Vilniaus universiteto Teisės fakulteto
Privatinės teisės katedra

Kotrynos Puodžiukaitės
V kurso, ES verslo teisės
studijų šakos studentės

Magistro darbas

Asmens duomenų apsaugos užtikrinimas ir kylančios problemos viešajame sektoriuje
Data Protection Assurance and Emerging Issues in the Public Sector

Vadovas: asist. dr. Julius Zaleskis
Recenzentas: doc. dr. Laurynas Didžiulis

Vilnius
2020

ANOTACIJA IR PAGRINDINIAI ŽODŽIAI

Šiame darbe analizuojama kaip asmens duomenų apsaugos institutas yra įgyvendinamas viešajame sektoriuje. Taip pat atskleidžiamos svarbiausios asmens duomenų apsaugos įgyvendinimo viešajame sektoriuje kylančios problemos ir aptariami kylančių problemų sprendimo būdai.

Pagrindiniai žodžiai: asmens duomenų samprata, asmens duomenų apsaugos įgyvendinimas viešajame sektoriuje, duomenų tvarkymo principai taikomi viešajame sektoriuje, duomenų apsaugos įgyvendinimo problemos viešajame sektoriuje, duomenų apsaugos įgyvendinimo problemų sprendimas viešajame sektoriuje.

This paper analyzes how the data protection institute is implemented in the public sector. It also reveals the most important problems in the implementation of data protection in the public sector and discusses solutions to the problems.

Keywords: the concept of personal data, the implementation of personal data protection in the public sector, the principles of data processing applied in the public sector, the problems of data protection implementation in the public sector, the solution of data protection implementation problems in the public sector.

TURINYS

ĮVADAS

Asmens duomenų apsauga dabartinėje visuomenėje yra laikoma viena iš prioritetinių krypčių. Nors požiūris į asmens privatumą keičiasi dėl sparčios technologijų pažangos, nuolatinių globalizacijos reiškinių bei išaugusio poreikio dalintis asmenine informacija, teisių į asmens duomenų apsaugą ir privatumą užtikrinimas išlieka itin svarbus reiškinys. Dėl nuolatinės išorinių priežasčių įtakos asmens duomenų apsaugai tampa būtina tobulinti teisės į asmens duomenų apsaugą politiką ir modernizuoti apsaugos priemones. Teisinis reglamentavimas privalo spėti apimti asmens duomenų apsaugos klausimą ir tada, kai asmens duomenų sistemos nenumaldomai tobulėja dėl socialinių, politinių ir ekonominių veiksnių.

Viešojo sektoriaus įstaigoms vykdant joms priskirtas funkcijas, būtina tvarkyti gan didelį kiekį asmens informacijos, todėl atsirado poreikis užtikrinti asmens duomenų apsaugos įgyvendinimo procesą viešajame sektoriuje. Siekiant viešajame sektoriuje užtikrinti asmens duomenų apsaugos įgyvendinimo procesą, reikia remtis teisės aktais bei Valstybinės duomenų apsaugos inspekcijos rekomendacijomis.

Temos naujumas. Temos naujumas atsiskleidžia analizuojant viešąjį sektorių asmens duomenų apsaugos užtikrinimo bei konkrečių problemų sprendimo aspektu. Atsakyti į klausimą, ar įmanoma nepažeisti pusiausvyros tarp viešojo sektoriaus vykdomos veiklos, keliamų reikalavimų asmens duomenų apsaugai bei pačių duomenų saugumo. Darbui naujumo suteikia tai, jog darbe analizuojami konkretūs viešojo sektoriaus pavyzdžiai. Viena iš viešojo sektoriaus institucijų, generuojanti bene didžiausią apimtį duomenų yra valstybės įmonė Registrų centras. Ši institucija sudaro sutartis su fiziniais ir juridiniais asmenimis, teikiant nekilnojamojo turto, gyventojų, juridinių asmenų bei kitų registrų ir informacinių sistemų duomenis, todėl labai svarbu, jog sudarytose sutartyse būtų aptarti visi su asmens duomenų saugumu bei konfidencialumu susiję klausimai. Darbe pateikiami ir kitų viešojo sektoriaus institucijų pavyzdžiai, analizuojant, kokia kryptinga pozicija einama saugant vienokio ar kitokio pobūdžio duomenis. Pavyzdžiai, kaip vykdoma asmens duomenų apsaugos politika tokiose viešojo sektoriaus institucijose kaip Lietuvos bankas, Valstybinė teismo medicinos tarnyba prie Lietuvos Respublikos teisingumo ministerijos, Lietuvos Respublikos socialinės apsaugos ir darbo ministerija, Valstybinė vartotojų teisių apsaugos tarnyba ir pan.

Nagrinėjamos temos aktualumas. Tema aktuali todėl, kad priėmus Europos Parlamento ir Tarybos reglamentą 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)[1] ypatingas dėmesys turi būti skiriamas asmens duomenų apsaugai, nes pažeidus Bendrojo duomenų apsaugos reglamento nuostatas gresia didelės baudos bei kitokios sankcijos. Dabartiniu laikotarpiu viešasis sektorius saugo daug įvairaus pobūdžio duomenų, kurie susiję su asmeniu. Todėl aktualu diskutuoti, kaip turi būti apsaugoti asmens duomenys, neprasilenkiant su teisės aktų reikalavimais, kartu taikant inovatyvias technologijas bei užtikrinant pažangą viešajame sektoriuje. Dabartiniu laikotarpiu viešajame sektoriuje duomenys saugomi elektroninėje erdvėje, teikiamos elektroninės paslaugos, todėl viešojoje erdvėje prieinami asmens duomenys turi atitikti Bendrajame duomenų apsaugos reglamente bei kituose teisės aktuose keliamus reikalavimus.

Problema. Viešojo administravimo institucijos, tenkindamos viešuosius interesus, kartu turi užtikrinti duomenų apsaugą bei nenukrypti nuo teisės aktų reikalavimų ir tapti šiuolaikinės inovatyvios visuomenės iššūkio dalyviu.

Šio darbo **tyrimo objektas** – asmens duomenų apsaugos užtikrinimas bei kylančios problemos viešajame sektoriuje.

Pagrindinis šio darbo **tikslas** – išsiaiškinti asmens duomenų apsaugos užtikrinimą bei kylančias problemas viešajame sektoriuje.

Numatytam tikslui pasiekti keliami tokie **uždavinia**i:

1. Atskleisti asmens duomenų ir viešojo administravimo įstaigų sampratas ir išskirtinumą.
2. Ištirti asmens duomenų tvarkymo principų išskirtinumą viešojo sektoriaus funkcijų vykdymui.
3. Išskirti asmens duomenų elementus ir jų atskleidimo pagrindus viešojo sektoriaus funkcijoms vykdyti.
4. Aptarti asmens duomenų apsaugos įgyvendinimo klausimų pokytį iki Bendrojo duomenų apsaugos reglamento ir priėmus Bendrąjį duomenų apsaugos reglamentą.
5. Išskirti asmens duomenų apsaugos įgyvendinimo problemų išskirtinumą ir jų sprendimo būdus viešajame sektoriuje.

Magistriniame darbe taikyti šie **tyrimo metodai:**

1. Lyginamasis metodas. Šio metodo pagalba lyginami teiginiai mokslinėje doktrinoje bei jų įtvirtinimas kasacinėje jurisprudencijoje. Aptariant asmens duomenų apsaugos klausimus, remiamasi teismų praktika, nacionaliniais ir tarptautiniais teisės aktais, Valstybinės duomenų apsaugos inspekcijos rekomendacijomis. Lyginama duomenų apsauga iki Bendrojo duomenų apsaugos reglamento priėmimo ir jam įsigaliojus.

[1] Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) Nr. 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) OL 2016 L 19, p. 1-88.

2. Sisteminis metodas. Šis metodas naudojamas darbe pateikiant asmens duomenų apsaugos požymius, principus, išskiriant viešojo administravimo subjektų kompetencijas, funkcijas, ribas, kas susiję su asmens duomenų apsauga.

3. Lingvistinis metodas. Šis metodas padeda atskleisti ir analizuoti teisines sąvokas, paaiškinti terminologiją, kas yra svarbu tiek mokslinės literatūros, tiek ir teisminės jurisprudencijos analizei.

4. Loginis – analitinis metodas. Šis metodas padeda suvokti ir analizuoti asmens duomenų apsaugos skirtuminius dalykus, tarpusavio sąsajas bei išskirti funkcijas, jas įvertinti.

5. Istorinis metodas. Šis metodas naudotas analizuojant duomenų apsaugą skirtingais istoriniais laikotarpiais.

Darbo struktūra. Pirmoji darbo dalis skirta duomenų sampratai, taip pat viešojo sektoriaus sampratai bei išskirtinumui atskleisti. Pristatomi viešojo administravimo principai, asmens duomenų samprata pateikiama remiantis nacionaliniais ir tarptautiniais teisės aktais. Pristatoma informacijos, kaip vieno iš asmens duomenų elementų samprata. Analizuojant duomenų sampratą, dėmesys skiriamas ypatingiems, t. y. biometriniams duomenims. Aptariamas tapatybės nustatymo klausimas. Pateikiami duomenų tvarkymo principai – teisėtumas, sąžiningumas, skaidrumas, apribojimas, duomenų kiekio mažinimas, tikslumas, trukmės ribojimas, vientisumas, konfidencialumas, siekiant išsiaiškinti, kiek šie principai svarbūs duomenų apsaugai viešajame sektoriuje. Aptariami asmens duomenų tvarkymo viešajame sektoriuje pagrindai. Antroji darbo dalis skirta asmens duomenų apsaugos problemoms, kylančioms viešajame sektoriuje, atskleisti. Išskiriamos problemos iki Bendrojo duomenų apsaugos reglamento ir po jo įsigaliojimo. Trečioji darbo dalis skirta asmens duomenų apsaugos įgyvendinimo problemų sprendimui viešajame sektoriuje.

Svarbiausi šaltiniai. Analizuojant šią temą, remiamasi nacionaliniais ir tarptautiniais teisės aktais. Šio darbo pagrindą sudaro Europos Sąjungos ir Lietuvos asmens duomenų apsaugos srityje taikomi teisės aktai, kompetentingų institucijų rekomendacijos ir nuomonės, taip pat mokslinė literatūra. Svarbiausi analizuojami teisės aktai darbe – tai Europos Parlamento ir Tarybos reglamentas 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), Europos Sąjungos pagrindinių teisių chartija, 2016/C 202/02, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas[2]. Duomenų bei viešojo sektoriaus sampratas analizuoja V. Giedraitytė (2016), J. E. Lane (2001), J. Zaleskis (2019), S. Jastiuginas (2011). Viešojo sektoriaus veiklą reglamentuoja tokie teisės aktai kaip Lietuvos Respublikos viešojo administravimo

[2] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (2018). TAR, 11733.

įstatymas[3], Lietuvos Respublikos valstybės informacinių išteklių įstatymas[4], o kad apsaugoti duomenis viešajam sektoriui labai svarbus Lietuvos Respublikos kibernetinio saugumo įstatymas[5].

[3] Lietuvos Respublikos viešojo administravimo įstatymas (1999). Valstybės žinios, 60-1945.
[4] Lietuvos Respublikos valstybės informacinių išteklių įstatymas (2011). Valstybės žinios, 163-7739.
[5] Lietuvos Respublikos kibernetinio saugumo įstatymas (2014). TAR, 20553.

1. DUOMENŲ APSAUGOS ĮGYVENDINIMAS VIEŠAJAME SEKTORIUJE

Duomenų apsaugos įgyvendinimas šiuolaikiniame pasaulyje tampa vienu iš prioritetų, nes svarbu tiek tinkamai generuoti ir apsaugoti duomenis, tiek duomenų valdytojams įgyvendinti savo teises ir pareigas, nepažeidžiant vieno iš svarbiausių dokumentų, t. y. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento 2016/679 dėl fizinių[6] asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau – Bendrasis duomenų apsaugos reglamentas). Mokslinė ir technologinė pažanga šiuolaikinėje visuomenėje yra labai sparti, dažnai aplenkianti teisėkūrą, todėl viešajame sektoriuje dažnai keliamas klausimas, kaip teikti ir tvarkyti duomenis, kad nebūtų atsiliekama nuo pažangos ir kartu įgyvendinami teisės aktų keliami reikalavimai.

Tinkamas asmens duomenų apsaugos įgyvendinimas pagal Bendrąjį duomenų apsaugos reglamentą tampa nacionalinio bei tarptautinio pobūdžio vertybe, ką parodo priimami teisės aktai, kuriamos programos. Kaip pavyzdys, Lietuvos Respublikos Seimo 2012 m. patvirtinta Valstybės pažangos strategija „Lietuvos pažangos strategija „Lietuva 2030“[7], kuri nubrėžė valstybės viziją ir raidos prioritetus bei jų įgyvendinimo kryptis iki 2030 metų. Pagal šią strategiją vienas iš prioritetų yra skirtas inovatyvaus viešojo sektoriaus temai, išskiriant tris pagrindinius viešojo sektoriaus bruožus – atvirumas (atviras ir skatinantis dalyvauti valdymas), atsakomybė (rezultatyvus, atitinkantis visuomenės poreikius ir užtikrinantis geros kokybės paslaugas valdymas) ir kūrybingumas (kompetentinga ir priimanti kryptingus strateginius sprendimus valdžia). Būtent su šiais bruožais ir ypač kūrybiškumu sietina inovatyvaus viešojo sektoriaus tema.

1.1. Asmens duomenų samprata

Analizuojant asmens duomenų klausimus viešajame sektoriuje, pirmiausia reikia išanalizuoti pačią viešojo sektoriaus sampratą, kuri aptariama tiek mokslinėje literatūroje, tiek teisės aktuose[8]. Viešojo administravimo subjektų sistemą sudaro valstybinio administravimo subjektai, regioninio administravimo subjektai ir savivaldybių administravimo subjektai. Lietuvos Respublikos viešojo administravimo įstatyme (toliau – Viešojo administravimo įstatymas)

[6] Pastebėtina, kad Bendrasis duomenų apsaugos reglamentas neįtvirtina fizinio asmens sąvokos. Visuotinės žmogaus teisių deklaracijos 6 straipsnyje įtvirtinta bendro pobūdžio nuostata, tačiau ji neapibrėžia fizinio asmens sąvokos. Fizinio asmens sąvokos įstatymų leidėjas neįtvirtino ir nacionalinėje teisėje. Lietuvos Respublikos civiliniame kodekse (toliau – Civilinis kodeksas) yra vartojama fizinio asmens sąvoka, tačiau jos apibrėžimas taip pat nėra įtvirtintas.

[7] Inovatyvus viešasis sektorius – misija įmanoma Vilnius, 2015.

[8] 2000 m. gruodžio 7 d. Nicoje pasirašyta Europos Sąjungos pagrindinių teisių chartija, kurios 41 straipsnis apibrėžia gero administravimo sąlygas. Tai reiškia, kad kiekvienam asmeniui garantuojama, kad visos institucijos ir organai visus reikalus tvarkytų nešališkai, sąžiningai ir per tam tikrą laiką. Šios chartijos 41 straipsnyje įtvirtinti gero administravimo principai (Europos Sąjungos 2000 m. gruodžio 7 d. pagrindinių teisių chartija Nr. 2016/C 202/02, p. 391-405.).

pateikiama tokia viešojo administravimo sąvoka – „tai teisės aktais reglamentuota viešojo administravimo subjektų veikla, skirta teisės aktams įgyvendinti: administracinis reglamentavimas, administracinių sprendimų priėmimas, teisės aktų ir administracinių sprendimų įgyvendinimo priežiūra, administracinių paslaugų teikimas, viešųjų paslaugų teikimo administravimas“[9]. V. Giedraitytė (2016) daktaro disertacijoje remiasi tokia viešojo sektoriaus samprata – tai iš valstybių ir savivaldybių biudžetų pilnai ar iš dalies išlaikomos įstaigos ar institucijos, kurių veikla yra vieša, o viešasis sektorius teikia viešąsias gėrybes, kurios turi būti prieinamos visiems piliečiams ir kitiems asmenims[10]. Kartu autorių analizuojamas viešojo sektoriaus inovacijų klausimas, t. y., kad viešasis sektorius turi modernėti ir keistis. Kartu sulig atsiradusia inovacijų sąvoka viešajame sektoriuje, atsiranda ir naujojo viešojo valdymo viešajame sektoriuje sąvoka – „tai viešojo valdymo modelis, pabrėžiantis mišrių (viešojo, verslo) organizacijų ir tinklinių struktūrų formavimą, bendruomeniškumo plėtojimą, pilietinių organizacijų vystymą, palankios erdvės įtraukiant piliečius į sprendimų priėmimą bei jų įgyvendinimą sukūrimą“[11]. J. E. Lane (2000) pažymi, kad šiuolaikinis viešasis administravimas yra ypač sudėtinga išteklių paskirstymo sistema, veikianti nuolat kintančioje aplinkoje, tad valdymas turi itin lanksčiai spręsti sudėtingiausius klausimus[12].

Analizuojant viešojo sektoriaus sampratą, svarbu išnagrinėti ir principus. Viešojo administravimo įstatyme[13] įtvirtinti tokie viešojo administravimo principai, kuriais remiantis kiekviena viešojo administravimo institucija yra saistoma bendrųjų ir konstitucinių teisės principų:

1) atsakomybės už priimtus sprendimus. Tai reiškia, jog viešojo administravimo subjektas, priimdamas sprendimus, turi galvoti apie padarinius ir prisiimti atsakomybę už tai, kokie jie gali būti.

2) draudimo keisti į blogąją pusę (*non reformatio in peius*). Šis *non reformatio in peius* principas yra suprantamas kaip draudimas priimti sprendimą besiskundžiančios šalies nenaudai, išskyrus įstatyme nustatytas šio principo taikymo išimtis, ir pagal administracinių teismų praktiką yra ypatingai aktualus[14].

3) efektyvumo. Šis principas reiškia, kad veikla turi būti proporcinga priimamiems sprendimams, sunaudojamiems ištekliams ir pasiekiamiems rezultatams.

4) įstatymo viršenybės. Visi priimti sprendimai viešajame sektoriuje turi būti pagrįsti teisės aktų reikalavimais.

[9] Lietuvos Respublikos viešojo administravimo įstatymas (1999). Valstybės žinios, 60-1945.
[10] GIEDRAITYTĖ, V. (2016) Viešojo sektoriaus inovacijų proceso trikdžių valdymas Lietuvos savivaldybių administracijose. Daktaro disertacija, socialiniai mokslai, vadyba, p.7.
[11] GIEDRAITYTĖ, V. (2016) Viešojo sektoriaus inovacijų proceso trikdžių valdymas Lietuvos savivaldybių administracijose. Daktaro disertacija, socialiniai mokslai, vadyba, p.8.
[12] LANE, J. E. (2001). Viešasis sektorius: sąvokos, modeliai ir požiūriai. Vilnius: Margi raštai.
[13] Lietuvos Respublikos viešojo administravimo įstatymas (1999). Valstybės žinios, 60-1945.
[14] Lietuvos Respublikos viešojo administravimo įstatymas (1999). Valstybės žinios, 60-1945.

5) išsamumo. Viešajame sektoriuje nemažai gaunama žmonių skundų, prašymų, į kuriuos turi būti atsakyta aiškiai ir išsamiai, argumentuotai, išnagrinėjus visas aplinkybes, turėjusias įtakos konkrečiai situacijai.

6) lygiateisiškumo. Lietuvos Respublikos Konstitucijos 29 straipsnyje įtvirtinta, jog įstatymui, teismui ir kitoms valstybės institucijoms ar pareigūnams visi asmenys lygūs[15]. Taip pat šio principo svarbą akcentavo tiek Lietuvos Respublikos Konstitucinis Teismas, tiek administracinis teismas[16], tiek ir tarptautiniai teismai. Konstitucinis Teismas yra konstatavęs, jog tai demokratijos ir nediskriminacijos[17] principas. Šis principas reiškia, kad viešojo administravimo subjektas, priimdamas administracinius sprendimus, turi atsižvelgti į tai, kad įstatymui visi asmenys lygūs, negali būti jokių privilegijų dėl jų lyties, rasės, tautybės, kalbos, kilmės, socialinės ir turtinės padėties, seksualinės orientacijos, išsilavinimo, religinių ar politinių pažiūrų, veiklos rūšies ir pobūdžio, gyvenamosios vietos ir kitų aplinkybių.

7) naujovių ir atvirumo permainoms. Kadangi viskas kinta, vadinasi, viešojo administravimo subjektas turi ieškoti naujų ir veiksmingų būdų kaip geriau spręsti problemas, iškylančias vykdant viešąjį administravimą, taikyti naujus metodus ir naująją gerąją praktiką.

8) nepiktnaudžiavimo valdžia. Šis principas reiškia, kad viešojo administravimo subjektams draudžiama atlikti viešojo administravimo funkcijas neturint šio įstatymo nustatyta tvarka suteiktų viešojo administravimo įgaliojimų arba priimti administracinius sprendimus siekiant kitų, negu įstatymų ar kitų teisės aktų nustatytų, tikslų.

9) objektyvumo. Šis principas reiškia, kad administracinio sprendimo priėmimas ir kiti oficialūs viešojo administravimo subjekto veiksmai turi būti nešališki ir objektyvūs.

10) proporcingumo. Šis principas reiškia, kad administracinio sprendimo mastas ir jo įgyvendinimo priemonės turi atitikti būtinus ir pagrįstus administravimo tikslus.

11) skaidrumo. Šis principas reiškia, kad viešojo administravimo subjekto veikla turi būti vieša, išskyrus įstatymų nustatytus atvejus.

12) subsidiarumo. Šis principas reiškia, kad viešojo administravimo subjektų sprendimai turi būti priimami ir įgyvendinami žemiausiu efektyvumą galinčiu užtikrinti viešojo administravimo sistemos lygmeniu.

13) vieno langelio. Tai reiškia, kad vienoje darbo vietoje asmuo turi gauti atsakymus į savo klausimus ar pateiktus dokumentus.

[15] Lietuvos Respublikos Konstitucija (1992). Valstybės žinios, 33-1014.
[16] Lietuvos vyriausiojo administracinio teismo 2015 m. gruodžio 15 d. nutartis byloje Nr. A-1544-552/2015.
[17] Diskriminacija paprastai suprantama kaip asmens ar asmenų grupės padėties kitų asmenų atžvilgiu pakeitimas be objektyviai pateisinamo pagrindo.

Vertinant viešojo administravimo principus, matyti, jog daugelis iš jų susiję su asmens duomenų apsauga, t. y. toks principas, kaip „atsakomybė už priimtus sprendimus“ reiškia, kad viešojo administravimo subjektas turi gebėti prisiimti atsakomybę už tai, ar tinkamai vykdo asmens duomenų apsaugą, ar priima tinkamus sprendimus ir apgalvoja jų pasekmes. Įstatymo viršenybės principas, kuris reiškia, kad teikiant asmens duomenis, pirmiausia reikia vadovautis teisės aktų nuostatomis. Naujovių ir atvirumo principas susijęs su duomenų atvėrimu, kuris atsirado po Bendrojo duomenų apsaugos reglamento įsigaliojimo.

Kadangi viešojo sektoriaus teikiamų paslaugų apimtis yra didelė, viešojo sektoriaus institucijos tvarko didelį kiekį asmens duomenų. Siekiant išnagrinėti asmens duomenų apsaugos užtikrinimą ir kylančias problemas viešajame sektoriuje, visų pirma, svarbu apibrėžti, kas laikytina asmens duomenimis.

Asmens duomenų sąvoka yra pamatinė kategorija privatumo apsaugos diskurse, aktyvinant sudėtingo asmens duomenų apsaugos teisinio režimo mechanizmą. Jeigu informacija nurodo ar gali nurodyti konkretų asmenį, situacija *prima facie* tampa asmens duomenų apsaugos taisyklių taikiniu[18]. Ji apibrėžiama tiek nacionaliniuose bei tarptautiniuose teisės aktuose, tiek ir mokslinėje literatūroje.

Bendrajame duomenų apsaugos reglamente nurodoma, kad asmens duomenys tai „bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (duomenų subjektas); fizinis asmuo, kurio tapatybę galima nustatyti, yra asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti, visų pirma, pagal identifikatorių, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius“ [19].

Asmens duomenų sąvoka taip pat įtvirtinta 1981 m. sausio 28 d. konvencijoje dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu, kurios 2 straipsnis įtvirtinta, jog asmens duomenys – „tai informacija apie nustatytos tapatybės asmenį arba asmenį, kurio tapatybę galima nustatyti”[20].

Nacionaliniu lygmeniu asmens duomenų sąvokos apibrėžimas nėra įtvirtintas, tačiau pastebėtina, kad Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo (toliau – Asmens duomenų teisinės apsaugos įstatymas) redakcijoje, galiojusioje nuo 2017 m. sausio 1 d. iki

[18] Duomenų apsauga pagal BDAR [interaktyvus]. Prieiga per internetą: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_lt.htm

[19] Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) Nr. 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) OL 2016 L 19, p. 1-88.

[20] Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis (1981). Valstybės žinios, 2001, 32-1059.

2018 m. birželio 30 d., buvo įtvirtinta, kad asmens duomenimis laikytina „bet kuri informacija, susijusi su fiziniu asmeniu – duomenų subjektu, kurio tapatybė yra žinoma arba gali būti tiesiogiai ar netiesiogiai nustatyta pasinaudojant tokiais duomenimis kaip asmens kodas, vienas arba keli asmeniui būdingi fizinio, fiziologinio, psichologinio, ekonominio, kultūrinio ar socialinio pobūdžio požymiai“[21]. Iš esmės šis asmens duomenų sąvokos apibrėžimas, kuris buvo įtvirtintas Asmens duomenų teisinės apsaugos įstatymo redakcijoje, galiojusioje nuo 2017 m. sausio 1 d. iki 2018 m. birželio 30 d., nežymiai skyrėsi nuo šiuo metu galiojančio Bendrojo duomenų apsaugos reglamento 4 straipsnyje įtvirtintos asmens duomenų sąvokos. Tačiau priešingai nei Bendrajame duomenų apsaugos reglamente, Asmens duomenų teisinės apsaugos įstatymo redakcijoje, galiojusioje nuo 2017 m. sausio 1 d. iki 2018 m. birželio 30 d., nebuvo įvirtinta fizinio asmens sąvoka. Šiuo metu galiojančioje Asmens duomenų teisinės apsaugos įstatymo redakcijoje asmens duomenų sąvoka nėra įtvirtinta, tačiau įstatymo 2 straipsnio 3 dalyje numatyta, jog įstatyme neapibrėžtos, tačiau vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Bendrajame duomenų apsaugos reglamente[22]. Vertinant įstatymo leidėjo ketinimus įstatyme neapibrėžti asmens duomenų sąvokos, manytina, jog iš įstatymo išbraukus asmens duomenų sąvokos apibrėžimą, jį pakeičiant bendra nuostata, įtvirtinančia, jog įstatyme neapibrėžtos, tačiau vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Bendrajame duomenų apsaugos reglamente, siekta įstatymo normas suderinti su Bendruoju duomenų apsaugos reglamentu ir išvengti galimo normų tarpusavio prieštaravimo.

Asmens duomenų sąvokos turinį išaiškino Europos Sąjungos 29 straipsnio duomenų apsaugos darbo grupė, kuri siekdama suformuluoti bendrąją asmens duomenų sąvokos sampratą, 2007 m. birželio 20 d. priėmė Nuomonę Nr. 4/2007 dėl asmens duomenų sąvokos (toliau – Nuomonė dėl asmens duomenų sąvokos)[23]. Svarbu pastebėti, kad Europos Sąjungos 29 straipsnio duomenų apsaugos darbo grupė asmens duomenų sampratą aiškino 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvos 95/46/EB kontekste[24]. Tačiau, atsižvelgiant į tai, kad 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvoje 95/46/EB įtvirtinta asmens duomenų sąvoka iš esmės atitinka šiuo metu galiojančiame Bendrajame duomenų apsaugos reglamente įtvirtintą asmens duomenų sąvoką, šiame darbe asmens duomenų sampratos aiškinimui bus pasitelkiama Nuomonė dėl asmens duomenų sąvokos.

[21] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (2018). TAR, 11733.
[22] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (2018). TAR, 11733.
[23] Europos Sąjungos 29 straipsnio duomenų apsaugos darbo grupės 2007 m. birželio 20 d. Nuomonė Nr. 4/2007 dėl asmens duomenų sąvokos Nr. WP 136, p. 3 [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_lt.pdf [žiūrėta 2020 m. rugsėjo 21 d.].
[24] Europos Parlamento ir Tarybos 1995 m. spalio 24 d. direktyva Nr. 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. OL 2004, p. 355-374.

Europos Sąjungos 29 straipsnio duomenų apsaugos darbo grupė, įvertinusi 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvoje 95/46/EB įtvirtintą asmens duomenų apibrėžtį nurodė, jog asmens duomenų sąvokos turinį sudaro keturi elementai: „bet kuri informacija“, „informacija, susijusi su asmeniu“, „asmuo, kurio tapatybė yra nustatyta arba gali būti nustatyta“, „fizinis asmuo“. Remiantis Europos Sąjungos 29 straipsnio duomenų apsaugos darbo grupės apibrėžtais asmens duomenų sąvokos turinio elementais bei įvertinus Bendrajame duomenų apsaugos reglamente įtvirtintos asmens duomenų sąvokos turinį, matyti, jog asmens duomenys – tai bet kuri informacija, susijusi su fiziniu asmeniu, kurio tapatybė gali būti nustatyta.

Apibendrinant reikėtų pastebėti, kad viešasis sektorius, kuris vykdo viešojo pobūdžio funkcijas, turi nenukrypti nuo teisės aktų reikalavimų ir suspėti su pažanga. Šiuolaikinis technologijų amžius viešajam sektoriui prideda naują sąvoka „inovatyvumas“ ir remiasi tokiais principais – atsakomybės už priimtus sprendimus, draudimo keisti į blogąją pusę, efektyvumo, įstatymo viršenybės, išsamumo, lygiateisiškumo, naujovių ir atvirumo permainoms, nepiktnaudžiavimo valdžia, objektyvumo, proporcingumo, skaidrumo, subsidiarumo, vieno langelio. Šie principai yra labai svarbūs asmens duomenų apsaugai, nes jais vadovaujantis įgyvendinama jų saugojimo politika, nepažeidžiant teisės aktų reikalavimų.

1.2. Duomenų tvarkymo principai viešajame sektoriuje

Bendrojo duomenų apsaugos reglamento 5 straipsnyje įtvirtinti pagrindiniai asmens duomenų tvarkymo principai: teisėtumo, sąžiningumo ir skaidrumo principas, tikslo apribojimo principas, duomenų kiekio mažinimo principas, tikslumo principas, saugojimo trukmės apribojimo principas, vientisumo ir konfidencialumo principas[25]. Iš esmės panašūs asmens duomenų tvarkymo principai yra įtvirtinti ir Europos Tarybos 1981 m. sausio 28 d. konvencijoje Nr. 108 dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (toliau – Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu): asmens duomenų tvarkymo sąžiningumo ir teisėtumo principas, tikslo teisėtumo principas, duomenų tvarkymo saugumo principas, asmens teisių ir garantijų principas, duomenų valdytojų atsakomybės principas ir ypatingų asmens duomenų apsaugos principas[26]. Viešasis sektorius privalo užtikrinti, kad nebūtų pažeisti šie duomenų tvarkymo principai, kartu nepažeidžiant teisės aktų reikalavimų būtų tenkinamas viešasis interesas.

[25] Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) Nr. 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) OL 2016 L 19, p. 1-88.

[26] Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis (1981). Valstybės žinios, 2001, 32-1059.

1.2.1. Teisėtumo, sąžiningumo ir skaidrumo principas

Duomenų tvarkymo teisėtumo, sąžiningumo ir skaidrumo principas yra svarbiausias ir bendriausias duomenų tvarkymo principas. Iš esmės visas asmens duomenų apsaugos teisės reguliavimas detalizuoja šį principą, įtvirtindamas konkrečius teisėto, sąžiningo ir skaidraus duomenų tvarkymo aspektus[27]. Duomenų tvarkymo teisėtumo, sąžiningumo ir skaidrumo principo svarbą pagrindžia teisingumo principo reikšmė. Teisingumo principas laikomas bendruoju, pamatiniu principu, kuriuo yra grindžiama visa teisinė sistema. Teisingumo imperatyvas teisiniame reguliavime, teismų jurisprudencijoje ir teisės doktrinoje siejamas su moralinėmis nuostatomis. Atitikimas šiam teisės principui konstatuojamas, vertinant atitiktį kitiems moraliniams kriterijams – gėriui, lygybei, žmoniškumui, sąžiningumui ir kitiems pamatiniams principams[28]. Teisėtumo principas duomenų tvarkymo srityje reikalauja, jog duomenys būtų tvarkomi laikantis teisės aktuose nustatytų reikalavimų. Tam, kad asmens duomenų tvarkymas būtų pripažintas teisėtu, būtina gauti asmens, kurio duomenys yra tvarkomi, sutikimą arba remtis kitu teisiniu pagrindu, suteikiančiu teisę tvarkyti asmens duomenis. Pažymėtina, kad reikalavimas turėti teisinį pagrindą tvarkyti duomenis yra svarbus duomenų tvarkymo teisėtumo požiūriu, tačiau būtina pastebėti, kad jis yra tik viena iš daugelio duomenų apsaugos vykdymo sąlygų[29]. Teisingumo principo užtikrinimo svarbą duomenų tvarkymo procese patvirtina Bendrojo duomenų apsaugos reglamento 13 straipsnio nuostata, kuri įtvirtina duomenų valdytojo pareigą pateikti duomenų subjektui išsamią informaciją apie duomenų subjekto renkamus duomenis. Taigi, duomenų valdytojas privalo pateikti duomenų subjektui tiek informacijos apie tvarkomus jo asmens duomenis, kad būtų užtikrintas teisingas asmens duomenų tvarkymas nepažeidžiant duomenų subjekto teisių. Atsižvelgiant į tai, kad teisingumo principas duomenų tvarkymo procese apibrėžia duomenų valdytojo bei duomenų tvarkytojo teisių ir pareigų ribas duomenų subjekto teisių atžvilgiu, darytina išvada, kad teisingumo principas duomenų tvarkymo procese iš esmės veikia kaip pusiausvyros mechanizmas tarp duomenų subjekto ir duomenų valdytojo bei duomenų tvarkytojo interesų. Analizuojant viešojo sektoriaus veiklą mūsų valstybėje ir nagrinėjant priimtus teisės aktus, reikėtų įvertinti šio principo svarbą. Kaip pavyzdys valstybės įmonė Registrų centras, kuris savo veikloje vadovaujasi Asmens duomenų tvarkymo

[27] ZALESKIS, J. (2019). Europos Sąjungos bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Vilnius: Registrų centras, p. 113.

[28] VAIČAITIS, V. (2009). Teisingumo samprata ir Lietuvos Respublikos Konstitucinis Teismas. Konstitucinė jurisprudencija, p. 206-221 [interaktyvus] Prieiga per internetą: https://www.tf.vu.lt/wp-content/uploads/2016/12/V.-Vaičaitis.-Teisingumo-samprata-ir-Lietuvos-Respublikos-Konstitucinis-Teismas.pdf [žiūrėta 2020 m. rugsėjo 25 d.].

[29] ZALESKIS, J. (2019). Europos Sąjungos bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Vilnius: Registrų centras, 114.

valstybės įmonėje Registrų centre tvarkos aprašu, kuriame akcentuojamas asmens duomenų tvarkymo teisėtumas, kokiems subjektams ir kokiais tikslais minėti duomenys gali būti atskleisti[30]. Kitas bendrasis teisės principas, kuriam turi paklusti asmens duomenų apsaugos teisės nuostatomis reguliuojamų visuomeninių santykių dalyviai – tai sąžiningumo principas, kuris reiškia bendro pobūdžio duomenų valdytojų ir duomenų tvarkytojų pareigą sąžiningai tvarkyti duomenis. Civilinio kodekso 1.5 straipsnis įtvirtina bendrąją pareigą civilinių teisinių santykių subjektams, įgyvendinant savo teises, veikti pagal sąžiningumo reikalavimus. Tai yra bendro pobūdžio nuostata, įpareigojanti laikytis sąžiningumo principo, tačiau šio principo turinys Civiliniame kodekse nėra atskleidžiamas, todėl šio principo turinio aiškinimas paliktas teisės doktrinai ir teismų praktikai. Teisės doktrinoje pripažįstama, kad sąžiningumas yra vertybinis teisinių santykių subjekto elgesio matas, kuris yra nustatomas pagal objektyvų ir subjektyvų kriterijus[31].

Teismų praktikoje sąžiningumo principas apibrėžiamas iš esmės taip pat. Be kita ko, Lietuvos Aukščiausiasis Teismas civilinėje byloje Nr. 3K-3-286/2014 pažymėjo, kad vadovaujantis objektyviuoju kriterijumi, sąžiningumas suprantamas kaip elgesys, kuris atitinka protingumo ir teisingumo principų turinį, t. y. rūpestingas, apdairus ir atidus elgesys. Vadovaujantis subjektyviuoju kriterijumi, sąžiningumas nusako asmens vidinę būseną konkrečioje situacijoje, kurią sąlygoja asmenį individualizuojančios savybės, pavyzdžiui, asmens amžius, išsilavinimas, praktiniai įgūdžiai ir pan. Pažymėtina, jog siekiant nustatyti, ar asmuo yra sąžiningas, būtina taikyti tiek objektyvųjį, tiek subjektyvųjį kriterijų[32]. Sąžiningumo principas duomenų tvarkymo procese lemia tai, jog duomenų tvarkytojas, siekdamas duomenų tvarkymo tikslų, privalo atsižvelgti į duomenų subjekto interesus ir jo pagrįstus lūkesčius. Tai reiškia, jog duomenų valdytojo elgesys, tvarkant asmens duomenis, bus laikytinas atitinkančiu sąžiningumo standartą, jei tvarkant asmens duomenis bus atsižvelgiama į duomenų subjekto interesus ir jo teisėtus lūkesčius, priešingu atveju, bus konstatuojamas duomenų valdytojo piktnaudžiavimo faktas, nes jo elgesys bus laikomas neatitinkančiu sąžiningumo standarto. Nors piktnaudžiavimo sąvokos įstatymų leidėjas neįtvirtino, tačiau Civilinio kodekso 1.137 straipsnio 3 dalyje įtvirtintas draudimas piktnaudžiauti savo teise, t. y. „draudžiama įgyvendinti civilines teises tokiu būdu ir priemonėmis, kurios be teisinio pagrindo pažeistų ar varžytų kitų asmenų teises ar įstatymų saugomus interesus ar darytų žalos kitiems asmenims arba prieštarautų subjektinės teisės paskirčiai“[33]. Taigi, piktnaudžiavimu laikytinas elgesys, kuris yra priešingas sąžiningam elgesiui. Pastebėtina, kad prielaidų piktnaudžiauti asmens

[30] Valstybės įmonės Registrų centro 2018 m. gegužės 24 d. direktoriaus įsakymas Nr. v-171 „Dėl asmens duomenų tvarkymo valstybės įmonėje Registrų centre tvarkos aprašo patvirtinimo“ [interaktyvus]. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/ TAD/1804741065d311e8b7d2b2d2ca774092/asr [žiūrėta 2020 m. lapkričio 10 d.].
[31] MIKELĖNAS, V. et al. (2001). Lietuvos Respublikos civilinio kodekso komentaras. Pirmoji knyga. Vilnius: Justitia, p. 77.
[32] Lietuvos Aukščiausiojo Teismo 2014 m. gegužės 22 d. nutartis civilinėje byloje Nr. 3K-3-286/2014.
[33] Lietuvos Respublikos civilinis kodeksas (2000). Valstybės žinios, 74-2262.

duomenų teisinės apsaugos srityje yra pakankamai daug, nes duomenų valdytoju laikytinas subjektas, kurio žinioje yra asmens duomenys ir kuris vienintelis turi išsamią informaciją apie duomenų subjekto asmens duomenų tvarkymą. Būtent nuo duomenų valdytojo sąžiningumo iš esmės priklauso, ar asmens duomenys bus tvarkomi, laikantis asmens duomenų teisinės apsaugos reikalavimų. Pažymėtina, kad duomenų valdytojas privalo vadovautis sąžiningumo principu, atlikdamas bet kurį su asmens duomenimis susijusį veiksmą. Tai reiškia, kad sąžiningumo imperatyvo laikymasis duomenų valdytojui privalomas tiek asmens duomenų rinkimo, tiek tvarkymo, tiek saugojimo procese[34].

Dar vienas bendrasis teisės principas, kuriam turi paklusti asmens duomenų apsaugos teisės nuostatomis reguliuojamų visuomeninių santykių dalyviai – duomenų tvarkymo skaidrumo principas. Atkreiptinas dėmesys, kad skaidrumas paprastai laikomas vienu iš viešojo sektoriaus subjektų veiklos standartų. Konstitucinis Teismas yra pažymėjęs, kad skaidrumas, kaip viešosios valdžios institucijų ir pareigūnų veiklos principas, suponuoja informacijos sklaidą ir komunikavimą, atvirumą ir viešumą (tiek, kiek tai nekenkia kitoms teisės saugomoms vertybėms), atskaitingumą atitinkamai bendruomenei ir sprendimus priimančių pareigūnų atsakomybę už tuos sprendimus. Skaidrumas sąlygoja ir reikalavimą, kad priimami sprendimai būtų pagrįsti, aiškūs, kad, iškilus reikalui, jie būtų racionaliai motyvuoti, o asmenys turėtų galimybę priimtus sprendimus ginčyti nustatyta tvarka[35].

Europos Sąjungos 29 straipsnio darbo grupė 2017 m. lapkričio 29 d. patvirtino gaires dėl skaidrumo pagal Bendrąjį duomenų apsaugos reglamentą, kuriose pasisakydama dėl skaidrumo principo reikšmės, pažymėjo, jog „fiziniams asmenims turėtų būti aišku, ar yra su jais susiję asmens duomenys renkami, naudojami, tvarkomi ar bus tvarkomi. Skaidrumo principas reikalauja, kad bet kokia informacija ir komunikacija, susijusi su tų asmens duomenų tvarkymu, būtų lengvai prieinama, lengvai suprantama ir vartojama aiškia kalba. Šis principas lemia informacijos perteikimą duomenų subjektams apie duomenų valdytojo tapatybę, tvarkymo tikslus ir papildomą informaciją, kuri būtina siekiant užtikrinti sąžiningą ir skaidrų duomenų tvarkymą“[36].

Taigi, skaidrumo principas siejamas su informacijos prieinamumu ir tuo pačiu nustato reikalavimą užtikrinti galimybę asmenims gauti informaciją apie tam tikrą veiklą ar procesą, kuris įgyvendinamas jo asmens duomenų atžvilgiu. Skirtingai nei viešumas, kuris užtikrinamas išimtinai

[34] PETRAITYTĖ, I. (2013). Asmens duomenų teisinės apsaugos principai. Daktaro disertacija, socialiniai mokslai, teisė, Vilniaus universitetas. Vilnius: Vilniaus universiteto leidykla [interaktyvus]. Prieiga per internetą: http://epublications.vu.lt/object/elaba:1823635/1823635.pdf [žiūrėta 2020 m. rugsėjo 20 d.].

[35] Lietuvos Respublikos Konstitucinio Teismo 2008 m. sausio 22 d. nutarimas. Valstybės žinios, 10-35.

[36] Europos Sąjungos 29 straipsnio darbo grupės 2017 m. lapkričio 29 d. Gairės dėl skaidrumo pagal reglamentą (ES) 2016/679 Nr. WP260, p. 6 [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id= 622227 [žiūrėta 2020 m. rugsėjo 26 d.].

tik informaciją turinčio subjekto iniciatyva bei pastangomis ir adresuojamas neapibrėžtam asmenų ratui, skaidrumas garantuoja prieigą prie informacijos tik tiems asmenims, kurie turi interesą šią informaciją gauti. Skaidrumo principas reikalauja, kad veikla ar procesas būtų aiškus ir suprantamas tiems asmenims, kurių asmens duomenys dalyvauja asmens duomenų tvarkymo procese[37]. Pastebėtina, kad duomenų tvarkymo skaidrumo principas apima kelis aspektus:

- duomenų tvarkymas turi būti skaidrus duomenų subjektų atžvilgiu;

- duomenų tvarkymas turi būti skaidrus priežiūros institucijos, kuri atlieka duomenų valdytojo priežiūrą, atžvilgiu.

Duomenų tvarkymo skaidrumas duomenų subjektų atžvilgiu susijęs su pareiga informuoti duomenų subjektą apie duomenų valdytojo tapatybę, duomenų tvarkymo tikslus ir pranešti kitą informaciją, kuri būtina sąžiningo ir skaidraus duomenų tvarkymo užtikrinimui. Taip pat duomenų tvarkymo skaidrumą duomenų subjektų atžvilgiu užtikrina duomenų subjektų teisė bet kuriuo metu iš duomenų valdytojo gauti atsakymą, ar su jais susiję asmens duomenys yra tvarkomi, ir teisę su jais susipažinti. Tuo tarpu duomenų tvarkymo skaidrumą priežiūros institucijų atžvilgiu lemia bendro pobūdžio pareiga gavus prašymą bendradarbiauti su priežiūros institucija. Duomenų valdytojas, gavęs priežiūros institucijos prašymą, turi institucijai atskleisti duomenų tvarkymo veiklos įrašus, kuriuose aprašomas duomenų tvarkymas[38].

Taigi, teisingumas, protingumas, sąžiningumas – vieni iš asmens duomenų teisinės apsaugos srityje veikiančių teisinių imperatyvų, atsispindinčių asmens duomenų tvarkymo teisiniame reguliavime ir nustatančių duomenų valdytojo veiklą, tvarkant asmens duomenis.

1.2.2. Duomenų tvarkymo tikslo apribojimo principas

Duomenų tvarkymo tikslo apribojimo principo turinys yra apibrėžtas Bendrojo duomenų apsaugos reglamento 5 straipsnyje, kuris įtvirtina, jog asmens duomenys turi būti renkami nustatytais, aiškiai apibrėžtais bei teisėtais tikslais ir toliau netvarkomi su tais tikslais nesuderinamu būdu[39]. Ši Bendrojo duomenų apsaugos reglamento nuostata atskleidžia, jog duomenų tvarkymo apribojimo principas susideda iš trijų elementų: pirma, duomenų tvarkymo tikslai turi būti nustatyti iš anksto, antra, tvarkymo tikslai turi būti aiškiai apibrėžti, trečia, tvarkymo tikslai turi būti teisėti.

---

[37] PETRAITYTĖ, I. (2013). Asmens duomenų teisinės apsaugos principai. Daktaro disertacija, socialiniai mokslai, teisė, Vilniaus universitetas. Vilnius: Vilniaus universiteto leidykla [interaktyvus]. Prieiga per internetą: http://epublications.vu.lt/object/elaba:1823635/1823635.pdf. [žiūrėta 2020 m. rugsėjo 20 d.], p. 132

[38] ZALESKIS, J. (2019). Europos Sąjungos bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Vilnius: Registrų centras, p. 117.

[39] Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) Nr. 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) OL 2016 L 19, p. 1-88.

Laikoma, jog duomenų tvarkymo tikslai yra nustatyti tada, kai jau galima įgyvendinti kitus asmens duomenų apsaugos teisės reikalavimus ir suprasti duomenų tvarkymo operacijų apimtį. Bet koks duomenų tvarkymas gali prasidėti, tik tada, kai yra nustatomas duomenų tvarkymo tikslas. Duomenų tvarkymo tikslai turi būti pakankamai detalūs, kad galima būtų nustatyti, kokį duomenų tvarkymą nustatytas tikslas apima, o kokio neapima. Be to, tikslas turi būti apibrėžtas kaip įmanoma konkrečiau, nes neaiškus, abstraktus, plačiau neaiškintas duomenų tvarkymo tikslas neatitinka konkretumo kriterijaus. Duomenų tvarkymo tikslo konkretumas turi būti įvertintas kiekvienu konkrečiu atveju, atsižvelgiant į faktines aplinkybes[40]. Viešasis subjektas valstybės įmonė Registrų centras, teikdamas fiziniams ir juridiniams asmenims įvairaus pobūdžio duomenis – gyventojų, adresų, nekilnojamojo turto, hipotekos, testamentų, sudaro sutartis. Šiuo atveju Registrų centras yra *duomenų valdytojas*, į kurį kreipiamasi dėl tam tikrų duomenų pateikimo, vadovaujantis teisės aktais. Duomenų tvarkymas gali būti pagrįstas bent viena teisėta asmens duomenų tvarkymo sąlyga, numatyta Bendrojo duomenų apsaugos reglamento 6 ir (ar) 9 straipsnyje, o tuo atveju, jei nėra nė vienos Bendrojo duomenų apsaugos reglamente nurodytos teisėto asmens duomenų tvarkymo sąlygos ir teisėto asmens duomenų tvarkymo tikslo, asmens duomenys negali būti tvarkomi.

Analizuojant teisės aktus ir valstybės įmonės Registrų centro puslapyje patalpintas duomenų teikimo sutartis, matyti, kad duomenys teikiami tik laikantis tam tikrų ypatumų:

- perduodant duomenis, turi būti įtvirtintas **konkretus tikslas**. Pastebėtina, kad asmens duomenų teikimo tikslas turi būti *pakankamai išsamus*, kad būtų galima nustatyti, kokios rūšies tvarkymą jis apima ir įvertinti, ar konkretus tikslas neprieštarauja teisės aktų reikalavimams[41]. Duomenų tvarkytojas, analizuojamu atveju, valstybės įmonė Registrų centras, turi kritiškai vertinti gautą prašymą, jame nurodyto tikslo konkretumą, aiškumą ir, kai taikoma, suderinamumą su tikslo apribojimo principo reikalavimais. Gavus prašymą, būtina įvertinti, ar toks duomenų teikimas ir teisėtumas yra neatsiejamai susijęs su Bendrajame duomenų apsaugos reglamente įtvirtintomis *teisėto tvarkymo sąlygomis*.
- **duomenų gavėjo tinkamumas**. Tai reiškia, jog prašymą gavęs duomenų valdytojas (tvarkytojas) turi įvertinti, ar asmens duomenis prašantis pateikti asmuo, turi teisę tokią informaciją gauti, ar teisės aktai numato galimybę gauti tokius duomenis. Taip pat ar asmeniui, norinčiam gauti duomenis, teisės aktai numato tokią galimybę.

[40] ZALESKIS, J. (2019). Europos Sąjungos bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Vilnius: Registrų centras, p. 118.

[41] 29 straipsnio duomenų apsaugos darbo grupės, įkurtos 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvos 95/46 EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo pagrindu (toliau – Darbo grupė), 2013 m. balandžio 2 d. nuomonė Nr. 03/2013 dėl tikslo ribojimo, kuri pasiekiama šia nuoroda: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (neoficialus vertimas į lietuvių kalba pasiekiamas Inspekcijos interneto svetainės skiltyje „Rekomendacijos, gairės ir kt.).

- **proporcinga asmens duomenų apimtis.** Duomenų valdytojas kiekvienu atskiru atveju turi vertinti, *ar asmens duomenų teikimas yra būtinas tikslui, dėl kurio pateiktas prašymas, pasiekti* ir, jei taip, kokia apimtimi. Tais atvejais, kai prašoma duomenų apimtis kelia abejonių, duomenų tvarkytojas turi kreiptis į prašymą pateikusį asmenį, kuris padėtų įsitikinti, ar asmens duomenų teikimas nepažeis teisės aktų reikalavimų.

Sutartyse įtvirtintos tokios nuostatos, kaip „*gautus duomenis tvarkyti tik Sutarties 5 punkte numatytu duomenų naudojimo tikslu ir tik esant bent vienai Reglamento 6 straipsnio 1 dalyje nustatytai asmens duomenų tvarkymo sąlygai, nurodytai Sutarties 4.1 papunktyje, laikantis Reglamento 5 straipsnyje nustatytų su asmens duomenų tvarkymu susijusių principų*“, „*įrodyti prašomų pateikti ir (ar) jau pateiktų duomenų ryšį su duomenų tvarkymo pagrindu*“, „*užtikrinti gautų duomenų apsaugą savo lėšomis ir tinkamomis organizacinėmis bei techninėmis priemonėmis, skirtomis apsaugoti duomenis nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo, kurios užtikrina tokį saugumo lygį, kuris atitiktų gautų duomenų pobūdį ir jų tvarkymo keliamą riziką*“; „*nedelsdamas sunaikinti pagal Sutartį gautus duomenis, kai šie duomenys nebereikalingi jų tvarkymo tikslams*“[42]. Analizuojant tokias sutartis, matyti, kiek dėmesio viešajame sektoriuje yra skiriama duomenų apsaugai, ką turi įsipareigoti duomenis gaunantis subjektas. Taip pat yra įtvirtinta, kas gresia pažeidus duomenų teikimo sutarčių nuostatas, t. y. vienašalis sutarties nutraukimas, jeigu nevykdomos sutarties nuostatos. Aiškiai apibrėžti duomenų tvarkymo tikslai yra tokie, kurie yra atskleisti, paaiškinti ir išreikšti suprantama forma[43]. Duomenų sąsajumo su konkrečiu tikslu svarba yra įtvirtinta ir Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 26 straipsnio 3 dalyje kur nustatyta, kad duomenys, registro informacija, registrui pateikti dokumentai ir (arba) jų kopijos gali būti naudojami tik tokiam tikslui, tokios apimties ir tokiu būdu, kokie buvo nurodyti juos gaunant[44]. Kalbant konkrečiai apie registrus, kaip pavyzdžiui gyventojų registras, duomenys teikiami pagal Lietuvos Respublikos gyventojų registro nuostatų 49 punktą, kuriame nustatyta, kad asmens duomenys teikiami pagal sutartį, kurioje turi būti nurodytas asmens duomenų gavimo tikslas, teikimo ir gavimo teisinis pagrindas, sąlygos, tvarka ir teikiamų asmens duomenų apimtis[45].

---

[42] Pagal Registrų centro ir duomenų gavėjo sudarytą duomenų teikimo sutartį (daugkartinio teikimo atveju). Sutartyje turi būti nurodytas asmens duomenų naudojimo tikslas, teisinis duomenų gavimo pagrindas, prašomų pateikti asmens duomenų apimtis, tvarka ir sąlygos (Valstybės įmonės Registrų centro 2018 m. gegužės 24 d. direktoriaus įsakymas Nr. v-171 „Dėl asmens duomenų tvarkymo valstybės įmonėje Registrų centre tvarkos aprašo patvirtinimo“ [interaktyvus]. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/ TAD/1804741065d311e8b7d2b2d2ca774092/asr).

[43] ZALESKIS, J. (2019). Europos Sąjungos bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Vilnius: Registrų centras, p. 119.

[44] Lietuvos Respublikos valstybės informacinių išteklių įstatymas (2011). Valstybės žinios, 163-7739.

[45] Lietuvos Respublikos Vyriausybės 2014 m. gruodžio 23 d. nutarimas Nr. 1495 „Dėl Lietuvos Respublikos gyventojų registro nuostatų patvirtinimo“ [interaktyvus]. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/478d0920903111e48028e9b85331c55d/asr [žiūrėta 2020 m. lapkričio 10 d.].

Europos Sąjungos 29 darbo grupė 2013 m. balandžio 3 d. pateikė Nuomonę dėl tikslo apribojimo, kurioje pažymėjo, jog asmens duomenys turi būti renkami aiškiais tikslais. Rinkimo tikslai neturi būti nurodyti tik už duomenų rinkimą atsakingų asmenų sąmonėje, jie turi būti aiškiai apibrėžti. Tai reiškia, kad asmens duomenų rinkimo tikslai būti aiškiai atskleisti, paaiškinti ar išreikšti suprantama forma. Svarbiausias šio reikalavimo tikslas yra užtikrinti, kad tikslai nebūtų nurodyti neaiškiai, arba, kad nekiltų neaiškumo dėl jų prasmės ar ketinimo. Svarbu, kad aprašyti tikslai būtų aiškūs, kad vienodai juos suprastų ne tik duomenų valdytojas (įskaitant visus susijusius darbuotojus) ir bet priežiūros institucijos ir atitinkami duomenų subjektai. Reikalavimas nurodyti tikslus „aiškiai“ prisideda prie skaidrumo principo. Tai leidžia nedviprasmiškai nustatyti ribas, kurias duomenų valdytojai sugeba naudoti surinktus asmens duomenis siekiant apsaugoti duomenų subjektus[46]. Šiame kontekste kyla klausimas kokiais būdais ir kam nurodyti tikslai turi būti aiškiai išreikšti? Praktikoje yra nemažai naudojamų būdų, kuriais galima išreikšti duomenų tvarkymo tikslus, pavyzdžiui, tikslams apibūdinti pateiktame pranešime, kurie yra įteikiami duomenų subjektams, pranešimais priežiūros institucijoms arba įstaigos viduje informaciją apie tvarkomų duomenų tikslą pateikiant įstaigos paskirtam duomenų apsaugos pareigūnui. Praktikoje duomenų subjektams, besikreipiantiems į valstybines institucijas, informacija apie jo pateikiamų duomenų tvarkymo tikslą (-us) yra pateikiama keliais būdais: pirma, skelbiant šią informaciją institucijos internetiniame tinklapyje, antra, įtvirtinant asmens duomenų tvarkymo tikslus institucijos vidaus dokumentuose, trečia, duomenų subjektui pateikiant šią informaciją prašymo (skundo, pranešimo) formoje, kurią pildo duomenų subjektas, besikreipiantis į valstybinę instituciją. Iš esmės visos valstybinės institucijos, kurios teikia paslaugas visuomenei ir to pasekoje tvarko besikreipiančių asmenų duomenis, informaciją apie duomenų subjekto duomenų tvarkymo tikslus skelbia internetiniuose tinklalapiuose ir vidaus dokumentuose (tvarkose, aprašuose, įsakymuose), kurie yra viešai skelbiami. Pavyzdžiui, Lietuvos Respublikos ryšių reguliavimo tarnybos (toliau – Ryšių reguliavimo tarnyba) internetiniame tinklalapyje skelbiamo Duomenų subjektų teisių įgyvendinimo Ryšių reguliavimo tarnyboje tvarkos aprašo, patvirtinto Ryšių reguliavimo tarnybos direktoriaus 2018 m. rugpjūčio 7 d. įsakymu Nr. 1V-714 (toliau – Duomenų subjektų teisių įgyvendinimo Ryšių reguliavimo tarnyboje tvarkos aprašas) 8 punkte yra aiškiai apibrėžta kokiais tikslais Ryšių reguliavimo tarnyba tvarko duomenų subjekto duomenis. Ryšių reguliavimo tarnyba duomenų subjektų asmens duomenis tvarko skundų ir prašymų nagrinėjimo tikslais, personalo administravimo tikslais, pretendentų į Ryšių reguliavimo tarnybos siūlomas pareigas administravimo tikslais, buhalterinės apskaitos tikslais, tapatybės nustatymo, apskaitos, ataskaitų formavimo tikslais,

[46] Europos Sąjungos 29 darbo grupės 2013 m. balandžio 3 d. Nuomonė dėl tikslo apribojimo Nr. WP203 [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files /201 3/ wp203en.pdf [žiūrėta 2020 m. rugsėjo 26 d.].

tiesioginės rinkodaros tikslu, aptarnavimo telefonu kokybės kontrolės tikslu, valdomo turto apsaugos tikslu, siekiant įsitikinti, kad asmuo turi praėjimo į Ryšių reguliavimo tarnybos patalpas teisę[47]. Lietuvos metrologijos inspekcijos (toliau – Metrologijos inspekcija) internetiniame tinklalapyje skiltyje „asmens duomenų apsauga“ skelbiami konkretūs ir aiškūs duomenų subjektų duomenų tvarkymo tikslai. Metrologijos inspekcijoje asmens duomenys tvarkomi siekiant tinkamai atlikti teisinę metrologinę priežiūrą ir kitas Metrologijos inspekcijai pavestas funkcijas, siekiant įdarbinti kandidatus, pretenduojančius dirbti Metrologijos inspekcijoje, siekiat tinkamai administruoti personalą ir siekiant sudaryti ir tinkamai įvykdyti sutartis su prekių ar paslaugų tiekėjais[48]. Lietuvos Respublikos sveikatos apsaugos ministerijos (toliau – Sveikatos apsaugos ministerija) internetinio tinklalapio skiltyje „asmens duomenų apsauga“ skelbiama, jog Sveikatos apsaugos ministerija tvarko pretendentų, darbuotojų, pacientų, asmens sveikatos priežiūros specialistų ir kitų duomenų subjektų grupių asmens duomenis, įgyvendindama Lietuvos Respublikos sveikatos sistemos įstatymo (toliau – Sveikatos sistemos įstatymas), Lietuvos Respublikos sveikatos priežiūros įstaigų įstatymo (toliau – Sveikatos priežiūros įstaigų įstatymas), Lietuvos Respublikos pacientų teisių ir žalos sveikatai atlyginimo įstatymo (toliau – Pacientų teisių ir žalos sveikatai atlyginimo įstatymas), Lietuvos Respublikos sveikatos draudimo įstatymo (toliau – Sveikatos draudimo įstatymas), Lietuvos Respublikos farmacijos įstatymo (toliau – Farmacijos įstatymas) ir kitų Lietuvos Respublikos ir Europos sąjungos teisės aktų, reglamentuojančių asmens ir visuomenės sveikatos priežiūrą, farmacinę ir kitą veiklą, susijusią su farmacijos produktais, sveikatos draudimą, nuostatas[49]. Pastebėtina, kad pateiktų įstaigų įtvirtinti asmens duomenų tvarkymo tikslai yra tiesiogiai susiję su institucijos vykdomomis funkcijomis. Institucijos kompetencijai priskirtos funkcijos iš esmės apibrėžia institucijos, tvarkančios duomenų subjekto asmens duomenis, duomenų tvarkymo tikslų ribas. Viešojo sektoriaus institucijų funkcijos yra įtvirtintos patvirtintuose institucijos nuostatuose. Pavyzdžiui, Metrologijos inspekcijos nuostatų, patvirtintų Lietuvos Respublikos ekonomikos ir inovacijų ministro 2014 m. rugpjūčio 6 d. įsakymu Nr. 4-527 „Dėl Lietuvos metrologijos inspekcijos nuostatų patvirtinimo“ (toliau – Metrologijos inspekcijos nuostatai), 10 punkte įtvirtinta, jog Metrologijos inspekcija atlieka matavimo priemonių, fasuotų prekių ir matavimo indų gamintojų, pardavėjų ir naudotojų Lietuvos Respublikos metrologijos

[47] Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2018 m. rugpjūčio 7 d. įsakymas Nr. 1V-714 dėl duomenų subjektų teisių įgyvendinimo Lietuvos Respublikos ryšių reguliavimo tarnyboje tvarkos aprašo patvirtinimo [interaktyvus]. Prieiga per internetą: https://www.rrt.lt/wp-content/uploads/2018/08/Duomen%C5%B3-subjekt%C5%B3-teisi%C5%B3-%C4%Afgyvendinimo-Lietuvos-Respublikos-ry%C5%A1i%C5%B3-reguliavimo-tarnyboje-tvarkos-apra%C5%A1as.p df [žiūrėta 2020 m. rugsėjo 27 d.].

[48] Lietuvos metrologijos inspekcija. Asmens duomenų apsauga (tinklalapio internete skiltis) [interaktyvus]. Prieiga per internetą: https://metrinsp.lrv.lt/lt/asmens-duomenu-apsauga [žiūrėta 2020 m. rugsėjo 26 d.].

[49] Lietuvos Respublikos sveikatos apsaugos ministerija. Asmens duomenų apsauga (tinklalapio internete skiltis) [interaktyvus]. Prieiga per internetą: https://sam.lrv.lt/lt/asmens-duomenu-apsauga/informacija-apie-sveikatos-apsaugos-ministerijoje-tvarkomus-asmens-duomenis [žiūrėta 2020 m. lapkričio 12 d.].

įstatymo ir kitų metrologijos srities teisės aktų reikalavimų laikymosi kontrolę; vykdo matavimo priemonių, fasuotų prekių ir matavimo indų rinkos priežiūrą; atlieka matavimo priemonių būklės ir naudojimo kontrolę; atlieka fasuotų prekių ir matavimo indų kontrolę; atlieka parduodant sveriamų, skaičiuojamų, matuojamų ar dozuojamų prekių kiekio kontrolę; nustato metrologijos srities teisės aktų pažeidimus; tvirtina matavimo priemonių, nepatenkančių į techninių reglamentų taikymo sritį, tipus; išduoda matavimo priemonių tipo patvirtinimo sertifikatus ir kitas funkcijas, įtvirtintas Metrologijos inspekcijos nuostatuose[50]. Atsižvelgiant į Metrologijos inspekcijos kompetencijai priskirtas funkcijas bei įvertinus Metrologijos inspekcijos įtvirtintus duomenų tvarkymo tikslus, matyti, jog Metrologijos inspekcijos įtvirtintų duomenų tvarkymo tikslų ribas apibrėžia būtent Metrologijos inspekcijos vykdomos funkcijos. Taigi, darytina išvada, kad duomenų tvarkymo tikslai tiesiogiai koreliuoja su institucijos vykdomomis funkcijomis. Bendrasis duomenų apsaugos reglamentas duomenų tvarkymo tikslo nustatymą palieka duomenų valdytojų diskrecijai, tačiau tai nesuponuoja duomenų valdytojo absoliučios laisvės, nes kaip minėta, duomenų tvarkymo tikslai turi būti nustatomi leistinose ribose, t. y. remiantis duomenų valdytojo (viešojo sektoriaus institucijos) vykdomomis funkcijomis.

Kitas, viešojo sektoriaus institucijų praktikoje taikomas informacijos apie duomenų tvarkymo tikslą pateikimo būdas – tai informacijos pateikimas prašymo (skundo, pranešimo) formoje, kurią pildo duomenų subjektas, besikreipiantis į valstybinę instituciją. Pavyzdžiui, Valstybinės vartotojų teisių apsaugos tarnybos patvirtintoje vartotojo prašymo formoje yra įtvirtinta nuostata „sutinku, kad mano prašymo nagrinėjimo tikslu būtų tvarkomi mano pateikti duomenys (nepažymėjus, prašymas nebus nagrinėjamas)“[51]. Šiuo atveju informacija apie duomenų subjekto (vartotojo) duomenų tvarkymo tikslą yra išreikšta aiškiai, išryškinta ir neužslėpta. Duomenų subjektas (vartotojas) pildydamas prašymo formą ir pateikęs ją Valstybinei vartotojų teisių apsaugos tarnybai gali aiškiai suprasti, jog jo pateikiami duomenys bus tvarkomi tik jo prašymo nagrinėjimo tikslu.

Atsakant į klausimą kam, t. y. kokiems subjektams nurodyti duomenų tvarkymo tikslai turi būti aiškiai išreikšti, pažymėtina, jog subjektui, kuriam tiesiogiai ši informacija daro įtaką ir yra aktualiausia – tai subjektas, kurio duomenys yra tvarkomi. Žinoma, informacija apie duomenų tvarkymo tikslus yra svarbi ir priežiūros institucijoms, tačiau tiesioginį suinteresuotumą turi pats duomenų subjektas.

[50] Lietuvos Respublikos ekonomikos ir inovacijų ministro 2014 m. rugpjūčio 6 d. įsakymas Nr. 4-527 „Dėl Lietuvos metrologijos inspekcijos nuostatų patvirtinimo“ [interaktyvus. Žiūrėta 2020 m. lapkričio 12 d.]. Prieiga per internetą: <https://www.e-tar.lt/portal/lt/legalAct/ff04dfe01d5611e4b542dec0b12e28b0/asr

[51] Valstybinė vartotojų teisių apsaugos tarnyba. Paslaugos (tinklalapio internete skiltis) [interaktyvus]. Prieiga per internetą: http://www.vvtat.lt/paslaugos/prasymai/vartotojo-prasymo-forma/345 [žiūrėta 2020 m. rugsėjo 26 d.].

Duomenų tvarkymo teisėtumo reikalavimas reiškia atitiktį teisiniam reglamentavimui ir iš įstatymų kylantiems reikalavimams plačiausia prasme. Tai reiškia, kad duomenų tvarkymas turi būti atliekamas atsižvelgiant į duomenų apsaugą reglamentuojančių teisės aktų nuostatas. Bendrojo duomenų apsaugos reglamento preambulės 40 punktas įtvirtina, kad tam, jog duomenų tvarkymas būtų teisėtas, asmens duomenys turėtų būti tvarkomi gavus atitinkamo duomenų subjekto sutikimą arba remiantis kitu teisėtu teisiniu pagrindu, nustatytu Bendrajame duomenų apsaugos reglamente[52]. Iš to darytina išvada, kad duomenų subjekto pateiktų duomenų tvarkymas turi būti suderintas su teisiniu reglamentavimu.

Aptarus duomenų tvarkymo tikslo apribojimo principo elementus, t. y. duomenų tvarkymo tikslo nustatymą, duomenų tvarkymo tikslo aiškų apibrėžimą ir duomenų tvarkymo tikslo teisėtumą, galima laikyti, jog duomenų tvarkymo tikslo nustatymas, duomenų tvarkymo tikslo aiškus apibrėžimas ir duomenų tvarkymo tikslo teisėtumas yra žingsniai, kuriuos privalu nustatyti iki pradedant tvarkyti duomenų subjekto pateiktus duomenis. Tuo tarpu jau pradėjus tvarkyti duomenų subjekto duomenis, būtina užtikrinti, jog surinkus duomenis, jie toliau nebūtų tvarkomi su pirminiais tikslais nesuderinamu būdu. Įprasta, jog tais atvejais, kai duomenų subjektas dalijasi asmens duomenimis su kitais, atsiranda lūkestis dėl tikslų, kuriems duomenys bus naudojami. Tikslinga patenkinti šiuos lūkesčius ir išsaugoti pasitikėjimą ir teisinį tikrumą, todėl tikslo ribojimas yra svarbus duomenų apsaugos pagrindas. Pavyzdžiui, jeigu duomenų subjektas sutiko, jog jo pateiktus duomenis Valstybinė vartotojų teisių apsaugos tarnyba tvarkytų jo prašymo nagrinėjimo tikslu, Valstybinė vartotojų teisių apsaugos tarnyba duomenų subjekto pateiktus duomenis negalės tvarkyti kitu tikslu, nepatenkančiu į duomenų subjekto (vartotojo) prašymo nagrinėjimo ribas.

Pastebėtina, kad nors iš Bendrojo duomenų apsaugos reglamento nuostatų išplaukia duomenų tvarkymo tikslo apribojimo principas, kuris riboja tolimesnį duomenų tvarkymą su pirminiu tikslu (-ais) nesuderinamu (-ais) būdu (-ais), tačiau Bendrajame duomenų apsaugos reglamente nėra įtvirtinta, kas yra laikytina tolesniu duomenų tvarkymu. Autorės nuomone, tolesniu duomenų tvarkymu turėtų būti laikomas bet koks duomenų tvarkymas, pasibaigus apibrėžtam duomenų tvarkymo tikslui. Pavyzdžiui, Lietuvos bankas, tvarko duomenų subjekto (vartotojo) duomenis vartotojų ir finansų rinkos dalyvių ginčų nagrinėjimo ne teismo tvarka tikslu. Tuo atveju, jei neteismine tvarka išnagrinėjęs ginčą, Lietuvos bankas kreipiasi į teismą dėl viešojo intereso gynimo, kurio metu yra tvarkomi duomenų subjekto (vartotojo) pateikti duomenys, autorės nuomone, nors pagrindas tvarkyti duomenų subjekto duomenis pirminiu duomenų tvarkymo tikslu

[52] Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) Nr. 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) OL 2016 L 19, p. 1-88.

yra pasibaigęs, t. y. ginčas tarp vartotojo ir finansų rinkos dalyvio yra išnagrinėtas, tačiau tolesnis duomenų subjekto duomenų tvarkymas viešojo intereso gynimo procese nebus laikomas nesuderinamu duomenų tvarkymu su pirminiu duomenų tvarkymo tikslu. Šią autorės įžvalgą pagrindžia Bendrojo duomenų apsaugos reglamento preambulės 50 punktas, kuris numato, jog asmens duomenų tvarkymas kitais tikslais nei tais, kuriais iš pradžių buvo rinkti asmens duomenys, turėtų būti leidžiamas tik tuomet, kai duomenų tvarkymas suderinamas su tikslais, kuriais iš pradžių buvo rinkti asmens duomenys. Tokiu atveju nereikalaujama atskiro teisinio pagrindo, užtenka to pagrindo, kuriuo remiantis leidžiama rinkti asmens duomenis. Be to, Bendrajame duomenų apsaugos reglamente įtvirtinta, kad tolesnis duomenų tvarkymas archyvavimo tikslais viešojo intereso labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais laikytinas suderinamomis ir teisėtomis duomenų tvarkymo operacijomis. Duomenų valdytojas siekdamas įsitikinti, kad tolesnio duomenų tvarkymo tikslas yra suderinamas su tikslu, kuriuo iš pradžių duomenys buvo rinkti, turi atsižvelgti, į sąsajas tarp tų tikslų ir numatomo tolesnio asmens duomenų tvarkymo tikslų, taip pat į aplinkybes, kuriomis asmens duomenys buvo surinkti. Be to, svarbu atsižvelgti į pagrįstus duomenų subjektų lūkesčius, tvarkomų asmens duomenų pobūdį, pasekmes, kylančias duomenų subjektams dėl numatomo tolesnio duomenų tvarkymo ir tinkamų apsaugos priemonių buvimą duomenų tvarkymo operacijose[53].

Būtina pastebėti, kad duomenų tvarkymo tikslo apribojimo principo taikymo ypatumas viešajame sektoriuje pasižymi tuo, jog tam tikrais atvejais gali būti nukrypstama nuo Bendrajame duomenų apsaugos reglamente įtvirtinto reikalavimo užtikrinti, jog asmens duomenys būtų renkami nustatytais, aiškiai apibrėžtais bei teisėtais tikslais ir toliau netvarkomi su tais tikslais nesuderinamu būdu. Išimtiniu atveju, kai viešojo sektoriaus institucijos gali nukrypti nuo bendrojo reikalavimo įgyvendinti duomenų tvarkymo tikslo apribojimo principo taikymą – tai viešojo intereso labui. Nors viešojo intereso sąvokos įstatymas neįtvirtina, tačiau autorės nuomone, viešuoju interesu turėtų būti laikoma vertybė (gėris), kurios užtikrinimu turi rūpintis viešojo sektoriaus institucijos, priešingu atveju, būtų pažeistos ne vieno, o daugelio žmonių teisės ir teisėti interesai. Būtina pastebėti, kad viešojo intereso siekis gali būti taikomas tiek privataus sektoriaus, tiek viešojo sektoriaus subjektams, tačiau viešojo intereso siekis yra aktualiausias viešojo sektoriaus subjektams, todėl būtent viešojo intereso gynimo siekis, laikytinas duomenų tvarkymo tikslo apribojimo principo taikymo ypatumu, leidžiančiu nukrypti nuo bendrojo reikalavimo užtikrinti, jog asmens duomenys būtų renkami nustatytais, aiškiai apibrėžtais bei teisėtais tikslais ir toliau netvarkomi su tais tikslais nesuderinamu būdu.

[53] Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) Nr. 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) OL 2016 L 19, p. 1-88.

Vertinant viešojo sektoriaus sudaromas sutartis, kurių pagrindu teikiami duomenys, reikėtų pastebėti, jog:

- asmens duomenys turi būti tvarkomi **teisėtai, skaidriai** ir sąžiningai asmens, kurio duomenys tvarkomi, atžvilgiu (teisėtumo, sąžiningumo ir skaidrumo principas);
- tvarkomi tik tie duomenys, kurių reikia tam tikslui pasiekti;
- būtina užtikrinti, kad asmens duomenys būtų **saugomi ne ilgiau nei būtina** tikslams, kuriems jie buvo surinkti;

Įmonė ar organizacija naudodamasi tinkamomis technologijomis turi įdiegti tinkamas **technines ir organizacines apsaugos priemones**, užtikrinančias asmens duomenų saugumą, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo (vientisumo ir konfidencialumo principas). Reikia pastebėti, kad duomenų tvarkymas viešojo administravimo įstaigose turi atitikti tam tikrus ypatumus – konkretų tikslą, duomenų gavėjo tinkamumą ir proporcingą asmens duomenų apimtį. Viešojo administravimo įstaigų sudaromų sutarčių pagrindu teikiami duomenys turi atitikti Bendrojo duomenų apsaugos reglamento 6 straipsnio 1 dalyje nustatytą asmens duomenų tvarkymo sąlygą, laikantis reglamento 5 straipsnyje nustatytų su asmens duomenų tvarkymu susijusių principų.

1.2.3. Duomenų kiekio mažinimo principas

Bendrojo duomenų apsaugos reglamento 5 straipsnio c punktas įtvirtina duomenų kiekio mažinimo principą, kuris numato, jog asmens duomenys turi būti adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie tvarkomi[54]. Pastebėtina, kad duomenų kiekio mažinimo principas yra glaudžiai susijęs su duomenų tvarkymo tikslo apribojimo principu, nes vadovaujantis duomenų kiekio mažinimo principu, reikalaujama užtikrinti tinkamą duomenų tvarkymo tikslų ir duomenų apimties santykį. Tvarkomų duomenų kiekį iš anksto turi apibrėžti duomenų valdytojo įvardintas duomenų tvarkymo tikslas, todėl nenustačius aiškiai apibrėžtų ir teisėtų duomenų tvarkymo tikslų, nėra įmanoma užtikrinti duomenų kiekio mažinimo principo taikymo. Duomenų kiekio mažinimo principas įpareigoja išsiaiškinti, ar konkrečiu atveju apskritai reikia tvarkyti duomenų subjekto duomenis, ir tik konstatavus, kad duomenų tvarkymas yra būtinas, sprendžiamas leistinos tvarkyti asmens duomenų apimties klausimas[55].

[54] Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) Nr. 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) OL 2016 L 19, p. 1-88.

[55] ZALESKIS, J. (2019). Europos Sąjungos bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Vilnius: Registrų centras, p. 121.

Vadovaujantis Bendrajame duomenų apsaugos reglamente įtvirtinta duomenų kiekio mažinimo principo samprata, darytina išvada, kad duomenų kiekio mažinimo principo turinį apima būtinumo, tinkamumo ir adekvatumo kriterijai. Būtinumo kriterijus pasireiškia Bendrajame duomenų apsaugos reglamente įtvirtintu reikalavimu numatančiu, jog asmens duomenys turėtų būti tvarkomi, jei asmens duomenų tvarkymo tikslo pagrįstai negalima pasiekti kitomis priemonėmis[56]. Tinkamumo kriterijus reiškia, kad duomenys apskritai gali būti reikšmingi siekiant duomenų tvarkymo tikslų. Be to, draudžiama rinkti ir tvarkyti duomenis, kurie niekaip nėra susiję su duomenų valdytojo veikla ir jo tikslais. Adekvatumo kriterijaus įgyvendinimas iš esmės reiškia reikalavimą, kad tvarkomi duomenys būtų proporcingi duomenų tvarkymo tikslams. Pažymėtina, kad proporcingumo reikalavimas apima visus asmens duomenų tvarkymo aspektus: asmens duomenų tvarkymo pradžią ir trukmę, duomenų subjektų, kurių asmens duomenys tvarkomi, grupes, tvarkomų asmens duomenų kategorijas, asmens duomenų tvarkymo būdus, atskirus asmens duomenų tvarkymo veiksmus[57]. Įvertinus tai, kas išdėstyta, matyti, jog taikant duomenų kiekio mažinimo principą, duomenų valdytojas nėra įpareigojamas apriboti tvarkomų asmens duomenų kiekį iki visiško minimumo, tačiau įpareigojamas duomenų rinkimą apriboti iki tokio lygio, kuris būtų suderinamas su duomenų tvarkymo tikslais[58]. Be kita ko, pastebėtina, kad duomenų apsaugos teisės reguliavimu neapibrėžiama, kokius duomenis duomenų valdytojui galima tvarkyti konkrečiu tikslu. Įstatyminis reglamentavimas neapibrėžia, kokie duomenys yra laikytini tinkamais ir tokiais, kurių reikia siekiant numatytų tikslų, dėl kurių duomenys yra renkami ir tvarkomi. Duomenų valdytojas, vadovaudamasis atskaitomybės principu, privalo pats imtis priemonių užtikrinti, kad asmens duomenys yra adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių duomenys yra tvarkomi, o esant būtinybei, tą įrodyti. Tokiu būdu duomenų valdytojas turi diskreciją nuspręsti, ar konkretūs duomenys yra būtini siekiant duomenų tvarkymo tikslų bei pagrįsti šių duomenų tvarkymo būtinumą, atsižvelgiant į siekiamus tikslus[59].

Duomenų kiekio mažinimo principo įgyvendinimą viešajame sektoriuje galima įvertinti pasitelkus Valstybinės vartotojų teisių apsaugos tarnybos pavyzdį. Duomenų subjektų teisių įgyvendinimo Valstybinėje vartotojų teisių apsaugos tarnyboje aprašo, patvirtinto Valstybinės vartotojų teisių apsaugos tarnybos direktoriaus 2018 m. gruodžio 31 d. įsakymu Nr. 1-200 „Dėl duomenų subjektų teisių įgyvendinimo Valstybinėje vartotojų teisių apsaugos tarnyboje aprašo

[56] Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) Nr. 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) OL 2016 L 19, p. 1-88.
[57] ZALESKIS, J. (2019). Europos Sąjungos bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Vilnius: Registrų centras, p. 122.
[58] ZALESKIS, J. (2019). Europos Sąjungos bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Vilnius: Registrų centras, p. 121.
[59] ZALESKIS, J. (2019). Europos Sąjungos bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Vilnius: Registrų centras, p. 122.

patvirtinimo ir Valstybinėje vartotojų teisių apsaugos tarnyboje įrengtų vaizdo stebėjimo kamerų naudojimo ir vaizdo duomenų tvarkymo tvarkos aprašo patvirtinimo“ (toliau – Duomenų subjektų teisių įgyvendinimo Valstybinėje vartotojų teisių apsaugos tarnyboje aprašas) 3.2 punkte įtvirtinta, kad Valstybinėje vartotojų teisių apsaugos tarnyboje, jai vykdant Lietuvos Respublikos vartotojų teisių apsaugos įstatymo (toliau – Vartotojų teisių apsaugos įstatymas) 12 straipsnyje įtvirtintas funkcijas ir teises, tvarkomi šie asmens duomenys: vardas ir pavardė, asmens kodas, gyvenamoji vieta, telefono numeris ir elektroninio pašto adresas. Taigi, duomenų subjektų teisių įgyvendinimo Valstybinėje vartotojų teisių apsaugos tarnyboje apraše yra įtvirtinta aiški Valstybinėje vartotojų teisių apsaugos tarnyboje tvarkomų duomenų apimtis. Tačiau patvirtintoje vartotojų prašymo formoje duomenų subjekto (vartotojo) yra prašoma pateikti ne visus Duomenų subjektų teisių įgyvendinimo Valstybinėje vartotojų teisių apsaugos tarnyboje aprašo 3.2 punkte įtvirtintus Valstybinės vartotojų teisių apsaugos tarnybos tvarkomus duomenų subjekto duomenis. Duomenų subjektas (vartotojas) teikdamas prašymą Valstybinei vartotojų teisių apsaugos tarnybai turi pateikti savo vardą ir pavardę, adresą, telefono numerį ir (arba) elektroninio pašto adresą, tačiau nėra įpareigojamas pateikti asmens kodą. Duomenų subjekto (vartotojo) asmens kodą Valstybinė vartotojų teisių apsaugos tarnyba tvarko prašymo nagrinėjimo tikslu, nurodydama jį sprendime (nutarime) dėl ginčo esmės. Duomenų subjekto (vartotojo) asmens kodo nurodymo sprendime būtinumas grindžiamas aplinkybe, jog Valstybinės vartotojų teisių apsaugos tarnybos sprendimas yra vykdomasis dokumentas, kuriame be duomenų subjekto (vartotojo) vardo ir pavardės turi būti nurodytas ir jo asmens kodas. Atsižvelgiant į tai, kad duomenų subjekto (vartotojo) asmens kodo rinkimas yra pagrįstas ir tiesiogiai susijęs su duomenų tvarkymo tikslu (prašymo nagrinėjimo tikslu), kyla klausimas, kodėl duomenų subjekto (vartotojo) nėra prašoma pildomoje prašymo formoje nurodyti savo asmens kodą? Autorės nuomone, tai yra tiesiogiai susiję su duomenų kiekio mažinimo principo įgyvendinimu. Valstybinė vartotojų teisių apsaugos tarnyba, gavusi duomenų subjekto (vartotojo) prašymą, įvertinusi pateiktus įrodymus, paaiškinimus, galiojantį teisinį reglamentavimą, vadovaudamasi Vartotojų teisių apsaugos įstatymo 23^3 straipsnio 1 dalimi gali atsisakyti nagrinėti ginčą. Tokiais atvejais Valstybinė vartotojų teisių apsaugos tarnyba nepriima sprendimo dėl ginčo esmės, t. y. nepriima nutarimo, kuris laikytinas vykdomuoju dokumentu, todėl tokiais atvejais duomenų subjekto (vartotojo) asmens kodo tvarkymas būtų laikomas pertekliniu ir prieštarautų duomenų kiekio mažinimo principui. Taigi, Valstybinė vartotojų teisių apsaugos tarnyba, neįpareigodama duomenų subjekto (vartotojo) prašyme nurodyti savo asmens kodo, tačiau turėdama teisę tvarkyti duomenų subjekto asmens kodą prašymo nagrinėjimo tikslu, užtikrina tvarkomų duomenų kiekio mažinimo principo įgyvendinimą.

Analizuojat šį principą, reikėtų įvertinti ir asmens teisę ištrinti duomenis, t. y. Bendrajame duomenų apsaugos reglamente įtvirtintą „teisę būti pamirštam“[60], kuri įtvirtinta minėto dokumento 17 straipsnio 1 dalyje nustatytais atvejais. Valstybės įmonės Registrų centro patvirtintame apraše nurodoma, jog „Duomenų subjekto prašyme ištrinti duomenis turi būti išsamiai argumentuota, dėl kokių priežasčių yra prašoma ištrinti jo asmens duomenis (prašyme turi būti nurodytas vienas Bendrojo duomenų apsaugos reglamento 17 straipsnio 1 dalies papunkčių)“. Duomenų subjekto teisė reikalauti ištrinti asmens duomenis („teisė būti pamirštam“) gali būti neįgyvendinta jeigu:

- duomenų tvarkymas yra grindžiamas Europos Sąjungos arba Lietuvos Respublikos teisės aktuose nustatytų reikalavimų vykdymu;
- siekiant pareikšti, vykdyti arba apginti teisinius interesus[61].

Jeigu duomenų subjekto asmens duomenys (ištrinti pagal duomenų subjekto prašymą) buvo perduoti duomenų gavėjams, valstybės įmonė Registrų centras šiuos duomenų gavėjus apie tai informuoja, nebent tai būtų neįmanoma ar pareikalautų neproporcingų pastangų. Duomenų subjektas turi teisę prašyti, kad jam būtų pateikta informacija apie tokius duomenų gavėjus.

Apibendrinant reikėtų pastebėti, jog reikia vertinti konkrečią situaciją, siekiant išsiaiškinti, kokio minimalaus duomenų kiekio užtenka iškeltam tikslui pasiekti ir tuomet tuos duomenis tvarkyti taip, kaip to yra reikalaujama duomenų valdytojo veiklą reglamentuojančiuose teisės aktuose. Taip pat būtina įgyvendinti Bendrajame duomenų apsaugos reglamente įtvirtintą „*teisę būti pamirštam*“. Jeigu duomenų valdytojas objektyviai gali atlikti savo funkcijas be tam tikrų asmens duomenų, tokie tvarkomi duomenys būtų pripažinti pertekliniais ir jų naudoti duomenų valdytojui nebūtų leidžiama[62].

1.2.4. Duomenų tikslumo principas

Duomenų tikslumo principas yra įtvirtintas Bendrojo duomenų apsaugos reglamento 5 straipsnio d dalyje, kuri numato, jog asmens duomenys turi būti „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“[63]. Duomenų tikslumas

[60] Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) Nr. 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) OL 2016 L 19, p. 1-88.

[61] Valstybės įmonės Registrų centro 2018 m. gegužės 24 d. direktoriaus įsakymas Nr. v-171 „Dėl asmens duomenų tvarkymo valstybės įmonėje Registrų centre tvarkos aprašo patvirtinimo“ [interaktyvus]. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/ TAD/1804741065d311e8b7d2b2d2ca774092/asr [žiūrėta 2020 m. lapkričio 10 d.].

[62] ZALESKIS, J. (2019). Europos Sąjungos bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Vilnius: Registrų centras, p. 122.

[63] Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) Nr. 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) OL 2016 L 19, p. 1-88.

suprantamas kaip duomenų ir faktinės, objektyvios tikrovės atitikimas. Pažymėtina, kad duomenų tikslumas apima duomenų aktualumą laiko požiūriu. Šiuo metu renkami duomenys gali būti tikslūs ir atitikti tikrovę, tačiau po kurio laiko pasikeitus aplinkybėms surinkti duomenys gali tapti neaktualūs. Duomenų tikslumo principas būtų pažeistas, jeigu duomenų valdytojas tvarkytų duomenis žinodamas, kad jie yra pasenę. Pažymėtina, kad duomenų tikslumas priklauso ne tik nuo duomenų valdytojo, bet ir nuo paties duomenų subjekto. Duomenų tikslumo principas formuluojamas ne kaip kategoriška ir absoliuti duomenų valdytojo pareiga, kuri reikštų duomenų valdytojo pareigą imtis visų įmanomų priemonių, kad tvarkomi duomenys būtų tikslūs, o kaip pareiga imtis visų pagrįstų priemonių, skirtų užtikrinti, kad tvarkomi duomenys būtų tikslūs. Įgyvendindamas šią pareigą duomenų valdytojas turi suformuoti tinkamas technines ir organizacines priemones, kuriomis būtų siekiama veiksmingai taikyti duomenų tikslumo principą. Svarbia organizacine priemone, duomenų valdytojo tvarkomų duomenų tikslumui užtikrinti, laikytinas atidus šaltinio, iš kurio bus renkami asmens duomenys, parinkimas. Minėta, jog patikimiausiu asmens duomenų šaltiniu pripažįstamas pats duomenų subjektas ir valstybiniai registrai[64]. Dažniausiu atveju valstybinės institucijos, siekdamos užtikrinti tvarkomų duomenų tikslumo užtikrinimą, pasitelkia patį duomenų subjektą, kuris, kaip minėta, yra patikimiausias duomenų surinkimo šaltinis. Duomenų subjektams teikiant rašytinius patvirtintos formos prašymus valstybinėms institucijoms užtikrinamas valstybinės institucijos renkamos ir tvarkomos informacijos tikslumas, nes už tikslios informacijos pateikimą tiesiogiai atsako duomenų subjektas. Pastebėtina, kad dažnu atveju patvirtintose prašymų, teikiamų valstybės institucijai, formose yra įtvirtintas duomenų subjekto patvirtinimas, jog jo pateikiami duomenys yra tikslūs. Pavyzdžiui, Ryšių reguliavimo tarnybos patvirtintoje prašymo formoje yra įtvirtinta nuostata „patvirtinu, kad visa mano pateikta informacija yra tiksli ir teisinga“[65]. Valstybinės duomenų inspekcijos patvirtintoje skundo formoje yra įtvirtintas analogiškas duomenų subjekto patvirtinimas. Be to, papildomai įtvirtinama nuostata, kuri informuoja duomenų subjektą, jog „už žinomai melagingų duomenų pateikimą Valstybinei duomenų apsaugos inspekcijai Lietuvos Respublikos administracinių nusižengimų kodekso 505 straipsnyje yra numatyta administracinė atsakomybė“[66]. Kita valstybės institucijų pasitelkiama priemonė, užtikrinanti tvarkomų duomenų tikslumą – viešųjų paslaugų perkėlimas į elektroninę erdvę. Duomenų subjektas naudodamasis viešųjų paslaugų portalu informacijai ar paslaugai gauti arba norėdamas pateikti prašymą ar skundą valstybės institucijai turi save

[64] ZALESKIS, J. (2019). Europos Sąjungos bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Vilnius: Registrų centras, p. 125.
[65] Ryšių reguliavimo tarnyba. Vartotojų teisių apsauga (tinklalapio internete skiltis) [interaktyvus]. Prieiga per internetą: https://www.rrt.lt/pastas/vartotoju-teisiu-apsauga/kaip-pateikti-skunda/ [žiūrėta 2020 m. rugsėjo 26 d.].
[66] Valstybinė duomenų apsaugos inspekcija. Skundų nagrinėjimas (tinklalapio internete skiltis) [interaktyvus]. Prieiga per internetą: https://vdai.lrv.lt/lt/veiklos-sritys-1/skundu-nagrinejimas [žiūrėta 2020 m. rugsėjo 26 d.].

identifikuoti, t. y. įrodyti savo tapatybę. Tokiu būdu yra užtikrinama, jog valstybės institucija tvarko tikslius duomenų subjekto duomenis. Pavyzdžiui, vartotojas, norintis pateikti prašymą vartojimo ginčus nagrinėjančiai institucijai, gali tą padaryti naudodamasis Vartotojų teisių informacine sistema (VTIS), prie kurios norėdamas prisijungti turi save identifikuoti arba prisijungdamas prie elektroninio banko, arba su elektronine atpažinties priemone[67].

Taikyti duomenų tikslumo principą padeda duomenų subjektui suteikiama galimybė kontroliuoti savo duomenų tvarkymą. Šiuo tikslu ypatingai svarbios nuostatos, įtvirtinančios duomenų subjekto teisę susipažinti su savo duomenimis ir reikalauti ištaisyti netikslius duomenis. Užtikrinant duomenų tikslumą, duomenų subjektas turi teisę iš duomenų valdytojo sužinoti, ar su juo susiję asmens duomenys yra tvarkomi, jeigu taip, tuomet duomenų subjektas turi teisę su jais susipažinti. Šią duomenų subjekto teisę garantuoja Bendrojo duomenų apsaugos reglamento 15 straipsnis, kuris įtvirtina, kad duomenų subjektas turi teisę iš duomenų valdytojo gauti patvirtinimą, ar su juo susiję asmens duomenys yra tvarkomi, o jei tokie asmens duomenys yra tvarkomi, turi teisę susipažinti su asmens duomenimis ir informacija apie: duomenų tvarkymo tikslus; atitinkamų asmens duomenų kategorijas; numatomą asmens duomenų saugojimo laikotarpį; teisę prašyti duomenų valdytojo ištaisyti arba ištrinti asmens duomenis arba apriboji su duomenų subjektu susijusių asmens duomenų tvarkymą; teisę pateikti skundą priežiūros institucijai ir kt[68].

Naudodamasis teise gauti su asmens duomenų tvarkymu susijusią informaciją ar kitais būdais susipažinęs su duomenų valdytojo tvarkomais asmens duomenimis, duomenų subjektas gali nustatyti, kad duomenų valdytojas neužtikrina tvarkomų asmens duomenų kokybės, t. y., jog tvarkomi asmens duomenys yra netikslūs ar neišsamūs. Nekokybiškų asmens duomenų tvarkymas kelia grėsmę duomenų subjekto interesams, todėl duomenų subjektui pripažįstama teisė reikalauti, kad duomenų valdytojas pakoreguotų tvarkomus asmens duomenis. Bendrojo duomenų apsaugos reglamento 16 straipsnis garantuoja duomenų subjekto teisę „reikalauti, kad duomenų valdytojas nepagrįstai nedelsdamas ištaisytų netikslius su juo susijusius asmens duomenis“. Atsižvelgiant į tikslus, kuriais duomenys buvo tvarkomi, duomenų subjektas turi teisę reikalauti, kad būtų papildyti neišsamūs asmens duomenys, be kita ko, pateikdamas papildomą pareiškimą“[69]. Pastebėtina, kad reglamentas neapibrėžia „netikslių duomenų“ bei „neišsamių duomenų“ reikšmės. Neišsamiais turėtų būti laikomi asmens duomenys, kurie tvarkomi per maža apimtimi, kad suteiktų pakankamą

[67] Vartotojų teisių informacinė sistema (VTIS). El. paslaugos (tinklalapio internete skiltis) [interaktyvus]. Prieiga per internetą: https://vtis.lt/portal/#/services/complaint/intro/4 [žiūrėta 2020 m. spalio 10 d.].
[68] Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) Nr. 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) OL 2016 L 19, p. 1-88.
[69] Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) Nr. 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) OL 2016 L 19, p. 1-88.

ir neklaidinančią informaciją tuo tikslu, dėl kurio šie asmens duomenys tvarkomi. Taigi, asmens duomenų pripažinimą neišsamiais lemia neatitikimas tarp duomenų valdytojo tvarkomų asmens duomenų apimties ir šių asmens duomenų tvarkymo tikslo. Svarbu atkreipti dėmesį, jog per maža tvarkomų asmens duomenų apimtis ne visais atvejais reiškia atitikimą asmens duomenų teisinės apsaugos reikalavimams, nes tam tikrais atvejais gali susiklostyti situacija, kai nepakankamo asmens duomenų kiekio tvarkymas gali neatitikti ne tik duomenų valdytojo, bet ir duomenų subjekto interesų. Tuo tarpu netiksliais turėtų būti laikomi tie asmens duomenys, kurie neatitinka jų apibūdinamų aplinkybių. Tai reiškia, jog asmens duomenų pripažinimą netiksliais sąlygoja duomenų turinio neatitikimas faktiniams duomenims[70].

Kaip matyti, duomenų subjekto teisės reikalauti ištaisyti ar papildyti duomenų valdytojo tvarkomus asmens duomenis, turinį ir įgyvendinimo sąlygas suponuoja duomenų tikslumo principas. Be to, šios duomenų subjekto teisės esmę sudaro duomenų subjekto diskrecija eliminuoti neigiamus padarinius, sukeltus iš rūpestingumo principo kylančios duomenų valdytojo pareigos tvarkyti kokybiškus asmens duomenis nevykdymas. Duomenų tikslumo principo taikymo viešajame sektoriuje ypatumai ryškėja, kai yra taikomos tęstinio pobūdžio viešosios paslaugos. Tokiais atvejais, kai duomenų subjektas yra davęs sutikimą tvarkyti jo asmens duomenis ir nuolat naudojasi duomenų valdytojo teikiamomis viešosiomis paslaugomis, duomenų valdytojas turi pareigą užtikrinti, kad tvarkomi asmens duomenys būtų nuolat peržiūrimi ir atnaujinami. Duomenų tikslumo principas įstaigose turi būti įgyvendinamas nuolat, tačiau įstaigos turi diskreciją įsitvirtinti, kokiu periodiškumu duomenų subjekto bus prašoma peržiūrėti ir atnaujinti jo teikiamus asmens duomenis duomenų valdytojui. Pavyzdžiui, viešosios bibliotekos reguliariai prašo lankytojų, besinaudojančių bibliotekos teikiamomis paslaugomis, atnaujinti skaitytojo pažymėjime esančią informaciją. Sodros arba Valstybinės mokesčių inspekcijos elektroninėmis paslaugomis besinaudojantys asmenys, elektroniniu būdu prisijungdami prie asmeninės paskyros, reguliariai gauna pranešimą, kuriuo informuojami, jog privalo peržiūrėti pateiktą asmens informaciją ir esant neatitikimų ją atnaujinti. Taigi, iš esmės duomenų tikslumo principo taikymo viešajame sektoriuje ypatumas yra tas, jog šio principo įgyvendinimą lemia duomenų subjekto ir duomenų valdytojo bendradarbiavimas. Duomenų valdytojas tvarkomų duomenų tikslumą gali užtikrinti, jei pats duomenų subjektas, būdamas patikimiausiu asmens duomenų šaltiniu, pateikia duomenų valdytojui tikslią su asmeniu susijusią informaciją, taip pat pats skatindamas duomenų subjektą peržiūrėti ir atnaujinti ar ištaisyti tvarkomus asmens duomenis.

[70] PETRAITYTĖ, I. (2013). Asmens duomenų teisinės apsaugos principai. Daktaro disertacija, socialiniai mokslai, teisė, Vilniaus universitetas. Vilnius: Vilniaus universiteto leidykla [interaktyvus]. Prieiga per internetą: http://epublications.vu.lt/object/elaba:1823635/1823635.pdf [žiūrėta 2020 m. rugsėjo 20 d.].

1.2.5. Duomenų saugojimo trukmės ribojimo principas

Duomenų saugojimo trukmės ribojimo principas, įtvirtintas Bendrojo duomenų apsaugos reglamento 5 straipsnio e dalyje, reiškia, jog asmens duomenys turi būti laikomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, nei būtina tais tikslais, kuriais asmens duomenys yra tvarkomi. Be to, Bendrasis duomenų apsaugos reglamentas nurodo, jog asmens duomenis galima saugoti ilgesnį laikotarpį, jeigu asmens duomenys bus tvarkomi tik archyvavimo tikslais viešojo intereso labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais, įgyvendinus atitinkamas technines ir organizacines priemones, kurių reikalaujama šiuo reglamentu siekiant apsaugoti duomenų subjekto teises ir laisves[71].

Pastebėtina, kad duomenų saugojimo trukmės ribojimo principas yra glaudžiai susijęs su duomenų kiekio mažinimo principu ir jį papildo. Tą patvirtina Bendrojo duomenų apsaugos reglamento preambulėje įtvirtinta nuostata, kuri numato, jog asmens duomenys turėtų būti tinkami, susiję su tikslais, kuriais jie tvarkomi ir riboti pagal tai, kiek jų yra būtina turėti atsižvelgiant į tikslus, kuriais jie tvarkomi. Tam pirmiausia reikia užtikrinti, kad asmens duomenų saugojimo laikotarpis būtų tikrai minimalus[72]. Atsižvelgiant į tai, darytina išvada, kad duomenų saugojimo trukmės apribojimo principas kelia reikalavimą duomenų tvarkymo tikslą susieti su duomenų saugojimo laiku. Laiko požiūriu duomenų tvarkymas turi būti grindžiamas būtinybe tvarkyti asmens duomenis, o jeigu duomenų valdytojui nebėra aktuali duomenų subjekto tapatybė, duomenys turėtų būti ištrinami arba nuasmeninami. Bendrojo duomenų apsaugos reglamento preambulėje įtvirtinta duomenų valdytojų pareiga nustatyti duomenų ištrynimo arba periodinės peržiūros terminus, tam, kad būtų užtikrinta, kad duomenys nebūtų laikomi ilgiau nei būtina[73]. Pastebėtina, kad nors Bendrasis duomenų apsaugos reglamentas įtvirtina pareigą duomenų valdytojams užtikrinti kuo trumpesnį duomenų saugojimo terminą, tačiau neapibrėžia konkrečių duomenų saugojimo terminų. Atsižvelgiant į tai, kiekvienam duomenų valdytojui paliekama laisvė spręsti kaip ilgai konkrečiu atveju duomenų subjekto duomenys turėtų būti saugomi, atsižvelgiant į duomenų tvarkymo tikslą. Duomenų saugojimo terminas turi būti grindžiamas būtinybe tvarkyti atitinkamus duomenis norint pasiekti konkretų duomenų tvarkymo tikslą. Be to, duomenų valdytojas turi atsižvelgti į jam

[71] Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) Nr. 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) OL 2016 L 19, p. 1-88.
[72] Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) Nr. 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) OL 2016 L 19, p. 1-88.
[73] Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) Nr. 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) OL 2016 L 19, p. 1-88.

taikomas teisės aktų nuostatas, kuriose yra įtvirtinti duomenų saugojimo terminai, taip pat konkrečių duomenų kategorijas bei kitas kiekvienoje situacijoje svarbias aplinkybes[74].

Praktikoje valstybės institucijos, besivadovaudamos atskaitomybės principu, vidaus dokumentuose nustato konkrečius duomenų saugojimo terminus, atsižvelgdamos į duomenų tvarkymo tikslus. Keletas viešojo sektoriaus institucijų pavyzdžių atskleidžia, kokie yra terminai duomenų saugojimo trukmės aspektu. Pavyzdžiui, Ryšių reguliavimo tarnyba patvirtintame Duomenų subjektų teisių įgyvendinimo Ryšių reguliavimo tarnyboje tvarkos apraše įtvirtino duomenų saugojimo terminus, atsižvelgiant į duomenų tvarkymo tikslus bei konkrečių duomenų kategorijas. Pavyzdžiui, asmenų, naudojančių EPIS, ir EPIS naudotojų asmens duomenys duomenų bazėse saugomi 10 metų nuo paskutinio EPIS naudotojo ir asmens, naudojančio EPIS, prisijungimo prie EPIS (Duomenų subjektų teisių įgyvendinimo Ryšių reguliavimo tarnyboje tvarkos aprašo 8.5.1.2 punktas); asmens duomenys numerių ir kodų valdymo bei teisės vartoti domenus su Lietuvos vardu ir elektroninių ryšių paslaugų ir tinklų teikėjų sąrašo administravimo informacinėje sistemoje duomenys duomenų bazėje saugomi 10 metų nuo jų įregistravimo (Duomenų subjektų teisių įgyvendinimo Ryšių reguliavimo tarnyboje tvarkos aprašo 8.5.3.2 punktas); duomenys, tvarkomi tiesioginės rinkodaros tikslu saugomi 10 metų nuo registracijos gauti naujienlaiškį momento (Duomenų subjektų teisių įgyvendinimo Ryšių reguliavimo tarnyboje tvarkos aprašo 8.6.3 punktas); duomenys, tvarkomi aptarnavimo telefonu kokybės kontrolės tikslu saugomi 6 mėnesius (Duomenų subjektų teisių įgyvendinimo Ryšių reguliavimo tarnyboje tvarkos aprašo 8.7.3 punktas); duomenys, tvarkomi valdomo turto apsaugos tikslu saugomi 14 dienų (Duomenų subjektų teisių įgyvendinimo Ryšių reguliavimo tarnyboje tvarkos aprašo 8.8.2 punktas); duomenys, tvarkomi praėjimo kontrolės tikslu, t. y. siekiant įsitikinti, kad asmuo turi praėjimo į Ryšių reguliavimo tarnybą patalpas teisę, saugomi 30 dienų (Duomenų subjektų teisių įgyvendinimo Ryšių reguliavimo tarnyboje tvarkos aprašo 8.9.2 punktas)[75].

Lietuvos banko bendrųjų asmens duomenų tvarkymo nuostatuose, patvirtintuose Lietuvos banko valdybos pirmininko 2018 m. liepos 20 d. įsakymu Nr. V 2018/(1.7.E-260603)-02-113 „Dėl Lietuvos banko bendrųjų asmens duomenų tvarkymo nuostatų patvirtinimo“ (toliau – Lietuvos banko bendrųjų asmens duomenų tvarkymo nuostatai) yra įtvirtintos bendro pobūdžio nuostatos, įtvirtinančios, jog asmens duomenų, tvarkomų Lietuvos banko oficialiuosiuose elektroniniuose dokumentuose, saugojimo bendrieji reikalavimai nustatyti Lietuvos banko dokumentų valdymo

[74] ZALESKIS, J. (2019). Europos Sąjungos bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Vilnius: Registrų centras, p. 127.

[75] Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2018 m. rugpjūčio 7 d. įsakymas Nr. 1V-714 dėl duomenų subjektų teisių įgyvendinimo Lietuvos Respublikos ryšių reguliavimo tarnyboje tvarkos aprašo patvirtinimo [interaktyvus]. Prieiga per internetą:https://www.rrt.lt/wp-content/uploads/2018/08/Duomen%C5%B3-subjekt%C5%B3-teisi%C5%B3-%C4%Afgyvendinimo-Lietuvos-Respublikos-ry%C5%A1i%C5%B3-reguliavimo-tarnyboje-tvarkos-apra%C5%A1as.p df [žiūrėta 2020 m. rugsėjo 27 d.].

Nestruktūrizuotų duomenų saugyklos ir grupinio darbo sistemoje ir elektroninių dokumentų valdymo taisyklėse, patvirtintose Lietuvos banko valdybos pirmininko 2017 m. sausio 16 d. įsakymu Nr. V 2017/(1.7-260603)-02-29 „Dėl Lietuvos banko dokumentų valdymo Nestruktūrizuotų duomenų saugyklos ir grupinio darbo sistemoje ir elektroninių dokumentų valdymo taisyklių patvirtinimo“, o asmens duomenys, tvarkomi elektroninėse ar popierinėse dokumentų bylose, saugomi vadovaujantis Lietuvos vyriausiojo archyvaro 2011 m. kovo 9 d. įsakymu Nr. V-100 „Dėl Bendrųjų dokumentų saugojimo terminų rodyklės patvirtinimo“ patvirtintoje Bendrųjų dokumentų saugojimo terminų rodyklėje (toliau – Bendrųjų dokumentų saugojimo terminų rodyklė), įstatymuose bei Lietuvos banko dokumentacijos plane nustatytais terminais[76]. Lietuvos bankas, vadovaudamasis Bendrųjų dokumentų saugojimo terminų rodyklėje nustatytais dokumentų saugojimo terminais, įsitvirtino duomenų saugojimo terminus, pavyzdžiui, duomenys, tvarkomi vartotojų ir finansų rinkos dalyvių ginčų nagrinėjimo ne teismo tvarka tikslu, saugomi 5 metus; biometriniai duomenys, tvarkomi patekimo kontrolės į Lietuvos banko specialiąsias patalpas tikslu, saugomi iki to laiko, kol galioja tarnautojui suteikta teisė patekti į biometrinės kontrolės priemonėmis kontroliuojamas patalpas; duomenys, tvarkomi asmenų, dėl kurių yra pateikti prašymai neleisti jiems sudaryti vartojimo kredito sutarčių, sąrašo tvarkymo tikslu, saugomi 5 metus nuo asmens išbraukimo iš asmenų, dėl kurių yra pateikti prašymai neleisti jiems sudaryti vartojimo kredito sutarčių, sąrašo dienos; duomenys tvarkomi asmenų prašymų, skundų ar pranešimo nagrinėjimo tikslu, saugomi 1 metus Lietuvos bankui priėmus sprendimą[77].

Analizuojant viešojo sektoriaus įstaigą valstybės įmonę Registrų centrą, valstybės įmonės Registrų centro patvirtintame apraše yra įtvirtinta, kad dokumentuose ar bylose saugomi asmens duomenys, atsižvelgiant į dokumento ar bylos, kuriuose šie duomenys yra nurodyti, rūšį, pagal Registrų centro dokumentacijos plane nurodytą terminą. Pasibaigus dokumento, kuriame šie duomenys yra nurodyti, saugojimo terminui, priimamas sprendimas dėl jo sunaikinimo arba dokumento saugojimo termino pratęsimo. Priėmus sprendimą dokumentą sunaikinti, dokumentas sunaikinamas Lietuvos Respublikos dokumentų ir archyvų įstatymo[78] nustatyta tvarka. Kaip

[76] Lietuvos banko valdybos pirmininko 2018 m. liepos 20 d. įsakymas Nr. V 2018/(1.7.E-260603)-02-113 dėl Lietuvos banko bendrųjų asmens duomenų tvarkymo nuostatų patvirtinimo [interaktyvus]. Prieiga per internetą: https://www.lb.lt/uploads/documents/files/Asmens%20duomenu%20tvarkymo%20nuostatainauja_2019_07_30.pdf [žiūrėta 2020 m. rugsėjo 27 d.].

[77] Lietuvos bankas. Informacija apie asmens duomenų apsaugą (tinklalapio internete skiltis) [interaktyvus]. Prieiga per internetą: https://www.lb.lt/lt/informacija-apie-asmens-duomenu-apsauga#ex-1-23 [žiūrėta 2020 m. rugsėjo 26 d.].

[78] Pagal šį įstatymą valstybės ir savivaldybių institucijos, įstaigos ir įmonės, valstybės įgalioti asmeny privalo saugoti dokumentus patikimoje ir saugioje aplinkoje, įvertindami galimus rizikos veiksnius; išsaugoti savo veiklos dokumentus reikiamą laiką, kad būtų užtikrinti veiklos įrodymai, apsaugotos su ja susijusių fizinių ir juridinių asmenų teisės; išsaugoti reikiamą laiką kitų juridinių ir fizinių asmenų veiklos dokumentus, perimtus šio Įstatymo ir kitų teisės norminių aktų nustatyta tvarka; užtikrinti, kad turimi elektroniniai ir kiti dokumentai, prie kurių prieinama tik specialios įrangos priemonėmis, išliktų autentiški, patikimi ir prieinami visą jų saugojimo laiką. Kartu su šiais dokumentais turi būti saugoma ir kontekstinė informacija (Lietuvos Respublikos dokumentų ir archyvų įstatymas (1995). Valstybės žinios, 107-2389).

pavyzdys, telefono įrašai saugomi 30 dienų, po to ištrinami; vaizdo kamerų įrašai saugomi 30 dienų, po to ištrinami; įstaigos į pastatą kontrolės duomenys saugomi 12 mėnesių, po to ištrinami; siekiančių įsidarbinti asmenų asmens duomenys saugomi 12 mėnesių, po to sunaikinami; tapatybės nustatymo (autentifikavimo) tikslu asmens duomenys saugomi 12 mėnesių, po to ištrinami[79]. Taigi, nors Bendrajame duomenų apsaugos reglamente konkretūs duomenų saugojimo terminai nėra įtvirtinti, valstybės institucijos, siekdamos užtikrinti duomenų saugojimo trukmės ribojimo principo įgyvendinimą, atsižvelgdamos į duomenų tvarkymo tikslus, savarankiškai nustato duomenų saugojimo terminus, kurių proporcingumą gali objektyviai pagrįsti.

1.2.6. Vientisumo ir konfidencialumo principas

Bendrojo duomenų apsaugos reglamento 5 straipsnio f punkte įtvirtintas duomenų vientisumo ir konfidencialumo principas reiškia, jog asmens duomenys turi būti tvarkomi tokiu būdu, kad taikant atitinkamas technines ar organizacines priemones būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo[80]. Pastebėtina, kad doktrinoje duomenų vientisumo ir konfidencialumo principas yra įvardijamas kaip duomenų saugumo principas. Duomenų vientisumo ir konfidencialumo principo esmę atskleidžia Bendrojo duomenų apsaugos reglamento 32 straipsnis, įtvirtinantis duomenų valdytojo ir duomenų tvarkytojo pareigą užtikrinti tvarkomų duomenų saugumą. Minimas straipsnis įtvirtina, jog duomenų valdytojas ir duomenų tvarkytojas privalo įgyvendinti tinkamas technines ir organizacines priemones, kad būtų užtikrintas pavojų atitinkančio lygio saugumas. Analizuojant valstybės įmonės Registrų centro sudaromas sutartis, kurios patalpintos internetiniame puslapyje, matyti, kad duomenų teikimo sutartyse įtvirtintos nuostatos, susijusios su konfidencialumu, duomenis gaunantys asmenys turi pasirašyti konfidencialumo pasižadėjimą. Sutartyse įtvirtintos tokios nuostatos, kaip *„užtikrinti, kad visi duomenų vartotojai būtų pasirašę konfidencialumo pasižadėjimus, parengtus pagal atitinkamą sutarties priedą“;* taip pat duomenis gaunantis subjektas *„turi prisiimti visišką atsakomybę už gautų duomenų konfidencialumą ir saugą nuo duomenų gavimo momento“, kai tuo tarpu duomenų valdytojas (tvarkytojas) turi* užtikrinti teikiamų duomenų saugumą ir teisingumą tik iki tol, kol duomenys pasieks gavėją. Tokios viešojo administravimo subjekto sutarčių nuostatos, pagal kurias

[79] Valstybės įmonės Registrų centro 2018 m. gegužės 24 d. direktoriaus įsakymas Nr. v-171 „Dėl asmens duomenų tvarkymo valstybės įmonėje Registrų centre tvarkos aprašo patvirtinimo“ [interaktyvus]. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/ TAD/1804741065d311e8b7d2b2d2ca774092/asr [žiūrėta 2020 m. lapkričio 10 d.].
[80] Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) Nr. 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) OL 2016 L 19, p. 1-88.

teikiami duomenys, įtvirtina konfidencialumą tiek iki duomenų teikimo momento (kuomet atsako duomenų valdytojas – tvarkytojas), tiek pateikus duomenis (atsako duomenų gavėjas).

Pažymėtina, kad duomenų saugumo srities teisės nuostatos grindžiamos principais, bet ne detaliomis taisyklėmis. Galima išskirti šiuos duomenų saugumo teisinio reguliavimo principus: duomenų valdytojų ir duomenų tvarkytojų diskrecijos principą, pavojumi asmenims grįsto požiūrio principą, duomenų konfidencialumo, vientisumo, prieinamumo ir atsparumo principą bei duomenų saugumo priežiūros principą[81].

Duomenų valdytojų ir duomenų tvarkytojų diskrecijos principas reiškia, kad Bendrasis duomenų apsaugos reglamentas įtvirtina nuožiūros laisvę neperžengiant reguliavimu nustatytų ribų pasirinkti, kokias konkrečias duomenų saugumo priemones įgyvendinti ir kaip tai padaryti. Ši diskrecija turėtų būti įgyvendinta taip, kad pasirinktomis duomenų saugumo priemonėmis būtų užtikrintas tinkamas saugumas, įskaitant konfidencialumą. Pavojumi asmenims grįsto požiūrio principas reiškia, kad atskaitos taškas turėtų būti asmens, kurio duomenys yra tvarkomi, gerovė. Siekdamas užtikrinti saugumą ir užkardyti asmens duomenų apsaugos teisę pažeidžiantį duomenų tvarkymą duomenų valdytojas arba duomenų tvarkytojas turėtų įvertinti su duomenų tvarkymu susijusius pavojus ir imtis priemonių jam sumažinti. Duomenų konfidencialumo, vientisumo, prieinamumo ir atsparumo principas apibrėžia klasikinius duomenų saugumo kriterijus, kuriuos turi atitikti duomenų tvarkymo sistemos ir paslaugos, kurias teikiant tvarkomi duomenys. Duomenų valdytojai ir tvarkytojai turi užtikrinti, kad jų taikomos technologijos būtų saugios ne periodiškai, tam tikru laiku, o nuolat ir nepertraukiamai. Konfidencialumas reiškia, kad duomenų tvarkymo sistemos ir paslaugos negali leisti atskleisti duomenų ar panaudoti juos neturint leidimo. Pagal vientisumo reikalavimą, taikomos technologijos turi užtikrinti, kad duomenys nebūtų pakeisti. Prieinamumas reiškia, kad duomenų tvarkymo sistemos ir paslaugos turi apsaugoti duomenis nuo atsitiktinio arba neteisėto asmens duomenų sunaikinimo ar praradimo. Atsparumas reiškia duomenų tvarkymo sistemos gebėjimą užtikrinti ir išlaikyti priimtiną paslaugų kokybę nepaisant normalių sistemos veiklos trikdžių. Pagal duomenų saugumo priežiūros principą, iš duomenų valdytojų ir duomenų tvarkytojų reikalaujama neapsiriboti duomenų saugumo priemonių įgyvendinimu, nes turėtų būti vykdomas reguliarus duomenų saugumo priemonių tikrinimo, vertinimo ir veiksmingumo vertinimo procesas[82].

[81] ZALESKIS, J. (2019). Europos Sąjungos bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Vilnius: Registrų centras, p. 129.
[82] ZALESKIS, J. (2019). Europos Sąjungos bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Vilnius: Registrų centras, p. 130-131.

1.3. Asmens duomenų informatyvumas

Analizuojant asmens duomenų sąvokos, pateiktos Bendrajame duomenų apsaugos reglamente apibrėžimą, galima būtų išskirti kelis pagrindinius elementus:

- Informacija;
- Informacijos susisiejimas su konkrečiu asmeniu;
- Tapatybė[83] jau yra nustatyta arba gali būti nustatyta (tapatybės nustymas gali būti **tiesioginis** (pagal asmens vardą, pavardę, asmens kodą ir pan.) arba **netiesioginis** (pagal asmeniui būdingus fizinius, fiziologinius, protinius, kultūrinius, ekonominius, socialinius tapatybės veiksnius).

Terminas „bet kuri informacija“ aiškiai rodo teisės aktų leidėjų norą nustatyti plačią asmens duomenų sąvoką. Pažymėtina, kad informacijos samprata yra aiškinama per tris aspektus: pirma, analizuojant informacijos pobūdį, antra, analizuojant informacijos turinį, trečia, analizuojant informacijos formatą.

Analizuojant informacijos pobūdį, asmens duomenų sąvokos požiūriu, informacija apima visus teiginius apie asmenį, t. y., tiek objektyvią informaciją, pavyzdžiui, tam tikros medžiagos buvimas asmens kraujyje, ir subjektyvią informaciją – nuomones arba vertinimus. Pažymėtina, kad asmens duomenimis bus laikytina ne tik ta informacija, kuri yra objektyviai teisinga, bet taip pat ir netiksli informacija. Nors asmens duomenų apsaugos teisėje pripažįstama, kad asmens duomenimis bus laikoma neteisinga informacija, tačiau duomenų subjektui suteikiama teisė susipažinti su neteisinga informacija bei ją užginčyti naudojantis atitinkamomis priemonėmis[84].

Informacijos turinio aspektu, asmens duomenų sąvoka apima tokius duomenis, kuriais pateikiama visa galima informacija. Tai apima ir informaciją, kuri dėl savo turinio būtų priskiriama ypatingiems duomenims, ir bendro pobūdžio informaciją. Sąvoka „asmens duomenys“ apima informaciją, susijusią su asmens asmeniniu ir šeimos gyvenimu *stricto sensu*, taip pat informaciją apie visas asmens vykdomos veiklos rūšis, pavyzdžiui, asmens darbo santykius arba ekonominį ar socialinį elgesį. Taigi, asmens duomenimis informacijos turinio aspektu, laikytina bet kokia informacija apie bet kokį asmenį, neatsižvelgiant į jo esamą socialinę padėtį ar einamas pareigas

[83] Tapatybės sąvoka Lietuvos teisinėje sistemoje nėra apibrėžta, tačiau remiantis tarptautinių žodžių žodynu, tapatybė yra siejama su identitetu (Tarptautinių žodžių žodynas [interaktyvus]. Prieiga per internetą: https://tzz.lt/i/identifikuoti/ [žiūrėta 2020 m. spalio 22 d.]. Identitetas (lot. *Identitas*) apibrėžiamas kaip ko nors apibrėžtumas, individualumas, tapatybė, visiškas, iki smulkiausių detalių, sutapimas (Identitetas (lot. *Identitas*) apibrėžiamas kaip ko nors apibrėžtumas, individualumas, tapatybė, visiškas, iki smulkiausių detalių, sutapimas). Taigi, iš esmės tapatybė yra sutapatinama su identitetu.

[84] Europos Sąjungos 29 straipsnio duomenų apsaugos darbo grupės 2007 m. birželio 20 d. Nuomonė Nr. 4/2007 dėl asmens duomenų sąvokos Nr. WP 136, p. 6 [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_lt.pdf [žiūrėta 2020 m. rugsėjo 21 d.].

(kaip vartotojo, paciento, darbuotojo, kliento, kt.)[85]. Tokį aiškinimą iš esmės pagrindžia ir Europos Žmogaus Teisių Teismas, kuris 2000 m. vasario 16 d. byloje Amann prieš Šveicariją pažymėjo, jog termino „asmeninis gyvenimas“ negalima aiškinti siaurai. Visų pirma, asmeninio gyvenimo gerbimas yra teisė užmegzti ir plėtoti santykius su kitais žmonėmis; be to, nėra priežasčių, dėl kurių į asmeninio gyvenimo sąvoką neturėtų būti įtraukta veikla, susijusi su profesija ar verslu“[86]. Nors Europos Žmogaus Teisių Teismas pažymėjo, jog asmens duomenų sąvoka aiškinama plečiamai, tačiau pažymėtina, kad asmens duomenų apsaugos turinys yra kur kas platesnis, nei Europos Žmogaus Teisių Teismo plačiai aiškinama teisės į pagarbą asmeniniam ir šeimos gyvenimui sąvoka. Reikia pažymėti, kad Europos Sąjungos pagrindinių teisių chartija teisę į asmens duomenų apsaugą įtvirtina kaip savarankišką teisę (8 straipsnis), kuri yra atskirta ir skiriasi nuo 7 straipsnyje įtvirtintos teisės į privatų ir šeimos gyvenimą[87].

Informacijos formos aspektu, asmens duomenų sąvoka apima bet kokios formos informaciją, neatsižvelgiant į tai, kokiu būdu ji yra pateikiama, t. y. raidėmis, skaičiais, grafiniu, fotografiniu vaizdu ar garso forma. Tai gali būti tiek rašytinė informacija, tiek informacija pateikiama pasitelkiant informacines technologijas, pavyzdžiui, informacija, kuri yra saugoma kompiuterio atmintyje. Tai yra loginis automatinio asmens duomenų tvarkymo įtraukimo į jos taikymo sritį padarinys. Informacijos formos aspektas informacijos sampratą apibrėžia iš esmės todėl, jog tiek garsiniai, tiek vaizdiniai duomenys yra asmens duomenys nes jie gali suteikti informacijos apie asmenį. Būtina pastebėti, jog, tam, kad informacija būtų laikytina asmens duomenimis, nėra būtina, jog ji būtų įtraukta į susistemintą duomenų bazę ar rinkmeną[88]. Nemažai informacijos apie asmenį suteikia biometriniai duomenys. Jie priskiriami prie specialių kategorijų asmens duomenų, kurių tvarkymui keliami griežtesni reikalavimai. Asmens biometriniai duomenys, tai itin specifinė asmens duomenų grupė, susijusi su asmens fizinėmis, fiziologinėmis ar elgesio savybėmis[89]. Valstybinė duomenų apsaugos inspekcija biometrinius duomenis apibūdina kaip

[85] Europos Sąjungos 29 straipsnio duomenų apsaugos darbo grupės 2007 m. birželio 20 d. Nuomonė Nr. 4/2007 dėl asmens duomenų sąvokos Nr. WP 136, p. 7 [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_lt.pdf [žiūrėta 2020 m. rugsėjo 21 d.].
[86] Amann prieš Šveicariją [EŽTT], Nr. 27798/95, [2000-02-16]. ECLI:CE:ECHR: 2000:0216JUD002779895.
[87] Europos Sąjungos 2000 m. gruodžio 7 d. pagrindinių teisių chartija Nr. 2016/C 202/02, p. 391-405.
[88] Europos Sąjungos 29 straipsnio duomenų apsaugos darbo grupės 2007 m. birželio 20 d. Nuomonė Nr. 4/2007 dėl asmens duomenų sąvokos Nr. WP 136, p. 7 [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_lt.pdf [žiūrėta 2020 m. rugsėjo 21 d.].
[89] Teise.pro. Nuo „gero administravimo“ principo verslo reguliavime iki asmens biometrinių duomenų panaudojimo viešajame administravime. [interaktyvus]. Prieiga per internetą: http://www.teise.pro/index.php/2019/06/07/nuo-gero-administravimo-principo-verslo-reguliavime-iki-asmens-biometriniu-duomenu-panaudojimo-viesajame-administravime [žiūrėta 2020 m. lapkričio 12 d.].

konkrečius požymius, pagal kuriuos galima nustatyti unikalias žmogaus savybes, tokias kaip piršto atspaudas, akies rainelė, balsas, kuriais remiantis galima patvirtinti žmogaus tapatybę[90].

Biometriniai duomenys ypatingi tuo, kad juos galima laikyti ir informacijos apie konkretų asmenį turiniu (t. y. konkretaus asmens pirštų atspaudai), ir elementu, leidžiančiu nustatyti ryšį tarp informacijos ir asmens (šį daiktą lietė kažkas, kam priklauso šie pirštų atspaudai; šie pirštų atspaudai atitinka konkretaus asmens pirštų atspaudus, todėl šį daiktą lietė konkretus asmuo), todėl jie gali būti naudojami kaip žymenys. Atsižvelgiant į tai, kad tarp konkretaus asmens ir jo biometrinių duomenų yra sąsajumas, biometriniai duomenys gali būti naudojami asmens tapatybei nustatyti. Toks dvejopas pobūdis būdingas ir DNR duomenims, suteikiantiems informacijos apie asmens kūną ir leidžiantiems visiškai tiksliai nustatyti konkretų asmenį. Nors žmogaus audinio mėginiai yra biometrinių duomenų šaltinis, tačiau patys mėginiai nėra laikytini biometriniais duomenimis (pavyzdžiui, biometriniais duomenimis laikytini pirštų atspaudai, tačiau pats pirštas – ne). Atsižvelgiant į tai, informacijos gavimas iš mėginių yra asmens duomenų rinkimas, kuriam taikomos Bendrojo duomenų apsaugos reglamento taisyklės[91].

Dabartiniu laikotarpiu biometriniai duomenys kol kas plačiausiai naudojami teisėsaugos institucijų veikloje nusikalstamų veikų prevencijos ir atkleidimo tikslais, o biometrinių duomenų naudojimas viešojo administravimo institucijose sietinas pirmiausia su viešųjų paslaugų spektro išplėtimu, o ne su kontrolės funkcija. Kaip pavyzdys viešojo administravimo institucijų, kurios naudoja biometrinius asmens duomenis yra SODRA, plėtojanti e. paslaugas viešajame sektoriuje. Buvo atliktas tyrimas, kurio metu buvo analizuoti bendrieji biometrinių duomenų naudojimo sprendimai. Ar teisėtai naudojami biometriniai duomenys, patikrinimus atlieka Valstybinė duomenų apsaugos inspekcija. Pirmiausia reikia atsakyti į klausimus, ar tokia institucija gali tvarkyti tokio pobūdžio duomenis, nes netinkamas tvarkymas gali kelti grėsmę asmens duomenų ir privatumo apsaugai. Valstybinės duomenų apsaugos inspekcijos atstovai teigia, kad „biometrinių duomenų tvarkymas yra išskirtinis, nes tai unikalūs asmens duomenys, todėl, atsižvelgiant į galimas rizikas asmens privatumui ir duomenų apsaugai, kiekvienu konkrečiu atveju turi būti sprendžiama, ar tokių duomenų naudojimas yra pateisinamas. Kol kas nėra vienareikšmiškų atsakymų leisti ar drausti tvarkyti biometrinius duomenis atskirais atvejais, taip pat Europos Sąjungos šalys šiuo klausimu neturi vienodos praktikos, todėl keičiamės informacija ir ieškome tinkamiausių sprendimų“[92].

[90] Valstybinė duomenų apsaugos inspekcija. Biometrinių duomenų tvarkymas elektroninėje erdvėje [interaktyvus]. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents /files/RekomendBiometriniai2017.pdf [žiūrėta 2020 m. spalio 21 d.].

[91] Europos Sąjungos 29 straipsnio duomenų apsaugos darbo grupės 2007 m. birželio 20 d. Nuomonė Nr. 4/2007 dėl asmens duomenų sąvokos Nr. WP 136, p. 8 [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_lt.pdf [žiūrėta 2020 m. rugsėjo 21 d.].

[92] Valstybinė duomenų apsaugos inspekcija. Atliekami tikrinimai dėl biometrinių duomenų tvarkymo teisėtumo. [interaktyvus]. Prieiga per internetą: https://vdai.lrv.lt/lt/naujienos/atliekami-tikrinimai-del-biometriniu-duomenu-tvarkymo-teisetumo [žiūrėta 2020 m. spalio 12 d.].

Reikalinga akcentuoti, kad daugelis duomenų šiuo laikotarpiu yra tvarkomi debesijos[93] pagalba, todėl svarbu, kad būtų užtikrintas kibernetinis saugumas[94], apsisaugota nuo kibernetinių atakų, kurių metu gali būti pažeisti asmens duomenys.

Informacijos samprata aiškinama per pobūdį, turinį ir formatą ir apima visus teiginius apie asmenį, kuri gali būti objektyvi ir subjektyvi. Informacijos formos aspektu ypatingai svarbūs biometriniai duomenys, o jų tvarkymas viešojo sektoriaus institucijose ypatingai svarbus, atsakant į klausimą, ar išlaikoma pusiausvyra tarp poreikio tvarkyti asmens duomenis ir asmenų teisės į asmens duomenų apsaugą, ar įgyvendinama kibernetinio saugumo politika. Tam, kad viešajame sektoriuje būtų užtikrintas kibernetinis saugumas, turi būti apgalvotos tiek teisinės, tiek informacijos sklaidos, organizacinės bei techninės priemonės. Analizuojant valstybės įmonės Registrų centro sudaromas sutartis, pastebėtina, kad remiamasi patvirtintu aprašu, kuriame yra įtvirtinta, jog organizacinės ir techninės asmens duomenų saugumo priemonės įmonėje yra skirtos apsaugoti asmens duomenis nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo, užtikrina tokį saugumo lygį, kuris atitinka Registrų centro valdomų duomenų pobūdį ir jų tvarkymo keliamą riziką. Vadinasi, tvarkydamas asmens duomenis, Registrų centras į duomenų apsaugą turėtų atsižvelgti pradiniuose tokio planavimo etapuose. Registrų centras imasi visų būtinų techninių ir organizacinių veiksmų, kad įgyvendintų asmens duomenų apsaugą. Tam, kad standartizuotų parametrų nustatymus, visada reikėtų garantuoti, kad tokie parametrai padėtų užtikrinti kuo didesnę privatumo apsaugą. Reikėtų paminėti, kad tokia institucija, kaip valstybės įmonė Registrų centras, turi vadovautis Lietuvos Respublikos kibernetinio saugumo įstatymu, kuriame numatyta, kad „subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, sudaro sąlygas Nacionaliniam kibernetinio saugumo centrui diegti ir valdyti technines kibernetinio saugumo priemones valstybės informaciniuose ištekliuose ir taikyti technines priemones, siekiant

Informacijos sąsajumas su asmeniu yra laikytinas esminiu asmens duomenų sąvokos turinio elementu, nes yra svarbu tiksliai nustatyti konkrečius santykius (ryšius) tarp informacijos ir asmens bei tai, kaip juos tarpusavyje atskirti. Iš esmės pripažįstama, kad informacija yra susijusi su asmeniu tada, kai ji yra apie tą asmenį. Neretu atveju tokį informacijos ir asmens santykį galima pakankamai lengvai nustatyti. Pavyzdžiui, įstaigos personalo skyriaus turimoje asmens byloje įrašyti darbuotojo (valstybės tarnautojo) duomenys akivaizdžiai yra susiję su asmens kaip darbuotojo (valstybės

[93] Debesijos paslaugos įvardijamos kaip tokios paslaugos, kurių gavėjai nuotoliniu būdu naudojasi šių paslaugų teikėjų valdoma ryšių ir informacinių sistemų infrastruktūra (Lietuvos Respublikos kibernetinio saugumo įstatymas (2014). TAR, 20553).

[94] Teisės aktuose kibernetinis saugumas tai visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, kuriomis siekiama išlaikyti atsparumą veiksniams, kibernetinėje erdvėje keliantiems grėsmę ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, ryšių ir informacinių sistemų netrikdomam veikimui, valdymui arba paslaugų šiomis sistemomis teikimui, taip pat kuriomis siekiama atkurti įprastinę ryšių ir informacinių sistemų veiklą (Lietuvos Respublikos kibernetinio saugumo įstatymas (2014). TAR, 20553).

tarnautojo) statusu. Tokiais duomenimis bus laikomi ir paciento medicininių tyrimų rezultatai, esantys asmens medicininių įrašų kortelėje, arba asmens atvaizdas filmuoto pokalbio (konkurso) įraše. Kaip pavyzdys, viešojo sektoriaus įstaigos – valstybės įmonė Registrų centras, kuriame sudaromos sutartys su fiziniais ir juridiniais asmenimis, teikiant duomenis bei juos tvarkant[95]. Svarbu, kad būtų įgyvendinti teisėkūros principai, t. y. asmenims teikiami duomenys taip, kaip numato teisės aktai, tačiau nebūtų teikiami pertekliniai duomenys ar asmeniui pagal vykdomą veiklą nepriklausantys duomenys. Tam, kad būtų tinkama asmens duomenų apsauga, tokiose viešojo sektoriaus įstaigose yra priimami atitinkami teisės aktai.

Konkrečiai Registrų centro atveju, 2018 m. gegužės 24 d. direktoriaus įsakymu Nr. v-171[96], patvirtintas asmens duomenų tvarkymo valstybės įmonėje Registrų centre tvarkos aprašas. Šiame apraše įtvirtinti šioje įstaigoje tvarkomi asmenys duomenys, asmens duomenų tvarkymo tikslai, asmens duomenų tvarkymo terminai. Registrų centras, kaip duomenų valdytojas, tiek nustatydamas duomenų tvarkymo priemones, tiek paties duomenų tvarkymo metu, įgyvendina tinkamas technines ir organizacines asmens duomenų saugumo priemones atsižvelgdamas į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas bei duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat į duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms. Šiomis priemonėmis siekiama veiksmingai įgyvendinti asmens duomenų apsaugos principus ir į duomenų tvarkymą integruoti būtinas apsaugos priemones, kad duomenų tvarkymas atitiktų Reglamento (ES) 2016/679 reikalavimus ir būtų apsaugotos duomenų subjektų teisės[97]. Analizuojant šį aprašą pastebima, kokių priemonių yra imamasi, kad būtų apsaugoti asmens duomenis juos teikiant bei kokių priemonių imamasi dėl darbuotojų, kurie dirba su tokiais asmens duomenimis. Pagal šį aprašą, prieiga prie asmens duomenų gali būti suteikta tik tam Registrų centro darbuotojui, kuriam asmens duomenys yra reikalingi jo funkcijoms vykdyti ir galima atlikti tik tuos veiksmus, kuriems atlikti darbuotojui yra suteiktos teisės. Vadinasi, toks darbuotojas turi laikytis asmens duomenų tvarkymo saugumo reikalavimų, įtvirtintų Bendrajame duomenų apsaugos reglamente, Asmens duomenų teisinės apsaugos įstatyme, minėtame apraše bei kituose teisės

[95] Duomenų tvarkymas – bet kokia automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis ar asmens duomenų rinkiniais atliekama operacija ar operacijų seka, kaip antai rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, išgava, *susipažinimas*, naudojimas, *atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis,* taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimas arba sunaikinimas (Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) Nr. 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) OL 2016 L 19, p. 1-88).

[96] Valstybės įmonės Registrų centro 2018 m. gegužės 24 d. direktoriaus įsakymas Nr. v-171 „Dėl asmens duomenų tvarkymo valstybės įmonėje Registrų centre tvarkos aprašo patvirtinimo“ [interaktyvus]. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/ TAD/1804741065d311e8b7d2b2d2ca774092/asr [žiūrėta 2020 m. lapkričio 10 d.].

[97] Valstybės įmonės Registrų centro 2018 m. gegužės 24 d. direktoriaus įsakymas Nr. v-171 „Dėl asmens duomenų tvarkymo valstybės įmonėje Registrų centre tvarkos aprašo patvirtinimo“ [interaktyvus]. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/ TAD/1804741065d311e8b7d2b2d2ca774092/asr [žiūrėta 2020 m. lapkričio 10 d.].

aktuose. Tokie darbuotojai privalo pasirašyti konfidencialumo pasižadėjimą, kurio formą ir turinį įsakymu tvirtina Registrų centro generalinis direktorius, o tokiu pasižadėjimu darbuotojas pasižada „neatskleisti, neperduoti ir nesudaryti sąlygų bet kokiomis priemonėmis susipažinti su asmens duomenimis nė vienam asmeniui, kuris nėra įgaliotas tvarkyti asmens duomenis“[98].

Paminėtina, kad pasitaiko atvejų, kai nepavyksta lengvai nustatyti, ar informacija yra susijusi su asmeniu. Tam tikrais atvejais iš duomenų gaunama informacija pirmiausia tiesiogiai siejasi su objektais, o ne su asmenimis. Tie objektai paprastai kam nors priklauso, jiems asmenys gali daryti tam tikrą poveikį arba jie gali daryti tam tikrą poveikį asmenims, taip pat objektai gali būti fizine ar geografine prasme artimi asmenims arba kitiems objektams. Tokiais atvejais galima laikyti, kad informacija su tais asmenimis arba objektais susijusi netiesiogiai. Atkreiptinas dėmesys, kad Europos Sąjungos 29 straipsnio duomenų apsaugos darbo grupė pažymėjo, jog tam, kad duomenys būtų laikomi susijusiais su asmeniu, turi būti nustatytas turinio elementas arba tikslo elementas, arba rezultato elementas[99].

Turinio elementą iš esmės apibrėžia visuomenei bendrai suprantamo žodžio „susijęs“ reikšmė, kas reiškia, jog informacija yra susijusi su asmeniu, kai ji yra apie tą asmenį, o tai turi būti įvertinta atsižvelgiant į visas konkretaus atvejo aplinkybes[100]. Pavyzdžiui, įstaigoje dirbančių darbuotojų (valstybės tarnautojų) vedamose asmens bylose saugoma informacija yra aiškiai susijusi su tuo darbuotoju (valstybės tarnautoju), taip pat asmens prašyme, kuris pagal kompetenciją adresuojamas valstybės institucijai, nurodyta informacija apie asmenį taip pat yra aiškiai susijusi su besikreipiančiu į valstybės instituciją.

Tikslo elementas nustatomas, kai atsižvelgiant į visas konkretaus atvejo aplinkybes duomenys naudojami arba greičiausiai bus naudojami siekiant įvertinti arba nagrinėti asmens padėtį ar elgesį arba daryti jiems įtaką. Atvejais, kai nėra nustatomas nei turinio, nei tikslo elementas, duomenys gali būti laikomi susijusiais su asmeniu, kai yra nustatomas rezultato elementas. Esant rezultato elementui, duomenis galima laikyti susijusiais su asmeniu, nes naudojantis jais greičiausiai būtų daromas poveikis konkretaus asmens teisėms ir interesams, tačiau vis tiek yra būtina atsižvelgti į visas konkretaus atvejo aplinkybes. Pastebėtina, jog nėra būtina, kad galimas poveikis būtų didelis,

[98] Valstybės įmonės Registrų centro 2018 m. gegužės 24 d. direktoriaus įsakymas Nr. v-171 „Dėl asmens duomenų tvarkymo valstybės įmonėje Registrų centre tvarkos aprašo patvirtinimo“ [interaktyvus]. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/ TAD/1804741065d311e8b7d2b2d2ca774092/asr [žiūrėta 2020 m. lapkričio 10 d.].

[99] Europos Sąjungos 29 straipsnio duomenų apsaugos darbo grupės 2007 m. birželio 20 d. Nuomonė Nr. 4/2007 dėl asmens duomenų sąvokos Nr. WP 136, p. 10 [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_lt.pdf [žiūrėta 2020 m. rugsėjo 21 d.].

[100] Europos Sąjungos 29 straipsnio duomenų apsaugos darbo grupės 2007 m. birželio 20 d. Nuomonė Nr. 4/2007 dėl asmens duomenų sąvokos Nr. WP 136, p. 10 [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_lt.pdf [žiūrėta 2020 m. rugsėjo 21 d.].

pakanka fakto, kad dėl tokių duomenų tvarkymo su asmeniu galėtų būti elgiamasi kitaip nei su kitais[101].

Atkreiptinas dėmesys, kad šiuos tris elementus (turinį, tikslą, rezultatą) reikia laikyti alternatyviomis sąlygomis. Visų pirma, jeigu yra turinio elementas, kiti elementai nebūtini, kad informacija būtų laikoma susijusia su asmeniu. Dėl to, ta pati informacija vienu metu gali būti susijusi su skirtingais asmenimis, priklausomai nuo kiekvieno asmens atžvilgiu egzistuojančio elemento. Pavyzdžiui, ta pati informacija gali būti susijusi su konkrečiu asmeniu dėl turinio elemento (duomenys akivaizdžiai yra apie konkretų asmenį) ir tuo pačiu metu susijusi su kitu asmeniu dėl tikslo elemento (jie bus naudojami siekiant atitinkamai elgtis su šiuo asmeniu) ir taip pat su dar kitu asmeniu dėl rezultato elemento (tikėtina, kad jie turės įtakos šio asmens teisėms ir interesams)[102]. Pavyzdžiui, įstaigos darbuotojas teikia atostogų prašymą, kuris yra talpinamas įstaigos dokumentų valdymo sistemoje. Atostogų prašyme darbuotojas, be kita ko, nurodo atostogų metu jį pavaduosiantį asmenį. Tokiu būdu informacija darbuotojo atostogų prašyme su darbuotoju siejasi dėl turinio elemento, o su šį darbuotoją pavaduosiančiu asmeniu dėl tikslo elemento. Vadinasi, tam, kad informacija būtų laikoma susijusia su konkrečiu asmeniu, nėra būtina reikalauti, jog duomenys būtų sutelkti į konkretų asmenį.

Vienas iš svarbiausių elementų – tapatybė. Lietuvos Respublikos asmens tapatybės kortelės ir paso įstatyme įtvirtinta, kad „asmens tapatybės kortelė ir pasas yra Lietuvos Respublikos piliečio asmens dokumentai, patvirtinantys jo asmens tapatybę ir pilietybę“[103]. Asmens tapatybę patvirtinančiuose dokumentuose įrašomi šie duomenys apie pilietį: vardas (vardai); pavardė; lytis; gimimo data; asmens kodas; pilietybė.

Be to, asmens tapatybę patvirtinančiuose dokumentuose įrašoma piliečio gimimo vieta bei yra piliečio veido atvaizdas ir piliečio parašas. Taigi, fizinio asmens tapatybė nustatoma, jeigu jis yra išskiriamas iš visų kitų grupei priklausančių asmenų, remiantis tam tikrais identifikatoriais, tokiais kaip: vardas (vardai), pavardė, lytis, gimimo data, asmens kodas, pilietybė. Fizinio asmens tapatybė gali būti nustatoma ne tik remiantis identifikatoriais, išskiriančiais asmenį iš kitų grupių asmenų, bet ir remiantis konkrečia informacija, kuri yra labai išskirtinai ir glaudžiai susijusi su konkrečiu asmeniu. Tai gali būti to asmens išvaizdos požymiai, pavyzdžiui, ūgis, plaukų spalva, apranga ir kt., arba asmens ypatybė, kuri leidžia sutapatinti šią informaciją su konkrečiu asmeniu,

[101] Europos Sąjungos 29 straipsnio duomenų apsaugos darbo grupės 2007 m. birželio 20 d. Nuomonė Nr. 4/2007 dėl asmens duomenų sąvokos Nr. WP 136, p. 10 [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_lt.pdf [žiūrėta 2020 m. rugsėjo 21 d.].
[102] Europos Sąjungos 29 straipsnio duomenų apsaugos darbo grupės 2007 m. birželio 20 d. Nuomonė Nr. 4/2007 dėl asmens duomenų sąvokos Nr. WP 136, p. 10 [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_lt.pdf [žiūrėta 2020 m. rugsėjo 21 d.].
[103] Lietuvos Respublikos asmens tapatybės kortelės ir paso įstatymas (2014). TAR, 21281.

pavyzdžiui, profesija ar užimamos pareigos[104]. Bendrajame duomenų apsaugos reglamente tie „žymenys tapatybei nustatyti“ minimi 4 straipsnyje, apibrėžiančiame asmens duomenų sąvoką: „tapatybė gali būti nustatyta tiesiogiai ar netiesiogiai, ypač pasinaudojus identifikatoriumi“[105]. Taigi, asmens tapatybė gali būti nustatoma tiesiogiai, arba netiesiogiai. Kalbant apie asmenis, kurių tapatybė yra arba gali būti nustatyta tiesiogiai, asmens vardas ir pavardė yra pats įprasčiausias žymuo tapatybei nustatyti. Vardas ir pavardė taip pat gali būti atskaitos taškas ieškant informacijos apie tai, kur asmuo gyvena arba kur jį galima rasti. Taip pat vardas ir pavardė gali suteikti informacijos apie šeimos narius (pagal pavardę) ir daug su tuo vardu ir pavarde susijusių teisinių bei socialinių santykių (įrašai apie išsilavinimą, medicininiai įrašai, banko sąskaitos)[106].

Kalbant apie asmenis, kurių tapatybė yra arba gali būti nustatyta netiesiogiai, ši kategorija paprastai susijusi su mažos arba didelės apimties unikalių junginių reiškiniu. Kai *prima facie* turimų žymenų tapatybei nustatyti nepakanka konkrečiam asmeniui išskirti, asmens tapatybę galima nustatyti, kai šie *prima facie* turimi žymenys sudedami su kita informacija. Tokiu būdu bus įmanoma išskirti tą asmenį iš kitų. Kai kurios asmenį identifikuojančios savybės yra tokios ypatingos, kad nustatyti tam tikrų asmenų tapatybę nėra sudėtinga. Tam tikrų duomenų pagal kategoriją (amžius, kilmės regionas ir t. t.) derinys taip pat gali gana daug lemti susidarius tam tikroms aplinkybėms, visų pirma, jeigu yra galimybė pasinaudoti tam tikra papildoma informacija[107]. Elektroninėse asmens duomenų registravimo rinkmenose registruojamiems asmenims paprastai suteikiamas unikalus kodas tapatybei nustatyti, tam, kad nebūtų supainioti rinkmenoje įregistruoti asmenys. Be to, internete asmens tapatybė gali būti nustatoma remiantis interneto protokolo IP adresu, pirkimo ir pirkinių istorija, asmens lankomų interneto puslapių istorija ir pan.

Taigi, asmens duomenys apima informaciją apie fizinius asmenis, kurie identifikuojami arba gali būti identifikuoti tiesiogiai iš atitinkamos informacijos, tačiau neapsiribojant gebėjimu žinoti asmens vardą ir pavardę. Asmenys taip pat gali būti netiesiogiai identifikuojami iš turimos informacijos kartu su kita informacija, t. y. skirtinga informacija, kuri surinkta kartu gali atskleisti konkretaus asmens tapatybę.

---

[104] Europos Sąjungos 29 straipsnio duomenų apsaugos darbo grupės 2007 m. birželio 20 d. Nuomonė Nr. 4/2007 dėl asmens duomenų sąvokos Nr. WP 136, p. 12 [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_lt.pdf [žiūrėta 2020 m. rugsėjo 21 d.].

[105] Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) Nr. 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) OL 2016 L 19, p. 1-88.

[106] Europos Sąjungos 29 straipsnio duomenų apsaugos darbo grupės 2007 m. birželio 20 d. Nuomonė Nr. 4/2007 dėl asmens duomenų sąvokos Nr. WP 136, p. 13 [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_lt.pdf [žiūrėta 2020 m. rugsėjo 21 d.].

[107] Europos Sąjungos 29 straipsnio duomenų apsaugos darbo grupės 2007 m. birželio 20 d. Nuomonė Nr. 4/2007 dėl asmens duomenų sąvokos Nr. WP 136, p. 14 [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_lt.pdf [žiūrėta 2020 m. rugsėjo 21 d.].

1.4. Duomenų saugumo priemonių ypatumai

Bendrajame duomenų apsaugos reglamente įtvirtinta, jog siekiant užtikrinti saugumą ir užkirsti kelią šį reglamentą pažeidžiančiam duomenų tvarkymui, duomenų valdytojas arba duomenų tvarkytojas, atsižvelgdamas į duomenų tvarkymo pobūdį, aprėptį, kontekstą bei tikslus, taip pat į įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, turi įgyvendinti tinkamas technines ir organizacines priemones, kad užtikrintų ir galėtų įrodyti, kad duomenys tvarkomi laikantis šio reglamento reikalavimų[108]. Nors Bendrasis duomenų apsaugos reglamentas įtvirtina pareigą duomenų valdytojui bei duomenų tvarkytojui duomenų tvarkymui pasitelkti tinkamas technines ir organizacines priemones, tačiau Bendrasis duomenų apsaugos reglamentas neįtvirtina konkrečių techninių standartų, kurie nurodytų, kas yra laikytina tinkamu techniniu ar organizaciniu duomenų saugumu. Atsižvelgiant į tai, aktualių ir konkrečių duomenų saugumo standartų kūrimas yra paliekamas kompetentingoms institucijoms[109]. Pavyzdžiui, Europos Sąjungos tinklų ir informacijos saugumo agentūra paskelbė rekomendaciją dėl techninių ir organizacinių priemonių asmens duomenų tvarkymo saugumo srityje[110], kurios pagrindu Valstybinė duomenų apsaugos inspekcija parengė tinkamų organizacinių ir techninių duomenų saugumo priemonių įgyvendinimo gaires asmens duomenų valdytojams ir tvarkytojams. Šiose gairėse inspekcija rekomenduoja 20 minimalių organizacinių ir techninių duomenų saugumo reikalavimų, pakankamų tose organizacijose, kurių tvarkomų asmens duomenų saugumo rizika, susijusi su pavojais fizinių asmenų teisėms ir laisvėms, yra žema. Tai reiškia, jog gairėse išdėstytus reikalavimus privalo įgyvendinti kiekviena asmens duomenis tvarkanti įstaiga, o daugelis imtis ir papildomų priemonių, kad užtikrintų tinkamą tvarkomų asmens duomenų saugumo lygį. Organizacinės duomenų saugumo priemonės yra susijusios su tuo, kaip organizacija yra įsteigta ir vykdo veiklą. Valstybinė duomenų apsaugos inspekcija organizacinėms duomenų saugumo priemonėms priskiria: pirma, *asmens duomenų saugumo politiką ir procedūras*. Pripažįstama, kad saugumo politika yra svarbus dokumentas, nustatantis pagrindinius informacijos saugumo ir asmens duomenų apsaugos principus institucijoje. Tai yra visų konkrečių techninių ir organizacinių priemonių įgyvendinimo pagrindas pagal Bendrojo duomenų apsaugos reglamento 32 straipsnį. Remiantis saugumo politika, konkrečios techninės ir organizacinės priemonės aprašomos detalesnėse politikose (pavyzdžiui, prieigos

[108] Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) Nr. 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) OL 2016 L 19, p. 1-88.

[109] ZALESKIS, J. (2019). Europos Sąjungos bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Vilnius: Registrų centras, p. 129.

[110] European Union Agency For Network and Information Security. Handbook on Security of Personal Data Processing. (2018). [interaktyvus]. Prieiga per internetą: https://op.europa.eu/lt/publication-detail/-/publication/1a860879-1dce-11e8-ac73-01aa75ed71a1 [Žiūrėta 2020 m. rugsėjo 26 d.].

kontrolės, įrenginių valdymo, išteklių valdymo ir kt.); antra, *vaidmenis ir atsakomybę*. Bendrasis duomenų apsaugos reglamentas numato, kad duomenų valdytojas ir duomenų tvarkytojas imasi priemonių, siekdami užtikrinti, kad bet kuris duomenų valdytojui arba duomenų tvarkytojui pavaldus fizinis asmuo, galintis susipažinti su asmens duomenimis, jų netvarkytų, išskyrus atvejus, kai duomenų valdytojas duoda nurodymus juos tvarkyti, nebent tas asmuo privalo tai daryti pagal Europos Sąjungos arba valstybės narės teisę. Pagrindinė asmens duomenų saugumo priemonė organizacijos personalui, turinčiam prieigą prie asmens duomenų – aiškiai apibrėžta ir dokumentuota atsakomybė bei vaidmenys, taip pat darbo su asmens duomenimis kompetencijos. Ypač svarbus vaidmuo tenka duomenų apsaugos pareigūnui, kuris prižiūri, kaip laikomasi Bendrojo duomenų apsaugos reglamento nuostatų; trečia, *prieigos valdymo politiką*. Būtina nustatyti prieigos kontrolės politiką sistemoms, naudojamoms tvarkant asmens duomenis. Kontrolė turi būti grindžiama principu „būtina žinoti“, t. y. kiekvienam vaidmeniui ar naudotojui turėtų būti suteiktas tik toks asmens duomenų prieinamumo lygis, kuris yra būtinas jo užduotims atlikti. Šis reikalavimas glaudžiai susijęs su duomenų kiekio mažinimo principu[111]. Autorės nuomone, šios priemonės įgyvendinimo problema gali ryškėti tais atvejais, kai įstaigos darbuotoją, kuriam, yra suteiktas tam tikros apimties duomenų prieinamumo lygis, jo atostogų ar laikino nedarbingumo metu pavaduoja kitas darbuotojas, kuriam suteiktas duomenų prieinamumo lygis yra kur kas mažesnis, nei darbuotojo, kurį jis pavaduoja; ketvirta, *išteklių ir turto valdymą*. Tinkamas techninės, programinės ir tinklo įrangos valdymas yra būtinas asmens duomenų saugumui ir vientisumui, nes tai leidžia kontroliuoti duomenų apdorojimo priemones. Išteklių valdymas būtinai turi apimti informacinių technologijų išteklių ir tinklo topologijos, kuri yra naudojama tvarkant asmens duomenis, registravimą; penkta, *pakeitimų valdymą*. Pakeitimų valdymo tikslas – sinchronizuoti ir kontroliuoti visus informacinių technologijų sistemose, naudojamose tvarkant asmens duomenis, atliekamus pakeitimus. Tai yra svarbi saugumo priemonė, nes nesėkmingas pakeitimų įgyvendinimas gali sukelti neteisėtą duomenų atskleidimą, pakeitimą ar sunaikinimą. Pakeitimų valdymas yra būtinas duomenų tvarkymo vientisumui užtikrinti ir duomenų valdytojo atskaitomybės principui įgyvendinti; šešta, *duomenų tvarkytojus*. Bendrojo duomenų apsaugos reglamento 28 straipsnis numato, kad „duomenų valdytojas pasitelkia tik tuos duomenų tvarkytojus, kurie pakankamai užtikrina, kad tinkamos techninės ir organizacinės priemonės bus įgyvendintos tokiu būdu, kad duomenų tvarkymas atitiktų šio reglamento reikalavimus ir būtų užtikrinta duomenų subjekto teisių apsauga“[112]. Tame pačiame

[111] Valstybinė duomenų apsaugos inspekcija. 2018 m. spalio 31. Tinkamų organizacinių ir techninių duomenų saugumo priemonių įgyvendinimo gaires asmens duomenų valdytojams ir tvarkytojams [interaktyvus]. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomendtechpriemonesgaires2018.pdf [žiūrėta 2020 m. rugsėjo 27 d.].
[112] Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) Nr. 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) OL 2016 L 19, p. 1-88.

straipsnyje teigiama, kad duomenų tvarkytojas turi veikti pagal sutartį ar kitą teisės aktą. Šios priemonės įgyvendinimą valstybės institucijos dažnu atveju įgyvendina valstybės tarnautojų ir darbuotojų, dirbančių pagal darbo sutartis, pareigybių aprašymuose įtvirtindamos reikalavimą išmanyti ir gebėti taikyti praktikoje teisės aktus, reguliuojančius dokumentų valdymą, tvarkymą ir saugojimą. Pavyzdžiui, Valstybinės vartotojų teisių apsaugos tarnybos Vidaus administravimo skyriaus vyriausiojo specialisto pareigybės aprašyme įtvirtinta, jog „darbuotojas, einantis šias pareigas, turi išmanyti ir gebėti pagal kompetenciją savo darbe taikyti <...> teisės aktus, reglamentuojančius dokumentų ir archyvų valdymą, elektroninių dokumentų valdymą, reikalingus darbo funkcijoms vykdyti <...>“[113]; septinta, *asmens duomenų saugumo pažeidimus ir incidentus*. Duomenų saugumo pažeidimo atveju organizacija turi įvertinti, ar tai turės įtakos „atsitiktiniam ar neteisėtam perduodamų, saugomų ar kitaip tvarkomų asmens duomenų sunaikinimui, praradimui, pakeitimui, neteisėtam atskleidimui ar prieigai prie jų“[114]. Duomenų valdytojai turi būti tikri, kad jie laikosi savo įsipareigojimų pagal Bendrojo duomenų apsaugos reglamento nuostatas, susijusias su pranešimu apie asmens duomenų saugumo pažeidimus priežiūros institucijai ir duomenų subjektams. Duomenų tvarkytojai taip pat turi būti tikri, kad jie laikosi savo įsipareigojimų pagal Bendrąjį duomenų apsaugos reglamentą ir galės nedelsdami pranešti duomenų valdytojui apie minėtus pažeidimus. Bet kuriuo atveju, tiek duomenų valdytojai, tiek ir tvarkytojai turi turėti tinkamas procedūras ne tik pranešti apie asmens duomenų pažeidimus, bet ir juos suvaldyti; aštunta, *veiklos tęstinumą*. Veiklos ar paslaugų tęstinumo planas yra būtinas nustatant procesus ir technines priemones, kurių organizacija turėtų laikytis incidento ar asmens duomenų pažeidimo atveju. Šis planas papildo organizacijos saugumo politiką[115]. Ši priemonė aiškiai susijusi su Bendrojo duomenų apsaugos reglamento 32 straipsnio 1 dalies c punktu, kuris įpareigoja duomenų valdytoją ir tvarkytoją „laiku atkurti sąlygas ir galimybes naudotis asmens duomenimis fizinio ar techninio incidento atveju“[116]; devinta, *personalo konfidencialumą*. Siekiant užtikrinti asmens duomenų konfidencialumą, įstaiga turi užtikrinti, kad jos darbuotojai gebėtų konfidencialiai tvarkyti informaciją tiek techniniu, tiek asmeninio sąžiningumo požiūriu. Be to, Bendrojo duomenų apsaugos

[113] Valstybinė vartotojų teisių apsaugos tarnyba. Padalinių uždaviniai ir funkcijos (tinklalapio internete skiltis) [interaktyvus]. Prieiga per internetą: http://www.vvtat.lt/struktura-ir-kontaktai/padaliniu-uzdaviniai-ir-funkcijos/596/vidaus-administravimo-skyrius/d51 [žiūrėta 2020 m. spalio 12 d.].

[114] Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) Nr. 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) OL 2016 L 19, p. 1-88.

[115] Valstybinė duomenų apsaugos inspekcija. 2018 m. spalio 31. Tinkamų organizacinių ir techninių duomenų saugumo priemonių įgyvendinimo gaires asmens duomenų valdytojams ir tvarkytojams [interaktyvus]. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomendtechpriemonesgaires2018.pdf [žiūrėta 2020 m. rugsėjo 27 d.].

[116] Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) Nr. 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) OL 2016 L 19, p. 1-88.

reglamento 32 straipsnio 4 dalis numato, kad „duomenų valdytojas ir duomenų tvarkytojas imasi priemonių, siekdami užtikrinti, kad bet kuris duomenų valdytojui arba duomenų tvarkytojui pavaldus fizinis asmuo, galintis susipažinti su asmens duomenimis, jų netvarkytų, išskyrus atvejus, kai duomenų valdytojas duoda nurodymus juos tvarkyti, nebent tas asmuo privalo tai daryti pagal Sąjungos arba valstybės narės teisę“. Šiuo tikslu turėtų būti nustatytos specialios priemonės, užtikrinančios, kad asmenys, dalyvaujantys tvarkant asmens duomenis, būtų tinkamai informuojami apie savo pareigą laikytis konfidencialumo. Praktikoje ši priemonė dažnu atveju įgyvendinama valstybės institucijos darbuotojus įpareigojant pasirašyti konfidencialumo pasižadėjimus. Pavyzdžiui, Valstybinės teismo medicinos tarnybos prie Lietuvos Respublikos teisingumo ministerijos (toliau – Valstybinė teismo medicinos tarnyba) direktoriaus patvirtintas Konfidencialios informacijos nustatymo ir naudojimo bei konfidencialumo laikymosi tvarkos aprašas įpareigoja asmenis, atliekančiu darbo funkcijas pagal darbo arba paslaugų teikimo sutartį, sudarytą su įstaiga, laikytis konfidencialumo reikalavimų bei pasirašyti konfidencialumo laikymosi pasižadėjimą;[117] dešimta, *mokymus*. Kiekviena valstybės institucija turi užtikrinti, kad visi darbuotojai būtų tinkamai informuoti apie informacinių sistemų saugumo kontrolę, susijusią su jų kasdieniu darbu. Personalo mokymai apie asmens duomenų apsaugos ir saugumo procedūras (pavyzdžiui, slaptažodžių naudojimas ir prieiga prie konkrečių sistemų) yra svarbūs tinkamam organizacinių ir techninių saugumo priemonių įgyvendinimui ir prevencijai dėl netyčinio duomenų sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jų (Bendrojo duomenų apsaugos reglamento 32 straipsnio 2 dalis)[118].

Techninių duomenų saugumo priemonių sąvoka apima mechanizmus, įrangą ir įrankius, skirtus užtikrinti informacijos saugumą[119]. Valstybinė duomenų apsaugos inspekcija organizacinėms duomenų saugumo priemonėms priskiria: pirma, *prieigų kontrolę ir autentifikavimą*. Prieigų kontrolė ir autentifikavimas yra esminiai saugos reikalavimai, siekiant apsisaugoti nuo neautorizuotos prieigos prie informacinės sistemos, kurioje yra apdorojami asmens duomenys. Šie saugos reikalavimai įgyvendina įstaigos prieigų kontrolės politiką. Pavyzdžiui, Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos (toliau – Socialinės apsaugos ir darbo ministerija) asmens duomenų apsaugos politikos, patvirtintoje Lietuvos Respublikos socialinės apsaugos ir darbo ministro 2018 m. spalio 31 d. įsakymu Nr. A1-610 „Dėl Lietuvos Respublikos

[117] Valstybinė teismo medicinos tarnyba prie Lietuvos Respublikos teisingumo ministerijos. Tvarkų aprašai, taisyklės, nuostatai (tinklalapio internete skiltis) [interaktyvus]. Prieiga per internetą: http://www.vtmt.lt/media/PDF_bylos/Konf.informacijos%20tvarka.pdf [žiūrėta 2020 m. spalio 10 d.].
[118] Valstybinė duomenų apsaugos inspekcija. 2018 m. spalio 31. Tinkamų organizacinių ir techninių duomenų saugumo priemonių įgyvendinimo gaires asmens duomenų valdytojams ir tvarkytojams [interaktyvus]. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomendtechpriemonesgaires2018.pdf [žiūrėta 2020 m. rugsėjo 27 d.].
[119] ZALESKIS, J. (2019). Europos Sąjungos bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Vilnius: Registrų centras, p. 132.

socialinės apsaugos ir darbo ministerijos asmens duomenų apsaugos politikos patvirtinimo“ (toliau – Asmens duomenų politika) 71.1 punkte įtvirtinta, jog atsakingi darbuotojai prieigai prie asmens duomenų naudoja unikalius slaptažodžius, kurie reguliariai keičiami ir saugomi užtikrinant jų konfidencialumą[120]; antra, *techninių žurnalų įrašai ir stebėsena*. Techninių žurnalų įrašai yra esminis saugos reikalavimas, kuris leidžia identifikuoti ir stebėti, sekti naudotojų veiksmus (kurie susiję su asmens duomenų apdorojimu), taip užtikrinant atskaitingumą (jei įvyktų neautorizuotas asmens duomenų atskleidimas, keitimas ar panaikinimas). Taip pat svarbu nuolat stebėti techninių žurnalų įrašus, kurie leistų identifikuoti potencialius vidinius ar išorinius bandymus pažeisti sistemos saugumą ir integralumą; trečia, *tarnybinių stočių, duomenų bazių apsauga*. Informacinių sistemų pagrindas yra tarnybinės stotys ir duomenų bazės. Jų apsauga privalo būti sustiprinta, siekiant užtikrinti saugią darbo aplinką; ketvirta, *darbo stočių apsauga*. Šis reikalavimas yra susijęs su saugos nustatymais naudotojų darbo stotyse ar kituose įrenginiuose. Yra svarbu priverstinai nustatyti specifinę saugos politiką ir apriboti naudotojų veiksmus, siekiant apsaugoti informacines sistemas (pavyzdžiui, antivirusinės programinės įrangos išjungimas, neautorizuotos programinės įrangos diegimas ir pan.); penkta, *tinklo ir komunikacijos sauga*. Tinklo ir komunikacijos sauga yra ypač svarbi, siekiant užtikrinti asmens duomenų saugą (tiek vidinių, tiek išorinių tinklų)[121]. Bendrojo duomenų apsaugos reglamento 32 straipsnis numato, kad „atsižvelgdamas į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas bei duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas ir duomenų tvarkytojas įgyvendina tinkamas technines ir organizacines priemones, kad būtų užtikrintas pavojų atitinkančio lygio saugumas, įskaitant *inter alia*, jei reikia: pseudonimų suteikimą asmens duomenims ir jų šifravimą; gebėjimą užtikrinti nuolatinį duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą“[122]. Pseudonimų suteikimas yra toks duomenų tvarkymas, kuomet duomenys nebegali būti priskirti konkrečiam duomenų subjektui neturint papildomos informacijos, jeigu tokia papildoma informacija yra saugoma atskirai ir jai taikomos techninės ir organizacinės priemonės siekiant užtikrinti asmens duomenų nepriskyrimą fiziniam asmeniui, kurio tapatybė yra arba gali būti nustatyta (Bendrojo duomenų apsaugos reglamento 4 straipsnio 5 punktas). Duomenų šifravimą

[120] Lietuvos Respublikos socialinės apsaugos ir darbo ministro 2018 m. spalio 31 d. įsakymas Nr. A1-610 „Dėl Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos asmens duomenų apsaugos politikos patvirtinimo“ [interaktyvus]. Prieiga per internetą: https://socmin.lrv.lt/uploads/socmin/documents/files/administracine-informacija/Asmens%20duomenu%20apsauga/Politika.pdf [žiūrėta 2020 m. spalio 12 d.].

[121] Valstybinė duomenų apsaugos inspekcija. 2018 m. spalio 31. Tinkamų organizacinių ir techninių duomenų saugumo priemonių įgyvendinimo gaires asmens duomenų valdytojams ir tvarkytojams [interaktyvus]. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomendtechpriemonesgaires2018.pdf [žiūrėta 2020 m. rugsėjo 27 d.].

[122] Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) Nr. 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) OL 2016 L 19, p. 1-88.

galima laikyti viena iš duomenų pseudonimizavimo formų. Tai duomenų saugumo technika, kurią taikant duomenys tampa nesuprantami asmenims, neturintiems leidimo su jais susipažinti ir leidžianti juos atkurti tik slaptu dešifravimo raktu;[123] šešta, *atsarginės kopijos*. Atsarginių kopijų sistema yra esminis veiksnys, užtikrinantis įstaigos darbo ir procesų atstatymą, įvykus duomenų praradimui ar sugadinimui. Duomenų kopijų darymo dažnumas ir poreikis priklauso nuo organizacijos ir joje apdorojamų duomenų; septinta, *mobilieji, nešiojami įrenginiai*. Mobilieji, nešiojami įrenginiai gali išplėsti paslaugas, kurias teikia duomenų valdytojas, tačiau padidina riziką juose esančių duomenų nutekėjimui. Mobiliuosius įrenginius, tokius kaip išmanieji telefonai ar planšetės, naudotojai gali panaudoti savo asmeninėms reikmėms, todėl reikia užtikrinti, kad naudotojų asmeniniai duomenys ir organizacijoje administruojami asmens duomenys nebūtų atskleisti; aštunta, *programinės įrangos sauga*. Visuose programinės įrangos kūrimo ir administravimo etapuose organizacija turi užtikrinti duomenų saugos laikymąsi, asmens duomenų apsaugą; devinta, *duomenų naikinimas, šalinimas*. Pagrindinis duomenų naikinimo tikslas yra negrįžtamas asmens duomenų šalinimas, sunaikinimas be teorinės ir praktinės galimybės juos pakartotinai nuskaityti ar atstatyti. Kai yra šalinama pasenusi, nenaudojama, nebereikalinga techninė įranga, duomenų valdytojas privalo užtikrinti, kad visi prieš tai joje buvę sukaupti duomenys būtų negrįžtamai pašalinti; dešimta, *fizinė sauga*. Fizinė apsauga yra ne mažiau svarbi negu technologinės saugumo priemonės, nes tiesioginės fizinės prieigos kontrolė prie informacinių technologijų infrastruktūros yra visos taikomos saugos strategijos pagrindas[124].

Atkreiptinas dėmesys, kad aptartos Valstybinės duomenų apsaugos inspekcijos įtvirtintos techninės ir organizacinės duomenų saugumo priemonės yra pavyzdinės, leidžiančios įstaigoms įsitvirtinti ir įgyvendinti tinkamas bei reikiamas technines ir organizacines duomenų saugumo priemones, kuriomis būtų užtikrinama tinkamo lygio duomenų apsauga.

1.5. Duomenų tvarkymo pagrindai

Analizuojant teisėto duomenų tvarkymo principo turinį, minėta, jog bendriausia prasme teisėtumo principas reikalauja, jog asmens duomenų tvarkymas būtų teisėtas bei atitiktų bendruosius ir specialiuosius duomenų tvarkymo reikalavimus. Vadovaujantis teisėto duomenų tvarkymo principo turiniu, asmens duomenų tvarkymas pripažįstamas teisėtu, kai yra gautas asmens, kurio

[123] Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) Nr. 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) OL 2016 L 19, p. 1-88.
[124] Valstybinė duomenų apsaugos inspekcija. 2018 m. spalio 31. Tinkamų organizacinių ir techninių duomenų saugumo priemonių įgyvendinimo gaires asmens duomenų valdytojams ir tvarkytojams [interaktyvus]. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomendtechpriemonesgaires2018.pdf [žiūrėta 2020 m. rugsėjo 27 d.].

duomenys yra tvarkomi, sutikimas arba remiamasi kitu teisiniu pagrindu, suteikiančiu teisę tvarkyti asmens duomenis. Tai reiškia, jog asmens duomenys turi būti tvarkomi teisėtu pagrindu.

Teisėtus duomenų tvarkymo pagrindus įtvirtina Bendrojo duomenų apsaugos reglamento 6 straipsnis, kuris numato, jog asmens duomenų tvarkymas bus laikomas teisėtu tik tuo atveju, jeigu taikoma bent viena iš šių sąlygų: a) duomenų subjektas davė sutikimą, kad jo asmens duomenys būtų tvarkomi vienu ar keliais konkrečiais tikslais; b) tvarkyti duomenis būtina siekiant įvykdyti sutartį, kurios šalis yra duomenų subjektas, arba siekiant imtis veiksmų duomenų subjekto prašymu prieš sudarant sutartį; c) tvarkyti duomenis būtina, kad būtų įvykdyta duomenų valdytojui taikoma teisinė prievolė; d) tvarkyti duomenis būtina siekiant apsaugoti gyvybinius duomenų subjekto ar kito fizinio asmens interesus; e) tvarkyti duomenis būtina siekiant atlikti užduotį, vykdomą viešojo intereso labui arba vykdant duomenų valdytojui pavestas viešosios valdžios funkcijas; f) tvarkyti duomenis būtina siekiant teisėtų duomenų valdytojo arba trečiosios šalies interesų, išskyrus atvejus, kai tokie duomenų subjekto interesai arba pagrindinės teisės ir laisvės, dėl kurių būtina užtikrinti asmens duomenų apsaugą, yra už juos viršesni, ypač kai duomenų subjektas yra vaikas.

Yra parengtos Europos Sąjungos apsaugos taisyklės, kurios reiškia, kad duomenų valdytojas duomenis turėtų tvarkyti sąžiningai ir teisėtai, siekdamas konkretaus ir teisėto tikslo, ir tvarkyti tik tuos duomenis, kurie yra būtini šiam tikslui pasiekti. Taigi, institucijos gali tvarkyti duomenis tokiais atvejais, kai:

- gautas asmens sutikimas;
- asmens duomenų reikia tam, kad būtų galima įvykdyti **sutartinius įsipareigojimus** asmens atžvilgiu;
- asmens duomenų reikia tam, kad galima būtų įvykdyti **teisinę prievolę**;
- asmens duomenų reikia tam, kad būtų galima apsaugoti asmens **gyvybiškai svarbius interesus**;
- asmens duomenys tvarkomi **viešojo intereso labui**;
- veikiama atstovaujant savo įmonės **teisėtiems interesams**, jeigu asmens, kurio duomenys yra tvarkomi, pagrindinėms teisėms ir laisvėms nedaromas didelis poveikis[125].

Vienas iš asmens duomenų teisėto tvarkymo pagrindų, kuriuo duomenų valdytojai dažnai remiasi, tvarkant asmens duomenis, yra duomenų subjekto sutikimas. Bendrasis duomenų apsaugos reglamentas duomenų subjekto sutikimą apibrėžia kaip bet kokį laisva valia duotą, konkretų ir nedviprasmišką tinkamai informuoto duomenų subjekto valios išreiškimą pareiškimu arba

[125] Duomenų apsauga pagal BDAR [interaktyvus]. Prieiga per internetą: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_lt.htm [žiūrėta 2020 m. rugsėjo 27 d.].

vienareikšmiais veiksmais kuriais jis sutinka, kad būtų tvarkomi su juo susiję asmens duomenys[126]. Remiantis šiuo duomenų subjekto sutikimo apibrėžimu, darytina išvada, kad duomenų subjekto sutikimui keliami šie reikalavimai: pirma, sutikimas turi būti duotas laisva valia (savanoriškai), antra, sutikimas turi būti konkretus, trečia, sutikimas turi būti nedviprasmiškas, ketvirta, sutikimas turi būti grindžiamas informacija, penkta, sutikimo davimo įrodomumas. Pažymėtina, kad sutikimas bus laikomas tinkamu, tik tuo atveju, jeigu atitiks visus aukščiau išvardytus reikalavimus. Esminis momentas dėl sutikimo – turi būti užtikrinama, kad asmuo suprastų, kad jis duoda sutikimą. Vadinasi, sutikimas turėtų būti duotas laisvai, būti konkretus, pagrįstas informacija ir vienareikšmiškas, atsižvelgiant į aiškia ir suprantama kalba surašytą prašymą. Sutikimas turėtų būti duodamas pritariamuoju veiksmu, pavyzdžiui, internete pažymint žymimąjį langelį arba pasirašant formą. Kai asmuo sutinka, kad būtų tvarkomi jo asmens duomenys, duomenų valdytojas duomenis gali tvarkyti tik tais tikslais, dėl kurių buvo duotas sutikimas. Taip pat duomenų valdytojas privalo suteikti galimybę atšaukti savo sutikimą[127].

Europos duomenų apsaugos valdybos patvirtintose gairėse 05/2020 „Dėl sutikimo pagal Reglamentą 2016/679“, kuriose paaiškinama, kokias sąlygas turi atitikti sutikimas, vadovaujantis Bendrojo duomenų apsaugos reglamento 4 straipsnio 11 punktu ir 7 straipsniu, įtvirtinta, jog sutikimo savanoriškumas reiškia realų duomenų subjektų pasirinkimą ir kontrolę. Pasirinkimas iš esmės reiškia duomenų subjekto galėjimą pasirinkti duoti sutikimą, ar jo neduoti. Tais atvejais, kai duomenų subjektas neturi realaus pasirinkimo, jis jaučiasi priverstas sutikti arba nesutikimo atveju jam gresia neigiamos pasekmės, sutikimas nebus laikomas savanorišku, išreikštu laisva valia. Kontrolės elementas apibrėžia duomenų subjekto galimybę spręsti dėl sutikimo galiojimo, t. y. sutikimo atšaukimo[128]. Duomenų subjekto sutikimas nebus laikomas savanorišku, jei duomenų subjektas negali atšaukti ar atsiimti savo sutikimo. Svarbu pastebėti, kad vertinant sutikimo savarankiškumą, būtina atsižvelgti į tai, jog kaip įtvirtinta Bendrojo duomenų apsaugos reglamento preambulės 43 punkte, duomenų subjekto sutikimas neturėtų būti laikomas duotu laisva valia (savanoriškai), kai yra aiškus duomenų subjekto ir duomenų valdytojo padėties disbalansas, ypač kai duomenų valdytojas yra valdžios institucija ir dėl to nėra tikėtina, kad sutikimas, atsižvelgiant į visas to konkretaus atvejo aplinkybes, buvo duotas laisva valia[129]. Taigi, tais atvejais, kai tarp

[126] Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) Nr. 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) OL 2016 L 19, p. 1-88.
[127] Duomenų apsauga pagal BDAR [interaktyvus]. Prieiga per internetą: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_lt.htm [žiūrėta 2020 m. rugsėjo 27 d.].
[128] Europos duomenų apsaugos valdybos patvirtintos gairės 05/2020 „Dėl sutikimo pagal Reglamentą 2016/679“ [interaktyvus]. Prieiga per internetą: https://edpb.europa.eu/sites/edpb/files/files/file1/edpbguidelines202005consent_en.pdf [žiūrėta 2020 m. lapkričio 5 d.].
[129] Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) Nr. 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) OL 2016 L 19, p. 1-88.

duomenų subjekto ir duomenų valdytojo (ypač tais atvejais, kai duomenų valdytoju yra valdžios institucija) galių nėra išlaikoma pusiausvyra, dažnu atveju yra kvestionuojamas duomenų subjekto sutikimo savanoriškumas. Dėl duomenų subjekto ir duomenų valdytojo, esančio valdžios institucija, santykių specifikos, nėra tikėtina, jog duomenų subjektas, besikreipdamas į valdžios instituciją dėl viešosios paslaugos suteikimo, neduos sutikimo dėl jo asmens duomenų tvarkymo. Dėl šios priežasties valdžios institucijai dalyvaujant asmens duomenų tvarkymo teisiniuose santykiuose, laikytina, jog duomenų subjektas yra nelygiavertėje padėtyje su duomenų tvarkytoju (duomenų valdytoju), todėl duomenų subjekto duotas sutikimas dėl jo asmens duomenų tvarkymo absoliučiai negali būti laikomas duotu laisva valia. Šiame kontekste verta prisiminti Valstybinės vartotojų teisių apsaugos tarnybos patvirtintoje vartotojo prašymo formoje įtvirtintą nuostatą dėl besikreipiančio vartotojo sutikimo dėl jo asmens duomenų tvarkymo. Valstybinės vartotojų teisių apsaugos tarnybos patvirtintoje vartotojo prašymo formoje įtvirtinta: „sutinku, kad mano prašymo nagrinėjimo tikslu būtų tvarkomi mano pateikti duomenys (nepažymėjus, prašymas nebus nagrinėjamas)“[130]. Įvertinus šios sąlygos formuluotę matyti, jog vartotojas norėdamas, kad jo prašymas dėl vartojimo ginčo nagrinėjimo būtų išspręstas, privalo pažymėti, jog sutinka, kad jo prašymo nagrinėjimo tikslu būtų tvarkomi asmens duomenys, priešingu atveju, jei vartotojas nesutiktų dėl jo asmens duomenų tvarkymo, jo prašymas nebūtų nagrinėjamas. Vertinant šį vartotojo duodamą sutikimą laisvos valios išreiškimo (savanoriškumo) požiūriu, autorės nuomone, įstaiga prašymo formoje įtvirtinusi, jog vartotojo prašymas nebus nagrinėjamas, jeigu jis neduos sutikimo dėl jo asmens duomenų tvarkymo, daro spaudimą vartotojui duoti sutikimą dėl jo asmens duomenų tvarkymo bei iš esmės neleidžia pasirinkti duoti sutikimą ar jo neduoti. Kita vertus, jei įstaiga galės pagrįsti, jog vartotojo prašymas tikrai negalės būti nagrinėjamas, jei nebus gautas jo sutikimas dėl jo asmens duomenų tvarkymo, vartotojo, davusio sutikimą dėl jo asmens duomenų tvarkymo, tvarkomi duomenys turėtų būti laikomi tvarkomais teisėtu pagrindu.

Sutikimo konkretumo reikalavimas yra įtvirtintas Bendrojo duomenų apsaugos reglamento 6 straipsnio 1 dalies a punkte, kuris numato, jog duomenų subjekto sutikimas turi būti duodamas dėl duomenų tvarkymo „vienu ar keliais konkrečiais tikslais“[131]. Konkretumo požiūriu sutikimas turi būti susietas su aiškiai apibrėžtomis duomenų tvarkymo operacijomis. Konkretumo reikalavimu, taikomu sutikimui, siekiama duomenų subjektui užtikrinti tam tikrą vartotojo turimą kontrolę ir skaidrumą. Tai reiškia, kad duomenų valdytojas, laikydamasis sutikimo konkretumo reikalavimo

[130] Valstybinė vartotojų teisių apsaugos tarnyba. Paslaugos (tinklalapio internete skiltis) [interaktyvus]. Prieiga per internetą: http://www.vvtat.lt/paslaugos/prasymai/vartotojo-prasymo-forma/345 [žiūrėta 2020 m. rugsėjo 26 d.].
[131] Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) Nr. 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) OL 2016 L 19, p. 1-88.

taiko konkretaus tikslo nustatymą kaip apsaugą nuo nemotyvuoto nukrypimo nuo funkcijų, detalizuoja sutikimo prašymus bei užtikrina, kad informacija apie sutikimo davimą aiškiai atskirta nuo informacijos, nesusijusios su duomenų subjekto sutikimo davimu[132]. Atsižvelgiant į sutikimo konkretumo reikalavimo turinį, pastebėtina, kad sutikimo konkretumo reikalavimas siejasi su Bendrojo duomenų apsaugos reglamento 5 straipsnio 1 dalies b punkte įtvirtintu tikslo apribojimo principu. Reikalavimas gauti konkretų sutikimą kartu su tikslo apribojimo principu veikia kaip apsaugos priemonė nuo vienašališko duomenų tvarkymo tikslų išplėtimo arba suliejimo po to, kai duomenų subjektas sutinka su pradiniu duomenų tvarkymu. Be to, sutikimas turi apimti visą duomenų tvarkymo veiklą, vykdomą vienu arba keliais tais pačiais tikslais. Šis sutikimo konkretumo elementas iš esmės įpareigoja duomenų valdytoją gauti duomenų subjekto sutikimą dėl kiekvieno tikslo, kuriuo jo asmens duomenys yra tvarkomi. Tai reiškia, kad tais atvejais, kai duomenų valdytojas duomenis tvarko remdamasis sutikimu, tačiau nori tuos pačius asmens duomenis tvarkyti ir kitais tikslais, duomenų valdytojas turi prašyti papildomo sutikimo dėl naujojo tikslo, kuriuos bus tvarkomi tie patys asmens duomenys, nebent būtų kitas teisėtas pagrindas, geriau atitinkantis esamą padėtį.

Dar vienas duomenų subjekto sutikimui keliamas reikalavimas, jog sutikimas būtų nedviprasmiškas. Kitaip tariant, duomenų subjekto duotas sutikimas turi būti išreikštas aiškiai ir nekelti abejonių dėl sutikimo davimo. Bendrojo duomenų apsaugos reglamento preambulės 32 punkte įtvirtina, jog sutikimas laikytinas nedviprasmišku, kai jis išreiškiamas raštu, įskaitant elektronines priemones, arba suprantamas žodinis pareiškimas. Tai galėtų būti atliekama pažymint langelį interneto svetainėje, pasirenkant informacinės visuomenės paslaugų techninius parametrus arba kitokiu pareiškimu (poelgiu), iš kurio aiškiai matyti, kad duomenų subjektas sutinka su siūlomu jo asmens duomenų tvarkymu. Tokiu būdu tyla, iš anksto pažymėti langeliai arba neveikimas neturėtų būti laikomi sutikimu[133].

Sutikimo pagrįstumo informacija reikalavimas glaudžiai susijęs su Bendrajame duomenų apsaugos reglamente įtvirtintu duomenų tvarkymo skaidrumo ir sąžiningumo principu. Bendrojo duomenų apsaugos reglamento preambulės 42 punkte įtvirtinta, jog tam, kad sutikimas būtų grindžiamas informacija, duomenų subjektas turėtų bent žinoti duomenų valdytojo tapatybę ir planuojamo asmens duomenų tvarkymo tikslus[134]. Duomenų valdytojo tapatybės žinojimas ir

[132] Europos duomenų apsaugos valdybos patvirtintos gairės 05/2020 „Dėl sutikimo pagal Reglamentą 2016/679“ [interaktyvus]. Prieiga per internetą: https://edpb.europa.eu/sites/edpb/files/files/file1/edpbguidelines202005consent_en.pdf [žiūrėta 2020 m. lapkričio 5 d.].

[133] Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) Nr. 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) OL 2016 L 19, p. 1-88.

[134] Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) Nr. 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) OL 2016 L 19, p. 1-88.

planuojamo asmens duomenų tvarkymo tikslo žinojimas yra minimalūs Bendrajame duomenų apsaugos reglamente įtvirtinti reikalavimai, kad sutikimą galima būtų laikyti grindžiamu informacija. Tuo tarpu Europos duomenų apsaugos valdybos patvirtintose gairėse 05/2020 „Dėl sutikimo pagal Reglamentą 2016/679“ yra įtvirtintas platesnis reikalavimų, kuriems esant sutikimą galima būtų laikyti grindžiamu informacija, sąrašas. Vadovaujantis minimomis gairėmis, kad sutikimas būtų pagrįstas informacija, būtina mažiausiai pateikti šią informaciją: pirma, duomenų valdytojo tapatybę; antra, kiekvienos iš duomenų tvarkymo operacijų, kurioms prašoma sutikimo, tikslą; trečia, kokie duomenys bus renkami ir naudojami; ketvirta, informaciją apie turimą teisę atšaukti sutikimą; penkta, kai tinka – informaciją apie duomenų naudojimą automatizuotai priimant sprendimus; šešta, informaciją apie galimą duomenų perdavimo riziką, kai nėra priimto sprendimo dėl tinkamumo ir nėra tinkamų apsaugos priemonių[135]. Pastebėtina, kad tam tikrais atvejais, duomenų valdytojas privalėtų pateikti daugiau informacijos tam, kad duomenų valdytojo tvarkomi duomenų subjekto asmens duomenys būtų laikytini tvarkomais teisėtu duomenų tvarkymo pagrindu. Be to, pastebėtina, kad reikalavimo, jog duomenų subjekto sutikimas būtų grindžiamas informacija, nereikia tapatinti arba sugretinti su duomenų valdytojo pareiga informuoti duomenų subjektą apie jo asmens duomenų tvarkymą.

Bendrojo duomenų apsaugos reglamento 7 straipsnio 1 dalyje įtvirtinta, duomenų valdytojo pareigą galėti įrodyti, kad duomenų subjektas davė sutikimą, kad būtų tvarkomi jo asmens duomenys[136]. Duomenų valdytojui gali tekti įrodinėti duomenų subjekto duotą sutikimą, kai kyla ginčas su duomenų subjektu dėl sutikimo tvarkyti duomenų subjekto asmens duomenis davimo fakto arba pareikalavus priežiūros institucijai.

Vertinant asmens duomenų subjekto sutikimo, kaip asmens duomenų teisėto tvarkymo pagrindo, taikymą viešajame sektoriuje, atkreiptinas dėmesys, jog analizuojant sutikimo savanoriškumą, padaryta išvada, jog valdžios institucijai dalyvaujant asmens duomenų tvarkymo teisiniuose santykiuose, duomenų subjektas yra nelygiavertėje padėtyje su duomenų tvarkytoju (duomenų valdytoju), todėl duomenų subjekto duotas sutikimas dėl jo asmens duomenų tvarkymo absoliučiai negali būti laikomas duotu laisva valia. Tokiu būdu, kai duomenų subjekto duotas sutikimas neatitinka laisva valia (savanoriškai) duoto sutikimo reikalavimo, kvestionuojamas sutikimo, kaip asmens duomenų teisėto tvarkymo pagrindo, taikymas viešajame sektoriuje.

[135] Europos duomenų apsaugos valdybos patvirtintos gairės 05/2020 „Dėl sutikimo pagal Reglamentą 2016/679“ [interaktyvus]. Prieiga per internetą: https://edpb.europa.eu/sites/edpb/files/files/file1/edpbguidelines202005consent_en.pdf [žiūrėta 2020 m. lapkričio 5 d.].

[136] Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) Nr. 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) OL 2016 L 19, p. 1-88.

Nepaisant to, viešojo sektoriaus subjektai asmens duomenis tvarko duomenų subjekto sutikimo pagrindu.

Kitas asmens duomenų teisėto tvarkymo pagrindas – sutartis su duomenų subjektu. Bendrojo duomenų apsaugos reglamento 6 straipsnio 1 dalies b punkte įtvirtinta, jog duomenų tvarkymas yra teisėtas, jei tvarkyti duomenis būtina siekiant įvykdyti sutartį, kurios šalis yra duomenų subjektas, arba siekiant imtis veiksmų duomenų subjekto prašymu prieš sudarant sutartį[137]. Pastebėtina, kad Bendrasis duomenų apsaugos reglamentas neapibrėžia, kas yra laikytina sutartimi Bendrojo duomenų apsaugos reglamento 6 straipsnio 1 dalies b punkto prasme, todėl sutartis apibrėžiama vadovaujantis civilinės teisės nuostatomis, įtvirtintomis nacionalinėje teisėje. Vadovaujantis Civilinio kodekso 6.154 straipsnio 1 dalimi, sutartimi laikomas dviejų ar daugiau asmenų susitarimas sukurti, pakeisti ar nutraukti civilinius teisinius santykius, kai vienas ar keli asmenys įsipareigoja kitam asmeniui ar asmenims atlikti tam tikrus veiksmus (ar susilaikyti nuo tam tikrų veiksmų atlikimo), o pastarieji įgyja reikalavimo teisę[138]. Vadovaujantis sutarčių laisvės principu, kuris laikytinas sutarčių teisės pagrindu, sutarties šalys, t. y. duomenų valdytojas ir duomenų subjektas turi teisę laisvai sudaryti sutartis ir savo nuožiūra nustatyti tarpusavio teises bei pareigas, taip pat sudaryti ir šio kodekso nenumatytas sutartis, jeigu tai neprieštarauja įstatymams (Civilinio kodekso 6.156 straipsnio 1 dalis)[139].

Vertinant Bendrojo duomenų apsaugos reglamento 6 straipsnio 1 dalies b punkto formuluotę, matyti, jog asmens duomenis sutarties su duomenų subjektu pagrindu galima tvarkyti tik tuo atveju, jei yra užtikrinama būtinumo sąlyga.

Kai asmens duomenų tvarkymas grindžiamas duomenų valdytojui taikoma teisine prievole arba užduotimi, vykdoma viešojo intereso labui arba vykdant viešosios valdžios funkcijas, taikomi Bendrojo duomenų apsaugos reglamento 6 straipsnio 1 dalies c ir e punktai (valstybės narės gali toliau taikyti jau esančias, arba nustatyti konkretesnes nuostatas Bendrojo duomenų apsaugos reglamento taisyklėms pritaikyti, nes Bendrojo duomenų apsaugos reglamento preambulės 41 punkte nurodyta – asmens duomenų tvarkymo pagrindai nacionalinėje teisėje gali būti įtvirtinti ne tik įstatymuose, bet ir kituose poįstatyminiuose teisės aktuose, kaip pavyzdžiui, Lietuvos Respublikos Vyriausybės nutarime, ministro įsakyme ir pan., tačiau juose nustatytas reglamentavimas turi būti aiškus ir tikslus). Pagal Valstybinės asmens duomenų apsaugos institucijos parengtas rekomendacijas, asmens duomenų tvarkymas, atliekamas valstybės ir savivaldybių institucijų ir įstaigų, t. y. viešųjų subjektų, iš esmės turėtų remtis Bendrojo duomenų

[137] Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) Nr. 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) OL 2016 L 19, p. 1-88.
[138] Lietuvos Respublikos civilinis kodeksas (2000). Valstybės žinios, 74-2262.
[139] Lietuvos Respublikos civilinis kodeksas (2000). Valstybės žinios, 74-2262.

apsaugos reglamento 6 straipsnio 1 dalies c ir e punktais. Tačiau Bendrojo duomenų apsaugos reglamento e punkto taikymo atveju, asmens duomenys saugomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, negu būtina tais tikslais, kuriais asmens duomenys buvo surinkti. Pavyzdžiui Lietuvos Respublikos pinigų plovimo ir teroristų finansavimo prevencijos įstatymo 19 straipsnio 9 dalyje numatyta, kad kliento tapatybę patvirtinančių dokumentų kopijos, sąskaitų ir (ar) sutarčių dokumentacija (dokumentų originalai) turi būti saugoma 10 metų nuo sandorių ar dalykinių santykių su klientu pabaigos dienos. Šio straipsnio 10 punkte nurodyta, kad kliento tapatybę patvirtinančių dokumentų kopijos, naudos gavėjo tapatybės duomenys, išmokos gavėjo tapatybės duomenys, tiesioginio vaizdo perdavimo (tiesioginės vaizdo transliacijos) įrašas, kiti duomenys, gauti kliento tapatybės nustatymo metu, sąskaitų ir (ar) sutarčių dokumentacija (dokumentų originalai) turi būti saugomi 8 metus nuo sandorių ar dalykinių santykių su klientu pabaigos dienos[140].

Viešasis subjektas yra išskirtinis tuo, kad jo padėtis yra kitokia, nes viešųjų funkcijų vykdymas turi būti paremtas Bendrojo duomenų apsaugos reglamento 6 straipsnio punktu, priklausomai nuo įgyvendinamo tikslo.

[140] Lietuvos Respublikos pinigų plovimo ir teroristų finansavimo prevencijos įstatymas (1997). Valstybės žinios, 64-1502.

2. DUOMENŲ APSAUGOS ĮGYVENDINIMO KLAUSIMŲ POKYTIS BENDROJO DUOMENŲ APSAUGOS REGLAMENTO KONTEKSTE

Duomenų apsaugos įgyvendinimo problematika bus analizuojama dviem aspektais. Visų pirma, bus analizuojama, su kokiomis asmens duomenų apsaugos įgyvendinimo problemomis buvo susiduriama iki Bendrojo duomenų apsaugos reglamento priėmimo, t. y. iki to momento, kai valstybės pradėjo ruoštis Bendrojo duomenų apsaugos reglamento įsigaliojimui. Taip pat bus analizuojama su kokiomis asmens duomenų apsaugos įgyvendinimo problemomis susiduriama priėmus Bendrąjį duomenų apsaugos reglamentą. Analizuojant buvusias asmens duomenų apsaugos problemas laikotarpiu iki Bendrojo duomenų apsaugos reglamento priėmimo, bus remiamasi valstybės kontrolės valstybinio audito 2013 m. gruodžio 11 d. ataskaita Nr. VA-P-90-3-21 „Automatiniu būdu tvarkomų asmens duomenų apsauga“, taip pat 2014 m. Valstybinės duomenų apsaugos inspekcijos atliktais duomenų subjektų teisių įgyvendinimo ir reglamentavimo valstybės institucijose teisėtumo patikrinimais. Duomenų apsaugos problemos, kylančios priėmus Bendrąjį duomenų apsaugos reglamentą, bus analizuojamos vertinant viešųjų paslaugų teikimo perkėlimo į elektroninę erdvę poveikį asmens duomenų apsaugai. Taip pat, atsižvelgiant į šiuo metu vykstančius darbo organizavimo pokyčius, kuriuos paskatino esanti epidemiologinė situacija, bus analizuojama, ar įstaigose organizuojant nuotolinį darbą, galimas visapusiškas duomenų apsaugos užtikrinimas?

2.1. Duomenų apsaugos įgyvendinimo problemos iki Bendrojo duomenų apsaugos reglamento priėmimo

Asmens duomenų apsauga Lietuvoje pradėta rūpintis 1992 m., priėmus Konstituciją, tačiau iš esmės asmens duomenų teisinės apsaugos mechanizmas šalyje pradėjo veikti tik 1996 m., įsigaliojus Asmens duomenų teisinės apsaugos įstatymui, kuris gina žmogaus teisę į privataus gyvenimo neliečiamumą tvarkant asmens duomenis. Iki 2010 m. teisės aktuose nebuvo numatyta subjekto, formuojančio asmens duomenų apsaugos politiką, o nuo 2011 m. Valstybės politiką asmens duomenų apsaugos srityje pradėjo formuoti, organizuoti, koordinuoti ir kontroliuoti jos įgyvendinimą Lietuvos Respublikos teisingumo ministerija (toliau – Teisingumo ministerija). Tuo tarpu, Valstybinė duomenų apsaugos inspekcija tapo asmens duomenų apsaugos politikoje dalyvaujanti, ją įgyvendinanti ir priežiūrą vykdanti įstaiga, priskirta teisingumo ministro valdymo sričiai. Sparčiai tobulėjant informacijos ir ryšių technologijoms, asmens duomenų apsaugos politiką formuojančios ir įgyvendinančios įstaigos susidūrė su problemomis, kurios ryškėjo saugios teisinės aplinkos asmens duomenų apsaugos srityje sukūrimu ir jos plėtra. Tai paskatino Valstybės kontrolę atlikti auditą, kurio pagrindiniu tikslu buvo siekis įvertinti, ar automatiniu būdu tvarkomų asmens

duomenų apsauga ir priežiūra vykdoma efektyviai. Šiam audito tikslui pasiekti buvo iškelti sekantys uždaviniai: įvertinti, ar asmens duomenų apsaugos reguliavimas atitinka duomenų tvarkymo praktiką; įvertinti, ar tinkamai tvarkomi viešojo sektoriaus įstaigose asmens duomenys; įvertinti, ar Valstybinės duomenų apsaugos inspekcijos vykdoma asmens duomenų tvarkymo priežiūra yra pakankama. Audito metu buvo analizuotas tuo metu galiojęs asmens duomenų apsaugos reguliavimas ir buvusi duomenų tvarkymo praktika, vertinta, kaip Valstybinė duomenų apsaugos inspekcija vykdė asmens duomenų tvarkymo priežiūrą ir kaip duomenų valdytojai ir duomenų tvarkytojai užtikrino informacijos apie asmenis, kaupiamos valstybės informaciniuose ištekliuose, saugumą, ar tinkamai ją tvarkė[141].

Valstybės kontrolė, siekdama įgyvendinti išsikeltus audito uždavinius, suformavo vertinamuosius kriterijus, kuriais remiantis buvo vertinama ar tvarkomų asmens duomenų apsauga ir priežiūra valstybės institucijose buvo vykdoma efektyviai. Pirmos išsikeltos užduoties įgyvendinimui Valstybės kontrolė įsitvirtino šį vertinimo kriterijų: asmens duomenų apsaugos reguliavimas visapusiškai užtikrina asmens duomenų apsaugą tada, kai jis neatsilieka nuo informacijos ir ryšių technologijų pažangos ir pakankamai reglamentuoja asmens duomenų apsaugos sritį. Šis kriterijus buvo pasirinktas, nes tobulėjant informacijos ir ryšių technologijoms, kai asmens duomenys tvarkomi automatiniu būdu, technologiniai veiksniai kelia naujų grėsmių asmens duomenų tvarkymo apsaugai. Teisės aktai ir metodiniai dokumentai, reglamentuojantys asmens duomenų apsaugą, turėtų būti parengiami laiku ir nustatyti tiek bendruosius, tiek ir specialiuosius šios srities tvarkymo reikalavimus, padedančius užtikrinti veiksmingą asmens duomenų apsaugą, o priežiūros institucija turėtų operatyviai reaguoti į probleminius klausimus, pokyčius ir naujus iššūkius, rengiant metodinius dokumentus ir skelbiant asmens duomenų tvarkymo praktiką. Valstybės kontrolė pastebėjo, jog Lietuvai įstojus į Europos Sąjungą, duomenų apsaugos teisinis reguliavimas buvo suderintas su Europos Sąjungos direktyva. 2008–2012 m. Asmens duomenų teisinės apsaugos įstatymas ir jį įgyvendinantys teisės aktai keisti keletą kartų, bet sparti informacijos ir ryšių technologijų plėtra nuolat iškeldavo asmens duomenų apsaugos praktinio taikymo klausimų, kurių tuo metu galioję teisės aktai negalėjo išspręsti. Šią problemą pagrindė praktinis pavyzdys: nors dėl sparčios technologinės plėtros ir globalizacijos kasdien buvo surenkamas didžiulis duomenų kiekis, tačiau teisės aktai nenumatė duomenų subjektui aiškios „teisės būti pamirštam“ t. y. reikalauti ištrinti asmens duomenis kai jis nebenori, kad jo duomenys būtų tvarkomi ir nėra teisėtų priežasčių juos saugoti. Technologijos leido perduoti asmens duomenis iš vieno paslaugų teikėjo kitam, tačiau

[141] Valstybės kontrolės valstybinio audito 2013 m. gruodžio 11 d. ataskaita Nr. VA-P-90-3-21 „Automatiniu būdu tvarkomų asmens duomenų apsauga“. [interaktyvus]. Prieiga per internetą: https://www.vkontrole.lt/failas.aspx?id=3088 [žiūrėta 2020 m. spalio 1 d.].

duomenų subjekto „teisė perkelti duomenis“ nebuvo aiškiai reglamentuota. Be to, įvertinusi tai, kad asmens duomenų apsaugos reguliavimas buvo atsilikęs nuo informacijos ir ryšių technologijų pažangos, Valstybės kontrolė pažymėjo, jog asmens duomenų apsaugai trūko aiškios ilgalaikės plėtros perspektyvos. Valstybės kontrolė, išnagrinėjusi įvairios trukmės valstybės planavimo dokumentus, nustatė, jog prieš 10 metų (auditas buvo atliktas 2013 m., tad čia minimi 2003 m. valstybės planavimo dokumentai) asmens duomenų apsauga buvo vienu iš svarbiausių horizontalių prioritetų Lietuvoje ir svarbi informacinės visuomenės plėtrai, tačiau audito metu ji neturėjo aiškios ilgalaikės (strateginės) krypties ir buvo siejama tik su skirtingais įvairių valstybės valdymo sričių planavimo dokumentais[142]. Autorės nuomone, valstybės ilgalaikės (strateginės) krypties asmens duomenų apsaugos srityje ženklų pasikeitimą lėmė tai, jog asmens duomenų apsaugos teisinio reglamentavimo kūrimą Lietuvoje sąlygojo pasiruošimas stojimui į Europos Sąjungą. Atsižvelgiant į tai, kad įstojus į Europos Sąjungą, asmens duomenų apsaugai nebuvo skiriama daug dėmesio, autorė daro išvadą, kad valstybės domėjimasis asmens duomenų apsauga bei asmens duomenų apsaugos politikos formavimas laikotarpiu iki 2004 m. buvo pakankamai formalus. Manytina, jog nebuvo aiški asmens duomenų apsaugos įgyvendinimo nacionaliniu lygiu svarba ir reikšmė, todėl asmens duomenų apsauga iki Valstybės kontrolės atlikto audito nacionaliniu lygiu buvo įgyvendinama formaliai.

Antros išsikeltos užduoties įgyvendinimui, t. y. įvertinimui, ar tinkamai tvarkomi viešojo sektoriaus įstaigose asmens duomenys, Valstybės kontrolė įsitvirtino kriterijų, kuris numatė, jog duomenų valdytojai ir tvarkytojai užtikrina asmens duomenų apsaugą tada, kai jie tinkamai įgyvendina teisės aktuose nustatytus asmens duomenų apsaugos reikalavimus. Valstybės kontrolė siekdama nustatyti, kaip duomenų valdytojai ir tvarkytojai įgyvendina teisės aktuose nustatytus reikalavimus dėl asmens duomenų apsaugos, atliko duomenų valdytojų ir tvarkytojų patikras vietoje. Patikrinimų metu buvo nustatyta, kad 84 proc. tikrintų įstaigų laikėsi ne visų teisės aktais nustatytų reikalavimų, susijusių su asmens duomenų apsauga. Patikrų metu išryškėjo šie pagrindiniai asmens duomenų tvarkymo trūkumai: įstaigose nebuvo rengiami asmens duomenų tvarkymo dokumentai (pavyzdžiui, asmens duomenų tvarkymo taisyklės, duomenų valdytojo ir duomenų tvarkytojo sutartys ir kt.), o parengtieji buvo neaktualūs, pasikeitę asmens duomenų tvarkymo tikslai ir apimtys, neskelbiamos duomenų subjekto teisių įgyvendinimo tvarkos ir būdai. Taip pat nebuvo laikomasi techninių saugos priemonių ir fizinės saugos reikalavimų, nepakankamai valdyta prieiga prie

[142] Valstybės kontrolės valstybinio audito 2013 m. gruodžio 11 d. ataskaita Nr. VA-P-90-3-21 „Automatiniu būdu tvarkomų asmens duomenų apsauga“. [interaktyvus]. Prieiga per internetą: https://www.vkontrole.lt/failas.aspx?id=3088 [žiūrėta 2020 m. spalio 1 d.].

informacinių sistemų, kai kurios įstaigos, tvarkiusios ypatingus asmens duomenis, neįgyvendino net minimalių organizacinių ir techninių duomenų saugos priemonių. Dėl išvardytų priežasčių Valstybės kontrolė padarė išvadą, jog tikrinti duomenų valdytojai ir tvarkytojai nesilaikė teisės aktų reikalavimų ir neužtikrino tokio saugumo lygio, kuris atitiktų saugotinų asmens duomenų pobūdį ir jų tvarkymo keliamą riziką. Be to, audito metu buvo nustatyta, kad nepakankamai buvo užtikrinama asmens teisė į privataus gyvenimo neliečiamumą. Daugiau kaip pusė (53 proc.) tikrintų duomenų valdytojų ir tvarkytojų nenustatė asmens duomenų subjekto teisių įgyvendinimo būdų, tvarkose neaprašė konkrečių veiksmų ir (ar) procedūrų, kurios leistų įgyvendinti kitus asmens duomenų tvarkymo reikalavimus, taigi apribojo asmens duomenų subjekto galimybes pasitikrinti kaip įgyvendinamos jo teisės. Asmens duomenų tvarkymo tikslai ir apimtis kai kuriose įtaigose buvo didesnės, nei jas skelbė Asmens duomenų valdytojų valstybės registras. Tokiu būdu asmuo galėjo nežinoti, kokia informacija apie jį kaupiama, o pateikęs paklausimą į Valstybinę duomenų apsaugos inspekciją, būtų gavęs informaciją, neatitinkančią asmens duomenų tvarkymo apimties[143].

Audito metu Valstybinės duomenų apsaugos inspekcijos vykdytos asmens duomenų tvarkymo priežiūros pakankamumas buvo vertintas kompleksiškai, pasitelkiant nustatytus vertinimo kriterijus. Audito metu buvo nustatyta, kad visi šie išvardinti vertinimo kriterijai nebuvo įvertinti teigiamai, todėl buvo padaryta išvada, jog Valstybinės duomenų apsaugos inspekcijos įgyvendinamoms funkcijoms trūksta kokybės ir efektyvumo, nes: pirma, Valstybinė duomenų apsaugos inspekcija planavimo dokumentuose pasirinkdavo priemones, kuriomis planavo rutininę veiklą, nustatydavo būsimų laikotarpių siekiamus uždavinius, vertinimo kriterijus ir veiklos efektyvumo rodiklius, kurių pasiekimas priklausė nuo duomenų valdytojų ir tvarkytojų ar duomenų subjektų aktyvumo; antra, organizuodama duomenų valdytojų priežiūrą, Valstybinė duomenų apsaugos inspekcija nenaudojo rizikos vertinimo ir valdymo sistemos, prevenciniai patikrinimai ir išankstinės patikros dažniausiai vyko susirašinėjimo būdu, inspekcija ne visais atvejais taikė kontrolės priemones, kurios padėtų išvengti duomenų saugumo pažeidimų; trečia, Valstybinė duomenų apsaugos inspekcija automatiniu būdu negaudavo duomenų apie asmens duomenų automatizuotą tvarkymą ir apsaugą viešajame sektoriuje, nes šiuos duomenis skirtingais tikslais ir priemonėmis kaupdavo įvairios įstaigos, be to, nė viena jų tarpusavyje nesuderindavo stebėjimo procesų ir įrankių; ketvirta, parengtos metodinės rekomendacijos buvo neaktualios ir apėmė ne visas problemines sritis susijusias su naujų technologijų taikymu, buvo nepakankamai užtikrinama duomenų valdytojų konsultavimo kokybė, interneto svetainėje skelbiama informacija buvo

[143] Valstybės kontrolės valstybinio audito 2013 m. gruodžio 11 d. ataskaita Nr. VA-P-90-3-21 „Automatiniu būdu tvarkomų asmens duomenų apsauga“. [interaktyvus]. Prieiga per internetą: https://www.vkontrole.lt/failas.aspx?id=3088 [žiūrėta 2020 m. spalio 1 d.].

peržiūrima nereguliariai; penkta, viešajame sektoriuje asmens duomenų saugos ir bendrieji duomenų (elektroninės informacijos) saugos reikalavimai tarpusavyje nebuvo suderinti, jų įgyvendinimo priemonės persidengdavo; šešta, iki 2013 m. Valstybinės duomenų apsaugos inspekcijos sukurtos elektroninės paslaugos buvo nepatrauklios ir mažai naudojamos. Nors 2013 m. Valstybinė duomenų apsaugos inspekcija patobulino teikiamas elektronines paslaugas ir Asmens duomenų valdytojų valstybės registrą, bet ne visi patobulinimai audito metu veikė be trikdžių. Trūko procedūrų, padedančių teikti elektronines paslaugas, o apklausos priemonės, kurios leistų įvertinti Valstybinės duomenų apsaugos inspekcijos teikiamų elektroninių paslaugų kokybę, veikė nepatikimai; septinta, kasmet Valstybinė duomenų apsaugos inspekcija parengdavo vis mažiau publikacijų apie asmens duomenų apsaugą, ne visa parengta medžiaga buvo viešinama ir atnaujinama, nebuvo išnaudojamos naujos visuomenės informavimo priemonės, galinčios padėti platinti informaciją apie asmens duomenų apsaugą ar įstaigos veiklą[144].

Taigi, audito rezultatai atskleidė, jog pagrindinėmis duomenų apsaugos įgyvendinimo problemomis iki Bendrojo duomenų apsaugos reglamento priėmimo buvo asmens duomenų apsaugos teisinio reguliavimo atsilikimas nuo informacijos ir ryšių technologijų pažangos, nepakankamas asmens duomenų tvarkymo organizavimas ir valdymas viešajame sektoriuje bei nepakankama Valstybinės duomenų apsaugos inspekcijos vykdoma asmens duomenų tvarkymo priežiūra.

Valstybinei duomenų apsaugos inspekcijai 2014 m. atlikus 49 duomenų subjektų teisių įgyvendinimo ir reglamentavimo valstybės institucijose teisėtumo patikrinimus, buvo nustatyta, kad 48 valstybės institucijos netinkamai reglamentavo ir įgyvendino duomenų subjekto teises. Patikrinimų metu buvo vertinama, kaip valstybės institucijos įgyvendina duomenų subjekto teises: teisę žinoti (būti informuotam) apie jo duomenų tvarkymą, teisę susipažinti su savo asmens duomenimis, teisę reikalauti ištaisyti, sunaikinti ar sustabdyti savo asmens duomenų tvarkymo veiksmus, teisę nesutikti, kad būtų tvarkomi jo asmens duomenys, kurias duomenų valdytojai privalo įgyvendinti. Patikrinimų metu nustatyta, kad 19 valstybės institucijų netinkamai įgyvendino reikalavimą informuoti duomenų subjektus, kokiais tikslais ketinami tvarkyti duomenų subjekto asmens duomenys ir nepateikė kitos papildomos informacijos (kam ir kokiais tikslais teikiami duomenų subjekto asmens duomenys, kokius savo asmens duomenis duomenų subjektas privalo pateikti ir kokios yra duomenų nepateikimo pasekmės, apie duomenų subjekto teisę susipažinti su

[144] Valstybės kontrolės valstybinio audito 2013 m. gruodžio 11 d. ataskaita Nr. VA-P-90-3-21 „Automatiniu būdu tvarkomų asmens duomenų apsauga“. [interaktyvus]. Prieiga per internetą: https://www.vkontrole.lt/failas.aspx?id=3088 [žiūrėta 2020 m. spalio 1 d.].

savo asmens duomenimis ir teisę reikalauti ištaisyti neteisingus, neišsamius, netikslius savo asmens duomenis), kiek jos reikia, kad būtų užtikrintas teisingas asmens duomenų tvarkymas nepažeidžiant duomenų subjekto teisių. Tikrinant kaip valstybės institucijos įgyvendina duomenų subjekto teisę susipažinti su tvarkomais asmens duomenimis, nustatyta, jog 24 institucijos netinkamai įgyvendino duomenų subjekto teisę susipažinti su savo asmens duomenimis. Kai kurios institucijos įgyvendindamos duomenų subjektų teisę susipažinti su savo asmens duomenimis nereikalavo pateikti asmens tapatybę patvirtinančio dokumento ar reikalavo prašyme nurodyti informacijos panaudojimo tikslą, aplinkybes, pagrindą. Patikrinimų metu taip pat nustatyta, jog 13 valstybės institucijų duomenų subjekto teisę reikalauti ištaisyti, sunaikinti ar sustabdyti savo asmens duomenų tvarkymo veiksmus įgyvendino pagal žodinį duomenų subjekto prašymą, nors pagal galiojantį teisinį reglamentavimą turėjo reikalauti rašytinio prašymo. Patikrinimų metu taip pat nustatyta, jog 44 valstybės institucijos, nereglamentavo duomenų subjekto teisių ir jų įgyvendinimo tvarkos rašytiniame dokumente (tvarkoje, apraše, taisyklėse, įsakyme ir pan.). Taip pat nustatyta, kad 18 institucijų vykdydamos vaizdo stebėjimą pažeidė pareigą informuoti duomenų subjektą apie vykdomą vaizdo stebėjimą. Nustatyta, kad 8 institucijose informacija apie vykdomą vaizdo stebėjimą, apie vaizdo stebėjimą vykdantį duomenų valdytoją, jo juridinio asmens kodą ir kontaktinę informaciją buvo pateikiama jau patekus į vaizdo kamerų stebėjimo lauką, tuo netinkamai įgyvendinant duomenų subjekto teisę žinoti (būti informuotam) apie savo asmens duomenų tvarkymą, 6 institucijos informaciniuose ženkluose nurodė telefono numerį, kuriuo neteikiama informacija apie vaizdo stebėjimą, 14 institucijų apie vykdomą vaizdo stebėjimą darbuotojų nesupažindino pasirašytinai, 10 institucijų asmens vaizdo duomenų tvarkymas nebuvo reglamentuotas, o 8 institucijos nesudarė sąlygų duomenų subjektui gauti savo vaizdo duomenis[145].

Vertinant kitose darbo dalyse viešojo administravimo institucijas ir jų sudaromas sutartis tiek dėl duomenų teikimo, tiek dėl konfidencialumo, reikėtų pastebėti, kad iki Bendrojo duomenų apsaugos reglamento įsigaliojimo nebuvo tinkamai užtikrinama asmens duomenų apsauga, buvo remiamasi tik Lietuvos Respublikos asmens duomenų apsaugos įstatymu, tiek dėmesio nebuvo skiriama konfidencialios informacijos apsaugai. Nebuvo privalomai skiriamas asmens duomenų pareigūnas, kuris prižiūrėtų, kaip tvarkomi asmens duomenys, ar laikomasi teisės aktų reikalavimų.

Taigi, įvertinus Valstybės kontrolės 2013 m. atlikto audito rezultatus bei Valstybinės duomenų apsaugos inspekcijos 2014 m. atliktus duomenų subjektų teisių įgyvendinimo ir reglamentavimo valstybės institucijose teisėtumo patikrinimus, darytina išvada, kad pagrindinė

[145] Valstybinė duomenų apsaugos inspekcija. Tikrinimų dėl duomenų subjekto teisių įgyvendinimo ir reglamentavimo valstybės institucijose teisėtumo rezultatų apibendrinimas, 2015 [interaktyvus]. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/apibendrinimassubjektoteisiu2015-02-25.pdf [žiūrėta 2020 m. spalio 12 d.].

duomenų apsaugos įgyvendinimo problema buvusi valstybės institucijose iki Bendrojo duomenų apsaugos reglamento priėmimo – duomenų valdytojų netinkamas teisės aktų įgyvendinimas bei neefektyvi Valstybinės duomenų apsaugos inspekcijos vykdoma duomenų valdytojų (valstybės institucijų) priežiūros veikla.

2.2. Duomenų apsaugos įgyvendinimo problemos po Bendrojo duomenų apsaugos reglamento priėmimo

Dėl sparčios technologinės plėtros ir globalizacijos kyla naujų asmens duomenų apsaugos sunkumų. Technologijos leidžia valdžios institucijoms vykdant savo veiklą naudotis asmens duomenimis precedento neturinčiu mastu. Elektroninei informacijai įgaunant vis didesnę reikšmę, valstybės institucijų veiklose nuolat didėja tikimybė susidurti su įvairiais informacijos saugumo incidentais – svarbių duomenų praradimais, konfidencialios informacijos paviešinimais, informacijos pasisavinimais, kenksmingomis programomis ir kt.

Kalbant apie informaciją viešojo sektoriaus įstaigose, galima pastebėti, kad šių įstaigų veikla paremta informacijos gavimu, saugojimu, apdorojimu ir pateikimu. Viešojo sektoriaus įstaigose rengiami įvairūs dokumentai: įstatymai, teisės aktai, reglamentai, įsakymai, potvarkiai, nutarimai, išvados, taisyklės ir pan. Bendravimas telekomunikacinių priemonių pagalba viešojo sektoriaus veikloje tapo kasdieniniu dalyku. Taip pat, kiekviena įstaiga savo darbe naudojasi kompiuteriais, dokumentų valdymo sistemomis, o pačias įstaigas internete reprezentuoja jų tinklalapiai. Informacijos, kaupiamos duomenų bazėse ar duomenų registruose, kiekis nuolat auga. Siekdamos pagreitinti aptarnavimą bei pagerinti teikiamų paslaugų kokybę, įstaigos stengiasi įgyvendinti „vieno langelio“ aptarnavimo principą, o taip pat didelė dalis informacijos perkeliama į elektroninę erdvę. Nuolat didėja viešųjų elektroninių paslaugų, tokių kaip pašto, bibliotekų paslaugų, pajamų deklaravimo, neteisminio ginčų nagrinėjimo, poreikis. Šių paslaugų įdiegimui yra būtinos saugios, patikimos, be trukdžių funkcionuojančios informacinės technologijos ir visa informacinė sistema, o tai – elektroninės valdžios požymis. Pastebėtina, kad viešųjų paslaugų teikimas elektroniniu būdu savaime nėra laikytinas priežastimi, sukeliančia informacijos saugumo pažeidimus, tačiau veikiau įrankis, kurio naudojimas sukelia riziką informacijos saugumo pažeidimui atsirasti. V. Domarkas (2009) elektroninę valdžią apibūdino kaip priemonę, kuri skirta valdžios įstaigų organizacinei ir administracinei veiklai gerinti, sudarant galimybę patiems piliečiams nuotoliniu būdu susipažinti su valdžios įstaigų informacija ir pasinaudoti jos teikiamomis paslaugomis[146]. Informacijos saugumo

[146] DOMARKAS, V. (2009). Įvadas į viešąjį valdymą. Elektroninė valdžia viešajame valdyme. Kaunas: Technologija, p. 151.

problemos, viešąsias paslaugas perkėlus į elektroninę erdvę, kyla iš esmės dėl to, jog asmuo, norėdamas pasinaudoti viešosiomis paslaugomis, teikiamomis elektroniniu būdu, turi save identifikuoti, tam, kad būtų užtikrinta, jog paslaugą gautų tas asmuo, kuriam ji yra skirta. Tam, kad asmuo būtų identifikuotas, reikalinga panaudoti asmens duomenis, kurie yra kaupiami viešąją paslaugą teikiančios įstaigos duomenų bazėse, sistemose, portaluose. Tačiau, kenksmingos programinės įrangos gali būti nukreiptos į viešąsias paslaugas teikiančius internetinius portalus, sistemas, bazes, o juose kaupiami duomenys gali būti surinkti. Taigi, galima teigti, kad viešųjų paslaugų perkėlimas į elektroninę erdvę yra viena iš pagrindinių priežasčių, lemiančių asmens duomenų apsaugos įgyvendinimo problemas.

Informacijos saugumo problemos viešajame sektoriuje neretai kyla dėl tokių priežasčių kaip netinkamas darbuotojų, vienaip ar kitaip susijusių su informacijos apdorojimu, elgesys. Netinkamu elgesiu galima laikyti informacinių sistemų arba informacijos panaudojimą asmeniniais ar komerciniais tikslais, t. y. su įstaigos funkcijomis nesusijusiais tikslais. Netinkamu elgesiu taip pat laikytina nesankcionuota prieiga prie įstaigos sistemų ar tinklų, įrangos gadinimas, virusų bei kenksmingų programų platinimas. Valstybinė duomenų apsaugos inspekcija, 2019 m. išanalizavusi nuo 2018 m. gautus pranešimus apie asmens duomenų saugumo pažeidimus, išskyrė dažniausią tokių pažeidimų priežastį – žmogiškąją klaidą. Pradėjus taikyti Bendrąjį duomenų apsaugos reglamentą Valstybinė duomenų apsaugos inspekcija išnagrinėjo 141 pranešimą apie asmens duomenų saugumo pažeidimą, 54 iš jų išnagrinėti nuo 2019 m. pradžios. Paveiktų fizinių asmenų skaičius sudarė daugiau nei 163 tūkstančius, o žmogiškoji klaida lėmė daugiau nei kas antrą asmens duomenų saugumo pažeidimą (71 iš 141). Valstybinė duomenų apsaugos inspekcija pažymėjo, jog dažniausia pažeidimo aplinkybė – neautorizuota prieiga prie duomenų ar jų atskleidimas (103 atvejai)[147].

Autorės nuomone, dar viena ypač svarbi informacijos saugumo problema viešojo sektoriaus įstaigose, kurią sąlygoja žmogiškoji klaida – informacijos persiuntimas. Pavyzdžiui, neteisminio ginčo nagrinėjimo institucija, išnagrinėjusi asmens prašymą (kreipimąsi), lydraščiu priimtą sprendimą per klaidą išsiunčia ne tam asmeniui, kurio atžvilgiu buvo priimtas sprendimas, o kitam. Tokiu atveju asmens, kurio atžvilgiu buvo priimtas neteisminio ginčo nagrinėjimo institucijos sprendimas, duomenys yra atskleidžiami trečiajam asmeniui, visiškai nesusijusiam nei su asmeniu, besikreipusiu į neteisminių ginčų nagrinėjimo subjektą, nei su nagrinėtu ginču. Dar viena probleminė sritis, kurią įžvelgia autorė, besisiejanti su informacijos persiuntimu – informacijos persiuntimas,

[147] Valstybinė duomenų apsaugos inspekcija. Dažniausia asmens duomenų saugumo pažeidimų priežastis – žmogiškoji klaida (tinklalapio internete skiltis) [interaktyvus]. Prieiga per internetą: https://vdai.lrv.lt/lt/naujienos/dazniausia-asmens-duomenu-saugumo-pazeidimu-priezastis-zmogiskoji-klaida [žiūrėta 2020 m. spalio 1 d.].

vykdomas tarp valstybės institucijų. Pastebėtina, kad Viešojo administravimo įstatymo 14 straipsnio 8 dalyje įtvirtinta, jog tuo atveju, kai viešojo administravimo subjektas pagal kompetenciją negali spręsti prašyme išdėstytų klausimų ar priimti administracinės procedūros sprendimo dėl skunde išdėstyto klausimo, jis jo nenagrinėja ir ne vėliau kaip per 5 darbo dienas nuo prašymo ar skundo gavimo dienos persiunčia jį kompetentingam viešojo administravimo subjektui, ir apie tai praneša asmeniui[148]. Šiame kontekste kyla klausimas, ar įstaiga, kuri turi pareigą besikreipusio asmens prašymą (skundą) pagal kompetenciją perduoti kitam viešojo administravimo subjektui, privalo gauti šio asmens sutikimą perduoti jo prašymą (skundą) kitai institucijai? Autorė šį klausimą kelia dėl to, jog asmens prašyme, kuris yra teikiamas įstaigai, yra nurodomi asmens duomenys. Minėta, jog, pavyzdžiui, vartotojas, teikdamas patvirtintos formos prašymą Valstybinei vartotojų teisių apsaugos tarnybai, prašyme nurodo vardą ir pavardę, gyvenamosios vietos adresą, telefono numerį ir elektroninio pašto adresą. Autorės nuomone, vienareikšmiško atsakymo į keliamą klausimą pateikti negalima, nes atsakymas į šį probleminį klausimą priklauso nuo tam tikrų aplinkybių. Pavyzdžiui, tais atvejais, kai asmuo, teikdamas patvirtintos formos prašymą valstybės institucijai, prašyme patvirtina, jog sutinka, kad jo teikiamo prašymo nagrinėjimo tikslu būtų tvarkomi jo asmens duomenys, autorės nuomone, atskiro sutikimo dėl jo prašymo persiuntimo pagal kompetenciją kitam viešojo administravimo subjektui, nereikia. Tuo tarpu, jei tokio sutikimo besikreipiančio asmens prašyme nebūtų, manytina, kad institucija, ketinanti asmens prašymą pagal kompetenciją perduoti kitam viešojo administravimo subjektui, turėtų gauti asmens sutikimą.

Po Bendrojo duomenų apsaugos reglamento įsigaliojimo, dar viena opi problema kibernetinės atakos ar duomenų nutekėjimai. Tokie atvejai, net jeigu būna ir netyčiniai, tačiau įstaigoms tai dideli nuostoliai ir duomenų apsaugos užtikrinimo problemos. Kartu tai ir viešojo sektoriaus įstaigų negautos pajamos, kol bus atstatyta sistemų veikla bei trečiųjų asmenų pareikštos pretenzijos dėl duomenų nutekėjimo. Taip pat naujasis Bendrasis duomenų apsaugos reglamentas įpareigoja informuoti apie galimą duomenų nutekėjimą, už kurį skiriamos ir didelės baudos. Priimtas Lietuvos Respublikos kibernetinio saugumo įstatymas nustato kibernetinio saugumo principus, kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijas, šių institucijų įgaliojimus kibernetinio saugumo srityje, kibernetinio saugumo subjektų pareigas, taip pat tarpinstitucinį bendradarbiavimą[149].

Įvertinus šiuo metu pasaulyje susiklosčiusią epidemiologinę situaciją dėl COVID-19 pandemijos, ir dėl to įstaigose pradėjus darbą organizuoti nuotoliniu būdu, kyla klausimas ar nuotolinio darbo organizavimas gali sukelti asmens duomenų apsaugos įgyvendinimo problemą? Ar

[148] Lietuvos Respublikos viešojo administravimo įstatymas (1999). Valstybės žinios, 60-1945.
[149] Lietuvos Respublikos kibernetinio saugumo įstatymas (2014). TAR, 20553.

vis dėl to įstaigose organizuojant nuotolinį darbą, galimas visapusiškas asmens duomenų apsaugos užtikrinimas? Pastebėtina, kad esanti epidemiologinė situacija, nors ir laikytina išskirtine, tačiau nepašalina įstaigos pareigos nuotolinio darbo organizavimo metu užtikrinti tinkamą asmens duomenų apsaugą. Pastebėtina, kad nuotolinis darbas savaime nesukuria asmens duomenų apsaugos įgyvendinimo problemų, tačiau yra terpė leidžianti atsirasti informacijos saugumo problemoms. To priežastis – nepakankamas saugumo priemonių panaudojimas nuotolinio darbo metu. Su šia informacijos saugumo pažeidimo rizika viešajame sektoriuje susiduriama pakankamai dažnai, nes didžioji dalis darbuotojų nėra aprūpinami darbo įrankiais, t. y. kompiuteriais ar mobiliaisiais telefonais, todėl nuotoliniu būdu jie dirba naudodamiesi asmeniniais kompiuteriais. Atsižvelgiant į tai, bei įvertinus, jog darbuotojų namuose retai yra įdiegtos papildomos tinklo saugumo priemonės, pavyzdžiui, ugniasienės, kyla informacijos saugumo pažeidimų rizika. Kita galima informacijos saugumo pažeidimo priežastis dirbant nuotoliniu būdu ir naudojantis asmeniniais darbo įrankiais (kompiuteriu) – surinktų asmens duomenų saugojimas asmeniniame kompiuteryje. Taip pat svarbi informacijos saugumo pažeidimo priežastis dirbant nuotoliniu būdu – prieigų kontrolės užtikrinimas. Tais atvejais, kai darbuotojas, dirbantis nuotoliniu būdu, dirba naudodamasis savo asmeniniu kompiuteriu, kuriuo taip pat naudojasi su kitu (-ais) šeimos nariu (-iais), kyla didelė rizika informacijos saugumo pažeidimui atsirasti, nes yra tikimybė, jog nebus pakankamai užtikrinamas prieigų kontrolės mechanizmas. Svarbu atkreipti dėmesį, kad prieigų kontrolės mechanizmo užtikrinimo pareiga tiesiogiai kyla pačiam darbuotojui, nes darbdavys negali tiesiogiai daryti įtakos nuotoliniu būdu dirbančio darbuotojo veiksmams ir reguliuoti prieigų kontrolės mechanizmo veikimo. Tačiau, nepaisant to, kad prieigų kontrolės mechanizmo užtikrinimo pareiga kyla nuotoliniu būdu dirbančiam darbuotojui, darbdavys turi pareigą pateikti informaciją darbuotojams, juos apmokyti, kad darbuotojai turėtų aišku supratimą ir įgūdžius, kaip turėtų būti užtikrinamas prieigų kontrolės mechanizmo veikimas. Praktikoje darbdavys savo pareigą supažindinti darbuotojus su informacijos saugos reikalavimais pagrindžia pateikdamas darbuotojams pasirašyti patvirtinimą dėl susipažinimo su informacijos saugumo ir konfidencialumo reikalavimais. Pavyzdžiui, Kalėjimų departamento prie Lietuvos Respublikos teisingumo ministerijos (toliau – Kalėjimų departamentas) direktoriaus 2019 m. spalio 9 d. įsakymu Nr. V-321 „Dėl Kalėjimų departamento prie Lietuvos Respublikos teisingumo ministerijos nuotolinio darbo tvarkos aprašo patvirtinimo“ patvirtinto Nuotolinio darbo tvarkos aprašo 7 punkte įtvirtinta, jog darbuotojas pirmą kartą teikdamas prašymą dirbti nuotoliniu būdu, turi užpildyti patvirtinimą dėl nuotolinio darbo sąlygų, kuris saugomas kiekvieno darbuotojo asmens byloje. Šiuo patvirtinimu darbuotojas patvirtina, kad yra susipažinęs su duomenų saugą reglamentuojančiais teisės aktais ir įsipareigoja laikytis aprašo reikalavimų bei užtikrinti asmens duomenų, neviešos, gaunamos, siunčiamos informacijos saugumą ir konfidencialumą, taip pat įsipareigoja laikytis būtinų elektroninės

informacijos saugos reikalavimų[150]. Būtina pastebėti, kad šis Kalėjimų departamento nuotolinio darbo tvarkos aprašas buvo patvirtintas ne dėl epidemiologinės situacijos, kuri paskatino darbdavius organizuoti darbą nuotoliniu būdu, o įgyvendinant Valstybės tarnybos įstatymo 50 straipsnio bei Lietuvos Respublikos Vyriausybės 2018 m. gruodžio 12 d. nutarimo Nr. 1296 „Dėl Valstybės tarnautojų ir diplomatų nuotolinio darbo tvarkos aprašo patvirtinimo“ nuostatas. Nepaisant to, nuotoliniu būdu organizuojant darbą pandemijos metu, darbuotojų pasirašytas patvirtinimas apie susipažinimą su duomenų saugą reglamentuojančiais teisės aktais bei įsipareigojimas užtikrinti asmens duomenų, neviešos, gaunamos, siunčiamos informacijos saugumą ir konfidencialumą, galioja ir nuotolinio darbo, organizuojamo pandemijos metu, laiku. Autorės nuomone, toks darbuotojų pasirašomas patvirtinimas dėl susipažinimo su informacijos saugos reikalavimais pilna apimtimi negali būti laikomas tinkamu darbdavio pareigos, informuoti (apmokyti) darbuotojus apie informacijos saugumo reikalavimus, įgyvendinimu. Manytina, jog toks darbuotojų pasirašytas patvirtinimas tik formaliai pagrindžia darbuotojų susipažinimą su informacijos saugumo reikalavimais, tačiau nereiškia, jog praktiškai tokia informacija darbuotojams buvo pateikta ir jie buvo tinkamai apmokyti bei informuoti apie kylančias grėsmes ir rizikas.

Reikėtų pastebėti dar vieną naujovę, susijusią su Bendrojo duomenų apsaugos reglamento priėmimu – tai duomenų atvėrimas[151]. Lietuvos Respublikos susisiekimo ministras 2016 m. liepos 20 d. įsakymu Nr. 3-245(1.5E) patvirtino viešojo sektoriaus duomenų atvėrimo rekomendacijas. Šiame įsakyme įtvirtinta tokia atvirų duomenų sąvoka – „tai laisvai prieinami institucijos veikloje ar dokumentuose užfiksuoti duomenys, informacija ar jos dalis, nepaisant jų pateikimo būdo, formos ir laikmenos, įskaitant registro duomenis, registro informaciją, registrui pateiktų dokumentų ir (arba) jų kopijų duomenis, valstybės informacinės sistemos duomenis, kuriuos visi asmenys gali pakartotinai naudoti ir platinti bet kokiu tikslu, nurodydami jų šaltinį ir tik tomis pačiomis sąlygomis, kuriomis buvo gauti“[152]. Atviriems duomenims yra nustatyti tam tikri kokybės kriterijai, tokie kaip tikslumas (duomenys turi būti teisingi ir tikslūs); prieinamumas (vadinasi nuorodos turi būti aktyvios ir prieinamos); išsamumas (turi apimti reikalingus duomenis, periodiškai atnaujinami duomenys), atitiktis (atiri standartai), nuoseklumas (kadangi duomenys iš skirtingų šaltinių, turi būti ištaisyti visi netikslumai); patikimumas (duomenys iš patikimų šaltinių); tinkamumas bei atnaujinimas. Tačiau kokybės kriterijai turi išlaikyti pusiausvyrą tarp duomenų teikimo bei jų apsaugos.

[150] Kalėjimų departamento prie Lietuvos Respublikos teisingumo ministerijos direktoriaus 2019 m. spalio 9 d. įsakymas Nr. V-321 „Dėl Kalėjimų departamento prie Lietuvos Respublikos teisingumo ministerijos nuotolinio darbo tvarkos aprašo patvirtinimo“ [interaktyvus]. Prieiga per internetą: http://www.kaldep.lt/download/62143/2019-10-09%20v-321.pdf [žiūrėta 2020 m. rugsėjo 21 d.].

[151] Europos Komisijos pranešimas Nr. 2014/C 240/01 „Rekomenduojamų standartinių licencijų, duomenų rinkinių ir mokesčio už pakartotinį dokumentų naudojimą apskaičiavimo gairės“.

[152] Lietuvos Respublikos susisiekimo ministro 2016 m. liepos 20 d. įsakymas Nr. 3-245(1.5E) „Dėl Viešojo sektoriaus duomenų atvėrimo rekomendacijų patvirtinimo“ [interaktyvus]. Prieiga per internetą: https://www.e-tar.lt/portal/lt/legalAct/3a0d20c04 e8311e6b72ff160 34f7f796 [žiūrėta 2020 m. lapkričio 13 d.

Kaip pavyzdžiui, valstybės įmonės Registrų centro internetinėje svetainėje yra akcentuojama, jog atviri duomenys yra laisvai prieinami Registrų centro tvarkomuose registruose ar informacinėse sistemose sukaupti duomenys ar jų dalis, kuriuos visi asmenys gali pakartotinai naudoti ir platinti bet kokiu tikslu, nurodydami jų šaltinį ir tik tomis pačiomis sąlygomis, kuriomis buvo gauti[153]. Tačiau kartu labai svarbu, kad duomenų atvėrimas nepanaikintų ribos tarp atvirų duomenų ir duomenų netinkamo ar perteklinio naudojimo. Tai tampa viena iš aktualiausių problemų šiuolaikiniu inovacijų laikotarpiu.

Išanalizavus asmens duomenų apsaugos įgyvendinimo problemas, matyti, jog laikotarpiu iki Bendrojo duomenų apsaugos reglamento priėmimo, pagrindine asmens duomenų apsaugos įgyvendinimo problema buvo duomenų valdytojų netinkamas teisės aktų įgyvendinimas bei neefektyvi Valstybinės duomenų apsaugos inspekcijos vykdoma duomenų valdytojų (valstybės institucijų) priežiūros veikla. Tuo tarpu po Bendrojo duomenų apsaugos reglamento priėmimo susiduriama su asmens duomenų apsaugos įgyvendinimo problemomis, kurios susijusios su technologijų plėtra ir šiuo metu vykstančiais darbo organizavimo pokyčiais, kuriuos paskatino esanti epidemiologinė situacija. Duomenų atvėrimas tampa viena iš prioritetinių krypčių, skatinant atvirumą ir naujumą bei prieinamumą visuomenei, tačiau kelia aibę klausimų dėl jų apsaugos.

[153] Registrų centras. Atviri duomenys (tinklalapio internete skiltis) [interaktyvus]. Prieiga per internetą: https://www.registrucentras.lt/atviri_duomenys [žiūrėta 2020 m. lapkričio 13 d.].

3. DUOMENŲ APSAUGOS ĮGYVENDINIMO PROBLEMOS IR JŲ SPRENDIMO BŪDAI VIEŠAJAME SEKTORIUJE

Išanalizavus asmens duomenų apsaugos įgyvendinimą viešosiose įstaigose bei kylančias asmens duomenų apsaugos įgyvendinimo problemas, svarbu aptarti, kokios priemonės pasitelkiamos sprendžiant problemas, kylančias įgyvendinant duomenų apsaugą viešajame sektoriuje. Pažymėtina, kad svarbiausia priemonė, pasitelkiama duomenų apsaugos įgyvendinimo problemoms spręsti – tai duomenų (informacijos) saugumo valdymas.

Informacijos saugumo valdymą apibrėžia trys elementai – strateginis, žmogiškasis ir technologinis. Strateginis elementas jungia administracinius, organizacinius, valdymo, ekonominius, standartų, teisinius, gerųjų praktikų ir panašius aspektus, žmogiškasis – saugumo kultūros, etinius, kompetencijų, mokymų, psichologinius ir panašius aspektus, o technologinis – informacinių technologijų, techninių ir programinių priemonių, matematinius, kriptografinius aspektus. Taigi informacijos saugumo valdymo turinys gali būti apibrėžiamas kaip siekis užtikrinti informacijos konfidencialumą, vientisumą ir prieinamumą proporcingai derinant strateginį, žmogiškąjį ir technologinį elementus[154].

Pastebėtina, kad siekiant valdyti informacijos saugumą nepakanka apibrėžti tik informacijos saugumo valdymo turinį, būtina numatyti ir priemones, kuriomis jis galėtų būti valdomas. Pažymėtina, kad garantuoti informacijos saugumą galima taikant įvairias apsaugos priemones. Nors šiame darbe dėmesys skiriamas asmens duomenų apsaugai viešajame sektoriuje, tačiau paminėtina, kad apsaugos priemonės yra taikomos trimis lygiais: jas taiko valstybė, taip pat duomenų apsauga rūpinasi kiekviena organizacija bei labai daug priklauso nuo konkretaus asmens suvokimo darant konkrečius veiksmus. Viešajame sektoriuje dažniausiai taikomos priemonės duomenų apsaugai yra šios: duomenų valdytojų tinkamas teisės aktų įgyvendinimas, tinkamai įgyvendinamos techninės ir organizacinės apsaugos priemonės bei įstaigos darbuotojų švietimas asmens duomenų apsaugos klausimu.

Duomenų valdytojų tinkamas teisės aktų įgyvendinimas, kaip priemonė taikoma duomenų apsaugai valdyti, yra pagrindžiama viešosios teisės principais, kurie įtvirtina, jog viešajam sektoriui leidžiama (ir privaloma) tik tai, kas nurodyta, t. y. viešasis sektorius yra įpareigotas aiškių teisinių rėmų, kurių atskiri sektoriaus subjektai negali peržengti pasirinkdami, kaip valdyti informacijos saugumą įstaigoje. Taigi, valstybės institucijų atveju labai svarbu, kad nustatyti reikalavimai būtų

[154] JASTIUGINAS, S. (2011). Informacijos saugumo valdymas Lietuvos viešajame sektoriuje. Informacijos mokslai, 57, p. 7-25 [interaktyvus]. Prieiga per interneta: https://www.zurnalai.vu.lt/informacijos-mokslai/article/view/3137/2261 [žiūrėta 2020 m. spalio 2 d.].

tikslūs, neprieštarautų teisiniam reglamentavimui ir užtikrintų efektyvų ir visapusišką informacijos saugumo valdymą, t. y. atitiktų apibrėžtą informacijos saugumo valdymo turinį[155].

Minėta, jog tinkamų techninių ir organizacinių apsaugos priemonių įgyvendinimo pareiga duomenų valdytojui tiesiogiai kyla iš Bendrojo duomenų apsaugos reglamento, kuris įtvirtina, jog atsižvelgdamas į duomenų tvarkymo pobūdį, aprėptį, kontekstą bei tikslus, taip pat į įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas įgyvendina tinkamas technines ir organizacines priemones, kad užtikrintų ir galėtų įrodyti, jog duomenys yra tvarkomi laikantis šio reglamento[156]. Organizacinės duomenų saugumo priemonės yra susijusios su tuo, kaip organizacija yra įsteigta ir vykdo veiklą, o techninių duomenų saugumo priemonių sąvoka apima mechanizmus, įrangą ir įrankius, skirtus užtikrinti informacijos saugumą[157].

Būtina paminėti, jog remiantis Bendrojo duomenų apsaugos reglamento 39 straipsnio 1 dalies a punktu[158], visos viešojo administravimo įstaigos privalo paskirti duomenų apsaugos pareigūną. Jeigu viešojo administravimo institucija ar įstaiga atitinka Asmens duomenų teisinės apsaugos įstatymo 2 straipsnio 2 dalies apibrėžimą, pagal kurią būtina turėti domenų apsaugos pareigūną, tokia institucija negali nuspręsti tokio pareigūno neskirti neskirti. O Bendrasis duomenų apsaugos reglamentas nenustato 37 straipsnio 1 dalies a punkto taikymo išimčių, todėl, vadinasi, nepriklausomai nuo to, kokia viešoji įstaiga ar koks jos dydis, asmens duomenų pareigūnas privalo būti skiriamas. Valstybinė duomenų apsaugos inspekcija pažymi, kad dėl žmogiškųjų ar finansinių išteklių trūkumo, skiriant duomenų apsaugos pareigūną, gali kilti sunkumų, todėl siūlo pasinaudoti Bendrojo duomenų apsaugos reglamento 37 straipsnio 3 dalimi, nustatančia, kad „jeigu duomenų valdytojas arba duomenų tvarkytojas yra valdžios institucija ar įstaiga, vienas duomenų apsaugos pareigūnas gali būti skiriamas kelioms tokioms institucijoms arba įstaigoms, atsižvelgiant į jų organizacinę struktūrą ir dydį“[159]. Tam tikra viešoji įstaiga gali paskirti tokį pareigūną ne tik centrinei būstinei aptarnauti, bet ir filialams. Taip pat apie paskirtą duomenų apsaugos pareigūną įstaigoje būtina pranešti Valstybinei duomenų apsaugos inspekcijai.

---

[155] JASTIUGINAS, S. (2012). Informacijos saugumo valdymas: Lietuvos Respublikos valstybės institucijų atvejis. Daktaro disertacija, humanitariniai mokslai, informacija ir komunikacija, Vilniaus universitetas. Vilnius: Vilniaus universiteto leidykla [interaktyvus]. Prieiga per internetą: http://epublications.vu.lt/object/elaba:2107839/2107839.pdf [žiūrėta 2020 m. spalio 13 d.].

[156] Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) Nr. 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) OL 2016 L 19, p. 1-88.

[157] ZALESKIS, J. (2019). Europos Sąjungos bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Vilnius: Registrų centras, p. 132.

[158] Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) Nr. 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) OL 2016 L 19, p. 1-88.

[159] Valstybinės duomenų apsaugos inspekcijos 2019 m. birželio 11 d. rekomendacija dėl duomenų apsaugos pareigūnų skyrimo viešajame sektoriuje ir jų veiklos reglamentavimo ypatumų [interaktyvus]. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomendacija-del-DAP-viesajame-sektroiuje-2019-06-13.pdf [Žiūrėta 2020 m. lapkričio 12 d.].

Šio asmens vaidmuo teisėkūros procese, kiek tai susiję su asmens duomenų tvarkymu, turėtų būti itin reikšmingas. Pastebėtina, kad viena iš užduočių, numatytų Bendrajame duomenų apsaugos reglamente – informuoti duomenų valdytoją arba duomenų tvarkytoją ir duomenis tvarkančius darbuotojus apie jų prievoles pagal šį reglamentą ir kitus Europos Sąjungos arba valstybės narės apsaugos nuostatas. Todėl viešojo administravimo įstaigos turi konsultuotis ir juos derinti su paskirtu duomenų apsaugos pareigūnu. Tokiu būdu būtų vykdoma ir duomenų valdytojui numatyta pareiga užtikrinti, kad duomenų apsaugos pareigūnas būtų tinkamai ir laiku įtraukiamas į visų su asmens duomenų apsauga susijusių klausimų nagrinėjimą.

Dažniausiai viešajame sektoriuje įgyvendinama techninė duomenų apsaugos priemonė – atitikimas nacionalinių ir tarptautinių standartizacijos organizacijų tvirtinamiems standartams. Pasauliniu mastu aktualiausi Tarptautinės standartizacijos organizacijos (*International Organisation for Standartisation – ISO*) priimti tarptautiniai susitarimai, kurie skelbiami kaip tarptautiniai standartai. Analizuojant ISO standartų katalogą, galima rasti per 350 standartų, susijusių su įvairiais informacijos saugumo valdymo aspektais, tačiau įvertinus jų turinio aprašymus svarbiausiais informacijos saugumo valdymo standartais galima įvardyti ISO 27000 grupės standartus. Šios grupės standartai skirti tiesiogiai informacijos saugumui valdyti, saugumo valdymo sistemai kurti, praktinėms priemonėms diegti, įvertinti ir organizacijai sertifikuoti, jie plačiausiai pripažįstami *de facto* informacijos saugumo valdymo geros praktikos pavyzdžiu[160]. Didžioji dalis Lietuvos viešojo sektoriaus įstaigų yra įsidiegusios informacijos saugumo valdymo sistemas, kurios atitinka ISO 27001 grupės standartų reikalavimus. Informacijos saugumo valdymo sistemos yra diegiamos tiek ministerijų lygmeniu[161], tiek ministerijoms pavaldžiose institucijose[162], tiek savivaldybės įstaigose ar valstybės ar savivaldybių įmonėse[163].

Nepaisant duomenų valdytojų tinkamo teisės aktų įgyvendinimo bei techninių ir organizacinių priemonių įgyvendinimo, asmens duomenys nebus tinkamai užtikrinami, jei įstaigos, esančios duomenų valdytoju, darbuotojai nebus tinkamai informuoti apie asmens duomenų apsaugą. Todėl įstaigos, tvarkančios asmens duomenis, darbuotojų švietimas asmens duomenų apsaugos klausimu gali padėti padidinti asmens duomenų apsaugos įgyvendinimo efektyvumą įstaigoje. Minėta, jog Valstybinė duomenų apsaugos inspekcija, 2019 m. išanalizavusi nuo 2018 m. gautus

[160] JASTIUGINAS, S. Informacijos saugumo valdymas lietuvos viešajame sektoriuje. *Informacijos mokslai*, 2011, t. 57 [interaktyvus. Žiūrėta 2020 m. spalio 2 d.]. Prieiga per interneta: < https://www.zurnalai.vu.lt/informacijos-mokslai/article/view/3137/2261>.

[161] Lietuvos Respublikos aplinkos ministerija įsidiegė informacijos saugos vadybos sistema, kuri atitinka ISO/IEC 27001 standarto reikalavimus, daugiau: https://am.lrv.lt/lt/apie-ministerija/vadybos-sistemos/kitos-sistemos.

[162] Valstybinė mokesčių inspekcija įsidiegė informacijos saugumo valdymo sistemą, kuri atitinka LST ISO/IEC 27001:2017 standarto reikalavimus mokesčių administravimo srityje, daugiau: https://www.vmi.lt/cms/informacijos-saugumo-valdymo-sistema.

[163] Žemės ūkio informacijos ir kaimo verslo centras įsidiegė informacijos saugumo valdymo sistemą, kuri atitinka standarto ISO/IEC 27001:2013 reikalavimus, daugiau: https://www.vic.lt/apie-mus/informacijos-saugumo-politika/.

pranešimus apie asmens duomenų saugumo pažeidimus, išskyrė dažniausią tokių pažeidimų priežastį – žmogiškąją klaidą. Atsižvelgiant į tai, darbuotojų mokymai duomenų saugumo ir saugumo procedūrų klausimu yra efektyviausia priemonė, skirta mažinti žmogiškąsias klaidas. Autorės nuomone, švietimas kaip informacijos saugumo valdymo įgyvendinimo priemonė yra efektyviai įgyvendinamas ne tik tada, kai yra šviečiami įstaigos darbuotojai, bet ir tuo atveju, kai šviečiama visuomenė. Jei kiekvienas asmuo žino savo, kaip duomenų subjekto teises, tuomet būdami duomenų valdytoju ar tvarkytoju, žino savo teisių ir pareigų ribas duomenų subjekto atžvilgiu. Kalbant apie visuomenės švietimą asmens duomenų apsaugos klausimu, būtina paminėti, jog 2019 m. Valstybinės duomenų apsaugos inspekcijos iniciatyva įmonė „Spinter tyrimai“ atliko Lietuvos gyventojų tyrimą, kurio tikslu buvo siekis išsiaiškinti gyventojų nuomonę ir informuotumą dėl asmens duomenų apsaugos. Atliekant gyventojų tyrimą apie asmens duomenų apsaugą respondentams buvo užduotas klausimas „*Ar teko girdėti apie 2018 m. gegužės 25 d. visoje Europoje ir Lietuvoje pradėtą taikyti naują asmens duomenų apsaugos teisės aktą – Bendrąjį duomenų apsaugos reglamentą?*“. Teigiamai į šį klausimą atsakė 72 proc. respondentų. Į klausimą „*Ar Jūs žinote apie įstatymų Jums suteiktas teises ar nustatytas pareigas asmens duomenų apsaugos srityje?*“ teigiamai atsakė 68 proc. respondentų. 70 proc. respondentų žinojo, kad asmens duomenų apsaugos teisės aktai jiems suteikia galimybę gauti informaciją apie savo asmens duomenų tvarkymą, po 66 proc. – susipažinti su savo asmens duomenimis, kurie yra tvarkomi ir nesutikti, kad asmens duomenys būtų tvarkomi rinkodaros tikslais arba nesutikti, kad būtų tvarkomi bet kokie su konkrečiu atveju susiję asmens duomenys[164].

Taigi, informacijos saugumo valdymu yra siekiama užtikrinti informacijos konfidencialumą, vientisumą ir prieinamumą proporcingai derinant strateginį, žmogiškąjį ir technologinį elementus. Viešajame sektoriuje informacijos saugumo valdymas yra įgyvendinamas pasitelkiant įvairias apsaugos priemones, tačiau dažniausiai taikomomis priemonėmis laikytinos šios: duomenų valdytojų tinkamas teisės aktų įgyvendinimas, tinkamai įgyvendinamos techninės ir organizacinės apsaugos priemonės bei įstaigos darbuotojų švietimas asmens duomenų apsaugos klausimu.

[164] Lietuvos gyventojų tyrimas apie asmens duomenų apsaugą [interaktyvus]. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/2019%20m_%20ADA%20apklausos%20ataskaitos%20skaidres%202020-01-15.pdf [žiūrėta 2020 m. spalio 11 d.].

IŠVADOS

1. Viešojo administravimo subjektų veiklos išskirtinumas yra tam tikra subjektų veikla, kuri skirta viešųjų paslaugų tenkinimui, įgyvendinant teisės aktus. Asmens duomenimis laikoma informacija, susijusi su fiziniu asmeniu, kurio tapatybė yra žinoma ar kurią galima tiesiogiai ar netiesiogiai nustatyti. Viešojo sektoriaus išskirtinumas – nepažeisti pusiausvyros tarp viešųjų interesų įgyvendinimo ir asmens duomenų apsaugos.

2. Viešojo sektoriaus veikla paremta duomenų tvarkymo principais, kurie daro įtaką tiek viešųjų interesų tenkinimui, tiek ir pusiausvyros teikiant duomenis palaikymui. Teisėtumo, sąžiningumo ir skaidrumo principai suponuoja informacijos sklaidą ir atskaitingumą visuomenei bei yra susiję su duomenų atvėrimu. Duomenų tvarkymo apribojimo principas suponuoja, kad duomenys būtų renkami pagal konkretų tikslą, nustatant duomenų gavėjo tinkamumą ir proporcingą asmens duomenų apimtį. Duomenų kiekio mažinimo principas reiškia, kad duomenys turi būti tvarkomi tik tam, jeigu to tikslo kitomis priemonėmis pasiekti nėra įmanoma, taip būtina įgyvendinti asmens teisę „būti pamirštam“. Vientisumo ir konfidencialumo principais grindžiamas tikslingas asmens duomenų atskleidimas, tam pasirašomi konfidencialumo pasižadėjimai tiek darbuotojų, tiek asmenų, kurie gauna duomenis.

3. Asmens duomenų sąvoka talpina savyje informaciją apie konkretų asmenį, kurio apsaugai reikia parinkti tinkamas organizacines ir technines priemones, kurios priklauso nuo duomenų tvarkymo pobūdžio, konteksto ir tikslų. Asmens duomenų tvarkymo pagrindai, įtvirtinti Bendrajame duomenų apsaugos reglamente įpareigoja viešojo sektoriaus funkcijas vykdyti tik siekiant konkretaus tikslo ir tvarkyti tik tuos duomenis, kurie reikalingi konkrečiam tikslui pasiekti. Problematiką suponuoja tai, kad tikslus iškeltas tikslas turi atitikti subjekto veiklą, kad duomenų tvarkymas būtų tikslingas ir proporcingas numatytam teisiniam reglmentavimui. Viešojo sektoriaus funkcijų vykdymas, remiantis Bendrojo duomenų apsaugos reglamento 6 straipsnio c ir e punktais suponuoja, kad valstybės nacionalinėje teisėje būtų įtvirtintas tikslus reglamentavimas.

4. Bendrojo duomenų apsaugos reglamento priėmimas atvėrė naują etapą duomenų apsaugos sferoje. Tikslingas duomenų atvėrimas visuomenei po Bendrojo duomenų apsaugos reglamento įsigaliojimo tapo vienu iš inovatyviausių, tačiau ir probleminių reiškinių, sąlygojantis atvirumą, skaidrumą bei prieinamumą visuomenei duomenų apsaugos sferoje. Duomenų atvėrimas visuomenei turi užtikrinti jų prieinamumą, patikimumą, tačiau jų teikimas, užtikrinant jų apsaugą, tapo nauju aspektu.

5. Duomenų saugumo valdymas viešajame sektoriuje ir konfidencialumo užtikrinimas, kartu suderinant duomenų prienamumą visuomenei tampa vienu svarbiausių iššūkių. Sugebėjimas išlaikyti pusiausvyrą tarp duomenų prieinamumo ir aiškaus teisinio reglamentavimo, įgyvendinant

Bendrojo duomenų apsaugos reglamento politiką, reikalauja viešojo sektoriaus įmonėms įgyvendinti tinkamas technines ir saugos priemones. Viešajame sektoriuje dažniausiai pasitaikančios žmogiškosios klaidos ir ne viasada tinkamai techniškai užtikrinama duomenų apsauga reikalauja didesnio dėmesio asmens duomenų apsaugos klausimams. Probleminiu aspektu tampa ir tai, kaip apsaugoti duomenis nuo bet kokių kibernetinių atakų, užtikrinant saugumą, kad negrėstų duomenų praradimas ar „nutekėjimas“. Duomenų apsaugos suvaldymas viešajame sektoriuje grindžiamas žmogiškaisiais, strateginiais ir technologiniais resursais, kuriuos diegia pati valstybė, įmonė ar konkretus individas.

ŠALTINIŲ SĄRAŠAS

TEISĖS NORMINIAI AKTAI

Tarptautinės sutartys

1. Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis (1981). *Valstybės žinios*, 2001, 32-1059.
2. Visuotinė žmogaus teisių deklaracija (1948). *Valstybės žinios*, 2006, 68-2497.

Europos Sąjungos teisės aktai

1. Europos parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) Nr. 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) OL 2016 L 19, p. 1-88.
2. Europos Sąjungos 2000 m. gruodžio 7 d. pagrindinių teisių chartija Nr. 2016/C 202/02, p. 391-405.
3. Europos Parlamento ir Tarybos 1995 m. spalio 24 d. direktyva Nr. 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. OL 2004, p. 355-374.

Lietuvos Respublikos teisės aktai

1. Lietuvos Respublikos Konstitucija (1992). *Valstybės žinios*, 33-1014.
2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (2018). TAR, 11733.
3. Lietuvos Respublikos civilinis kodeksas (2000). *Valstybės žinios*, 74-2262.
4. Lietuvos Respublikos asmens tapatybės kortelės ir paso įstatymas (2014). TAR, 21281.
5. Lietuvos Respublikos viešojo administravimo įstatymas (1999). *Valstybės žinios*, 60-1945.
6. Lietuvos Respublikos valstybės informacinių išteklių įstatymas (2011). *Valstybės žinios*, 163-7739.
7. Lietuvos Respublikos kibernetinio saugumo įstatymas (2014). *TAR*, 20553.
8. Lietuvos Respublikos dokumentų ir archyvų įstatymas (1995). *Valstybės žinios*, 107-2389.
9. Lietuvos Respublikos pinigų plovimo ir teroristų finansavimo prevencijos įstatymas (1997). *Valstybės žinios*, 64-1502.

Lietuvos Respublikos Vyriausybės nutarimai

1. Lietuvos Respublikos Vyriausybės 2006 m. birželio 19 d. nutarimas Nr. 601 „Dėl Elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinės strategijos iki 2008 metų ir jos įgyvendinimo priemonių plano patvirtinimo“. Valstybės žinios, 70-2575.

SPECIALIOJI LITERATŪRA

1. DOMARKAS, V. (2009). *Įvadas į viešąjį valdymą. Elektroninė valdžia viešajame valdyme*. Kaunas: Technologija.
2. GIEDRAITYTĖ, V. (2016) *Viešojo sektoriaus inovacijų proceso trikdžių valdymas Lietuvos savivaldybių administracijose*. Daktaro disertacija, socialiniai mokslai, vadyba.
3. GUISE, P. (2017). *Data Protection: Ensuring Data Availability* [interaktyvus], Auerbach Publications. Prieiga per internetą: https://books.google.lt/books?id=As1BDgAAQBAJ&printsec=frontcover&hl=lt#v=onepage&q&f=false [žiūrėta 2020 m. rugsėjo 20 d.].
4. JASTIUGINAS, S. (2011). Informacijos saugumo valdymas Lietuvos viešajame sektoriuje. *Informacijos mokslai*, 57, p. 7-25 [interaktyvus]. Prieiga per interneta: https://www.zurnalai.vu.lt/informacijos-mokslai/article/view/3137/2261 [žiūrėta 2020 m. spalio 2 d.].
5. JASTIUGINAS, S. (2012). *Informacijos saugumo valdymas: Lietuvos Respublikos valstybės institucijų atvejis*. Daktaro disertacija, humanitariniai mokslai, informacija ir komunikacija, Vilniaus universitetas. Vilnius: Vilniaus universiteto leidykla [interaktyvus]. Prieiga per internetą: http://epublications.vu.lt/object/elaba:2107839/2107839.pdf [žiūrėta 2020 m. spalio 13 d.].
6. LANE, J. E. (2001). *Viešasis sektorius: sąvokos, modeliai ir požiūriai*. Vilnius: Margi raštai.
7. MIKELĖNAS, V. et al. (2001). *Lietuvos Respublikos civilinio kodekso komentaras. Pirmoji knyga*. Vilnius: Justitia.
8. PETRAITYTĖ, I. (2013). *Asmens duomenų teisinės apsaugos principai*. Daktaro disertacija, socialiniai mokslai, teisė, Vilniaus universitetas. Vilnius: Vilniaus universiteto leidykla [interaktyvus]. Prieiga per internetą: http://epublications.vu.lt/object/elaba:1823635/1823635.pdf [žiūrėta 2020 m. rugsėjo 20 d.].

9. VAIČAITIS, V. (2009). Teisingumo samprata ir Lietuvos Respublikos Konstitucinis Teismas. *Konstitucinė jurisprudencija,* p. 206-221 [interaktyvus] Prieiga per internetą: https://www.tf.vu.lt/wp-content/uploads/2016/12/V.-Vaičaitis.-Teisingumo-samprata-ir-Lietuvos-Respublikos-Konstitucinis-Teismas.pdf [žiūrėta 2020 m. rugsėjo 25 d.].
10. VITKEVIČIUS, P. (2004a). *Civilinė teisė*. Vilnius: Mykolo Romerio universiteto Leidybos centras.
11. VITKEVIČIUS, P. (2004b). Civilinės teisės subjekto ir civilinio teisinio subjektiškumo problemos. *Jurisprudencija*, 55 (47), p. 102–113 [interaktyvus]. Prieiga per internetą http://www.mruni.eu/lt/mokslodarbai/jurisprudencija/archyvas/dwn.php?id=279391 [žiūrėta 2020 m. rugsėjo 24 d.].
12. ZALESKIS, J. (2019). *Europos Sąjungos bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: Registrų centras.

TEISMŲ PRAKTIKA

Europos Žmogaus Teisių Teismo sprendimai:

1. *Amann prieš Šveicariją* [EŽTT], Nr. 27798/95, [2000-02-16]. ECLI:CE:ECHR: 2000:0216JUD002779895.

Europos Sąjungos Teisingumo Teismo sprendimai:

1. *Bodil Lindqwist* [ESTT], Nr. C-101/2001, [2003-11-06]. ECLI:EU:C:2003:596.

Konstitucinio teismo jurisprudencija:

1. Lietuvos Respublikos Konstitucinio Teismo 2008 m. sausio 22 d. nutarimas. Valstybės žinios, 10-35.
2. Lietuvos Respublikos Konstitucinio Teismo 2002 m. rugsėjo 19 d. nutarimas, *Valstybės žinios*, Nr. 93-4000.

Bendros kompetencijos teismų praktika:

1. Lietuvos Aukščiausiojo Teismo 2014 m. gegužės 22 d. nutartis civilinėje byloje Nr. 3K-3-286/2014.

Specializuotų teismų praktika:

1. Lietuvos Vyriausiojo administracinio teismo 2015 m. gruodžio 15 d. nutartis byloje Nr. A-1544-552/2015.

KITI ŠALTINIAI

Europos Sąjungos *soft-law* šaltiniai

1. European Union Agency For Network and Information Security. Handbook on Security of Personal Data Processing. (2018). [interaktyvus]. Prieiga per internetą: https://op.europa.eu/lt/publication-detail/-/publication/1a860879-1dce-11e8-ac73-01aa75ed71a1 [Žiūrėta 2020 m. rugsėjo 26 d.].
2. Europos Sąjungos 29 straipsnio darbo grupės 2017 m. lapkričio 29 d. Gairės dėl skaidrumo pagal reglamentą (ES) 2016/679 Nr. WP260 [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id= 622227 [žiūrėta 2020 m. rugsėjo 26 d.].
3. Europos Sąjungos 29 darbo grupės 2013 m. balandžio 3 d. Nuomonė dėl tikslo apribojimo Nr. WP203 [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files /201 3/ wp203en.pdf [žiūrėta 2020 m. rugsėjo 26 d.].
4. Europos Sąjungos 29 straipsnio duomenų apsaugos darbo grupės 2007 m. birželio 20 d. Nuomonė Nr. 4/2007 dėl asmens duomenų sąvokos Nr. WP 136 [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_lt.pdf [žiūrėta 2020 m. rugsėjo 21 d.].
5. Europos Sąjungos 29 straipsnio duomenų apsaugos darbo grupės 2016 m. gruodžio 13 d. Gairės dėl duomenų apsaugos pareigūnų Nr. WP 243 [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/newsroom/document.cfm?docid=44100 [žiūrėta 2020 m. spalio 5 d.].
6. Europos Komisijos pranešimas Nr. 2014/C 240/01 „Rekomenduojamų standartinių licencijų, duomenų rinkinių ir mokesčio už pakartotinį dokumentų naudojimą apskaičiavimo gairės“.
7. Europos duomenų apsaugos valdybos patvirtintos gairės 05/2020 „Dėl sutikimo pagal Reglamentą 2016/679“ [interaktyvus]. Prieiga per internetą: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf [žiūrėta 2020 m. lapkričio 5 d.].
8. European Union Agency For Network and Information Security. Handbook on Security of Personal Data Processing (2018) [interaktyvus]. Prieiga per internetą:

https://op.europa.eu/lt/publication-detail/-/publication/1a860879-1dce-11e8-ac73-01aa75ed71a1 [žiūrėta 2020 m. rugsėjo 26 d.].

Lietuvos nacionaliniai *soft-law* šaltiniai

1. Valstybinė duomenų apsaugos inspekcija. 2018 m. spalio 31. Tinkamų organizacinių ir techninių duomenų saugumo priemonių įgyvendinimo gaires asmens duomenų valdytojams ir tvarkytojams [interaktyvus]. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomendtechpriemonesgaires2018.pdf [žiūrėta 2020 m. rugsėjo 27 d.].
2. Valstybinė duomenų apsaugos inspekcija. Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gaires duomenų valdytojams ir duomenų tvarkytojams, 2019 m. gruodžio 18 d. [interaktyvus]. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/VDAIsaugumopriemoniugaires-2019-12-18.pdf [žiūrėta 2020 m. rugsėjo 30 d.].
3. Valstybinė duomenų apsaugos inspekcija. Biometrinių duomenų tvarkymas elektroninėje erdvėje [interaktyvus]. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/RekomendBiometriniai2017.pdf [žiūrėta 2020 m. spalio 21 d.].
4. Kalėjimų departamento prie Lietuvos Respublikos teisingumo ministerijos direktoriaus 2019 m. spalio 9 d. įsakymas Nr. V-321 „Dėl Kalėjimų departamento prie Lietuvos Respublikos teisingumo ministerijos nuotolinio darbo tvarkos aprašo patvirtinimo“ [interaktyvus]. Prieiga per internetą: http://www.kaldep.lt/download/62143/2019-10-09%20v-321.pdf [žiūrėta 2020 m. rugsėjo 21 d.].
5. Lietuvos Respublikos socialinės apsaugos ir darbo ministro 2018 m. spalio 31 d. įsakymas Nr. A1-610 „Dėl Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos asmens duomenų apsaugos politikos patvirtinimo“ [interaktyvus]. Prieiga per internetą: https://socmin.lrv.lt/uploads/socmin/documents/files/administracine-informacija/Asmens%20duomenu%20apsauga/ Politika.pdf [žiūrėta 2020 m. spalio 12 d.]..
6. Valstybinė duomenų apsaugos inspekcija. Rekomendacija dėl reikalavimų teisės aktų projektams, kuriais reglamentuojamas asmens duomenų tvarkymas (20180 [interaktyvus]. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/Infobdarteisekuros20170425.pdf [žiūrėta 2020 m. rugsėjo 30 d.].
7. Lietuvos Respublikos sveikatos apsaugos ministro 2015 m. balandžio 2 d. įsakymas Nr. V-456 „Dėl duomenų subjektų teisių įgyvendinimo Sveikatos apsaugos ministerijoje tvarkos aprašo patvirtinimo“ [interaktyvus]. Prieiga per internetą:

https://sam.lrv.lt/uploads/sam/documents/files/Administracine_informacija/Asmensduomenuapsauga/2015-04-02%20V-456%20Del%20Duomenu%20subjektu%20teisiu%20igyvendinimo%20Sveikatos%20apsaugos%20ministerijoje%20tvarkos%20apraso%20patvirtinimo.pdf [žiūrėta 2020 m. spalio 12 d.].

8. Lietuvos Respublikos vyriausiojo valstybinio darbo inspektoriaus įsakymu patvirtintas Asmens duomenų tvarkymo, saugojimo ir šių duomenų subjektų teisių įgyvendinimo Valstybinėje darbo inspekcijoje prie Socialinės apsaugos ir darbo ministerijos tvarkos aprašas [interaktyvus]. Prieiga per internetą: https://www.vdi.lt/PdfUploads/Asmens duomenu_tvarkymas.pdf [žiūrėta 2020 m. spalio 12 d.].
9. Lietuvos banko valdybos pirmininko 2018 m. liepos 20 d. įsakymas Nr. V 2018/(1.7.E-260603)-02-113 dėl Lietuvos banko bendrųjų asmens duomenų tvarkymo nuostatų patvirtinimo [interaktyvus]. Prieiga per internetą: https://www.lb.lt/uploads/documents/files/Asmens%20duomenu%20tvarkymo%20nuostatainauja_2019_07_30.pdf [žiūrėta 2020 m. rugsėjo 27 d.].
10. Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2018 m. rugpjūčio 7 d. įsakymas Nr. 1V-714 dėl duomenų subjektų teisių įgyvendinimo Lietuvos Respublikos ryšių reguliavimo tarnyboje tvarkos aprašo patvirtinimo [interaktyvus]. Prieiga per internetą: https://www.rrt.lt/wp-content/uploads/2018/08/Duomen%C5%B3-subjekt%C5%B3-teisi%C5%B3-%C4%Afgyvendinimo-Lietuvos-Respublikos-ry%C5%A1i%C5%B3-reguliavimo-tarnyboje-tvarkos-apra%C5%A1as.p df [žiūrėta 2020 m. rugsėjo 27 d.].
11. Valstybės įmonės Registrų centro 2018 m. gegužės 24 d. direktoriaus įsakymas Nr. v-171 „Dėl asmens duomenų tvarkymo valstybės įmonėje Registrų centre tvarkos aprašo patvirtinimo“ [interaktyvus]. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/1804741065d311e8b7d2b2d2ca774092/asr [žiūrėta 2020 m. lapkričio 10 d.].
12. Lietuvos Respublikos Vyriausybės 2014 m. gruodžio 23 d. nutarimas Nr. 1495 „Dėl Lietuvos Respublikos gyventojų registro nuostatų patvirtinimo“ [interaktyvus]. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/478d0920903111e48028e9b85331c55d/asr? [žiūrėta 2020 m. lapkričio 10 d.].
13. Valstybinės duomenų apsaugos inspekcijos 2019 m. birželio 11 d. rekomendacija dėl duomenų apsaugos pareigūnų skyrimo viešajame sektoriuje ir jų veiklos reglamentavimo ypatumų [interaktyvus]. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomendacija-del-DAP-viesajame-sektroiuje-2019-06-13.pdf [Žiūrėta 2020 m. lapkričio 12 d.].
14. Lietuvos Respublikos susisiekimo ministro 2016 m. liepos 20 d. įsakymas Nr. 3-245(1.5E) „Dėl Viešojo sektoriaus duomenų atvėrimo rekomendacijų patvirtinimo“ [interaktyvus].

Prieiga per internetą: https://www.e-tar.lt/portal/lt/legalAct/3a0d20c04_e8311e6b72ff16034f7f796 [žiūrėta 2020 m. lapkričio 13 d.

15. Lietuvos Respublikos ekonomikos ir inovacijų ministro 2014 m. rugpjūčio 6 d. įsakymas Nr. 4-527 „Dėl Lietuvos metrologijos inspekcijos nuostatų patvirtinimo“ [interaktyvus]. Prieiga per internetą: <https://www.e-tar.lt/portal/lt/legalAct/ff04dfe01d5611e4b542dec0b12e28b0/asr Žiūrėta 2020 m. lapkričio 12 d.].

Internetiniai tinklalapiai

1. Valstybinė vartotojų teisių apsaugos tarnyba. Struktūra ir kontaktai (tinklalapio internete skiltis) [interaktyvus]. Prieiga per internetą: http://www.vvtat.lt/struktura-ir-kontaktai/padaliniu-uzdaviniai-ir-funkcijos/596/vidaus-administravimo-skyrius/d51 [žiūrėta 2020 m. rugsėjo 26 d.].
2. Valstybinė vartotojų teisių apsaugos tarnyba. Paslaugos (tinklalapio internete skiltis) [interaktyvus]. Prieiga per internetą: http://www.vvtat.lt/paslaugos/prasymai/vartotojo-prasymo-forma/345 [žiūrėta 2020 m. rugsėjo 26 d.].
3. Lietuvos bankas. Informacija apie asmens duomenų apsaugą (tinklalapio internete skiltis) [interaktyvus]. Prieiga per internetą: https://www.lb.lt/lt/informacija-apie-asmens-duomenu-apsauga#ex-1-23 [žiūrėta 2020 m. rugsėjo 26 d.].
4. Valstybinė duomenų apsaugos inspekcija. Skundų nagrinėjimas (tinklalapio internete skiltis) [interaktyvus]. Prieiga per internetą: https://vdai.lrv.lt/lt/veiklos-sritys-1/skundu-nagrinejimas [žiūrėta 2020 m. rugsėjo 26 d.].
5. Ryšių reguliavimo tarnyba. Vartotojų teisių apsauga (tinklalapio internete skiltis) [interaktyvus]. Prieiga per internetą: https://www.rrt.lt/pastas/vartotoju-teisiu-apsauga/kaip-pateikti-skunda/ [žiūrėta 2020 m. rugsėjo 26 d.].
6. Lietuvos metrologijos inspekcija. Asmens duomenų apsauga (tinklalapio internete skiltis) [interaktyvus]. Prieiga per internetą: https://metrinsp.lrv.lt/lt/asmens-duomenu-apsauga [žiūrėta 2020 m. rugsėjo 26 d.].
7. Valstybės kontrolės valstybinio audito 2013 m. gruodžio 11 d. ataskaita Nr. VA-P-90-3-21 „Automatiniu būdu tvarkomų asmens duomenų apsauga“. [interaktyvus]. Prieiga per internetą: https://www.vkontrole.lt/failas.aspx?id=3088 [žiūrėta 2020 m. spalio 1 d.].
8. Valstybinė mokesčių inspekcija. Informacijos saugumo valdymo sistema (tinklalapio internete skiltis) [interaktyvus]. Prieiga per internetą: https://www.vmi.lt/cms/informacijos-saugumo-valdymo-sistema [žiūrėta 2020 m. spalio 1 d.].

9. Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos. Informacijos saugos valdymo sistema (tinklalapio internete skiltis) [interaktyvus]. Prieiga per internetą: https://www.ird.lt/lt/veiklos-sritys/informacijos-sauga/informacijos-saugos-valdymo-sistema [žiūrėta 2020 m. spalio 1 d.].
10. Lietuvos statistikos departamentas. Informacijos saugos valdymo sistema (tinklalapio internete skiltis) [interaktyvus]. Prieiga per internetą: https://www.stat.gov.lt/informacijos-saugumo-valdymo-sistema [žiūrėta 2020 m. spalio 1 d.].
11. Žemės ūkio informacijos ir kaimo verslo centras. Informacijos saugumo politika (tinklalapio internete skiltis) [interaktyvus]. Prieiga per internetą: https://www.vic.lt/apie-mus/informacijos-saugumo-politika/ [žiūrėta 2020 m. spalio 1 d.].
12. Valstybinė duomenų apsaugos inspekcija. Dažniausia asmens duomenų saugumo pažeidimų priežastis – žmogiškoji klaida (tinklalapio internete skiltis) [interaktyvus]. Prieiga per internetą: https://vdai.lrv.lt/lt/naujienos/dazniausia-asmens-duomenu-saugumo-pazeidimu-priezastis-zmogiskoji-klaida [žiūrėta 2020 m. spalio 1 d.].
13. Lietuvos gyventojų tyrimas apie asmens duomenų apsaugą [interaktyvus]. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/2019%20m_%20ADA%20apklausos%20ataskaitos%20skaidres%202020-01-15.pdf [žiūrėta 2020 m. spalio 11 d.].
14. Spaudos centras „Seimo Pirmininko pavaduotojo G. Kirkilas: švietimas apie asmens duomenų apsaugą jau reikalingas mažiausiems piliečiams“ [interaktyvus]. Prieiga per internetą: https://sc.bns.lt/view/item/158942 [žiūrėta 2020 m. spalio 10 d.].
15. Vartotojų teisių informacinė sistema (VTIS). El. paslaugos (tinklalapio internete skiltis) [interaktyvus]. Prieiga per internetą: https://vtis.lt/portal/#/services/complaint/intro/4 [žiūrėta 2020 m. spalio 10 d.].
16. Valstybinė teismo medicinos tarnyba prie Lietuvos Respublikos teisingumo ministerijos. Tvarkų aprašai, taisyklės, nuostatai (tinklalapio internete skiltis) [interaktyvus]. Prieiga per internetą: http://www.vtmt.lt/media/PDFbylos/Konf.informacijos%20tvarka.pdf [žiūrėta 2020 m. spalio 10 d.].
17. Valstybinė duomenų apsaugos inspekcija. Tikrinimų dėl duomenų subjekto teisių įgyvendinimo ir reglamentavimo valstybės institucijose teisėtumo rezultatų apibendrinimas, 2015 [interaktyvus]. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/apibendrinimassubjektoteisiu2015-02-25.pdf [žiūrėta 2020 m. spalio 12 d.].
18. Valstybinė vartotojų teisių apsaugos tarnyba. Padalinių uždaviniai ir funkcijos (tinklalapio internete skiltis) [interaktyvus]. Prieiga per internetą: http://www.vvtat.lt/struktura-ir-kontaktai/padaliniu-uzdaviniai-ir-funkcijos/596/vidaus-administravimo-skyrius/d51 [žiūrėta 2020 m. spalio 12 d.].

19. Duomenų apsauga pagal BDAR [interaktyvus]. Prieiga per internetą: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_lt.htm [žiūrėta 2020 m. rugsėjo 27 d.].
20. Tarptautinių žodžių žodynas [interaktyvus]. Prieiga per internetą: https://tzz.lt/i/identifikuoti/ [žiūrėta 2020 m. spalio 22 d.
21. Valstybinė lietuvių kalbos komisija [interaktyvus]. Prieiga per internetą: http://www.vlkk.lt/konsultacijos/5177-identitetas [žiūrėta 2020 m. spalio 22 d.
22. Teise.pro. *Nuo „gero administravimo“ principo verslo reguliavime iki asmens biometrinių duomenų panaudojimo viešajame administravime*. [interaktyvus]. Prieiga per internetą: http://www.teise.pro/index.php/2019/06/07/nuo-gero-administravimo-principo-verslo-reguliavime-iki-asmens-biometriniu-duomenu-panaudojimo-viesajame-administravime [žiūrėta 2020 m. lapkričio 12 d.].
23. Valstybinė duomenų apsaugos inspekcija. *Atliekami tikrinimai dėl biometrinių duomenų tvarkymo teisėtumo.* [interaktyvus]. Prieiga per internetą: https://vdai.lrv.lt/lt/naujienos/atliekami-tikrinimai-del-biometriniu-duomenu-tvarkymo-teisetumo [žiūrėta 2020 m. spalio 12 d.].
24. Lietuvos Respublikos sveikatos apsaugos ministerija. Asmens duomenų apsauga (tinklalapio internete skiltis) [interaktyvus]. Prieiga per internetą: https://sam.lrv.lt/lt/asmens-duomenu-apsauga/informacija-apie-sveikatos-apsaugos-ministerijoje-tvarkomus-asmens-duomenis [žiūrėta 2020 m. lapkričio 12 d.].
25. Registrų centras. Atviri duomenys (tinklalapio internete skiltis) [interaktyvus]. Prieiga per internetą: https://www.registrucentras.lt/atviri_duomenys [žiūrėta 2020 m. lapkričio 13 d.].
26. Duomenų apsauga pagal BDAR [interaktyvus]. Prieiga per internetą: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_lt.htm

SANTRAUKA

Asmens duomenų apsauga yra viena iš pamatinių teisių, o laisvas asmens duomenų judėjimas – tai visuotinė gerovė. Nors požiūris į asmens privatumą keičiasi dėl sparčios technologijų pažangos, nuolatinių globalizacijos reiškinių bei išaugusio poreikio dalintis asmenine informacija, teisių į asmens duomenų apsaugą ir privatumą užtikrinimas išlieka itin svarbus reiškinys. Viešojo sektoriaus įstaigoms vykdant joms priskirtas funkcijas tapo būtina tvarkyti tam tikrą kiekį asmens informacijos, todėl atsirado poreikis užtikrinti duomenų apsaugos įgyvendinimo procesą viešajame sektoriuje. Siekiant viešajame sektoriuje užtikrinti duomenų apsaugos įgyvendinimo procesą buvo reikalinga patvirtinti duomenų apsaugai skirtą vidinių dokumentų paketą, kuris reglamentuotų duomenų tvarkymo pagrindus, įstaigoms tvarkant duomenis, taip pat duomenų tvarkymo procese vadovautis duomenų tvarkymo principais bei taikyti tinkamas duomenų saugumo priemones.

Svarbi duomenų apsaugos įgyvendinimo problema, vyraujanti viešajame sektoriuje – tai sparti technologinė plėtra, sukelianti naujų asmens duomenų apsaugos sunkumų. Technologijos leidžia valdžios institucijoms vykdant savo veiklą naudotis asmens duomenimis precedento neturinčiu mastu. Elektroninei informacijai įgaunant vis didesnę reikšmę, valstybės institucijų veiklose nuolat didėja tikimybė susidurti su įvairiais informacijos saugumo incidentais – svarbių duomenų praradimais, konfidencialios informacijos paviešinimais, informacijos pasisavinimais, kenksmingomis programomis ir kt.

SUMMARY

The protection of personal data is a fundamental right and the free movement of personal data is a common good. Although attitudes towards personal privacy are changing due to rapid technological progress, the constant phenomena of globalization and the increased need to share personal information, the enforcement of personal data protection and privacy rights remains a crucial phenomenon. The exercise of the functions assigned to them by public sector bodies has made it necessary to process a certain amount of personal information, which has created the need to ensure the implementation of data protection in the public sector. In order to ensure the implementation process of data protection in the public sector, it was necessary to adopt a package of internal documents for data protection, which would regulate the basics of data processing by institutions, as well as data processing principles and appropriate data security measures.

An important issue in the implementation of data protection in the public sector is rapid technological development, which poses new challenges for the protection of personal data. Technology enables public authorities to use personal data on an unprecedented scale in the course of their activities. As electronic information becomes more and more important, the probability of encountering various information security incidents in the activities of state institutions is constantly increasing – loss of important data, disclosure of confidential information, misappropriation of information, malware, etc.