtą duomenų erdvę. Nors jis turi didelį potencialą, tačiau kyla nemažai neaiškumų dėl siūlomo reglamento aiškinimo ir jame numatytos apsaugos. Visų pirma kyla abejonių dėl to, kaip antrinio naudojimo sąvoka derės su BDAR, pagal kurį duomenų naudotojams, norintiems tvarkyti sveikatos duomenis antriniais tikslais, reikalingas teisinis pagrindas (European Parliament. European health data..., 2022). Kitos keliamos problemos yra susijusios su saugumu ir tuo, kaip pasiūlymas padės užtikrinti saugių apdorojimo aplinkų funkcionalumą bei taip pat kokios priemonės bus įgyvendintos siekiant apsaugoti duomenų turėtojų teises teikiant duomenis (European Parliament. European health data..., 2022). Neabejotina, kad ESDER gali suteikti didelių galimybių, tačiau teisėkūros procedūra šiuo metu dar tik įsibėgėja, todėl įstatymo leidėjas prieš tai minėtus sunkumus turės apsvarstyti išsamiau bei parengti tinkamas gaires dėl minėtų neaiškumų keliančių sričių.

Šiuo metu, sveikatos technologijų įmonės galėtų apsvarstyti savo duomenų strategijos sukūrimą arba patobulinimą, siekiant prisitaikyti prie minėtų pokyčių, taip pat jos turėtų užsitikrinti pakankamą įgūdžių ir išteklių kiekį, siekiant pasinaudoti būsima prieiga prie sveikatos duomenų.

Apibendrinus, svarbu paminėti tai, kad ESDER įgyvendinimui yra skirtas gan trumpas laikotarpis. Siekiama, kad ESDER turi būti pradėtas įgyvendinti nuo 2025 m. bei būti pilnai įgyvendintas iki 2030 m. (Euractiv. Council hashes out secondary..., 2023). Todėl visi subjektai susiję su sveiktos sektoriumi – paslaugų teikėjai, gamintojai ir mokslininkai – turėtų nedelsdami pradėti ruoštis šiems pokyčiams. Šis pasiruošimas turėtų apimti tiek esamus produktus, tiek būsimus inovacijų projektus.

IŠVADOS

1. Į išmaniųjų sveikatos aplikacijų ir prietaisų sąvoką patenka: į mobilius įrenginius instaliuotos išmaniosios sveikatos ar sveikatingumo, kūno rengybos ir gyvenimo būdo aplikacijos, bei dėvimieji ar nešiojami prietaisai, kurie yra susieti su šiomis aplikacijomis ir yra jų kaip technologijos neatsiejama dalis. Šios aplikacijos ir prietaisai susiduria su tam tikrais privatumo ir saugumo iššūkiais, tokiais kaip pvz., duomenų vagystė ar nepageidaujamas dalijimasis su trečiosiomis šalimis.
2. Vienas iš esminių reguliavimo ypatumų taikomų sveikatos aplikacijoms ir prietaisams yra BDAR išskirtas specialiųjų kategorijų duomenų (sveikatos duomenų) tvarkymas. BDAR įtvirtinta, jog yra draudžiama tvarkyti specialiųjų kategorijų duomenis, išskyrus tam tikras išimtis. Šiuo atžvilgiu, kalbant apie išmaniąsias sveikatos aplikacijas ir prietaisus, labiausiai aktuali būtų išimtis, kurioje minima būtinybė gauti aiškų duomenų subjekto sutikimą tvarkyti jo asmens duomenis. Sutikimas turi būti konkretus ir duodamas laisva valia bei duodamas vienu ar keliais konkrečiais, aiškiais ir teisėtais tikslais. Aiškus duomenų subjekto sutikimas reiškia, kad duomenų subjektas turi pateikti aiškų sutikimo pareiškimą.
3. BDAR taip pat nustatyta, kad kai specialiųjų kategorijų duomenys yra tvarkomi dideliu mastu, duomenų valdytojams yra privaloma atlikti PDAV. Tai procesas skirtas duomenų tvarkymui aprašyti ir tokio tvarkymo reikalingumui ir proporcingumui įvertinti, padedantis valdyti pavojų, kuris fizinių asmenų teisėms ir laisvėms kyla dėl asmens duomenų tvarkymo. Siekiant vykdyti teisėtą duomenų tvarkymą išmaniųjų aplikacijų ir prietaisų kūrėjams yra privalu gauti aiškų duomenų subjektų sutikimą ir atlikti PDAV.
4. BDAR iš esmės yra pakankama reguliavimo priemonė duomenų subjektų sveikatos duomenims apsaugoti, tačiau praktikoje jis ne visada yra tinkamai įgyvendinamas. Dėl šios priežasties alternatyvūs reguliavimo būdai, kaip išmaniųjų sveikatos aplikacijų reguliavimas aplikacijų parduotuvėse taikant peržiūros procedūras, gali tapti sprendimu siekiant užpildyti spragas. Nors šis savireguliacijos mechanizmas turi trūkumų, tačiau įvertinus aplikacijų parduotuvių įtaką bei ypač svarbią padėtį, kaip vienintelių skaitmeninių platformų, kuriose gali vykti prekyba išmaniosiomis aplikacijomis, toks papildomas reguliavimas kol kas išlieka daugiausiai galimybių žadančia priemone siekiant gerinti sveikatos aplikacijų naudotojų duomenų apsaugos lygį.
5. Pagrindinė Pasiūlyme dėl ESDER pateikta naujovė reikšminga išmaniųjų sveikatos aplikacijų ir prietaisų kontekste yra antrinis sveikatos duomenų panaudojimas (sveikatos duomenų tvarkymas kitais tikslais, nei pirminiai tikslai, dėl kurių duomenys buvo surinkti).

Tai reiškia, kad sveikatos technologijų įmonės kuriant savo produktus galės efektyviai ir saugiai naudotis dideliu kiekiu sveikatos duomenų, kuriuos antriniam naudojimui pateikė kiti sveikatos duomenų turėtojai. Atitinkamai šios įmonės taip pat turės pareigą savo tvarkomus sveikatos duomenis pateikti antriniam naudojimui.

6. Kol kas esminis probleminis aspektas susijęs ESDER pasiūlyme pateiktomis naujovėmis yra EDAV ir EDAPP paskelbta nuomonė, kurioje įstatymų leidėjui rekomenduojama sveikatos aplikacijas išbraukti iš antrinio elektroninių sveikatos duomenų naudojimo taikymo srities. Todėl svarbu, kad pasiūlymas nebūtų pakeistas atsižvelgiant į nuomonėje pateiktą rekomendaciją ir išmaniųjų sveikatos aplikacijų ir prietaisų kūrėjai išsaugotų galimybę naudotis antrinio duomenų naudojimo mechanizmu.

ŠALTINIŲ SĄRAŠAS

Teisės norminiai aktai

Europos Sąjungos teisės aktai

1. 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). OJ L 119, p. 1.

2. Europos Parlamento ir Tarybos 2017 m. balandžio 5 d. reglamentas (ES) 2017/745 dėl medicinos priemonių, kuriuo iš dalies keičiama Direktyva 2001/83/EB, Reglamentas (EB) Nr. 178/2002 ir Reglamentas (EB) Nr. 1223/2009, ir kuriuo panaikinamos Tarybos direktyvos 90/385/EEB ir 93/42/EEB. OJ L 117, p. 1–175.

3. Europos Parlamento ir Tarybos 2007 m. rugsėjo 5 d. direktyva 2007/47/EB, iš dalies keičianti Tarybos direktyvą 90/385/EEB dėl valstybių narių įstatymų, reglamentuojančių aktyviuosius implantuojamus medicinos prietaisus, suderinimo, Tarybos direktyvą 93/42/EEB dėl medicinos prietaisų ir Direktyvą 98/8/EB dėl biocidinių produktų pateikimo į rinką. OJ L 247, p. 21–55.

Soft law šaltiniai

4. European Commission. Draft Code of Conduct on privacy for mobile health applications (2016) [interaktyvus]. Prieiga per internetą: Prieiga per internetą: https://digital-strategy.ec.europa.eu/en/library/code-conduct-privacy-mhealth-apps-has-been-finalised [žiūrėta 2023 m. vasario 15 d.].

5. Europos Komisija. Žalioji knyga dėl mobilios sveikatos. (2014) [interaktyvus]. Prieiga per internetą: https://op.europa.eu/lt/publication-detail/-/publication/0de99b25-c0af-11e3-86f9-01aa75ed71a1 [žiūrėta 2023 m. vasario 13 d.].

6. European Data Protection Board. EDPB-EDPS Joint Opinion on the Proposal for a Regulation on the European Health Data Space (2022) [interaktyvus]. Prieiga per internetą: https://edps.europa.eu/data-protection/our-work/publications/edps-edpb-joint-opinions/european-health-data-space_en [žiūrėta 2023 m. kovo 1 d.].

7. Article 29 data protection working party. Letter to Paul Timmers, Annex I - Health Data in Apps and Devices (2015) [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf [žiūrėta 2023 m. vasario 15 d.].

8. Article 29 data protection working party. Opinion on Privacy and Data Protection Issues relating to the Utilisation of Drones (2015) [interaktyvus]. Prieiga per internetą: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiBu7Ly9en9AhU1gv0HHZnfAfcQFnoECA4QAQ&url=https%3A%2F%2Fec.europa.eu%2Fnewsroom%2Farticle29%2Fredirection%2Fdocument%2F56119&usg=AOvVaw160RK5IVSvOJ8_yDqj7ikv [žiūrėta 2023 m. vasario 15 d.].

9. Europos duomenų apsaugos valdyba. Gairės dėl sutikimo pagal Reglamentą 2016/679 (2020) [interaktyvus]. Prieiga per internetą: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_lt_0.pdf [žiūrėta 2023 m. vasario 15 d.].

10. 29 straipsnio duomenų apsaugos darbo grupė. Poveikio duomenų apsaugai vertinimo (PDAV) gairės, kuriomis Reglamento 2016/679 taikymo tikslais nurodoma, kaip nustatyti, ar duomenų tvarkymo operacijos gali sukelti didelį pavojų (2017) [interaktyvus]. Prieiga per internetą: Prieiga per internetą: https://am.lrv.lt/uploads/am/documents/files/wp248_PDAV_gaires_2017-04-04.pdf [žiūrėta 2023 m. vasario 15 d.].

11. Europos Komisijos Gairėse dėl sveikatos apsaugos sektoriuje naudojamos autonominės programinės įrangos priskyrimo ir klasifikacijos medicinos priemonių reglamentavimo sistemoje, MEDDEV 2.1/6. (2016) [interaktyvus]. Prieiga per internetą: https://www.medical-device-regulation.eu/wp-content/uploads/2019/05/2_1_6_072016_en.pdf [žiūrėta 2023 m. kovo 1 d.].

Specialioji literatūra

12. Tzanou, M. (2020) The GDPR and (big) health data: Assessing the EU legislator's choices. Iš *Health Data Privacy under the GDPR: Big Data Challenges and Regulatory Responses*. Routledge [interaktyvus]. Prieiga per internetą: Prieiga per internetą: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3654116 [žiūrėta 2023 m. vasario 15 d.].

13. van Kolfschooten, H. (2022) The mHealth Power Paradox: Improving Data Protection in Health Apps through Self-Regulation in the European Union. Iš Cohen, I. G., Minssen, T., Price II, W. N., Robertson, C., and Shachar, C. (eds) *The Future of Medical Device Regulation: Innovation and Protection*. Cambridge: Cambridge University Press, 63–76 [interaktyvus]. Prieiga per internetą: Prieiga per internetą: https://www.cambridge.org/core/books/future-of-medical-device-regulation/mhealth-power-paradox/16BAD74F91E6337156ABF5C32019920A#CN-bp-5 [žiūrėta 2023 m. vasario 13 d.].

Elektroniniai leidiniai

14. Fong, A. (2017). The role of app intermediaries in protecting data privacy, *International Journal of Law and Information Technology*, 25 (2), p. 85–114 [interaktyvus]. Prieiga per internetą: https://academic.oup.com/ijlit/article/25/2/85/3737841?guestAccessKey=f5c21977-3d11-46c7-8f85-85648d896a66&login=false [žiūrėta 2023 m. kovo 1 d.].

15. Fromel, A. (2022) Will the European Health Data Space change the face of digital health?. Zuhlke. [interaktyvus]. Prieiga per internetą: https://www.zuehlke.com/en/insights/will-the-european-health-data-space-change-the-face-of-digital-health [žiūrėta 2023 m. kovo 1 d.].

16. Grundy, Q., Chiu, K., Held, F., Continella, A., Bero, L., & Holz, R. (2019). Data sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis. *BMJ* [interaktyvus]. Prieiga per internetą: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6425456/ [žiūrėta 2023 m. kovo 1 d.].

17. Gupta, A. K., Lad, L. J. (1983). Industry Self-Regulation: An Economic, Organizational, and Political Analysis. *The Academy of Management Review*, 8(3), 416–425 [interaktyvus]. Prieiga per internetą: https://www.jstor.org/stable/257830?seq=6 [žiūrėta 2023 m. kovo 1 d.].

18. Monegier, H. R. (2020) *When does my app qualify as medical device?*. LexGo [interaktyvus]. Prieiga per internetą: https://www.lexgo.be/en/news-and-articles/7458-when-does-my-app-qualify-as-medical-device [žiūrėta 2023 m. vasario 13 d.].

19. Mulder, T. (2019). Health Apps, Their Privacy Policies and the GDPR. *European Journal of Law and Technology*, 10 (1) [interaktyvus]. Prieiga per internetą: https://ejlt.org/index.php/ejlt/article/view/667/898 [žiūrėta 2023 m. kovo 1 d.].

20. Shad, R. (2022) What is mHealth? Everything You Need to Know When Developing a mHealth App. OSP [interaktyvus]. Prieiga per internetą: https://www.osplabs.com/insights/what-is-mhealth/ [žiūrėta 2023 m. vasario 13 d.].

Teismų praktika

21. *Brain Products GmbH prieš BioSemi VOF ir kt*. [ESTT], Nr. C-219/11, [2012-11-22]. ECLI:EU:C:2012:742.

22. Generalinio advokato Paolo Mengozzi išvada. [2012-05-15]. ECLI:EU:C:2012:299.

Travaux préparatoires

23. Europos Komisija. Pasiūlymas dėl reglamento dėl Europos bendros sveikatos duomenų erdvės (2022) [interaktyvus]. Prieiga per internetą: https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:52022PC0197 [žiūrėta 2023 m. kovo 1 d.].

Kiti šaltiniai

24. Apple App Store. Apple Developer Program License Agreement (2022) [interaktyvus]. Prieiga per internetą: https://developer.apple.com/support/downloads/terms/apple-developer-program/Apple-Developer-Program-License-Agreement-20220606-English.pdf [žiūrėta 2023 m. kovo 1 d.].

25. Apple App Store. App Store Review Guidelines (2022) [interaktyvus]. Prieiga per internetą: https://developer.apple.com/app-store/review/guidelines/ [žiūrėta 2023 m. kovo 1 d.].

26. Euractiv. Council hashes out secondary use of data in EU health data space (2023) [interaktyvus]. Prieiga per internetą: https://www.euractiv.com/section/health-consumers/news/council-hashes-out-secondary-use-of-data-in-eu-health-data-space/ [žiūrėta 2023 m. kovo 1 d.].

27. Europos Komisija. *Klausimai ir atsakymai, ES sveikata, Europos sveikatos duomenų erdvė (EDHS)* (2022) [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/commission/presscorner/detail/lt/QANDA_22_2712 [žiūrėta 2023 m. kovo 1 d.].

28. European Commission. *Shaping Europe's digital future* (2020) [interaktyvus]. Prieiga per internetą: https://digital-strategy.ec.europa.eu/en/policies/privacy-mobile-health-apps [žiūrėta 2023 m. vasario 15 d.].

29. European Parliament. European health data space, overview (2022) [interaktyvus]. Prieiga per internetą: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733646/EPRS_BRI(2022)733646_EN.pdf [žiūrėta 2023 m. kovo 1 d.].

30. European Union Agency for Cybersecurity (2018). Privacy and Data Protection in Mobile Applications [interaktyvus]. Prieiga per internetą: https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications [žiūrėta 2023 m. kovo 1 d.].

31. Google Play. Google Play Developer Distribution Agreement (2022) [interaktyvus]. Prieiga per internetą: https://play.google.com/about/developer-distribution-agreement.html [žiūrėta 2023 m. kovo 1 d.].

32. Google Play. Google Play Developer Program Policies 2022) [interaktyvus]. Prieiga per internetą: https://support.google.com/googleplay/android-developer/answer/10144311?hl=en&ref_topic=9877467#1&2&3&4&5&6&7&87&9&zippy=%2Cexamples-of-common-violations [žiūrėta 2023 m. kovo 1 d.].

33. Onetrust. *Understanding the 7 Principles of the GDPR* [interaktyvus]. Prieiga per internetą: Prieiga per internetą: https://www.onetrust.com/blog/gdpr-principles/ [žiūrėta 2023 m. vasario 15 d.].

34. The Data Protection Commission of Ireland. Data Protection Impact Assessments [interaktyvus]. Prieiga per internetą: https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments [žiūrėta 2023 m. vasario 15 d.].

35. The Data Protection Commission of Ireland. *Principles of Data Protection* [interaktyvus]. Prieiga per internetą: https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection [žiūrėta 2023 m. vasario 15 d.].

36. The Data Protection Commission of Ireland. *Codes of conduct* [interaktyvus]. Prieiga per internetą: https://www.dataprotection.ie/en/organisations/codes-conduct [žiūrėta 2023 m. kovo 1 d.].

37. What is Wearable Tech? Everything You Need to Know Explained (2019) [interaktyvus]. Prieiga per internetą: https://www.wareable.com/wearable-tech/what-is-wearable-tech-753 [žiūrėta 2023 m. vasario 13 d.].

38. World Health Organization. Meeting on secondary use of health data (2022) [interaktyvus]. Prieiga per internetą: https://www.who.int/europe/news-room/events/item/2022/12/13/default-calendar/meeting-on-secondary-use-of-health-data [žiūrėta 2023 m. kovo 1 d.].

39. WHO Global Observatory for eHealth, *mHealth: New Horizons for Health through Mobile Technologies* (2011) [interaktyvus]. Prieiga per internetą: https://apps.who.int/iris/bitstream/handle/10665/44607/9789241564250_eng.pdf?sequence=1&isAllowed=y [žiūrėta 2023 m. vasario 13 d.].

SANTRAUKA

Išmaniųjų sveikatos aplikacijų ir prietaisų problematika pagal ES duomenų apsaugos teisę

Elzė Markauskaitė

Mūsų kūnai nuolatos skleidžia duomenų srautus: viską – nuo fizinio aktyvumo, suvartojamų kalorijų, miego ir laikysenos iki lytinių santykių, menstruacijų ciklo, vaisingumo ir kvėpavimo įpročių – galima sekti, matuoti, registruoti ir analizuoti, siekiant stebėti sveikatos pokyčius bei pažinti save. Nuo praeito dešimtmečio pabaigos, kai buvo atidarytos pirmosios aplikacijų parduotuvės, mobiliųjų aplikacijų skaičius išaugo ypač dideliu mastu. Šiuo metu rinkoje yra daugiau kaip 250 000 sveikatos aplikacijų (pvz., viena iš jų – aplikacija Flo, kurioje galima stebėti ir prognozuoti menstruacijų ciklą) ir su jomis susietų dėvimųjų bei nešiojamų prietaisų, (tokių kaip: išmanieji laikrodžiai; kūno rengybos (angl. *fitness*) sekimo įrenginiai pvz., Fitbit bevielis matuoklis, išmanieji drabužiai pvz., išmaniosios vaikų sauskelnės ar kojinė kuri matuoja kūdikio temperatūrą, širdies ritmą, deguonies prisotinimą ir judėjimą, tai pat išmanieji juvelyriniai dirbiniai bei implantai).

Taigi, kūno stebėjimas pasitelkiant technologijas tapo kasdienio mūsų gyvenimo dalimi. Būtent dėl šios priežasties, siekiant didinti visuomenės informuotumą apie sveikatos technologijų tvarkomus asmens duomenis ir kuriamų produktų atitiktį galiojančiam reglamentavimui yra ypač aktuali ir reikalinga išsami išmaniųjų sveikatos aplikacijų ir prietaisų sampratos ir reguliavimo analizė, kuri yra atliekama šiame darbe.

Pirmoje darbo dalyje yra nagrinėjama išmaniųjų sveikatos aplikacijų ir prietaisų sąvoka, privalumai, naudojimo iššūkiai bei atskyrimo nuo medicinos prietaisų reikšmė ir svarba. Antroje dalyje aptariami šios sveikatos technologijos reguliavimo ypatumai ir problematika BDAR kontekste atskleidžiant specialiųjų kategorijų – sveikatos duomenų esmę, aiškaus duomenų subjekto sutikimo reikalavimą, PDAV proceso sampratą ir BDAR netinkamo įgyvendinimo apsaugant sveikatos duomenis problemą. Trečioje dalyje kalbama apie alternatyvius išmaniųjų sveikatos aplikacijų ir prietaisų reguliavimo būdus duomenų apsaugos kontekste. Galiausiai ketvirtoje dalyje, nagrinėjamos svarbiausios ESDER pasiūlyme pateiktos teisinės naujovės reikšmingos išmaniųjų sveikatos aplikacijų ir prietaisų prasme.

SUMMARY

Issues of Smart Health Applications and Devices under the EU Data Protection Law

Elzė Markauskaitė

Our bodies produce a constant data stream that can be recorded, evaluated, registered, and analyzed in order to track changes in our health. This data ranges from calorie consumption, daily exercise, sleep and body position to sexual activity, fertility, menstrual cycles and breathing patterns. Since the end of the last decade, when the first app stores were launched, the number of mobile applications has grown tremendously. There are currently more than 250,000 health applications (for example, the Flo app that can track and predict your menstrual cycle) and related wearable devices (such as: smart jewelry and implants; fitness tracking devices such as the Fitbit wireless meter, smart watches; as well as smart baby diapers or socks that measures the baby's heart rate, temperature, oxygen saturation and movement) on the market.

Thus, body tracking through technology has become part of our daily lives. It is for this reason that a comprehensive analysis of the concept and regulation of smart health apps and devices, which is the subject of this paper, is particularly relevant and necessary in order to raise public awareness on the processing of personal data by health technologies and the compliance of emerging products with the existing regulation.

The first part of the thesis explores the concept, benefits, challenges of smart health applications as well as the meaning and importance of the distinction between smart health applications and medical devices. The second part discusses the specificities and challenges of the regulation of this health technology in the context of the GDPR, highlighting the essence of the special categories of data (health data), the requirement of explicit consent of the data subject, the concept of the DPIA process and the problem of inadequate implementation of the GDPR to protect health data. The third part focuses on alternative ways of regulating smart health applications and devices in the context of data protection. Finally, the fourth part examines the key legal innovations contained in the EHDSR proposal in terms of the relevance for smart health applications and devices.