MYKOLO ROMERIO UNIVERSITETO

VIEŠOJO SAUGUMO AKADEMIJA

DOVILĖS BILEVAITĖS

TEISĖS IR POLICIJOS VEIKLOS

ASMENS DUOMENŲ APSAUGOS KONTROLĖS ĮGYVENDINIMO PROBLEMINIAI ASPEKTAI

Magistro baigiamasis darbas

Vadovė: Dr. A. Margevičiūtė

.....

(parašas)

Darbo autorė: D. Bilevaitė

.....

(parašas)

Kaunas, 2024

TURINYS

SANTRUMPŲ SĄRAŠAS

BDAR – 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB;

ES – Europos Sąjunga;

ETDA - Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ets nr. 108);

ES chartija - Europos Sąjungos pagrindinių teisių chartija;

VDAI – Valstybinė duomenų apsaugos priežiūros institucija;

LR ADTAĮ – Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

LR KSĮ – LR kibernetinio saugumo įstatymas;

DAP – duomenų apsaugos pareigūnas;

DAP gairės – 29 straipsnio darbo grupė Skaidrumo užtikrinimo pagal Reglamentą (ES) 2016/679 gairės;

ADSP – asmens duomenų saugos pažeidimas;

VTP – veiklos tęstinumo planas;

IT – informacinės technologijos;

LVAT - Lietuvos vyriausiasis administracinis teismas.

ĮVADAS

Baigiamojo darbo aktualumas. Paskutiniais dešimtmečiais, sparčiai vystantis informacinėms technologijoms, bei informacijos sklidimo laisve pasaulyje, pastebimai kito ir asmenų požiūris į asmenų privatumą ir asmens duomenis. XX a. privatumas įgavo teisinį apibrėžimą, kuris pradėjo galioti tarptautinėse bendruomenėse, kurios pripažino privatumą kaip būtiną teisės normą, ko pasekoje pradėjo formuotis teisės normos bei nacionaliniai teisės aktai, tuo pačiu metu vystėsi teismų praktika ir teisės doktrina. Išskiriant vis specifiškesnes privatumo detales, teisės reguliavimo aspektus galima pastebėti asmens duomenų apsaugos sampratos formavimąsi. 1967 m. žymus amerikiečių teisės mokslininkas Alan F. Westin suformavo naują požiūrį į privatumą, kuris akcentuoja asmens informacijos kontrolę, suteikiant duomenų subjektui svarbią vietą.[1]

Su interneto atsiradimu, teisės į privatumą koncepcija mokslinėje doktrinoje pasikeitė. Prisitaikant prie XXI a. yra inovacijų ir technologinių pažangų, be abejonės keičiasi ir požiūris į asmeninį privatumą ir jo apsaugą. D. Solove, komentuodamas vartotojų lūkesčius dėl privatumo užtikrinimo, pabrėžia, kad šiomis dienomis privatumo užtikrinimas yra paremtas idėja apie asmeninės informacijos perdavimą ir prieigos suteikimą, bei paties duomenų subjekto efektyvia informacijos kontrole.[2] Viena iš svarbiausių figūrų, kuriai skiriama daug dėmesio nagrinėjant teisę apie privatumą, tampa pats duomenų subjektas bei jo galimybė apsaugoti ir ginti savo prigimtines teises.

Šiai dienai asmens asmens duomenų apsauga yra viena iš esminių fundamentalių žmogaus teisių bei šiandieninėje visuomenėje ji tampa vis svarbesnė, dėl ko kyla klausimas kaip apsaugoti individualaus subjekto duomenis. Technologijų, tokių kaip dirbtinis intelektas, pažanga sparčiai tobulėja ir greita duomenų analizė, leidžia organizacijoms gauti, tvarkyti bei naudoti asmens duomenis kaip niekada anksčiau. Ši technologijų pažanga suteikia tiek teigiamų aspektų, tokių kaip didesnis efektyvumas ir inovacijos, tačiau tuo pačiu metu atsiranda ir neigiamų aspektų – didina pavojų asmeninių duomenų nesaugumui ir suteikia kitiems asmenims piktnaudžiavimo galimybę. Tačiau ši nuolatinė duomenų skaida, be abejo, suteikia daugiau galimybių, bet kartu ir padidina pažeidžiamumą dėl galimų duomenų nutekinimų ar kibernetinių išpuolių tikimybę.

Pastaraisiais dešimtmečiais sustiprintas teisinis reguliavimas, nes dėl technologijų, kurių pagalba asmenys viešai skelbia savo asmens duomenis pasauliniu mastu.[3] Pagrindinis Europos asmens duomenų teisės reguliavimas įtvirtintas Europos Bendrasis Duomenų Apsaugos Reglamentas

---

[1] Alan F. Westin, *Privacy and Freedom*, (Washington and Lee Law Review, Vol. 25, 1968,) 166-170, https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20/

[2] Daniel J. Solove, *Understanding Privacy*. (The George Washington University Law School, Public law and legal theory working paper, No. 420, 2008), 3, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1127888

[3] „Europos parlamento ir tarybos reglamentas (ES) 2016/679 2016 m. balandžio 27 d. dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas)“, EUR-Lex, žiūrėta 2024 m. sausio 2 d. https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex%3A32016R0679

(toliau - BDAR), kuris įpareigoja organizacijas atsakingai tvarkyti ir saugoti asmens duomenis, stiprinant asmenų teisių apsaugą. Šio teisės aktų laikymasis yra ne tik privalomas, bet ir svarbus organizacijos reputacijos ir klientų pasitikėjimo veiksnys. Šiuo darbu siekiama išsamiai išnagrinėti ir įvertinti šias ir kitas svarbias priežastis, dėl kurių asmens duomenų apsauga yra iššūkis, organizacijoms, kurį organizacijos turi įveikti, siekdamos užtikrinti tinkamą asmens duomenų apsaugą, saugojimą ir tvarkymą.

Baigiamojo darbo naujumas. Su gyvenimo būdo pokyčiais, sparčiai progresuojančiomis technologijomis ir didėjančiu dėmesiu valstybių ir jų piliečių žmogaus teisių apsaugai, kaičiasi ir teisinis reguliavimas šioje sferoje. Prieš BDAR įsigaliojimą visuomenėje bei viešajame sektoriuje buvo ganėtinai siaura ir menkai nagrinėta asmens duomenų apsaugos instituto samprata, tačiau buvo išskiriamos pagrindinės gairės ir principai. Lietuvos Respublikoje 2003 m. sausio 21 d. buvo priimtas asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas, kuris praplėtė atsakomybės ribas už duomenų apsaugos pažeidimus. Asmens duomenų apsaugos sampratos plėtra ir šios teisės užtikrinimo reikalavimų išplėtimas suaktyvino valstybinių įstaigų, organizacijų, mokslininkų bei teisininkų analizes, aptarimus dėl problemiškų situacijų ir jų sprendimo būdų šioje srityje. Asmens duomenų apsaugos sampratos plėtra ir didesni reikalavimai šios teisės užtikrinimui paskatino valstybinių institucijų, organizacijų, mokslininkų ir teisininkų analizes, diskusijas apie problemiškas situacijas ir būdus, kaip jas spręsti šioje srityje.

Pastarojo penkmečio kontekste duomenų apsaugos tematika tapo išties intensyviai ir plačiai analizuojama sritis. Šia tema yra gausu monografijų straipsnių leidinių ir kitų šaltinių. Vienas iš svarbiausių pastaruoju metu atliktu tyrimų, tyrinėjančių asmens duomenų apsaugos teisę yra, 2019 metais J. Zaleckio išleista monografija. Šiame darbe išsamiai aprašyta duomenų apsaugos teisęs raida, analizuojami šaltiniai, principai ir ypač akcentuojama kaip BDAR specifiškai užtikrina asmens duomenų apsaugą.[4] Iki šiol šią temą taip pat nagrinėjo I. Petraitytė, kuri išsamiai nagrinėjo asmens duomenų apsaugos teisę kaip neatsiejamą teisę į privatų gyvenimą.[5] Ji taip pat tyrinėjo, kaip asmens duomenų teisė yra įgyvendinama Lietuvoje.[6] M. Civilis, savo ruožtu nagrinėjo interneto fenomeną ir jo sąveiką su asmens duomenų apsauga.[7] I. Malinauskaitė-van de Castel, analizavo duomenų subjekto specifinių erdvių teisinio reguliavimo ir jo įgyvendinimo klausimus, tokius kaip – virtualių

[4] Julius Zaleskis, *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė* (Vilnius: VĮ Registrų centras, 2019).
[5] Ilona Petraitytė, „*Asmens duomenų apsauga ir teisė į privatų gyvenimą*“, *Teisė,* 80, (2011): 163. https://www.lituanistika.lt/content/33625
[6] Ilona Petraitytė, *„Asmens duomenų apsaugos teisinis reguliavimas Lietuvos teisės sistemoje“, Teisė*, 79, (2011): 125. https://www.lituanistika.lt/content/33198
[7] Mindaugas Civilika, „Europos Sąjungos asmens duomenų apsaugos teisinis reguliavimas interneto kontekste“. Iš Europos Sąjungos teisė ir Lietuva, Vilenas Vadapalas, (Vilnius : Justitia, 2002), 226.

socialinių tinklų sferoje iškylančias problemas.[8] R. Andrijauskas nagrinėjo kaip teisinis reguliavimas numato asmens duomenų skelbimą internete viešo intereso tikslais, t.y. iššūkių, susijusių su teisės į asmens duomenų apsaugą ir informacijos laisvę derinimu, problema.[9] E. Kavoliūnaitė-Ragauskienė, vertino dirbtinio intelekto sistemų tendencijas ir bruožus, kurios gali turėti didžiausią poveikį teisėms į privatumą ir asmens duomenų apsaugą dirbtinio intelekto sistemų kontekste.[10] Klaudija Jagminaitė nagrinėjo, kokie asmens duomenų apsaugos pažeidimai vyrauja socialiniuose tinkluose ir juos vertino per BDAR prizmę.[11] Tačiau mokslinėje literatūroje nėra nagrinėta kokia yra asmens duomenų pareigūno funkcija ir kaip jis prisideda prie asmens duomenų kontrolės. Taip pat literatūroje nėra nagrinėta kaip ir dėl kokių priežasčių įvyksta organizacijos surinktų duomenų praradimai.

Tyrimo problema. Su kokiomis asmens duomenų apsaugos kontrolės įgyvendinimo problemomis susiduria organizacijos? Kokios yra pagrindinės priežastys kurios lemia duomenų nutekėjimą? Kokie padariniai fiziniams ir juridiniams asmenims dėl duomenų nutekėjimo?

Darbo objektas. Asmens duomenų apsaugos kontrolės įgyvendinimo iššūkiai ir problemos.

Darbo tikslas. Atlikti analizę ir įvertinti asmens duomenų apsaugos kontrolės sistemų efektyvumą organizacijose bei identifikuoti kylančius iššūkius, su kuriais jos susiduria įgyvendindamos asmens duomenų apsaugą. Taip pat išnagrinėti teisinius, technologinius, organizacinius, komunikacijos ir privatumo aspektus, išanalizuoti sąveiką ir nustatyti, kaip sistemos atitinka teisinius reikalavimus, siekiant užtikrinti asmens duomenų saugumą bei privatumą.

Darbo uždaviniai:

1. Išnagrinėti asmens duomenų apsaugos reglamentavimą nacionaliniu ir tarptautiniu lygmeniu;
2. Identifikuoti asmens duomenų apsaugos kontrolės įgyvendinimo iššūkius;
3. Išanalizuoti duomenų apsaugos funkciją ir kaip pareigūnas dalyvauja asmens duomenų kontrolės procese;
4. Išnagrinėti teismų praktiką dėl asmens duomenų pažeidimų, nustatyti kokia yra atsakomybė asmenims už duomenų pažeidimus bei identifikuoti pagrindines

[8] Inga Malinauskaitė-van De Castel, „Duomenų Subjekto Teisės Virtualiuose Socialiniuose Tinkluose.“ (daktaro disertacija, Mykolo Romerio Universitetas, 2017), 183, https://talpykla.elaba.lt/elaba-fedora/objects/elaba:23456482/datastreams/MAIN/content

[9] Raimondas Andrijauskas, „Asmens Duomenų Viešas Skelbimas Ir Asmens Duomenų Apsauga: Suderinamumo Klausimas", *Lietuvos Teisė: esminiai Pokyčiai* (2022): 161. https://cris.mruni.eu/server/api/core/bitstreams/22bb8d59-ead8-429b-937d-0f37064136f5/content

[10] Eglė Kavoliūnaitė-Ragauskienė, *Teisė į Privatumą, Asmens Duomenų Apsauga Ir Dirbtinis Intelektas: Teisinio Reguliavimo Iššūkiai Lietuvoje Ir Europoje* (Lietuvos Socialinių Mokslų Centro Teisės Institutas, 2023), https://teise.org/wp-content/uploads/2023/05/Teise_i_privatuma.pdf

[11] Klaudija Jagminaitė, „Asmens Duomenų Apsaugos Pažeidimai Socialiniuose Tinkluose Pagal ES Bendrąjį Duomenų Apsaugos Reglamentą“, *Teisinės minties šventė, studentų mokslinių straipsnių rinkinys*, (2022), 217. https://cris.mruni.eu/server/api/core/bitstreams/03ef4924-f9c7-46d3-86b1-786095a904ae/content

organizacijose esančias problemas dėl kurių įvyksta minėti veiksniai, bei kokia atsakomybė yra už asmens duomenų pažeidimus.

Ginamasis teiginys. Asmens duomenų pažeidimai įvyksta dėl žmogiškosios klaidos, asmenų nekompetencijos.

Darbo metodologija. Lingvistinis bei mokslinių šaltinių analizės metodai naudoti asmens duomenų bei kitoms darbe analizuojamoms sąvokoms atskleisti. Sisteminės analizės metodas naudotas analizuojant Lietuvos teisinį reglamentavimą kuriuo siekiama apsaugoti asmens duomenis. Lyginamosios analizės metodu analizuoti ir lyginti Lietuvos ir užsienio valstybių teisės aktus. Analitinis-kritinis metodas buvo naudojamas atskleisti ir kritiškai vertinti teisinio reglamentavimo už asmens duomenų nutekinimą trūkumus, galimas interpretacijas, prieštaravimus.

Darbo struktūra ir apimtis. Darbą sudaro įvadas, trys skyriai, išvados, literatūros sąrašas, santrauka.

Pirmajame skyriuje analizuojama asmens duomenų apsaugos teoriniai aspektai, pateiktos asmens duomenų, duomenų apsaugos pareigūno instituto sampratos ir jų turinio elementai, analizuotos asmens duomenų teisės ir asmens teisės į privatumą sąsajos, apibrėžti teisėtam duomenų tvarkymui keliami reikalavimai ir taikomi principai.

Antrajame skyriuje bus išsamiai analizuojamas asmens duomenų surinkimo, tvarkymo ir saugojimo procesas organizacijose, nagrinėjami iššūkiai, su kuriais organizacijos susiduria įgyvendindamos efektyvias asmens duomenų apsaugos kontrolės sistemas.

Trečiame skyriuje bus išnagrinėta teismų praktika susijusi su asmens duomenų pažeidimais. Nagrinėjamos organizacijų patirtys ir iššūkiai, su kuriais jos susiduria įgyvendindamos asmens duomenų apsaugos priemones, bei kokia atsakomybė kyla dėl asmens duomenų pažeidimų.

1. ASMENS DUOMENŲ APSAUGOS SAMPRATA IR REGLAMENTAVIMAS

Šiame skyriuje pus nagrinėjama asmens duomenų apsaugos samprata, reglamentavimas bei pagrindiniai principai. Principai yra pamatas siekiant užtikrinti tinkamą asmens duomenų apsaugą. Principai yra svarbus asmens duomenų apsaugos elementas, nes būtent jie nustato teisingą ir saugų duomenų tvarkymą. Taip pat bus analizuojami tarptautiniai ir nacionaliniai reglamentai, kurie apibrėžia tinkamą duomenų rinkimą, tvarkymą bei jų saugojimą organizacijose.

1.1. Asmens duomenų apsaugos samprata, sąvoka ir principai

Su vis sparčiau augančiais informacijos srautais, technologijų tobulėjimu ir besikeičiant įprastam gyvenimo būdui bei bendravimo formoms, vis daugiau dėmesio skiriama asmens duomenų sąvokai ir šios koncepcijos ypatumams. ES komisija asmens duomenis aiškina kaip bet kokia informacija, apie gyvą asmenį, kurio tapatybė yra nustatyta arba gali būti nustatyta. Informacija, kuri surinkta visumoje, gali atskleisti konkretaus asmens tapatybę, taip pat yra laikoma asmens duomenimis. [12] Nagrinėjant plačiau šią sąvoką ES duomenų apsaugos grupė nustatė jog apibrėžimą sudaro 4 elementai:[13]

1. „Bet kuri informacija“ - analizuojant sąvoką per informacijos turinio prizmę, terminas „asmens duomenys apibrėžia visus duomenis, kuriuose pateikiama visa galima informacija. Tai apima duomenis apie asmenį, kuriuos pagal BDAR 8 str. laikoma „ypatingais duomenimis“ ir platesnio pobūdžio informacija. Šis terminas apima duomenis susijusius su asmens asmeniniu ir šeimos gyvenimu *stricto sensu* , informacija apie asmens vykdomą veiklą, tokias kaip asmens darbo santykiai, ekonominis ar socialinis elgesys. Šiuo atveju jis apima ir informaciją apie asmenis, nepriklausomai nuo jų padėties ar pareigų. [14]
2. „Informacija susijusi su asmeniu“ – šia apibrėžimo dalį galime laikyti pagrindine, nes svarbu nustatyti tikslius specifinius santykius ir/ar ryšius bei suprasti kaip juos defirencijuoti. Paprasčiau suprantama, informacija yra laikoma „susijusi su“ asmeniu, kai ji apima duomenis apie šį asmenį. Turinio elementas atsiranda tais atvejais, kai vadovaujanti aiškiąją ir visuotinai suprantama „susijęs“ žodžio reikšmę, pateikiama informacija apie konkretų asmenį ir nepriklausomai nuo duomenų valdytojo ar trečiosios šalies tikslų arba

[12] „Kas yra asmens duomenys?“, Europos komisija, žiūrėta 2024 m. sausio 10 d., https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_lt
[13] 29 straipsnio duomenų apsaugos darbo grupė „nuomonė 4/2007 dėl asmens duomenų sąvokos“, Europa.eu, žiūrėta 2024 m. vasraio 15 d., https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_lt.pdf
[14] Ibid.

tokių duomenų poveikio duomenų subjektui. Informacija laikoma susijusia su asmeniu, kai ji yra apie tą asmenį.[15]

3. „Fizinis asmuo, kurio tapatybė yra nustatyta arba gali būti nustatyta“ – fizinio asmens tapatybė laikoma nustatyta, kai jis yra išskirtas nuo visų kitų tai grupei priklausančių asmenų. Taip pat tapatybė gali būti nustatyta, kai ji dar nenustatyta, bet yra duomenų, kad bus galima nustatyti asmens tapatybę. Asmens tapatybė gali būti nustatoma tiesiogiai ir netiesiogiai. [16] Tiesiogiai tapatybė nustatoma įprastai pagal vardą ir pavardę, tačiau norint įsitikinti, kad tapatybė nustatyta teisingai, asmens informacija turi būti susieta su kita informacija tokia kaip gimimo data, asmens kodas. Netiesiogiai tapatybė yra nustatoma, kai yra žinoma dalis informacijos apie asmenį. Pavyzdžiui automobilio numeriai, kurie nėra tiesiogiai susiję su asmeniu, tačiau su tam tikromis priemonėmis ar priėjimu prie informacinių sistemų asmens tapatybė gali būti nustatyta.
4. „Fizinis asmuo“ – fizinio asmens samprata minima Visuotinės žmogaus teisių deklaracijos 6 str., kuriame teigiama, kad „Kiekvienas, kad ir kur būtų, turi teisę būti pripažintas teisinių santykių subjektu“.[17] Ši sąvoka dažniausiai yra apibrėžiama valstybių narių teisės aktuose, civilinėje teisėje. Konkrečiau, ji nusako žmogaus asmenybės sąvoką, kaip asmens gebėjimą tapti teisinių santykių subjektu nuo gimimo momento iki jo mirties. Dėl šios priežasties asmens duomenys yra esminiai duomenys, susiję su gyvais asmenimis, kurių tapatybė nustatyta arba gali būti nustatyta. [18] Tad galima daryti išvadą, jog asmens duomenys apima bet kokia informacija susijusi asmeniu iš kurios tiesiogiai arba netiesiogiai galima nustatyti asmens tapatybę.

Gilinantis toliau į asmens duomenų temą būtina išsiaiškinti kokie konkretūs duomenys yra laikomi asmens duomenimis. Pagrindiniai asmens duomenys, kuriais galima identifikuoti konkretų asmenį, yra įvairūs, tačiau dažniausiai tai yra informacija, kuri tiksliai nustato arba leidžia nustatyti tam tikrą fizinį asmenį. Asmens duomenys gali būti pavyzdžiui: vardas ir pavardė, gimimo data, elektroninio pašto adresas, asmens tapatybės kortelės numeris, buvimo vietos duomenys, interneto protokolo adresas (IP).[19] Tapatybės dokumento numeris, gali būti panaudojamas tapatybės patvirtinimui, registracijai prie tam tikrų svetainių, portalų. Biometriniai duomenys, prie jų yra priskiriami akių rainelė, pirštų ir pėdų atspaudai pas kiek vieną asmenį yra unikalūs, todėl juos yra sunku suklastoti, šie duomenys yra itin jautrūs, todėl didelis dėmesys yra skiriamas jų apsaugai ir

[15] 29 straipsnio duomenų apsaugos darbo grupė, supra note 13: 12.
[16] Ibid.
[17] „Visuotinė žmogaus teisių deklaracija“ LRS, žiūrėta 2024 m. Vasario 15 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.278385
[18] 29 straipsnio duomenų apsaugos darbo grupė, op. cit. 13.
[19] Europos komisija, supra note: 12.

tvarkymui. Telefono numeris taip pat yra priskiriamas prie asmens duomenų, nes dažnu atveju telefono numeris yra abonementinis ir šis yra susietas su konkrečiu asmeniu, turint jį taip pat galima identifikuoti asmenį.[20] Aukščiau išvardinti asmens duomenys yra visuomenei plačiai žinomi ir svarbūs dėl jų naudojimo įvairiose srityse. Tačiau reikėtų pabrėžti, kad yra ir mažiau žinomų bei su rečiau sutinkamų asmens duomenų, kurie taip pat turi svarbų vaidmenį tyrimuose ir visuomenės informacijos apsaugoje. Vieni iš tokių duomenų yra buvimo vietos duomenys, kurie naudojami išmaniuosiuose įrenginiuose yra laikomi labai jautriais, nes jie suteikia informaciją apie asmens judėjimo modelius, kas gali lemti privatumo pažeidimą. Šios informacijos naudojimas gali būti vykdomas tik su asmens sutikimu, [21] tačiau per pandemijos laikotarpį (COVID-19) Europos Sąjungos valstybėse iš elektroninių ryšių paslaugų tiekėjų bei programėlių, buvo gaunama informacija apie asmenis, kurie buvo tam tikru laiku tam tikroje vietoje, kurioje buvo potencialus užsikrėtimo šaltinis,[22] arba asmenys kurie turėjo tiesioginį kontaktą su sergančiuoju. Šis procesas buvo įgyvendinamas su tikslu nustatyti potencialius užsikrėtusius asmenis, juos identifikuoti ir taip užkirsti kelią tolimesniam viruso plitimui. 2016 m. Europos teisingumo teismas nustatė, kad prie asmens duomenų yra priskiriamas ir išmaniųjų įrenginių IP (angl. Internet Protocol adresas) yra unikalus identifikatorius, priskirtas įrenginiui, prijungtam prie interneto, ir jis leidžia nustatyti, iš kur buvo atliktas tam tikras interneto ryšys.[23] Ligoninės arba gydytojo turimi duomenys, pagal kurias galima konkrečiai nustatyti asmens tapatybę,[24] dažnai apima medicininės dokumentacijos numerius arba paciento identifikacinį numerį. Šie numeriai yra unikalūs ir skirti konkrečiam pacientui, leidžiantys medicinos specialistams efektyviai identifikuoti ir sekti jo sveikatos priežiūros istoriją bei teikiamas paslaugas.

Norint išsamiau tyrinėti asmens duomenų apsaugos sritį yra svarbus suprasti, kokie esminiai principai dalyvauja vykstant procesui. Principų pagrindinė užduotis – užtikrinti, kad duomenys būtų tvarkomi teisėtai, sąžiningai bei saugiai, atsižvelgiant į asmenų teises ir laisves. Vieni iš svarbiausių šių principų elementų – sąžiningumas, skaidrumas, tikslumas, ribojimas bei saugumo principas, kuris kiekvienas, savo ruožtu lemia atsakingą ir proporcingą duomenų tvarkymą. Šių elementų laikymasis ne tik atspindi teisinį įsipareigojimą, bet ir garantuoja aukštą asmens duomenų apsaugos lygį, kuris prisideda prie bendro privatumo ir duomenų saugumo stiprinimo. Norint suprasti, kaip veikia

[20] Europos komisija, *supra note*: 12.
[21] Your Europe, „Duomenų apsauga pagal BDAR“. Europa.eu, žiūrėta 2024 m. vasario 20 d. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_lt.htm
[22] EDPB „Gairės Nr. 04/2020 dėl buvimo vietos duomenų ir sąlytį turėjusių asmenų išaiškinimo priemonių naudojimo COVID- 19 protrūkio aplinkybėmis“, Europa.eu, žiūrėta 2024 m. vasario 20 d. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_lt.pdf
[23] Judment of the court „Patrick Breyer vs Bundesrepublik Deutschland“, Europa.eu, žiūrėta 2024 m. vasario 20 d. https://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1075747
[24] Europos komisija, *supra note*: 12

principai asmens duomenų kontekste, būtina įsigilinti į kiekvieno principo veikimą. Nuo sąžiningumo iki saugumo – kiekvienas principas yra esminis ir atlieka svarbų vaidmenį užtikrinant, kad duomenys būtų tinkamai tvarkomi.

Pirmasis principas yra *teisėtumo, sąžiningumo ir skaidrumo principa*s. Šis principas įtvirtintas BDAR 5 str. 1 d. a p., taip pat ir ETDA 5 str. 3 d., 4 d. a ir b p. *Teisėtumas* šiame principe reiškia kadangi asmens duomenys turi būti tvarkomi pagal bent vieną iš oficialiai nustatytų BDAR sąlygų, įskaitant duomenų subjekto sutikimą, sutarties su duomenų subjektu vykdymą, teisinę prievolę, duomenų subjekto ar kito fizinio asmens gyvybinių interesų apsaugą, užduoties vykdymą viešojo intereso labui, teisėtus duomenų valdytojo ar trečiosios šalies interesus. Įmonės taip pat privalo laikytis teisėtumo principo, ypač tvarkant specialių kategorijų asmens duomenis ar asmens duomenis apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas, ir tai privalo būti vykdoma pagal BDAR nustatytas sąlygas.[25] *Sąžiningumas* reiškia, kad tvarkant asmens duomenis būtina laikytis sąžiningumo principo. Tai apima duomenų subjekto informavimą apie jo asmens duomenų tvarkymą ir su tuo susijusias rizikas. Be to, sąžiningumas reikalauja, kad duomenų subjektas būtų tinkamai informuojamas ir nesuklaidinamas apie tai, kaip bus renkami, tavrkomi ir saugojami jo surinkti duomenys.[26] *Skaidrumas* reiškia, kad asmenims turi būti aišku, kaip yra surenkami, naudojami ar kitaip tvarkomi jų asmens duomenys, taip pat kokiais tikslais ir kokia apimtimi šie duomenys yra ar bus tvarkomi.[27]

Sekantis principas yra *duomenų tvarkymo tikslo apribojimo principas*, šis principas įtvirtintas BDAR 5 str. 1 d. b p., ETDA 5 str. 4 d. b p. Šis principas reiškia ir reikalauja surinkti asmens duomenis tik nustatytais, aiškiai apibrėžtais ir teisėtais tikslais, netvarkyti šių duomenų tokiu būdu, kuris būtų nesuderinamas su nustatytais tikslais. Todėl, kai tvarkymo tikslai nėra aiškiai apibrėžti arba riboti, ar kai asmens duomenys yra renkami tik su galimybe, kad jie gali būti naudingi ateityje, tai laikoma neteisėtu.[28] Dėl šios priežasties svarbu aiškiai nurodyti, kokiais tikslais vykdomas asmens duomenų tvarkymas. Svarbu pabrėžti, kad asmens duomenų tvarkymo tikslas turi būti aiškiai apibrėžiamas ne vėliau kaip pradedamas asmens duomenų rinkimas. [29] Tikslo apribojimo principas glaudžiai siejasi su teisėtumo, sąžiningumo ir skaidrumo principais, nes pasirinktas asmens duomenų tvarkymo tikslas turi būti teisėtas. a

---

[25] Solving privacy paradox, „Assmens duomenų apsaugos gairės smulkiajam ir vidutiniam verslui“, LRV, žiūrėta 2024 m. vasario 26 d. https://vdai.lrv.lt/uploads/vdai/documents/files/01_%20SolPriPa%20Asmens%20duomenu%20apsaugos%20gaires%20SMULKIAJAM%20IR%20VIDUTINIAM%20VERSLUI%202019-11-08.pdf

[26] *Ibid.*, 11.

[27] *Ibid.,* 11-12.

[28] *Ibid.,* 13-14.

[29] EDPB, „Gairės 05/2020 dėl sutikimo pagal Reglamentą 2016/679“, Europa.eu, žiūrėta 2024 m. vasario 27 d. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_lt.

Kitas principas yra *duomenų kiekio mažinimo principas* BDAR 5 str. 1 d. c p., ETDA 5 str.1 d. Asmens duomenys turi būti tinkamai parinkti, tinkami ir naudojami tik tie, kurie būtini siekiant tikslų, dėl kurių jie yra tvarkomi. Šis principas pareiškia, kad asmens duomenys turėtų būti tvarkomi tik tada, jei kitomis priemonėmis negalima pagrįstai pasiekti asmens duomenų tvarkymo tikslo.[30] Jei, siekiant tikslų, negalima pagrįstai pasiekti be asmens duomenų tvarkymo, tuomet būtina pasirinkti minimalų asmens duomenų kiekį, kuris būtų reikalingas siekiamam tikslui pasiekti.

Taip pat yra taikomas ir *duomenų tikslumo principas* BDAR 5 str. 1 d. d p., ETDA 5 str. 4 d. d p. Šis principas reiškia, kad asmens duomenys privalo būti tikslūs ir periodiškai atnaujinami. Taip pat reikia imtis visų pagrįstų priemonių, kad asmens duomenys, kurie nėra tikslūs, atsižvelgiant į jų tvarkymo tikslus, būtų nedelsiant ištrinami arba pataisomi.[31] Todėl BDAR įpareigoja imtis aktyvių veiksmų ir priemonių, kad asmens duomenys būtų tiksli, pavyzdžiui, nustatant terminus jų ištrynimui arba periodiniam peržiūroms.[32] Jei nustatoma, kad asmens duomenys yra nereikalingi arba netikslūs, turi būti imtasi visų pagrįstų veiksmų, siekiant užtikrinti, kad netiksli informacija būtų ištaisyta arba pašalinta.

Taipogi BDAR 5 str. 1 d. e p., ETDA 5 str. 4 d. e p., įtvirtintas *duomenų saugojimo trukmės ribojimo principas*. Šis principas nustato, kad asmens duomenys turėtų būti saugomi tokia forma, kad duomenų subjektų tapatybė galėtų būti nustatyta tik tiek laiko, kiek tai yra būtina atitinkamiems asmens duomenų tvarkymo tikslams.[33] Atsižvelgiant į tai, kiek laiko yra ketinama saugoti asmens duomenis, svarbu pirmiausia įvertinti asmens duomenų tvarkymo tikslą, nes nuo jo priklauso, kokie asmens duomenys bus privalu tvarkyti. [34] Todėl svarbu užtikrinti, kad asmens duomenų saugojimo laikotarpis būtų kuo trumpesnis, tačiau BDAR neįtvirtina konkretaus laikotarpio asmens duomenų saugojimui. Taigi, BDAR nėra nurodyto kokretaus laiko, kiek organizacija turi ir gali saugoti asmens duomenis. Tokia nuostata suteikia lankstumo organizacijai ir leidžia pačioms nustatyti asmens duomenų saugojimo poreikį ir tinkamą saugojimo laikotarpį. Nustatant asmens duomenų saugojimo laikotarpį, organizacijos turi atsižvelgti į tikslus, kuriais jie renkami ir tvarkomi.

BDAR 5 str. 1 d. f p., ETDA 7 str. *vientisumo ir konfidencialumo principas*, kuris nustato, kad būtina tvarkyti asmens duomenis taip, jog taikant reikiamas technines ar organizacines priemones būtų užtikrintas tinkamas asmens duomenų saugumas.[35] Tai apima apsaugą nuo duomenų tvarkymo be leidimo, neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo. Šis

[30] Solving privacy paradox, *supra note,* 25: 14-15.
[31] *Ibid.*
[32] „2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB ”, EUR-LEX, žiūrėta 2024 m. vasario 27 d. https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex%3A32016R0679
[33] *Ibid.*
[34] Solving privacy paradox, *op. cit.,* 16.
[35] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB ”, *op.cit.*

principas įpareigoja tvarkytojus turėti tinkamas saugumo priemones, siekiant užtikrinti asmens duomenų apsaugą.[36] Taigi duomenų valdytojai ar tvarkytojai privalo įdiegti tinkamas saugumo priemones, kad būtų užtikrinta asmens duomenų apsauga. Tai yra esminis elementas kurio siekiama, jog organizacijos laikytųsi teisės aktų nustatytų normų bei užtikrintų, kad asmens duomenų subjektai pasitikėtu duomenų tvarkymo procesu.

Šiame skyriuje išnagrinėta asmens duomenų apsaugos sąvokos, principai ir jų taikymas, pabrėžiant principų svarbą. Taikant anksčiau minėtus principus, jais galima užtikrinti veiksmingą asmens duomenų tvarkymą, kuris atitinka numatytus teisės aktus ir jų normas.

Apibendrinus galima teigti, kad tinkamai įgyvendinus aukščiau aptartus principus aptartus ir sąvoką, išryškinta jų esminė reikšmė teisėtai, sąžiningam ir saugiam asmens duomenų tvarkymui. Taikant šiuos principus, galima užtikrinti tinkamą asmens duomenų apsaugos lygį bei skatinti atsakingą informacijos tvarkymą tiek viešajame, tiek privačiame sektoriuose.

[36] Solving privacy paradox, supra note, 25: 16.

1.2. Teisinis reglamentavimas ir tarptautiniai standartai asmens duomenų pasaugos kontekste

Kiekvienam asmeniui yra suteikta teisė reikalauti, kad jo privatus gyvenimas būtų neliečiamas, todėl valstybių pareiga yra užtikrinti savo piliečių privatumo saugumą. Ši teisė apima asmens privatumo teisę, kuri yra viena iš pagrindinių prigimtinių žmogaus teisių. Duomenų apsaugos teisės yra iš esmės susijusios su asmens privataus gyvenimo neliečiamumo teise, nurodančia, kad visas žmogaus teises galima įvardinti kaip privataus gyvenimo apsaugos aspektais. Labai svarbu pripažinti, kad žmogaus teisių išsaugojimas yra ne tik nacionalinis, bet ir tarptautinis klausimas. Ši apsauga neapsiriboja vienos valstybės teritorija, o yra tarptautinės bendrijos dėmesio centre. Todėl svarbu yra atlikti teisės aktų regalmentuojančių asmens apsaugą analizę. Asmens duomenų apsauga tarptautinėje teisėje yra neatsiejama nuo teisės į privatumą. Tai reikšminga studijų sritis, kuri padeda geriau suprasti, kaip tarptautinė teisė yra susijusi su asmens duomenų apsauga.

Vienas iš pirmųjų teisės aktų, siekusių apsaugoti žmogaus teises, buvo ***Visuotinė žmogaus teisių deklaracija*****,** priimta 1948 m. Jungtinės Tautos ir oficialiai patvirtina Deklaraciją kaip tarptautinį teisinį dokumentą, kuriuo siekiama užtikrinti teisinę apsaugą ne tik nuo privačių asmenų, bet ir nuo valstybės įsikišimo. Deklaracijos 12 str. nurodo, kad niekas neturėtų patirti nepagrįsto įsikišimo į savo asmeninį gyvenimą, šeimos santykius, buitį, susirašinėjimą arba įžeidžiančio elgesio, kuris gali pakenkti jų garbei ir reputacijai.[37] Šio dokumento įgyvendinimas turėjo didelės įtakos kitoms žmogaus teisių normoms Europoje. [38] Akivaizdu, kad žmogaus teisių apsauga yra būtina, nes žmogaus teisės ir laisvės gali būti pažeistos privatumo srityje. Nepaisant to, kad deklaracija iš pradžių buvo patariamojo pobūdžio, ji turėjo didelį poveikį žmogaus teisių raidai visame pasaulyje. Jo priėmimas tapo pagrindu kitiems oficialiems susitarimams ir dokumentų, kuriuose buvo atsižvelgta į tarptautinius ir nacionalinius įstatymus.

Vienas iš svarbiausių asmens duomenų apsaugos reglamentų yra tarptautinė sutartis, įpareigojanti šalis užtikrinti teisę į privatų gyvenimą. Vienas iš šių dokumentų yra ***Europos žmogaus teisių konvencija*** (Žmogaus teisių ir pagrindinių laisvių apsaugos konvencija), vienas iš svarbiausių tarptautinių teisinių dokumentų, kuris buvo priimtas 1950 m. Europos Tarybos. Konvencija buvo siekiama užtikrinti, kad žmogaus teisės ir laisvės būtų apsaugotos visose Europos valstybėse.[39] Konvencija svarbi ir asmens duomenų apsaugai. Nors jis tiesiogiai nereglamentuoja asmens duomenų apsaugos, vis dėlto ji užtikrina, kad valstybės narės laikytųsi bendrų principų, kuriais atsižvelgiama į žmogaus teises, įskaitant teisę į privatumą. Konvencijos 8 str. 1 d., nurodo, kad kiekvienam asmeniui

[37] „Visuotinė žmogaus teisių deklaracija“, *supra note,* 17.
[38] Dainius Žalimas, „Visuotinė žmogaus teisių deklaracija – svarus ginklas kovojant dėl visų žmonių laisvės, lygybės ir orumo“, LRKT, žiūrėta 2024 m. vasario 27 d. https://lrkt.lt/lt/dainius-zalimas-visuotine-zmogaus-teisiu-deklaracija-svarus-ginklas-kovojant-del-visu-zmoniu-laisves-lygybes-ir-orumo/1207
[39] „Europos žmogaus teisių konvencija (EŽTK)“, Europa.eu, žiūrėta 2024 m. vasario 27 d. https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=LEGISSUM:eu_human_rights_convention

suteikta teisė, jog asmens privatus bei šeimos gyvenimas būtų gerbiamas, taip pat turi teisę į būsto neliečiamybę ir privataus susirašinėjimo konfidencialumą.[40] Tačiau tos pačios konvencijos 8 str. 2 d. išskiria atvejus, kada asmens duomenų apsauga gali būti pažeidžiama. Šie atvejai dažniausiai susiję su situacijomis, kai duomenis tvarkyti būtina siekiant apsaugoti kitus svarbius interesus, tokius kaip nacionalinis saugumas ar viešoji tvarka[41] Be to, Konvencijoje gali būti numatytos ir kitos ypatingos aplinkybės, kai duomenis leidžiama tvarkyti be asmens sutikimo, pavyzdžiui, teisėsaugos institucijų atliekamos tyrimo veiklos kontekste arba teisės aktų numatytais atvejais. Taigi, nors konvencija pripažįsta asmens duomenų svarbą ir jų apsaugą, ji taip pat atsižvelgia į situacijas, kuriose duomenų apsauga gali būti sumažinta dėl kitų svarbių visuomenės ar valstybės interesų. Asmuo sužinojęs apie savo asmens duomenų pažeidimą, savo teises gali ginti Europos žmogaus teisių teisme (toliau - EŽTT).[42]

Europos Sąjungos Pagrindinių Teisių Chartija (toliau - ES chartija) yra svarbus dokumentas, kurį Europos Sąjunga priėmė 2000 m. gruodžio 7 d. Ši Chartija yra susijusi su ES institucijomis ir valstybėmis narėmis ir įtvirtina pagrindines teises, kurias turi ES piliečiai ir gyventojai.[43] ES chartijoje 7 str. įtvirtina asmenų teisę į privatumą, 8 str. įtvirtina, jog visi asmenys turi teisę į asmens duomenų apsaugą, taip pat šis straipsnis numato, jog asmens duomenys gali būti renkami turint teisėtus tikslus bei su asmens sutikimu.[44] Ši ES chartija turi didelę įtaką asmens duomenų apsaugos kontrolei. Ji nustato svarbias teises ir principus, kurie formuoja pagrindą ES teisės aktams, susijusiems su duomenų apsauga. Šie teisės aktai apima Bendrąją duomenų apsaugos reglamentą (BDAR), kuris įtvirtina bendrus reikalavimus dėl duomenų apsaugos visoje ES.

Europos Tarybos duomenų apsaugos konvencija (toliau – ETDA konvencija) (Europos Tarybos 108-oji konvencija) yra tarptautinis teisinis dokumentas, kuris buvo priimtas 1981 m. ir įsigaliojo 1985 m. Ši konvencija yra pirmasis teisinis dokumentas, skirtas reglamentuoti asmens duomenų apsaugą tarptautiniu lygiu. ETDA konvencija įtvirtino asmens duomenų sąvoką, kuri nurodo, jog asmens duomenys yra duomenys apie asmenį, kurio tapatybė yra žinoma arba asmenį, kurio tapatybė gali būti identifikuojama.[45] Įtvirtino, pagrindinius principus, kad asmens duomenys turi būti tvarkomi sąžiningai ir teisingai, duomenų rinkimas turi būti turint tikslą, duomenys turi būti

[40] „Europos žmogaus teisių konvencija“, ECHR, žiūrėta 2024 m. kovo 1 d. https://www.echr.coe.int/documents/d/echr/convention_lit
[41] *Ibid.*
[42] *Ibid.*
[43] „Europos Sąjungos pagrindinių teisių chartija“, Europa.eu, žiūrėta 2024 m. kovo 1d. https://eur-lex.europa.eu/LT/legal-content/summary/charter-of-fundamental-rights-of-the-european-union.html
[44] „Europos pagrindinių teisių chartija“, Europa.eu, žiūrėta 2024 m. kovo 1 d. https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:12012P/TXT
[45] „Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis“, LRS, žiūrėta 2024 m. kovo 1 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.129872

tokios apimties kurie leistų įgyvendinti išsikeltą tikslą, duomenys turi būti atnaujinami. [46] ETDA konvencija suteikia duomenų subjektams įvairias teises, kurios apima: teisę į informaciją, tiesę į prieigą, teisę ištaisyti neteisingus duomenis, teisę į pašalinimą, apribojimą bei perkėlimą. Pagrindinis Konvencijos tikslas – apsaugoti duomenis ir užkirsti kelią neteisėtai prieigai prie duomenų, jų perdavimui ar naudojimui.[47] Valstybės narės privalo imtis būtinų priemonių duomenų saugumui užtikrinti. Konvencija nustato tarptautinio duomenų perdavimo sąlygas ir principus. [48] Tai svarbu dėl didėjančio verslo, kuris apima ne vieną valstybę ir kurios tarpusavyje turi keistis informacija siekdamos įgyvendinti tinkamai savo įmonės tikslus. Taip pat yra skatinama valstybių narių bendradarbiavimas dauomenų apsaugos srityje, siekiant užtikrinti efektyvią duomenų apsauga ne tik nacionaliniu, bet ir tarptautiniu lygmeniu.[49] Ši Konvencija kaip teisės aktas yra svarbus dokumentas, kuris padeda sukurti bendrą duomenų apsaugos lygį Europoje ir užtikrina, kad asmens duomenys būtų tvarkomi ir naudojami tinkamai, pagal aiškias teisės normas. Taip pat svarbu paminėti, kad Konvencija skatina valstybių narių tarptautinį bendradarbiavimą ir vienodą požiūrį į duomenų apsaugą visoje Europos Sąjungoje.

Bendrasis duomenų apsaugos reglamentas (BDAR) yra vienas svarbiausių teisės aktų Europos Sąjungoje, susijęs su asmens duomenų apsauga. Reglamentas, patvirtintas 2016 m. balandžio 27 d., įsigaliojo 2018 m. gegužės 25 d. ir pakeitė ankstesnę Direktyvą 95/46/EB. BDAR yra privalomas visose Europos Sąjungos valstybėse narėse ir taikomas visoms organizacijoms, kurios tvarko asmens duomenis. BDAR suteikia asmenims teises ir apsaugos priemones, o asmens duomenis tvarkančioms organizacijoms nustato griežtas taisykles ir pareigas. Pagrindinis šio reglamento tikslas – užtikrinti, kad asmens duomenys būtų tvarkomi sąžiningai, skaidriai ir saugiai bei būtų gerbiamos jų teisės. BDAR stiprina asmenų teises ir suteikia joms didesnę kontrolę bei apsaugą jų asmens duomenims. Asmenis yra suteikiamos naujos teisės, tokios kaip – teisė į informaciją, teisė į prieigą prie duomenų, teisę į taisymą ir teisę duomenų ištrynimą.[50] BDAR numato griežtas baudžiamąsias priemones organizacijoms, kurios pažeidžia reglamento nuostatas.[51] Numatytos sankcijos apima dideles finansines baudas, kurios gali turėti reikšmingų finansinių ir reputacinės rizikos padarinių įmonėms.[52] BDAR nustato tam tikras taisykles ir procedūras, kurios susijusios su apskundimo tvarka,

[46] Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis“, *supra note,* 45.
[47] Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis“, *supra note*, 45.
[48] *Ibid.*
[49] *Ibid.*
[50] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB“, *supra note,* 32.
[51] *Ibid.*
[52] *Ibid.*

kai asmuo mano, kad jo duomenys buvo neteisingai tvarkyti ar buvo pažeistos jų duomenų teisės.[53] Šios taisyklės skirtos užtikrinti, kad asmenus turėtų galimybę ginti savo duomenų teisę ir kreiptis į kompetentingas institucijas dėl pagalbos. BDAR numato kad valstybės narės turi įsteigti nepriklausomą valstybinę arba viešąją instituciją, atsakingą už asmens duomenų apsaugos priežiūrą. Ši institucija yra pavadinta duomenų apsaugos priežiūros institucija (VDAI). Jos pagrindinis tikslas yra užtikrinti, kad organizacijos laikytųsi BDAR nuostatų ir gerbtų asmens duomenų teises. VDAI priima ir tiria skundus, kurie susiję su asmens duomenų apsaugos pažeidimasi.[54] Tai gali būti skundai dėl netinkamo asmens duomenų tvarkymo ar duomenų pažeidimi bei kitų BDAR pažeidimų. VDAI turi teisę atlikti tyrimus ir patikrinimus, siekdama įsitikinti ar organizacija laikosi BDAR nuostatų.[55] Tai gali apimti duomenų tvarkymo procedūras, saugos priemonių ir kitų aspektų vertinimą susyjusių su duomenų sauga. Jei VDAI nustato, kad organizacija pažeidė BDAR nuostatas, ji turi teisę skirti administracines baudas ar kitas sankcijas organizacijai.[56] Šios baudos gali būti didelės, jei organizacija nesilaiko duomenų apsaugos taisyklių. Primtus VDAI sprendimus organizacija gali skųsti.

Iš pirmo žvilgsnio, BDAR ir Europos Tarybos duomenų apsaugos konvencija turi daug bendrų bruožų. Abu dokumentai siekia užtikrinti aukštą asmens duomenų apsaugos lygį ir nustato pagrindinius principus bei teises, susijusias su duomenų tvarkymu. *Tačiau jų skirtumai atsispindi įvairiose srityse*. Teisinis reguliavimas: BDAR yra teisinis aktas, kuris tiesiogiai taikomas visose Europos Sąjungos šalyse.[57] ETDA konvencija, nors turi įtakos, tačiau reikalauja, kad šalys ją ratifikuotų, kad jis taptų privalomas.[58] Teisinės priemonės ir priežiūra: BDAR nustato vieningas taisykles dėl duomenų apsaugos visoje ES, taip pat įsteigia nacionalines priežiūros institucijas ir numato sankcijas už pažeidimus. Europos Tarybos konvencija nustato bendrus principus, tačiau palieka valstybėms narėms didelį leidimo laisvę interpretuoti ir pritaikyti šiuos principus savo nacionalinėje teisėje. Duomenų perdavimas į trečiąsias šalis: BDAR nustato griežtas taisykles dėl

[53] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB“, *supra note,* 32

[54] „2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB“, *supra note,* 32.

[55] *Ibid.*

[56] *Ibid.*

[57] Lietuvos Respublikos tesingumo ministerija, „ Europos Sąjungos reikalų koordinavimas“, LRV, žiūrėta 2024 m. kovo 3 d. https://tm.lrv.lt/lt/veiklos-sritys-1/es-reikalu-koordinavimas/

[58] „Pasiūlymas tarybos sprendimas kuriuo, atsižvelgiant į Europos Sąjungos interesus, valstybės narės įgaliojamos ratifikuoti Protokolą, kuriuo iš dalies keičiama Europos Tarybos konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108)“, EUR-LEX, žiūrėta 2024 m. kovo 3 d. https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A52018PC0451

duomenų perdavimo į trečiąsias šalis, pvz., reikalauja, kad duomenų gavėjas šalyje, kurioje vykdomas perdavimas, turėtų tinkamą duomenų apsaugos lygį. Europos Tarybos konvencija nenumato tokio griežto reguliavimo, paliekant valstybėms narėms daugiau laisvės šioje srityje. Apibendrinant galima teigti, kad BDAR ir ETDA konvencijos pirmasis įspūdis rodo, kad abu dokumentai siekia užtikrinti aukštą asmens duomenų apsaugos lygį bei nustato pagrindinius principus ir teises, susijusias su duomenų tvarkymu. Tačiau jų skirtumai aiškiai atsispindi įvairiose srityse. BDAR yra teisinis aktas, taikomas tiesiogiai visoje Europos Sąjungoje, kuris nustato vieningas taisykles ir numato nacionalines priežiūros institucijas bei sankcijas už pažeidimus. Priešingai, ETDA konvencija, nors nustato bendrus principus, palieka valstybėms narėms didelę laisvę interpretuoti ir pritaikyti šiuos principus savo nacionalinėje teisėje.

Nacionalinėje teisėje įgyvendinti įvairūs įstatymai, kurie skirti asmens duomenų apsaugai, yra esminis teisinis ramstis, kuris reglamentuoja, kaip organizacijos ir institucijos turėt tvarkyti asmens duomenis. Šie įstatymai, kurie integruojami į teisinę sistemą, nustato išsanias taisykles ir standartus dėl asmens duomenų apsaugos, rūpinasi jų teisėtu tvarkymu bei užtikrina, kad duomenys būtų naudojami atitinkamai ir sąžiningai. Teisės aktai šioje srityje nuolat yra atnaujinami ir keičiami siekiant atitikti naujus technologinius, socialinius ir teisinius iššūkius, norint užtikrinti tinkamą asmens duomenų apsaugos lygį.

Lietuvos Respublikos pagrindinis teisinis dokumentas yra ***Konstitucija***, kuri sustato šalies politinę sistemą, piliečių teises ir laisves. Remiantis Konstitucija, nauji įstatymai yra priimami ir veikia tik tuo atveju, jeigu jie nesukuria prieštaravimų šioje aukščiausioje teisės aktų hierarchijoje. Nors Konstitucijoje tieisiogiai neįtvirtinta asmens duomenų apsaugos sąvoka, tačiaus jos 22 straipsnyje pabrėžiama, kad žmogaus privatus gyvenimas yra neliečiamas.[59] Ši privatumo apsauga yra svarbi ir apima asmens sritis, įskaitant asmens duomenų konfidencialumą. Tai reiškia, kad asmens duomenų saugumas ir kontrolė yra neatsiejami nuo privataus gyvenimo, kurį saugo konstituciniai principai.[60] Ši nuostata yra svarbus pagrindas siekiant užtikrinti asmens duomenų apsaugą bei pagarbą asmens teisėms ir laisvėms.

Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymas (toliau – LR ADTAĮ) yra pagrindinis teisinis aktas, reglamentuojantis asmens duomenų apsaugą Lietuvos Respublikoje. Šis įstatymas nustato principus, taisykles ir procedūras, susijusias su asmens duomenų rinkimu, tvarkymu, saugojimu ir perdavimu. LR ADTAĮ *įgyvendina BDAR* ir užtikrinant, kad asmenų

[59] „Lietuvos Respublikos konstitucija“, LRS, žiūrėta 2024 m. kovo 5 d. https://www.lrs.lt/home/Konstitucija/Konstitucija20220522.htm
[60] Toma Birmonaitė ir kt., *Lietuvos konstitucinė teisė,* (Vilnius: Lietuvos teisės universitetas, 2002), 292, https://cris.mruni.eu/server/api/core/bitstreams/3058e0ba-7737-445b-8208-a076edd9d2f2/content

duomenys būtų tvarkomi teisėtai, sąžiningai ir saugiai. Įstatymas taip pat nustato asmens teises dėl jo duomenų, įskaitant teisę į informaciją, prieigą prie duomenų, jų taisymą ar ištyrimą. LR ADTAI apima įgaliojimus bei pareigas, skirtas valstybės institucijoms ir kitoms organizacijos, kurios tvarko asmens duomenis. Jis taip pat nustato sankcijas už pažeidimus, siekiant užtikrinti, jog subjektai laikytųsi duomenų apsaugos taisyklių ir standartų.[61] LR ADTAI veikia kaip vienas iš pagrindinių dokumentų, padedantis užtikrinti, kad Lietuvoje būtų laikomasi Europos Sąjungos duomenų apsaugos standartų ir principų, nustatytų BDAR. Šis įstatymas yra esminis elementas, kuris užtikrina, kad Lietuvoje būtų laikomasi asmens duomenų apsaugos standartų ir gerbiamos piliečių teisės bei laisvės.

Lietuvos Respublikos kibernetinio saugumo įstatymo (toliau – LR KSĮ) paskirtis yra įtvirtinti kibernetinio saugumo principus, sukurti struktūras ir procesus, skirtus valstybės kibernetiniam saugumui užtikrinti bei skatinti bendradarbiavimą tarp skirtingų institucijų.[62] Šis įstatymas įtvirtina standartus, kuriuos organizacijos turi laikytis, siekdamos užtikrinti saugią kibernetinę aplinką. Be to, jis nustato procedūras ir veiksmus, kurie turi būti įgyvendinami tais atvejais, kai įvyksta kibernetiniai incidentai. Nacionalinis kibernetinio saugumo centras ir VDAI bendradarbiauja tiriant kibernetinius incidentus, susijusius su asmens duomenų ir privatumo apsaugos pažeidimais, keičiasi informacija, reikalinga teisės aktų nustatytoms funkcijoms, susijusiomis su asmens duomenų ir privatumo apsaugą pažeidžiančių kibernetinių incidentų tyrimu, atlikti.[63] Nacionalinis kibernetinio saugumo centro ir VDAI bendradarbiavimas leidžia greičiau ir efektyviau tirti kibernetinius incidentus, ypač tuos, kurie susiję su asmens duomenų ar privatumo pažeidimais. Dalinimasis informacija ir resursais padeda suvokti institucijų icidentų mastą bei imtis veiksmų incidentams išspręsti.[64] Tai leidžia abiem institucijoms geriau suprasti kibernetinės saugos iššūkius ir pasirengti būsimiems incidentams. Šių dviejų institucijų tarpusavis bendradarbiavimas padidina pasitikėjimą visuomenėje. Žmonės ir organizacijos jaučiasi saugesni, žinodami, kad valstybinės institucijos veikia kartu siekdamos užtikrinti kibernetinę saugą ir duomenų apsaugą. Bendradarbiavimas yra esminis veiksnys kibernetinės saugos srityje, leidžiantis efektyviau reaguoti į kibernetinius iššūkius ir apsaugoti asmenų duomenis bei privatumą.

Apibendrinant galima teigti, kad analizuoti teisės aktai, įskaitant tarptautinius bei nacionalinius dokumentus, sudaro stabilų teisinį pagrindą asmens duomenų apsaugai Europoje ir Lietuvoje. Jie

---

[61] „Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas“, LRS, žiūrėta 2024 m. kovo 6 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.29193/asr

[62] „Lietuvos Respublikos kibernetinio saugumo įstatymas“, TAR, žiūrėta 2024 m. kovo 6 d. https://www.e-tar.lt/portal/lt/legalAct/5468a25089ef11e4a98a9f2247652cf4/asr?fbclid=IwAR1o5bF8eM01wwhQ_ye6ZxqFVIqoOa5hxOoIUCm6XbGetm8RJiCO9FO1PWM\

[63] *Ibid.*

[64] Krašto apsaugos ministerija, „Nacionalinė kibernetinio saugumo būklės ataskaita“, LRV, žiūrėta 2024 m. kovo 6 d. https://vdai.lrv.lt/uploads/vdai/documents/files/2020%20m_%20Nacionalinio%20kibernetinio%20saugumo%20būklės%20ataskaita%20el_%20versija.pdf

įtvirtina svarbius principus ir teises, užtikrinant teisingą ir saugų duomenų tvarkymą bei asmens teisių gerbimą. Be to, nacionalinės ir tarptautinės institucijos aktyviai bendradarbiauja, siekdamos efektyviau reaguoti į kibernetinius iššūkius ir užtikrinti duomenų saugumą bei privatumą. Šis reguliavimas svarbus ne tik teisinėje, bet ir socialinėje bei ekonominėje srityse, nes ji įtakoja verslo veiklą, technologijų vystymąsi ir visuomenės pasitikėjimą elektronine erdve.

1.3. Asmens duomenų rinkimas, tvarkymas ir saugojimas

Asmens duomenų rinkimas, tavrkymas bei saugimas yra svarbios ir aktualios temos, kurios kyla tiek verslo, tiek viešojo sektoriaus kontekste. Šios veiklos sritys reglamentuojamos įstatymais, kuriuose nustatomi principai, reikalavimai ir procedūros, kurios skirtos užtikrinti asmens duomenų teisėtumą, saugumą ir privatumą. Duomenų rinkimas, tvarkymas ir saugojimas yra veiksmų seka kurios apima veiksmus nuo duomenų rinkimo, apdorojimo, saugojimo iki naudojimo. Duomenų tvarkymas vykdomas laikantis asmens apsaugos principų ir siekiant išvengti duomenų pažeidimų, neteisėtų duomenų naudojimų ir sumažinti kitas rizikas, kurios gali pažeisti asmens teises į privatumą. Atsižvelgiant į didėjančią duomenų apsaugos svarbą ir sparčius pokyčius technologijų erdvėje tai tampa ypač svarbu.

Siekiant įsigilinti į asmens duomeų tvarkymo ciklą, svarbu išnagrinėti, kas apibrėžiama kaip duomenų rinkimas ir kokie yra pagrindiniai duomenų rinkimo pagrindai. ADTAĮ ir BDAR nėra išskiriama tokia sąvoka kaip „rinkimas“. Tačiau asmens duomenų rinkimas suprantamas kaip asmens duomenų telkimas į vieną vietą t.y. duomenų bazę.[65] Rinkimo procesas gali būti įvairių formų ir metodų – nuo rankinio duomenų įvedimo iki automatizuotų duomenų rinkimo sistemų.[66] Duomenų rinkimas apima sistemingą arba struktūrizuotą procesą, kuris apibrėžią, kaip ir kokius duomenis reikia surinkti, iš kur jie gaunami, kokia tvarka jie bus tvarkomi ir saugomi.

Asmens duomenų rinkimas ir tvarkymas yra glaudžiai susiję BDAR 4 str. 1 d. 2 p. aiškiai apibrėžia, kas yra *asmens duomenų tvarkymas*. Šis teisės aktas nurodo, kad kai atliekama operacija ar operacijų seka, susijusių su asmens duomenimis ar asmens duomenų rinkiniais, naudojant bet kokias automatizuotas ar neautomatizuotas priemones. Tai gali apimti veiksmus, tokius kaip duomenų rinkimas, įrašymas, kategorizavimas, saugojimas, pritaikymas ar redagavimas, duomenų išgavimas, peržiūra, naudojimas, atskleidimas per siuntimą, platinimą ar kitus būdus, taip pat duomenų sujungimą ar suvedimą su kitais duomenimis, apribojimą, duomenų trynimą ar sunaikinimą.

[65] Justė Mažeikaitė, „Asmens duomenų rinkimas ir naudojimas elektroninėje erdvėje: probleminiai aspektai“, (magistro darbas, Vilniaus Universitetas, 2017), 31-32 https://talpykla.elaba.lt/elaba-fedora/objects/elaba:35437133/datastreams/MAIN/content
[66] Solving privacy paradox, *supra note,* 25, 33.

[67] Kaip anksčiau darbe minėta, kad turi būti teisinis pagrindas norint tvarkyti asmens duomenis, vienas iš jų asmens duomenų subjekto sutikimas. Asmens duomenų valdytojas turėtų turėti galimybę įrodyti, kad duomenų subjektas sutiko su duomenų tvarkymo operacija, taip pat asmens duomenų subjektas turi būti supažindintas su duomenų tvarkymo tikslu, tai yra viena iš duomenų subjekto teisių. Tačiau įstatymas numato išimtį, kada asmens duomenys gali būti tvarkomi be duomenų subjekto, t.y. apginti viešąjį interesą, viešąjį saugumą.

Įstatymas nurodo, kad asmens duomenys gali būti tvarkomi dviem būdais: 1) automatizuotomis priemonėmis, 2) neautomatizuotomis priemonėmis. Kaip BDAR preambulės 15 punkte nurodoma, kad svarbu užtikrinti, kad apsauga fizinių asmenų būtų neutrali technologijų požiūriu ir nepriklausytų nuo naudojamų metodų, siekiant išvengti rimtos teisės aktų apėjimo grėsmės. Fizinių asmenų apsauga turėtų būti taikoma, nepriklausomai nuo to, ar asmens duomenys tvarkomi automatizuotomis, ar rankinėmis priemonėmis, ypač jei šie duomenys yra laikomi arba ketinama laikyti sudėtingame rinkinyje.[68] Svarbu laikytis technologinio neutralumo principo, taikant asmens duomenų apsaugos reguliavimą.[69] Tai reiškia, kad vertinant, ar su konkrečiu fiziniu asmeniu susijusi informacija tvarkoma automatiniu būdu, būtina atlikti analizę, nagrinėjant pagrindines informacijos tvarkymo operacijas.[70] BDAR ir ADTVĮ nėra įtvirtintų šių duomenų tvarkymo būdų sąvokų.

BDAR 2 str. 1 d. b. p. nurodoma kad asmens duomenų tvarkymas įtraukia tokius veiksmus kaip: rinkimą, užrašymą, rūšiavimą, saugojimą, adaptavimą ar keitimą, atkūrimą, paiešką, naudojimą, atskleidimą perduodant, platinant ar kitaip prieinamą, duomenų išdėstymą reikiamoje tvarkoje arba jų sujungimą derinant, blokavimą, trynimą ar naikinimą.[71] Svarbu pažymėti, kad dėl asmens duomenų tvarkymo reguliavimas yra svarbus. Šiam procesui yra skirtas visas BDAR II skyrius, kuriame numatytos bendrosios asmens duomenų tvarkymo teisėtumo taisyklės, kurių privalo laikytis ES valstybės narės, tvarkydamos asmens duomenis. Tačiau reikia atkreipti dėmesį, kad ES valstybės narės gali nustatyti tikslesnes asmens duomenų tvarkymo sąlygas pagal savo nacionalinius teisės aktus.[72] LR ADTAĮ 3 str. numato, kad asmens kodas, kuris yra neatsiejamas nuo asmens duomenų ir gali būti tvarkomi kai atitinka bent vieną BDAR 6 str. 1 d. nurodytą sąlygą, minėtas straipsnis taip

[67] „2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB ", *supra note,* 32.
[68] „2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB ", *supra note*, 32.
[69] Julius Zaleckis, *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė* (Vilnius: VĮ Registrų centras, 2019), 90.
[70] *Ibid.*
[71] „2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB ", *op. cit*.
[72] *Ibid.*

pat numato kad asmens kodą draudžiama skelbti viešai bei asmens kodą tvarkyti tiesioginės rinkodaros tikslais.[73] Įstatymas taip pat numato, asmens duomenų tvarkymą susijusią su darbo santykiais (5 str.). Taigi BDAR 6 str. numato jog duomenų valdytojui turi užtikrinti, kad jo asmens duomenys bus tvarkomi teisėtai ir tinkamai. Be to, šios nuostatos reikalauja, kad duomenys būtų surinkti aiškiais apibrėžtais ir teisėtais tikslais ir tik po to būtų tvarkomi tokiais būdais, kurie yra suderinti su nustatytais teisės aktais. Tai būtina siekiant išvengti netinkamo duomenų tvarkymo ir neleistino asmens duomenų naudojimo.

Svarbu pažymėti, kad kalbant apie reikalavimus duomenų tvarkymui, yra svarbus BDAR 7 str., kuriame įtvirtinami konkretūs šeši kriterijai, nusakantys, kada asmens duomenų tvarkymas laikomas teisėtu. Direktyvoje įvardinti kriterijai: 1) duomenų subjektas aiškiai ir neabejotinai, laisva valia duoda sutikimą; 2) duomenų tvarkymas būtinas vykdant sutartį, kurioje duomenų subjektas yra viena iš šalių, arba atsižvelgiant į duomenų subjekto reikalavimus prieš sudarant sutartį; 3) duomenų tvarkymas būtinas vykdant teisinę pareigą, kuri yra privaloma duomenų valdytojui; 4) duomenų tvarkymas būtinas, siekiant apsaugoti duomenų subjekto gyvybinius interesus; 5) kai duomenų tvarkymas yra būtinas vykdant užduotį, kuri yra vykdoma visuomenės labui, arba vykdant oficialius įgaliojimus, suteiktus duomenų valdytojui arba trečiajai šaliai, kuriai duomenys yra atskleidžiami; 6) duomenų tvarkymas būtinas dėl teisėtų interesų, kurių siekia duomenų valdytojas arba trečioji šalis (šalys), kuriai duomenys yra atskleidžiami, išskyrus atvejus, kai duomenų subjekto, kuriam būtina apsauga, ir laisvės yra svarbesnės nei šie interesai.[74] Tai yra esminiai aspektai, kurie nustato, ar duomenų tvarkymas yra atliekamas pagal teisės aktus. Įvertinant šiuos kriterijus, galima nustatyti, ar duomenų tvarkymas atitinka teisės aktų nustatytus reikalavimus ir ar jis atliekamas pagal įstatymų nustatytas taisykles. Taigi, šie aspektai tampa lemiamais vertinant duomenų tvarkymo veiksmus ir užtikrinant, kad jie vyktų teisėtai bei laikytųsi asmens duomenų apsaugos principų.

Svarbu pažymėti, kad viena iš paminėtų BDAR 7 str. sąlygų detalizuojama BDAR 12 straipsnyje, kuriame numatoma duomenų subjekto teisė gauti informaciją apie tvarkomus asmens duomenis (pvz., įgauti informaciją apie tai, ar duomenys yra tvarkomi, ir reikalauti pataisyti netikslius duomenis), bei to paties dokumento14 str., kuriame įtvirtinama duomenų subjekto teisė prieštarauti asmens duomenų tvarkymui.[75] Taigi, galime daryti išvadą, kad direktyvos nuostatomis siekiama nustatyti reguliavimą, kuris užtikrintų tam tikrą duomenų subjekto teisių apsaugą, kai yra tvarkomi asmens duomenys. Svarbu pabrėžti, kad BDAR 17 str. numato, kad duomenų valdytojas turi

[73] „Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas“, *supra note,* 61.
[74] „2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB ”, supra note, 32.
[75] *Ibid.*

įgyvendinti tinkamas technines ir organizacines priemones, skirtas užtikrinti, kad asmens duomenys nebūtų netyčia ar neteisėtai sunaikinti ar netyčia prarasti, pakeisti, neleistinai atskleisti ar palikti prieinami, ypač perduodant duomenis tinklu. Be to, šios priemonės turi apsaugoti nuo bet kokių kitų neteisėtų duomenų tvarkymo būdų. Atsižvelgiant į technologijų lygį ir jų įdiegimo išlaidas, šios priemonės turi užtikrinti tokią saugumo lygį, kuris atitiktų tvarkymo sukeltą riziką ir saugotinų duomenų pobūdį.

Kalbant apie asmens duomenų saugojimą vienas iš BDAR įvardintų asmens duomenų apsaugos principų yra saugojimo trukmės apribojimas, kuris kaip anksčiau darbe buvo minėta, kad privalo garantuoti, jog asmens duomenys yra saugomi ne ilgiau nei reikia siekiant tikslų, dėl kurių jie buvo surinkti. [76] Tačiau maksimalaus asmens duomenų saugojimo laiko BADAR ar LR ATDAĮ nėra nustatyto. BDAR yra nurodyta, jog asmeniui atšaukus sutikimą dėl asmens duomenų tvarkymo įmonė ar organizacija nebegalės tvarkyti jo asmens duomenų. Kiekviena įmonė ir organizacija turi numatę savo individualias asmens duomenų tvarkymo taisykles, kurios turi atitikti BDAR bei LR ATDAĮ.

Apibendrinant galima teigti, kad šiame poskyryje aptariamos svarbios temos, susijusios su asmens duomenų rinkimu, tvarkymu ir saugojimu yra išsamiai išanalizuotos. Įstaymų reglamentuojamos veiklos sritys, kurios yra pradedamos nuo duomenų surinkimo iki tvarkymo ir saugojimo yra svarbios tiek verslo, tiek viešojo sektoriaus atžvilgiu. Svarbu laikytis BDAR nuostatų, kuriomis siekiams užtikrinti asmens duomenų teisėtumą, saugumą ir privatumą. Duomenų tvarkymo cikla, įskaitant duomenų rinkimą, tvarkymą ir saugojimą, privalo atitikti įstatymų nustatytus principus ir reikalavimus. Taip pat būtina užtikrinti, kad asmens duomenys būtų saugomi tik tiek, kiek reikia siekiant įgyvendinti nustatytus tikslus ir būtų laikomasi technologinio neutralumo principo. Taigi, galima daryti išvadą, kad tinkamas asmens duomenų tvarkymas yra lemiamas siekiant užtikrinti duomenų saugumą ir asmens teisių apsaugą.

[76] „Praktinis bedrojo duomenų apsaugos reglamento taikymas“, LRV, žiūrėta 2024 m. kovo 9 d. https://aad.lrv.lt/uploads/aad/documents/files/Darbuotojams/Praktinis%20BDAR%20taikymas.pdf

2. ASMENS DUOMENŲ APSAUGOS KONTROLĖS ĮGYVENDINIMAS

Šiame skyriuje bus analizuojama samprata ir principai, pagal kuriuos veikia duomenų apsaugos pareigūnas, kur bus nagrinėjami duomenų apsaugos valdytojų vaidmenys ir principai, kurių jie turi laikytis. Antroje šio skyriaus dalyje bus nagrinėjama asmens duomenų apsaugos kontrolės įgyvendinimo problemos ir aptariamos galimos problemos ir iššūkiai, su kuriais susiduria organizacijos siekdamos užtikrinti tinkamą asmens duomenų apsaugą. Bei galiausiai, trečiame poskyryje, bus aptariamos duomenų subjektų teisės ir jų įgyvendinimas organizacijose, kur bus nagrinėjamos duomenų subjektų teisės ir būdai, kaip organizacijos gali užtikrinti šių teisių įgyvendinimą savo veikloje.

2.1. Duomenų apsaugos pareigūno vaidmuo asmens duomenų kontrolės procese

BDAR 28 str. nustatyta, jog kiekviena valstybė narė yra įpareigota užtikrinti, kad viena ar daugiau valdžios institucijų kontroliuotų, kaip jų teritorijoje yra taikomos BDAR nuostatos. Lietuvos Respublikos kontekste, VDAI funkcija yra patikrinti, kaip yra taikomos asmens duomenų apsaugos taisyklės, patikrinti jų laikymąsi ir užtikrinti, kad duomenų tvarkymas vyktų pagal BDAR reikalavimus. Tai reiškia, kad Lietuvos Respublikoje duomenų apsaugos institucija, vadovaudamasi BDAR nuostatomis, atlieka svarbų vaidmenį kontroliuojant ir užtikrinant asmens duomenų teisėtumą, saugumą ir privatumą. Norint kad įmonės ar organizacijos tinkamai užtikrintų asmens duomenų apsaugą pagal esamus teisinius reglamentus, įmonės ir organizacijos turi, asmens duomenų pareigūnus (toliau – DAP), kurie atliekant svarbų vaidmenį ir siekia užtikrinti asmens duomenų apsaugą.

Mokslinėje literatūroje nėra išskirtos DAP sąvokos, tačiau VDAI pareigūno sąvoką apibrėžia kaip, jog DAP kaip pareigybė nustatyta pagal BDAR ir buvo pradėta taikyti nuo 2018 m. gegužės 25 d. Lietuvoje ir kitose ES valstybės narėse. Pagal A. Šidlauską šis nurodo, kad pareigūnas veikia kaip tarpininkas tarp duomenų subjektų, duomenų valdytojo ar tvarkytojo bei duomenų apsaugos priežiūros institucijos.[77] Norint tinkamai suprasti kaip asmens duomenų pareigūnas prisideda prie asmens duomenų apsaugos būtina detaliau įvertinti, kokia yra DAP veikla ir funkcijos prisideda prie asmens duomenų apsaugos. Tai apima ne tik pareigūno vaidmenį užtikrinant teisės aktų laikymąsi, bet ir jo funkcijų svarbą asmens duomenų saugumui ir privatumui užtikrinti.

[77]Aurimas Šidlauskas, „The Role and Significance of the Data Protection Officer in the Organization.“, *Socialiniai tyrimai* 44, 2021, 10. https://etalpykla.lituanistika.lt/fedora/objects/LT-LDB-0001:J.04~2021~1662652990611/datastreams/DS.002.1.01.ARTIC/content

Pradžioje svarbu išnagrinėti, kuriose organizacijose turi būti skiriamas DAP ir kokios yra jo paskyrimo procedūros. Europos duomenų apsaugos darbo grupė yra parengusi duomenų apsaugos pareigūnų gaires (toliau – DAP gairės), kuriose yra išsamiai paaiškinti atitinkamas Bendrojo duomenų apsaugos reglamento nuostatas siekiant padėti duomenų valdytojams ir tvarkytojams laikytis teisės aktų, taip pat užtikrinti, kad duomenų apsaugos pareigūnai galėtų sėkmingai vykdyti savo funkcijas. Pagal BDAR 37 str. nurodyta, kad dokumentų valdytojas ir duomenų tvarkytojas privalomai paskiria DAP tais atvejais, kai: a) Duomenų tvarkymą atlieka valdžios institucija ar organizacija (išskyrus teismus, kai jie vykdo savo teismines pareigas); b) Duomenų valdytojo arba duomenų tvarkytojo pagrindinė funkcija yra atlikti duomenų tvarkymo operacijas, kurios reikalauja reguliaraus ir sistemingo didelio masto duomenų subjektų stebėjimo arba c) Duomenų valdytojo arba duomenų tvarkytojo esminė užduotis yra specialių kategorijų duomenų tvarkymas dideliu mastu.[78]

BDAR nėra apibrėžta, kas yra valdžios institucija ar įstaiga. Tačiau DAP gairėse išaiškinta, kad toks terminas turi būti apibrėžtas remiantis nacionalinės teisės nuostatomis. [79] Visuotinėje lietuvių enciklopedijoje valstybės institucija apibrėžiama kaip savarankiška, apibrėžta, struktūriškai atskirta valstybės aparato grandis, vykdanti valstybės funkcijas ir atlikdama priskirtas pareigas, pagal konstituciją ir teisės aktus.[80] Taigi valdžios institucijos ir įstaigos apima ne tik nacionalines, bet ir regionines ir vietos valdžios institucijas, bet pagal taikytinus nacionalinės teisės aktus ši sąvoka apima ir kitas viešosios teisės reguliuojamas įstaigas. Tokioms institucijoms DAP paskirti privaloma. [81] Tačiau yra ir tokių atvejų, kai yra akivaizdu, kad organizacijai yra nereikalingas DAP, Europos komisijos darbo grupė rekomenduoja duomenų valdytojams ir tvarkytojams atlikti vidinę analizę ir įvertinti ar reikalingas DAP. [82] Ši rekomendacija taikoma situacijoms, kai, kilus problemoms (pvz., asmens duomenų tvarkymo pažeidimui), buvo imtasi visų būtinų priemonių užtikrinti, kad asmens duomenys būtų teisingai tvarkomi, ir taip būtų įgyvendintas BDAR 24 str. Organizacijos gali nepriklausomai nuspręsti paskirti DAP ir jam priskirti pareigas, lyg šis paskyrimas būtų privalomas, taikydamos tuos pačius reikalavimus kaip ir privalomai paskirtam DAP.

[78] „2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB ", *supra note*, 32.
[79] „29 straipsnio duomenų apsaugos darbo grupė gairės dėl pranešimo apie asmens duomenų saugumo pažeidimą pagal Reglamentą (ES) 2016/679", Europa.eu., žiūrėta 2024 m. kovo 12 d. https://ec.europa.eu/newsroom/article29/items/612048
[80] Visuotinė Lietuvių enciklopedija, „Valstybės institucija", VLE, žiūrėta 2024 m. kovo 12 d. https://www.vle.lt/straipsnis/valstybes-institucija/
[81] „29 straipsnio duomenų apsaugos darbo grupė gairės dėl pranešimo apie asmens duomenų saugumo pažeidimą pagal Reglamentą (ES) 2016/679", *op. cit.*
[82] *Ibid.*

BDAR 37 str. 1 d. b ir c. p. nurodoma, kad duomenų valdytojo arba duomenų tvarkytojo pagrindinė veikla ir (arba) reguliarus ir sistemingas dideliu mastu duomenų subjekto stebėjimas.[83] BDAR 97 konstatuojamojoje dalyje pabrėžiama, kad duomenų valdytojo pagrindinė veikla yra glaudžiai susijusi su jo *svarbiausia veikla ir nesusijusi su asmens duomenų tvarkymu kaip papildoma veikla*. [84] Taigi, svarbiausios operacijos, skirtos duomenų valdytojo arba duomenų tvarkytojo tikslams pasiekti, gali būti laikomos pagrindine veikla. Pagrindinė organizacijos veikla, suprantama kaip esminis veiklos aspektas siekiantis organizacijos iškeltų tikslų, tai gali apimti asmens duomenų tvarkymą kaip veiklos dalį arba jo nebuvimą kaip papildomą veiklą. Siekiant įvertinti, ar organizacija vykdo reguliarų ir sistemingą duomenų tvarkymo stebėjimą, turėtų būti atsižvelgiama į tai, ar duomenų tvarkymas: atliekamas tam tikrais intervalais ar konkrečiu laikotarpiu, vyksta nuolatos, ar yra pasikartojantis tik tam tikrais periodais, vyksta pagal tam tikrą sistemą, ar yra iš anksto suplanuotas pagal darbo metodikas ir yra įgyvendinamas kaip strategijos dalis.[85] Norint nustatyti, ar duomenų tvarkymas vykdomas dideliu mastu, turėtų būti atsižvelgiama į tokius veiksnius kaip susijusių duomenų subjektų skaičius arba gyventojų procentinė dalis, tvarkomų asmens duomenų kiekis ir intervalas, asmens duomenų tvarkymo veiklos trukmė. [86] Tačiau teisės aktuose ir mokslinėje literatūroje nėra išaiškinta kas yra didelis mastas. Iš teisės aktų nuostatų aišku, kad siekiant išsiaiškinti ar organizacijai reikalingas DAP, organizacija turi vykdyti reguliarų ir sistemingą asmens duomenų stebėjimą dideliu mastu.

Siekiant išsiaiškinti ar organizacijai yra reikalingas DAP yra duomenų valdytojo arba duomenų tvarkytojo esminė užduotis yra specialių kategorijų duomenų tvarkymas dideliu mastu.[87] BDAR 9 str. 1 d. nurodyta, kad specialios kategorijos duomenys yra informacija kurioje atskleidžiami kilmės, politiniai, religiniai įsitikinimai, profesinės sąjungos narystė, taip pat tvarkyti genetinius, biometrinius duomenis siekiant konkrečiai nustatyti fizinio asmens tapatybę, sveikatos būklę arba duomenis apie lytinį gyvenimą ir lytinę orientaciją.

Norint išsamiau suprasti, kaip DAP prisideda prie asmens duomenų kontrolės, būtina išnagrinėti, kas gali būti skiriamas DAP. Pagal BDAR 37 str. 5 d. nurodyta, kad pareigūnas gali būti paskirtas remiantis asmens ekspertinių žinių lygiu, profesinėmis savybėmis, ypač turint duomenų

[83] „2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB ", *op. cit.*
[84] „2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB ", *supra note*, 32.
[85] „29 straipsnio duomenų apsaugos darbo grupė gairės dėl pranešimo apie asmens duomenų saugumo pažeidimą pagal Reglamentą (ES) 2016/679", *supra note,* 79.
[86] Valstybinė duomenų apsaugos inspekcija, „Viešoji koncultacija dėl pareigos paskirti duomenų apsaugos pareigūna", LRV, žiūrėta 2024 m. kovo 13 d. https://vdai.lrv.lt/uploads/vdai/documents/files/Viesoji%20-%20dap_2017.pdf
[87] „2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB ", *op. cit.*

apsaugos tiesės žinių ir praktikos, taip pat apsvarsčius ar asmuo gebės atlikti DAP funkcijas ir užduotis. DAP gairėse nurodoma, kad įmonės turėtų įvertinti tvarkomų duomenų sudėtingumą ir nuspręsti ar asmuo pretenduojantis į DAP pareigas gebės tinkamai tvarkyti asmens duomenis. [88] Taip pat BDAR nėra nurodoma į kokias konkrečiai profesines savybes turi būti atsižvelgiama paskiriant DAP, tačiau DAP gairėse yra pabrėžiama, kad asmuo, kuris yra skiriamas duomenų apsaugos pareigūnu, turėtų gerai suprati nacionalinius ir Europos duomenų apsaugos teisės aktus bei praktiką, ypač BDAR. [89] DAP gairių rengėjai taip pat nurodo, kad būtų naudinga, jei priežiūros institucijos organizuotų ar finansuotų tinkamą ir nuolatinį duomenų apsaugos pareigūnų mokymą ir užtikrintų, kad duomenų apsaugos pareigūnai nuolatos atnaujintų savo žinias.

BDAR 37 str. 6 d. nurodyta, kad organizacijos DAP gali būti duomenų valdytojo arba duomenų tvarkytojo darbuotojas arba įmonė atliekanti DAP funkcijas su kuria turi būti pasirašoma paslaugų teikimo sutartis. Jei DAP paskyrimas organizacijos darbuotojas organizacija turi užtikrinti, kad pareigų ir atliekamų užduočių, susijusių su duomenų apsauga, vykdymo nekiltų interesų konfliktas, kurį gali sukelti DAP skiriamas darbuotojas, turintis įtakos asmens duomenų tvarkymo tikslams ir metodams.[90] Paprastai pareigos, kurios gali sukelti interesų konfliktą, apima vadovo, operacijų vadovo, finansininko, rinkodaros ar žmogiškųjų išteklių skyriaus vadovo, informacinių technologijų vadovo ir panašių pareigų funkcijas. Jei DAP pasirenkamas išorinis paslaugų teikėjas reikėtų užtikrinti, kad rengiant paslaugų teikimo sutartį ir yra pasirenkamas fizinis asmuo vykdantis individualią veiklą, ar kitas juridinis asmuo, turi būti užtikrinta kad dėl DAP atliekamų užduočių ir pareigų nekiltų interesų konfliktas. Tokiu atveju reikėtų užtikrinti, kad toks asmuo negalės atstovauti įmonei teismuose, kai nagrinėjamos bylos, susijusios su duomenų apsauga.[91] Internete yra gausu įmonių, kurios kitoms organizacijoms atlieka DAP funkcijas. Taigi abiem atvejais nesvarbu koks asmuo pasirenkamas DAP funkcijoms vykdyti svarbiausia užtikrinti, kad dėl asmens, kuris vykdys DAP funkcijas nekiltų interesų konfliktas ir asmuo būtų kvalifikuotas. Pagal BDAR 37 str. 7 d. paskyrus DAP duomenų valdytojas arba duomenų tvarkytojas pareigūno kontaktinius duomenis perduoda asmens duomenų tvarkymą prižiūrinčiai institucijai Lietuvos atveju duomenys apie DAP perduodami VDAI.

Norint išnagrinėti, kaip DAP prisideda prie asmens duomenų apsaugos kontrolės, būtina analizuoti DAP funkcijas. BDAR 39 str. 1 d. b. p. viena iš pareigų nurodoma, jog DAP pavesta stebėti kaip laikomasi BDAR. Taip pat 97 konstatuojamojoje dalyje nurodyta, kad DAP duomenų valdytojui

[88] „29 straipsnio duomenų apsaugos darbo grupė gairės dėl pranešimo apie asmens duomenų saugumo pažeidimą pagal Reglamentą (ES) 2016/679“, *op. cit.*
[89] „29 straipsnio duomenų apsaugos darbo grupė gairės dėl pranešimo apie asmens duomenų saugumo pažeidimą pagal Reglamentą (ES) 2016/679“, *supra note,* 79.
[90] Šidlauskas, *supra note* 77: 13.
[91] *Ibid.*

ar duomenų tvarkytojui turėtų padėti stebėti, kaip organizacijos viduje yra laikomasi BDAR nuostatų. Reikėtų pažymėti, jog DAP turi užtikrinti slapto arba konfidencialaus pobūdžio informacijos saugumą, vykdant savo pareigas (užduotis) ir laikantis Sąjungos ar valstybės narės teisės.[92] Tai reiškia kad pavyzdžiui įmonės darbuotojas, skundžiasi, jog darbdavys darbuotojų duomenis tvarko neteisingai, tad DAP turėtų užtikrinti tokių pranešimų konfidencialumą ir patikrinti gautą informaciją ir atlikti vertinimą ar yra pažeidžiamos duomenų subjekto teisės ar ne. Pagal DAP gaires anksčiau minėtas straipsnis apima ir informacijos rinkimą duomenų tvarkymo veiklai identifikuoti, tikrinti ir vertinti, ar duomenų tvarkymo procesas atitinka nustatytus reikalavimus, kartu teikiant informaciją, konsultacijas ir rekomendacijas duomenų valdytojui ar tvarkytojui.[93] Stebėjimas, siekiant užtikrinti reglamento laikymąsi, nereiškia, kad duomenų apsaugos pareigūnas yra asmeniškai atsakingas už reglamento pažeidimus. BDAR 24 str. 1 d. aiškiai nurodyta, kad atsakomybė už tinkamų techninių ir organizacinių priemonių įgyvendinimą, kad būtų užtikrinta ir įrodyta duomenų tvarkymo atitiktis reglamentui, tenka duomenų valdytojui, o ne DAP.

Sekanti DAP funkcija yra konsultavimas dėl poveikio duomenų apsaugai vertinimo ir stebėjimas, kaip jis vykdomas. BDAR 35 str. 1 d. konkrečiai nurodyta, kad būtenti duomenų valdytojas, o ne DAP, turi atlikti poveikio duomenų apsaugai vertinimą. Nepaisant to, duomenų apsaugos pareigūnas gali atlikti svarbų vaidmenį, padedant duomenų valdytojui atlikti poveikio vertinimą. Atsižvelgiant į pritaikytosios duomenų apsaugos principą, 35 str. 2 d. aiškiai nurodoma, kad duomenų valdytojas, atlikdamas poveikio duomenų apsaugai vertinimą, turi konsultuotis su duomenų apsaugos pareigūnu.[94] Be to, 39 str. 1 d. c p. duomenų apsaugos pareigūnui nustatoma pareiga paprašyti konsultacijos dėl poveikio duomenų apsaugai vertinimo ir stebėti jo vykdymą pagal 35 straipsnį. Pagal DAP gaires taip pat duomenų valdytoją ar duomenų tvarkytoją DAP gali konsultuoti tokiais klausimais kaip: ar reikalinga atlikti duomenų apsaugai vertinimą, kokia metodika vadovautis atliekant vertinimą, ar duomenų apsaugos vertinimą gebės atlikti pati organizacija ar ją užsakyti iš paslaugų teikėjų, kokios apsaugos priemonės būtų naudingos ir padėtų sumažinti riziką duomenų subjektų teisėms ir interesams, įvertinti ar tinkamai atliktas poveikio duomenų apsaugai vertinimas ir ar poveikio vertinimo išvados atitinka BDAR. [95] Taigi DAP gali teikti konsultacijas dėl poveikio duomenų apsaugai vertinimo ir taip dalyvauti poveikio vertinime.

[92] „2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB ", *supra note*, 32.
[93] „29 straipsnio duomenų apsaugos darbo grupė gairės dėl pranešimo apie asmens duomenų saugumo pažeidimą pagal Reglamentą (ES) 2016/679", *supra note*, 79.
[94] „2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB ", *op. cit.*
[95] „29 straipsnio duomenų apsaugos darbo grupė gairės dėl pranešimo apie asmens duomenų saugumo pažeidimą pagal Reglamentą (ES) 2016/679" *op. cit.*

Kita DAP funkcija yra nurodyta BDAR 39 str. d ir e p. kuriuose nurodoma, kad viena iš DAP funkcijų yra bendradarbiavimas su priežiūros institucija ir kontaktinio asmens funkcija funkcijas priežiūros institucijai kreipiantis su duomenų tvarkymu susijusiais klausimais, įskaitant 36 straipsnyje nurodytas išankstines konsultacijas, ir prireikus konsultuoja visais kitais klausimais.[96] DAP gairėse išaiškinta, jog DAP veikia kaip kontaktinis asmuo su VDAI ir padeda priežiūros institucijai gauti dokumentus ir informaciją, kad būtų įgyvendintos BDAR 57 str. nurodytos VDAI užduotys. [97] DAP gali konsultuotis su VDAI dėl iškilusių klausimų susijusių su asmens duomenų tvarkymu. [98] Taigi, DAP pareigūnui veikiant kaip kontaktinio asmeniui, padeda užtikrinti tinkamą duomenų apsaugą ir padeda įgyvendinti nustatytas priežiūros institucijos užduotis.

Dar viena iš DAP funkcijų yra rizika pagrįstas požiūris, BDAR 39 str. 2 d. iš DAP reikalaujama, kad pareigūnas tinkamai įvertintų su duomenų tvarkymo operacijomis susijusį pavojų, atsižvelgdamas į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus. DAP gairėse nurodoma, kad šiame straipsnyje yra primenamas protingumo principas. Protingumo principas yra bendrasis teisės principas, kuris reikalauja, kad asmuo elgtųsi atidžiai, apdairiai, sąžiningai ir teisingai.[99] Tai reiškia, kad DAP turi organizuoti savo veiklą taip, kad daugiausia dėmesio būtų skirta klausimams, tiesiogiai susijusiems su grėsmėmis duomenų apsaugos ir kitose rizikos srityse. Šis požiūris turėtų leisti DAP konsultuoti duomenų valdytoją dėl to, kokią metodiką pasirinkti poveikio duomenų apsaugai vertinimui, kokie vidaus ar išorės duomenų apsaugos audito aspektai turi būti apimti, kokius vidaus mokymus organizuoti darbuotojams ar vadovybei, atsakingiems už duomenų tvarkymo veiklą, ir kurias duomenų tvarkymo operacijas skirti daugiau dėmesio ir resursų.[100] DAP, remdamasis rizikos pagrįstu požiūriu, vertina pavojus, susijusius su duomenų tvarkymo operacijomis ir teikia konsultacijas dėl tinkamų veiksmų. Šio požiūrio esmė – užtikrinti, kad dėmesys būtų sutelktas į pagrindines duomenų apsaugos grėsmių ir rizikos sritis, suteikiant galimybę DAI konsultuoti organizaciją dėl metodo pasirinkimo, visų duomenų apsaugos audito ir mokymo aspektų.

DAP atlieka svarbų vaidmenį ir užtikrina asmens duomenų kontrolę organizacijos viduje. Tačiau pagrindinę duomenų apsaugos kontrolę valstybės mastu atlieka VDAI. DAP funkcijos apima

---

[96] „2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB ", *supra note*, 32.

[97] „29 straipsnio duomenų apsaugos darbo grupė gairės dėl pranešimo apie asmens duomenų saugumo pažeidimą pagal Reglamentą (ES) 2016/679", *supra note*, 79.

[98] Valstybinė duomenų apsaugos inspekcija, „Duomenų apsaugos pareigūnas", LRV, žiūrėta 2024 m. kovo 15 d. https://vdai.lrv.lt/lt/adsp-ir-dap/duomenu-apsaugos-pareigunas/

[99] „Dėl Lietuvos Respublikos administracinių teisės pažeidimų kodekso 40 straipsnio pripažinimo netekusiu galios ir 251 straipsnio pakeitimo įstatymo 1 ir 2 straipsnių, Lietuvos Respublikos mokesčių administravimo įstatymo 27 straipsnio 5 dalies, 50 straipsnio 3 ir 9 dalių atitikties Lietuvos Respublikos Konstitucijai", LRS, žiūrėta 2024 m. kovo 15 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.115172

[100] „29 straipsnio duomenų apsaugos darbo grupė gairės dėl pranešimo apie asmens duomenų saugumo pažeidimą pagal Reglamentą (ES) 2016/679", *op. cit.*

ne tik rizikos vertinimo, konsultavimo vaidmenį, tačiau bendradarbiauja kaip kontaktinis asmuo su VDAI ir koncultuojasi dėl tinkamo duomenų duomenų tvarkymo procedūrų. Taip pat, svarbu pažymėti, kad nors DAP dalyvauja duomenų tvarkymo procese, tačiau jis nėra tiesiogiai atsakingas už pažeidimus ar netinkamą duomenų tvarkymą. Atsakomybė dėl asmens duomenų tvarkymo pažeidimų tenka duomenų valdytojui arba tvarkytojui, kurie pagal BDAR yra tiesiogiai atsakingi už duomenų tvarkymo atliekamus veiksmus ir naudojamas apsaugos priemones. Todėl DAP veikia kaip konsultantas, kuris padeda organizacijoms įgyvendinti tinkamas priemones, siekiant užtikrinti duomenų apsaugą ir skaidrumą, tačiau jis pats neneša atsakomybės už pažeidimus ar neteisingą duomenų tvarkymą.

2.2. Asmens duomenų apsaugos kontrolės įgyvendinimo problemos

Asmens duomenų apsaugos kontrolės įgyvendinimo problemas bus identifikuojamos analizuojant asmens duomenų saugos pažeidimų (toliau – ADSP) tendencijas, nes tai padeda suvokti sisteminės duomenų apsaugos trūkumus bei rizikos veiksnius organizacijų veikloje. Šios analizės metu galima atskleisti potencialias spragas duomenų saugumo srityje, nustatyti ir įvertinti pažeidžiamumo lygį, bei identifikuoti veiksnius, darančius įtaką duomenų saugumui. Aptariant kontrolės įgyvendinimo problemas, galima geriau suprasti, kaip organizacijos įgyvendina duomenų apsaugos politiką praktikoje ir ar jos veiksmai yra pakankami, kad apsaugotų asmens duomenis nuo netinkamo naudojimo, vagysčių ar kitų pažeidimų. Tai svarbu siekiant efektyviau užtikrinti asmens duomenų saugumą, padidinti organizacijos atsparumą pažeidimams bei prisidėti prie teisės aktų laikymosi ir visuomenės pasitikėjimo organizacija duomenų tvarkymo atžvilgiu.

BDAR 4 str. 1 d. 12 p. duomenų saugumo pažeidimas yra incidentas kurio metu asmens duomenys netyčia arba neteisėtai sunaikinami, prarandami, modifikuojami, atskleidžiami, siunčiami, saugomi ar kitaip tvarkomi, neturint leidimo prie jų prieigos. [101] Pagal BDAR duomenų valdytojas sužinojęs apie ADSP nedelsdamas per 72 valandas apie incidentą turi informuoti VDAI.[102] Pranešime organizacija turi nurodyti koks duomenų saugumo pažeidimo pobūdis, taip pat nurodyti incidento paveiktų duomenų skaičių bei duomenų kategorijas, taip pat nurodomi įmonės DAP kontaktai, su kuriuo VDAI bendraus siekiant sužinoti kuo daugiau reikšmingų detalių apie incidentą (jei įmonė neturi DAP, nurodomi asmens kontaktiniai duomenys, kuris bendraus su priežiūros institucija). Nustačius ADSP, organizacija turi numatyti kokios gali būti pasekmės dėl įvykusio incidento ir apie galimas pasekmes pranešti VDAI. Taip pat pranešime priežiūros institucijai, duomenų valdytojas turi

[101] „2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB ”, *supra note*, 32.
[102] *Ibid.*

nurodyti, kokių priemonių imasi ar planuoja imtis, kad būtų pašalintas ADSP, bei nurodo kokių priemonių planuojama imtis neigiamoms pasekmėms sumažinti .[103] Jei numatoma, kad ADSP gali sukelti didelį pavojų fizinių asmenų teisėms ir laisvėms duomenų valdytojas nedelsdamas apie ADSP turi pranešti duomenų subjektui pranešimu, kuris turi atitikti BDAR 34 str. reikalavimus. BDAR preambulės 85 punkte apibrėžiama, kad didelis pavojus yra, kai dėl ADSP fiziniai asmenys gali patirti fizinę, materialią ir ne materialią žalą, kaip pavyzdžiui kaip asmuo dėl ADSP gali prarasti savo duomenų kontrolę, patirti diskriminaciją, dėl prarastų duomenų gali būti suklastota duomenų subjekto tapatybė, gali patirti finansinių nuostolių. [104] Taigi, numanant kad fiziniam asmeniui (duomenų subjektui) gali kilti didelis pavojus dėl kurio asmuo gali patirti fizinę, materialią ar nematerialią žalą, duomenų valdytojas nedelsdamas turi pranešti fiziniam asmeniui dėl ADSP.

Lietuvoje per 2023 metus VDAI gavo 254 pranešimus dėl ADSP, kurių metu buvo paveikti 571 833 duomenų subjektai, 2022 metais VADI gavo 304 pranešimus, kurių metu buvo paveikti 1 955 382 duomenų subjektai.[105] Vertinant 2023 metų ADSP pagal pobūdį daugiausiai vyrauja konfidencialumo pažeidimai, kurie sudaro 76 proc. visų pažeidimų, taip pat po 10 proc. sudaro vientisumo ir prieinamumo pažeidimai, taip pat 4 proc. gautų pranešimų nebuvo laikomi ADSP.[106] 2022 metais konfidencialumo pažeidimai sudarė 88 proc. visų pažeidimų, 6 proc. sudarė vientisumo pažeidimai, 7 proc. sudarė prieinamumo pažeidimai, 6 proc. visų gautų pranešimų nebuvo laikomi ADSP. [107] Norint tinkamai suprasti ADSP pobūdį būtina išsiaiškinti kaip yra suprantami pažeidimų tipai, pagrinde yra 3 pažeidimų tipai. *Konfidencialumo pažeidimu* laikomi pažeidimai, kurie įvyksta, kai asmens duomenys yra atskleidžiami arba prie jų gaunama prieiga be leidimo arba neteisėtai. [108] *Prieinamumo pažeidimu* laikomi, kai dėl netyčia ar neteisėtos veikos dingsta prieiga prie asmens duomenų arba jie būna sunaikinti.[109] *Vientisumo pažeidimu* laikomas incidentas kurio metu asmens duomenys yra neleistinai arba netyčia keičiami.[110] Tad 2023 metais daugiai vyravo konfidencialumo pažeidimai, kurio pagrindine priežastimi laikoma neteisingas techninių priemonių taikymas siekiant

[103] „2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB ", *supra note*, 32.
[104] *Ibid.*
[105] „Valstybinė duomenų apsaugos inspekcija, asmens duomenų saugumo pažeidimai Lietuvoje 2023 m.", LRV, žiūrėta 2024 m. kovo 16 d. https://vdai.lrv.lt/media/viesa/saugykla/2024/1/Mdb7Qax9xsk.pdf
[106] *Ibid.*
[107] Valstybinė duomenų apsaugos inspekcija, „2022 metų asmens duomenų apsaugos priežiūros Lietuvoje apžvalga", LRV, žiūrėta 2024 m. kovo 16 d.
https://vdai.lrv.lt/uploads/vdai/documents/files/2022%20ADA%20prieziuros%20apzvalga.pdf
[108] „Valstybinė duomenų apsaugos inspekcija rekomendacija dėl asmens duomenų saugumo pažeidimų nustatymo, tyrimo, pranešimo apie juos ir dokumentavimo tvarkos", LRV, žiūrėta 2024 m. kovo 16 d.
https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomend_ADSP_2018.pdf
[109] „29 straipsnio duomenų apsaugos darbo grupė gairės dėl pranešimo apie asmens duomenų saugumo pažeidimą pagal Reglamentą (ES) 2016/679", *supra note*, 79.
[110] „Valstybinė duomenų apsaugos inspekcija rekomendacija dėl asmens duomenų saugumo pažeidimų nustatymo, tyrimo, pranešimo apie juos ir dokumentavimo tvarkos", *op. cit.*

užtikrinti konfidencialumą.[111] Tai rodo daugiausiai dėmesio turėtų būti skiriama konfidencialumo užtikrinimui siekiant sumažinti asmens duomenų saugumo riziką.

Analizuojant incidento tipus pagrinde išskiriami 2 tipai, t.y. kibernetinis incidentas ir kitas incidentas. [112] *Kibernetiniu incidentu laikomas įvykis* ar veika kibernetinėje erdvėje, kuris gali arba sukelia grėsmę ar neigiamą poveikį ryšiams ir informacinėms sistemoms, dėl elektroninės informacijos prieinamumo, autentiškumo, vientisumo ir konfidencialumo pažeidimų, kurie gali trukdyti arba sutrikdyti ryšių ir informacinių sistemų veiklą, valdymą ir paslaugų teikimą.[113] Kibernetinis incidentas apima duomenų šifravimo klaidas, išpirkų reikalavimą už pasisavintus duomenis, duomenų viliojimo atakas. Remiantis statistika svarbu pažymėti, kad nors kibernetiniai įvykiai sudarė tik 15 proc. visų 2023 m. įvykusių ADSP, jų metu buvo paveikti 49 proc. subjektų duomenys (iš visų 2023 m. paveiktų subjektų), o dėl kitų priežasčių buvo paveikti 51 proc. subjektų duomenys. [114] Lyginant su praėjusių metų duomenimis, pastebima, kad dėl 2022 m. įvykusių kibernetinių įvykių buvo paveikta 82 proc. duomenų subjektų (iš visų 2022 m. paveiktų duomenų subjektų skaičiaus), o dėl kitų priežasčių - 18 proc. duomenų subjektų. [115] VDAI atliko vertinimą, ir identifikavo pagrindines kibernetinio incidento priežastis ir nustatė esmines duomenų saugumo valdymo spragas, kurios lemia asmens duomenų apsaugos pažeidimus. Priežiūros instucija remdamasi šiais rezultatais, parengė rekomendacijas organizacijoms, kuriomis siekiama padėti organizacijoms išvengti kibernetinių incidentų ir būtų tinkamai užtikrinamas asmens duomenų saugumas.

Remiantis VDAI atliktu vertinimu, priežiūros institucija identifikuoja esmines duomenų valdymo spragas, kurios leido įvykti *kibernetiniams incidentams*. Pagrindinės duomenų apsaugos spragos dėl kurių įvyksta duomenų pažeidimai yra organizacijų darbuotojų kvalifikacijos stoka, nes organizacijoje nėra organizuojami kursai, kurių metu darbuotojai būtu supažindinami ir mokomi apie kibernetinį saugumą. Darbuotojams nesuprantant kibernetinio saugumo svarbos ir neturint kibernetinio raštingumo įgūdžių, darbuotojai nemoka kritiškai įvertinti gaunamų elektroninių laiškų ir juos atidarius paspaudžia ant kenkėjiškų nuorodų ir elgiasi neatsargiai t.y. suveda savo darbovietės paskyros prisijungimus. Ypač yra pavojinga kai į darbo vietos programinę įrangą įdiegia nežinomos kilmės programas, darbuotojas, kuris turi programinės įrangos administratoriaus teises, nes įdiegus nežinomos kilmės programą, ši gali sukelti saugumo pavojų ir padidinti tikimybė potencialiems

[111] Jgminaitė, *supra note,* 11: 221.
[112] „Valstybinė duomenų apsaugos inspekcija, asmens duomenų saugumo pažeidimai Lietuvoje 2023 m.“, *supra note,* 105: 3.
[113] „Lietuvos Respublikos kibernetinio saugumo įstatymas“, *supra note,* 62.
[114] „Valstybinė duomenų apsaugos inspekcija, asmens duomenų saugumo pažeidimai Lietuvoje 2023 m.“, *op. cit.,* 9.
[115] *Ibid.*

įsilaužimams ar duomenų nutekėjimams.[116] Organizacija gali sumažinti kibernetinių incidentų riziką vykdydama įvairias *prevencines priemones ir paruošdama atsakomąsias strategijas*. Pirmiausia organizacijos vadovai turėtų *organizuoti nuolatinius mokymus apie kibernetinį saugumą*, nes darbuotojai būtų informuoti ir supažindinti su kibernetinio saugumo grėsmėmis.[117] Mokymai turėtų apimti ir duomenų viliojimo (angl. Phisging) atakų atpažinimą, nes nemaža dalis kibernetinių atakų įvyksta dėl duomenų viliojimo. [118] Suteikiant šiuos mokymus, organizacija siekia padidinti savo darbuotojų sąmoningumą ir gebėjimą atpažinti bei įveikti kibernetines grėsmes, kurių rezultatas yra didesnis bendras kibernetinis saugumas. Sekanti prevencinė priemonė *elektroninio pašto filtravimo mechanizmai*. [119] Organizacija į savo programinę įrangą turėtų įdiegti arba užsakyti paslaugą, kurios atliktų elektroninio pašto filtravimo funkciją, kuri automatiškai tikrintų ir filtruotų įeinančius laiškus pagal turinį ir siekdami atpažinti ir atskirti potencialiai pavojingus laiškus. Tai padeda organizacijoms išvengti įvairių kibernetinių grėsmių, tokių kaip „phishing“ atakos, taip pat ir kenksmingų programų platinimo per el. paštą. [120] Taigi, el. pašto filtravimo mechanizmai yra svarbi priemonė užtikrinant bendrą organizacijos kibernetinį saugumą ir apsaugant jos infrastruktūrą bei duomenis nuo potencialių pavojų. Kita prevencinė priemonė yra *imitacinis kibernetinis pavojus*. Periodiškai organizuojant kibernetinių atakų simuliacijas naudojant duomenų viliojimo metodą yra praktiškas būdas išbandyti įmonės darbuotojus, kaip atpažinti ir reaguoti į potencialiai kenksmingus laiškus ar kitas kibernetinių atakų formas. Šios simuliacijos leidžia įmonės personalui praktiškai patirti, kaip veikia įvairios kibernetinės grėsmės, padeda suprasti, kaip jas atpažinti, bei kokių veiksmų imtis, jei susiduriama su kibernetiniu incidentu. [121]Be to, tokios simuliacijos taip pat padeda įvertinti įmonės kibernetinio saugumo lygį ir identifikuoti sritis, kurias reikia tobulinti, siekiant padidinti organizacijos pasirengimą ir atsparumą kibernetinėms grėsmėms. Dar viena kibernetinių incidentų *prevencijos priemonė yra išsamus veiklos tęstinumo planas* (toliau – VTP). VTP turi apibrėžti procedūras ir veiksmus, kuriuos reikėtų įgyvendinti kibernetinio incidento atveju. Šis planas turėtų apimti veiksmus atkūrimui, strategijas duomenų atsarginėms kopijoms, komunikacijos protokolus ir

---

[116] „Kibernetinių atakų atpažinimas“, VU, žiūrėta 2024 m. kovo 19 d. https://cyberphish.knf.vu.lt/upload/lm/59a44v1ZnWpJ9nBFOgX5im6KcGOHX7EllXV82d6b.pdf

[117] „Kibernetinio saugumo mokymai darbuotojams: kas yra tikrasis laimėtojas?“, Verslo žinios, 2021 m. gegužės 03d. https://www.vz.lt/verslo-sprendimai/2021/05/03/kibernetinio-saugumo-mokymai-darbuotojams-kas-yra-tikrasis-laimetojas

[118] Justinas Rastenis, „Duomenų viliojimo elektroniniais laiškai atakų tyrimas“ (daktaro disertacija, Vilniaus Gedimino technikos universitetas, 2022), 8. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiKwtnoguOFAxUILRAIHbtzAQ0QFnoECA8QAQ&url=https%3A%2F%2Fvb.vgtu.lt%2Fobject%2Felaba%3A136466537%2F136466537.pdf&usg=AOvVaw00JARoXDxiUl52VspivzhF&opi=89978449

[119] „Valstybinė duomenų apsaugos inspekcija, asmens duomenų saugumo pažeidimai Lietuvoje 2023 m.“, *supra note*, 105: 3.

[120] „Nacionalinis kibernetinio saugumo centras, kibernetinis saugumas ir verslas. Ką turėtų žinoti kiekvienas įmonės vadovas 2020“, NKSC, žiūrėta 2024 m. kovo 19 d. https://www.nksc.lt/doc/Kibernetinio_saugumo_vadovas_verslui_2020.pdf

[121] *Ibid.,* 51.

kitas būtinas priemones, skirtas atkurti normalią įmonės veiklą po incidento. [122] VTP svarbu turėti, nes tai padeda organizacijai greitai ir efektyviai reaguoti į kibernetinius įvykius, sumažinti jų poveikį bei užtikrinti, kad verslo veikla būtų atkurta kuo greičiau ir sklandžiai. Aptarus šias VADI siūlomas prevencines priemones akivaizdu, jog organizacijos turi dėti daugiau pastangų į savo darbuotojų kibernetinio saugumo mokymus ir jų sąmoningumo didinimą, siekiant sumažinti kibernetinių incidentų riziką.

VDAI išskiria dar vieną kategoriją duomenų saugos valdymo spragų, dėl kurių įvyksta kibernetiniai incidentai – *prieigų kontrolės ir autentifikavimo pažeidimai*. Ši kategorija susijusi su prieigų kontrolės ir autentifikavimo pažeidimais, kurios atskleidžia svarbias organizacijos saugumo spragas, kurios gali lemti saugumo pažeidimus. Šios spragos apima įvairius aspektus, pradedant netinkamu IT administratorių prieigos valdymu, kuriose nepanaikinamos prieigos teisės po jų išėjimo iš darbo, ir baigiant bendro naudojimo vartotojų paskyromis bei per paprastais slaptažodžiais. Be to, trūksta tinkamų autentifikavimo priemonių, tokios kaip kelių veiksnių autentifikavimo metodai, kurie būtų būtini siekiant apsaugoti sistemos prieigas nuo nepageidaujamų asmenų.[123] Šie pažeidimai sudaro palankią aplinką potencialiems neteisėtiems veiksmams, todėl organizacijoms labai svarbu identifikuoti ir spręsti šias spragas, siekiant užtikrinti optimalų duomenų saugumą.[124] Norint išvengti šios kategorijos pažeidimų VDAI rekomenduoja kaip prevencinę priemonę *panaikinti visas prieigas IT administratoriams (-ui) išėjus iš darbo ar pasikeitus paslaugos teikėjui.* [125] Tai reiškia, kad IT administratoriui palikus darbovietę ir išėjus iš darbo arba pasikeitus tokio tipo paslaugų teikėjui svarbu tuoj pat, nieko nelaukiant panaikinti visas jo turimas prieigas teises prie sistemų. Tai reiškia, kad visi ryšiai su sistemomis, programomis ar duomenų bazėmis, kurie buvo suteikti šiam administratoriui, turėtų būti panaikinami, kad administratorius neturėdamas teisės neprisijungtų prie sistemų. Šis veiksmas padeda užtikrinti, kad buvęs darbuotojas ar paslaugų teikėjas nebeturėtų prieigos prie jokių neskelbtinos informacijos šaltinių, jog sistema nebūtų pažeidžiama dėl nepageidaujamų prisijungimų.[126] Tai labai svarbus žingsnis siekiant užtikrinti organizacijos duomenų saugumą ir apsaugoti neskelbtiną informaciją nuo neteisėtos prieigos ir neteisėto sistemų bei

[122] Valstybinė duomenų apsaugos inspekcija, „Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams“, LRV, žiūrėta 2024 m. kovo 19 d. https://vdai.lrv.lt/uploads/vdai/documents/files/VDAI_saugumo_priemoniu_gaires-2020-06-18.pdf

[123] Agnė Vilkišienė, „Asmens duomenų saugumo pažeidimai Lietuvoje 2023 m. I pusmetį“, B1, žiūrėta 2024 m. kovo 20 d. https://www.b1.lt/wiki/asmens-duomenu-saugumo-pazeidimai-lietuvoje-2023-m-i-pusmeti-3789

[124] Valstybinė duomenų apsaugos inspekcija, asmens duomenų saugumo pažeidimai Lietuvoje 2023 m.“, *supra note*, 105: 9.

[125] *Ibid.*

[126] „Tiksinti bomba: įmonę paliekantis darbuotojas išsineša slaptažodžius, banko duomenis – apie virtualų saugumą nepagalvoja net pusė darbdavių“, Delfi, žiūrėta 2022 m. rugpjūčio 4 d. https://www.delfi.lt/darbas/patarimai/tiksinti-bomba-imone-paliekantis-darbuotojas-issinesa-slaptazodzius-banko-duomenis-apie-virtualu-sauguma-nepagalvoja-net-puse-darbdaviu-90885973

duomenų naudojimo. Kita prevencinė priemonė siekiant apsaugoti organizacijos duomenis – užtikrinti, kad *būtų pakeistas pagrindinis sistemos slaptažodis*.[127] Tai apima poreikį pakeisti pagrindinį slaptažodį, naudojamą pagrindinės sistemos paleidimui arba prieigai prie svarbių duomenų bazių, sistemų. Tai leidžia apsaugoti sistemą nuo nepageidaujamos prieigos ir galimų saugumo pažeidimų. Dar viena prevencinė priemonė yra *įdiegti prieigos kontrolę pagal organizacijos saugumo politiką, taikant „mažiausių teisių privilegijos" ir „būtina žinoti" principus*.[128] Ši priemonė reiškia, įgyvendinti technines priemones, kuriomis reguliuojamos ir saugomos darbuotojų, sistemų ir duomenų prieigos teisės organizacijos informacinėje infrastruktūroje. Šių priemonių tikslas – užtikrinti, kad kiekvienas darbuotojas, laikantis organizacijos nustatytų saugumo taisyklių ir politikos, turėtų prieigą tik prie jo darbui būtinų informacinių sistemų ir jų funkcijų. Tai apima technologijų ir procedūrų, tokių kaip vartotojo autentifikavimas, prieigos prie sistemų teisių valdymas, vartotojo prieigos stebėjimas, duomenų šifravimas ir kt., techninių primeonių naudojimą.[129] Šios priemonės padeda sumažinti netikėtų veiksmų, riziką kaip pvz., neteisėtos prieigos ar duomenų modifikavimo, riziką, taip prisidedant prie organizacijos informacijos saugumo ir sklandžių sistemų veikimo. Paskutinė šios kategorijos prevencijos priemonė yra *nenaudoti tų pačių slaptažodžių skirtingoms paskyroms, naudoti kelių faktorių autentifikavimą*.[130] Ši priemonė atspindi, jog organizacijos darbuotojai neturėtų naudoti tokių pat slaptažodžių skirtingoms paskyroms Tai reiškia, kad kiekvienai paskyrai turėtų būti priskirti unikalūs slaptažodžiai, kad būtu sumažinta tikimybė, jog pašalinis asmuo patekęs į vieną paskyrą, patektų į kitas. Taip pat kelių faktorių autentifikavimas yra apsaugos priemonė, kuri reikalauja ne tik slaptažodžio, bet ir papildomo patikrinimo, pavyzdžiui, patvirtinimo kodo, kuris padidinant organizacijos duomenų saugumą.[131] Aptarus šias siūlomas priemones pastebima, kad organizacijos duomenų saugumo stiprinimas yra būtinas norint apsisaugoti nuo kibernetinių grėsmių.

Asmens duomenų apsaugos priežiūros institucija nurodo, jog analizuojant padaromus pažeidimus yra nustatomi *pažeidimai susiję su netinkamais serverio nustatymais ir taisyklėmis*.[132] Pažeidimai, susiję su netinkamais serverio nustatymais ir taisyklėmis, išryškino kelias svarbias problemas. Pirma, paveiktuose serveriuose saugomi pertekliniai asmens duomenys, kurie neturėtų būti saugomi ir turėtų būti ištrinti iš išoriškai paveiktų serverių. Ši situacija kelia pavojų asmens

[127] Valstybinė duomenų apsaugos inspekcija, asmens duomenų saugumo pažeidimai Lietuvoje 2023 m.", *op. cit.*
[128] Valstybinė duomenų apsaugos inspekcija, asmens duomenų saugumo pažeidimai Lietuvoje 2023 m.", *supra note*, 105: 9.
[129] „Nacionalinis kibernetinio saugumo centras, kibernetinis saugumas ir verslas. Ką turėtų žinoti kiekvienas įmonės vadovas 2020", *supra note,* 120: 36.
[130] Valstybinė duomenų apsaugos inspekcija, asmens duomenų saugumo pažeidimai Lietuvoje 2023 m.", *op.cit.,* 9.
[131] „Nacionalinis kibernetinio saugumo centras, kibernetinis saugumas ir verslas. Ką turėtų žinoti kiekvienas įmonės vadovas 2020", *op. cit.,* 30.
[132] Valstybinė duomenų apsaugos inspekcija, asmens duomenų saugumo pažeidimai Lietuvoje 2023 m.", *op.cit.,* 9.

duomenų privatumui ir gali padidinti riziką dėl duomenų nutekėjimo ar neteisėtos prieigos prie šių duomenų.[133] Antra, specialioms duomenų kategorijoms priklausantys asmens duomenys saugomi nešifruoti. Dėl to jie lengvai pasiekiami pašaliniams asmenims, todėl kyla duomenų pažeidimo arba neteisėtos prieigos rizika.[134] Trečia, pažeidimo metu buvo pastebėtas gamyklinių nustatymų naudojimas serveriuose.[135] Šios nuostatos dažnai yra gamykliškai nustaytos ir yra standartinės, todėl gali neatitikti organizacijos saugumo standarto. Dėl to sistemos tampa pažeidžiamos kibernetiniams įsilaužėliams ir padidėja duomenų pažeidimų ir kitų saugumo incidentų rizika. Šios problemos rodo, kad reikia tinkamai įvertinti ir nustatyti serverio bei duomenų bazių nustatymus, kad būtų užtikrintas duomenų saugumas ir būtų apsaugoti organizacijos saugomi duomenys. Šiems pažeidimams VDAI numato prevencines priemones. Pirmoji prevencinė priemonė yra *tvarkyti asmens duomenis pagal nustatytus tikslus*.[136] Šia prieomone rekomenduojama aiškiai apibrėžti, kam ir kokiu tikslu yra renkami ir tvarkomi asmens duomenys. Tai padeda išvengti netinkamo duomenų naudojimo ar perdavimo bei užtikrina, kad duomenys būtų naudojami tik tiems tikslams, kuriems jie buvo gauti ir tvarkomi, gaunat duomenų subjekto leidimą. Sekanti priemonė yra *šifruoti specialių kategorijų asmens duomenis*.[137] Ši priemonė apima šifravimo technologijos naudojimą, kad būtų išvengta nepageidaujamos prieigos arba neteisėto duomenų naudojimo. Specialios asmens duomenų kategorijos apima neskelbtiną informaciją, tokią kaip sveikatos būklė, rasė, religija, politika ar seksualinė orientacija. Dėl šifravimo duomenys tampa neįskaitomi arba suprantami be specialių raktų, reikalingų jiems atkurti.[138] Tai padeda užtikrinti duomenis, kad duomenis būtų, sunku ar net neįmanoma naudoti be tinkamo raktų rinkinio, kuriuos turi organzizacija. Tai suteikia papildomą duomenų apsaugą, ir prisideda prie asmens privatumo ir duomenų saugumo. Paskutinė šio kategorijos prevencinė priemonė yra *vengti gamyklinių serverių nustatymų*.[139] Ši priemonė rekomenduoja organizacijoms vengti naudoti numatytuosius serverio, programinės įrangos konfigūracijos nustatymus.[140] Vietoj to turėtų būti naudojamos patikrintos ir saugios bei tinkamai nustatytos programinės įrangos parinktys, tam kad organizacija atitiktų konkrečius saugos reikalavimus ir būtų užtikrintas sklandus bei saugus organizacijos programų veikimas. Tai padeda sumažinti pažeidžiamumų riziką ir užtikrina tinkamą sistemos apsaugą nuo galimų kibernetinių

[133] „Valstybinė duomenų apsaugos inspekcija, asmens duomenų saugumo pažeidimai Lietuvoje 2023 m.“, *supra note*, 105: 9.
[134] *Ibid.*
[135] *Ibid.*
[136] *Ibid.*
[137] *Ibid.*
[138] Nacionalinis kibernetinio saugumo centras, kibernetinis saugumas ir verslas. Ką turėtų žinoti kiekvienas įmonės vadovas 2020“, *supra note*, 120: 47.
[139] „Valstybinė duomenų apsaugos inspekcija, asmens duomenų saugumo pažeidimai Lietuvoje 2023 m.“, *op. cit.*
[140] Nacionalinis kibernetinio saugumo centras, kibernetinis saugumas ir verslas. Ką turėtų žinoti kiekvienas įmonės vadovas 2020“, *op. cit.,* 41.

grėsmių. Šios VDAI prevencinės priemonės turėtų padėti sumažinti duomenų praradimo riziką ir užtikrinti duomenų saugumą bei privatumą.

Kita duomenų saugumo valdymo spragų kategorija yra *pažeidimai susiję su operacinių sistemų ar antivirusinių programų pažeidžiamumais*.[141] Pažeidimai, susiję su operacinių sistemų ar antivirusinių programų pažeidžiamumas, kelia rimtą grėsmę visapusiškai organizacijų saugumui. VDAI nustatė, kad, naudojamos nebepalaikomos operacinės sistemos. Organizacijos, kurios naudoja operacines sistemas, kurias gamintojai nebepalaiko arba nesuteikia saugumo atnaujinimų, yra lengvai pažeidžiamos. Antra, operacinių sistemų saugos atnaujinimai yra atliekami nereguliariai. Nereguliarūs saugumo atnaujinimai palieka sistemose spragas, kurios kelia pavojų organizacijos duomenų saugumui. Trečia, antivirusinės programų versijos yra neatnaujinamos arba jos yra išjungiamos. Nepakankamai atnaujintos arba išjungtos antivirusinės programos padidina pavojų organizacijai susidurti su pašalinėmis ir kenksmingomis programomis. Norint užkirsti kelią šios kategorijos pažeidims susijusiems būtent su operacinių sistemų ar antivirusinių programų pažeidžiamumais, VDAI pataria įgyvendinti pagrindines šias prevencijos priemones. Visų pirma organizacijoms *patariama įdiegti pažangią antivirusinę programinę įrangą.*[142] Pažangi antivirusinė programa turi daugau apsaugos funkcijų nei įprastos programos. Todėl turinti geresnes progrmos funkcijas yra sudaromos tinkamos sąlygos kovoti su įvairiomis kibernetinėmis grėsmėmis, tokiomis kaip virusai, kenkėjiškos programos, šnipinėjimo programos ir kt. ir jas saugiai bei tinkamai įveikti.[143] Tai apima tokias funkcijas kaip suplanuotas duomenų nuskaitymas, kenkėjiškų programų aptikimas ir jų blokavimas bei apsauga nuo naujų grėsmių. Be to, šios programos dažnai turi automatinio atnaujinimo mechanizmus, kurios leidžia joms visada išlaikyti tinkamą organizacijos apsaugos lygį. Sekanti prevencinė priemonė yra *reguliariai daryti pilnas ir dalines atsargines kopijas.*[144] Ši priemonė apima reguliarias duomenų atsargines kopijas, įskaitant visas ir dalines tam tikrų duomenų atsargines kopijas. Reguliarios atsarginės kopijos padeda organizacijoms apsisaugoti nuo duomenų praradimo, duomenų sugadinimo ar kitų netikėtų įvykių, pvz., įsilaužėlių ar kenkėjiškų programų atakų.[145] Tai svarbi prevencinė priemonė, užtikrinanti, kad organizacijos galėtų greitai atkurti duomenis ir tęsti veiklą incidento ar duomenų praradimo atveju. Visi šie įrankiai suteikia geresnę apsaugą nuo kibernetinių grėsmių ir padeda atkurti duomenis po duomenų pažeidimo.

---

[141] „Valstybinė duomenų apsaugos inspekcija, asmens duomenų saugumo pažeidimai Lietuvoje 2023 m.“, op. cit.
[142] „Valstybinė duomenų apsaugos inspekcija, asmens duomenų saugumo pažeidimai Lietuvoje 2023 m.“, *supra note*, 105: 9.
[143] „Nacionalinis kibernetinio saugumo centras, kibernetinis saugumas ir verslas. Ką turėtų žinoti kiekvienas įmonės vadovas 2020“, *supra note*, 120: 32.
[144] „Valstybinė duomenų apsaugos inspekcija, asmens duomenų saugumo pažeidimai Lietuvoje 2023 m.“, *op. cit.*
[145] „Atsarginės duomenų kopijos: kokių taisyklių reikėtų laikytis?“, 15min, 2022 m. balandžio 15 d., https://www.15min.lt/verslas/naujiena/mokslas-it/atsargines-duomenu-kopijos-kokiu-taisykliu-reiketu-laikytis-1290-1667486

Paskutinė kategorija duomenų saugos valdymo spragų yra *pažeidimai susiję su tinklo ir komunikacijos sauga.*[146] Pažeidimai, susiję su tinklo ir komunikacijos sauga, apima kelias problemas. Pirma, naudojami nešifruoti komunikacijos kanalai, kurie kelia riziką, jog duomenys gali būti peržiūrimi arba paimti. Antra, IT sistemų pasiekiamumas nėra apribotas tik tam tikriems vartotojams, kas gali lemti nepageidaujamą prieigą prie jautrios informacijos. Trečia, informacinės sistemos tinklas nėra atskirtas nuo kitų duomenų valdytojų tinklų, kuri tai palieka ją pažeidžiamą kibernetinėms grėsmėms iš išorės. Šie pažeidimai svarsto būtinybę stiprinti tinklo ir komunikacijos saugą, naudojant šifravimą, ribojant prieigą ir skaidant tinklus, siekiant užtikrinti duomenų saugumą ir apsaugoti sistemą nuo nepageidaujamo įsilaužimo. Kad apsisaugoti asmens duomenis nuo kylančio pavojaus VADI rekomenduoja prevencijos priemones kuriomis *apribojama išorinio prisijungimo galimybes* pasitelkiant specifinius interneto prievadus. Taip pat viena iš priemonių yra *leisti prie interneto tinklo prisijungti tik žinomų IP adresų programinę įrangą arba naudoti virtualaus privataus tinklo technologijas.*[147] Ši priemonė padeda apsaugoti organizacijų naudojamą programinę įrangą nuo nepageidaujamų prisijungimų, taip užtikrinant, kad prisijungimai būtų tik iš patikimų ir nustatytų įrenginių.[148] Paskutinė VDAI rekomenduojama prevencinė priemonė yra *tinkamai sukonfigūruoti išorinėje komunikacijoje dalyvaujantys serveriai.*[149] Ši priemonė apima programinės įrangos saugos parametrų nustatymą ir reguliarų jos atnaujinimą, siekiant apsisaugoti nuo galimų kibernetinių grėsmių.[150] Visos šios aprašytos priemonės skirtos apsaugoti organizaciją nuo pažeidimų, susijusių su tinklų ir ryšių apsauga, kurie būtini asmens duomenų saugumui užtikrinti ir sistemų apsaugai nuo nepageidaujamų įsilaužėlių.

Šiame poskyryje aptarti pažeidimai ir rekomendacijos yra svarbios siekiant užtikrinti asmens duomenų apsaugą ir tvarkymą, mažinant kibernetinių incidentų riziką. Pažeidimai tokiose srityse kaip darbuotojų informavimas apie kibernetinį saugumą, prieigos kontrolės trūkumai ir netinkami serverio nustatymai yra svarbūs kibernetinio saugumo iššūkiai, galintys sukelti duomenų pažeidimus ir net duomenų praradimą.

Analizuojant VDAI asmens duomenų saugumo pažeidimą dėl paveiktų subjektų skaičiaus kaip anksčiau buvo minėta, jog 2023 metais 49 proc. Duomenų subjektų buvo paveikti dėl kibernetinių incidentų, o 51 proc. visų paveiktų duomenų subjektų buvo paveikti dėl kitų incidentų iš kurių 72

[146] „Valstybinė duomenų apsaugos inspekcija, asmens duomenų saugumo pažeidimai Lietuvoje 2023 m.“, *op. cit.*
[147] „Valstybinė duomenų apsaugos inspekcija, asmens duomenų saugumo pažeidimai Lietuvoje 2023 m.“, *supra note*, 105: 9.
[148] „Valstybinė duomenų apsaugos inspekcija, 2022 m. I pusmečio pranešimų apie asmens duomenų saugumo pažeidimus apžvalga“, LRV, žiūrėta 2024 m. kovo 28 d. https://vdai.lrv.lt/lt/naujienos/2022-m-i-pusmecio-pranesimu-apie-asmens-duomenu-saugumo-pazeidimus-apzvalga/
[149] „Valstybinė duomenų apsaugos inspekcija, asmens duomenų saugumo pažeidimai Lietuvoje 2023 m.“, *op. cit.*
[150] „Nacionalinis kibernetinio saugumo centras, kibernetinis saugumas ir verslas. Ką turėtų žinoti kiekvienas įmonės vadovas 2020“, *supra note*, 120:41.

proc. buvo įvykę dėl žmogiškosios klaidos. ADSP dėl žmogiškosios klaidos daugėja nes statistines duomenimis 2022 metais tokių incidentų buvo 60 proc. Žmogaus klaidos yra viena iš pagrindinių kibernetinių incidentų priežasčių, dėl kurių gali būti pažeisti duomenys ar net prarasti saugomi duomenys.[151] Darbuotojų mokymas yra pagrindinė priemonė siekiant pagerinti jūsų organizacijos duomenų saugojimo lygį. Organizacijos gali padidinti darbuotojų kibernetinį sąmoningumą apmokydamos duomenų saugumo specialistus, kurie sumažintų kibernetinių incidentų tikimybę. Taip pat darbuotojų mokymai turėtų apimti ne tik technines priemones, bet ir organizacijos informacinių technologijų specialistams rengti simuliacines situacijas, kurios padėtų darbuotojams suprasti, identifikuoti ir išvengti duomenų praradimo. Taip pat simuliacinės situacijos padėtų susidaryti esamą vaizdą apie darbuotojų kibernetinį raštingumą ir sąmoningumą. Svarbu užtikrinti, kad darbuotojai supranta ne tik, ką daryti, bet ir kodėl tai svarbu ir kokie gali būti padariniai, jei nebuvo laikomasi saugumo taisyklių. Be to, įmonės gali taikyti technines priemones, kad sumažintų žmogiškųjų klaidų įtaką, pavyzdžiui, automatinį duomenų konfidencialumo lygio nustatymą ar ribojimus, kurie neleistų darbuotojams atlikti potencialiai pavojingų veiksmų. Tačiau net ir turint tokių priemonių, svarbu, kad darbuotojai būtų tinkamai informuoti ir apmokyti, kad jie galėtų suprasti, kodėl saugumo priemonės yra būtinos ir kaip jų vaidmuo prisideda prie organizacijos bendro saugumo.

Apibendrinus galima teigti, jog analizuojant asmens duomenų saugos pažeidimų tendencijas galima atskleisti sisteminės duomenų apsaugos trūkumus bei rizikos veiksnius organizacijų veikloje. Atlikus analizę galima identifikuoti pagrindines asmens duomenų apsaugos kontrolės įgyvendinimo problemas. 1. Iš analizės galima pastebėti, jog organizacijos pasirenka neteisingas technines priemones konfidencialumo užtikrinimui, tai rodo, kad organizacijos nesilaiko tinkamų techninių priemonių, kad užtikrintų duomenų konfidencialumą, kyla rizika dėl duomenų nutekėjimo ir neteisėtos prieigos. 2. Dėl darbuotojų nepakankamos kvalifikacijos neteisingi arba neatsakingi veiksmai gali lemti duomenų pažeidimus, todėl svarbu teikti nuolatinį kibernetinio saugumo mokymą ir padidinti darbuotojų sąmoningumą. 3. Nepakankamas kibernetinių incidentų atpažinimas ir prevencija, rodo kad organizacija turėtų stiprinti kibernetinį saugumą, imdamasi prevencinių priemonių, pvz., elektroninio pašto filtravimo, kibernetinių atakų simuliacijų ir išsamų veiklos tęstinumo planą. 4. Organizacija netinkamai nustato serverio nustatymus ir numato taisykles, todėl dėl netinkamų nustatymų gali kilti pavojus asmens duomenų apsaugai, todėl organizacija turi pasirūpinti, jog serverio nustatymai būtų optimizuoti, kad būtų užtikrintas tinkamas duomenų saugumas ir duomenys būtų apsaugoti nuo neleistinos prieigos.

[151] „Valstybinė duomenų apsaugos inspekcija, asmens duomenų saugumo pažeidimai Lietuvoje 2023 m.“, *op. cit*., 5.

Šiame skyriuje yra išskirtos pagrindinės organizacijos problemos ir rizikos veiksniai kurie rodo, kad organizacijos turi daugiau dėmesio skirti kibernetinio saugumo įvertinimui, tobulinimui bei pasirinkti tinkamą kibernetinio saugumo strategiją bei efektyvias priemones, kurios padėtų tinkamai ir veiksmingai įgyvendinti asmens duomenų apsaugos. Tai apima tokias priemones kaip: tinkamų techninių priemonių parinkimą ir jų tinkamą konfigūravimą, reguliarų ir sistemingą darbuotojų kvalifikacijos kėlimą kibernetinio saugumo sferoje, taip pat efektyvias kibernetinio saugumo priemones ir tinkamą serverių veikimo nustatymą. Jei organizacijos nesiima prevencinių priemonių, asmens duomenų kontrolės įgyvendinimas gali būti neefektyvus ir organizacijai gali kilti kibernetinio incidento pavojus.

3. TEISMŲ PRAKTIKOS ANALIZĖ DĖL ASMENS DUOMENŲ PAŽEIDIMŲ

Šiame skyriuje bus analizuojama teismų praktika, susijusi su asmens duomenų praradimu ir asmens duomenų pažeidimais. Analizuojant šio pobūdžio bylas, pagrindinis tikslas yra išsiaiškinti kaip yra parandami asmens duomenys. Taip pat šios analizes metu bus išgryninamos pagrindinės problemos, dėl kurių organizacijos praranda surinktus duomenis ir analizuojamos pagrindinės problemos dėl kurių įvyksta asmens duomenų tvarkymo ir saugojimo pažeidimai. Taip pat bus analizuojama kokia yra atsakomybė juridiniams asmenims už duomenų pažeidimų.

3.1. Organizacijų problemos įgyvendinant asmens duomenų apsaugą

Dėl sparčios technologijų pažangos šiame, skaitmeniniame amžiuje kyla pavojus asmens duomenų praradimui (nutekėjimui). Po asmens duomenų nutekėjimo kyla pavojus asmeninei informacijai, kurią gali pasisavinti kiti asmenys. Dėl organizacijos saugomų ir tavrkomų asmens duomenų praradimo, duomenų subjektas gali patirti didelį pavojų patirti fizinę ar (ir) materialią žalą. Duomenų saugumas yra ne tik žinojimas, kokius duomenis organizacija tvarko, tačiau ir turi suprasti susijusią riziką dėl asmens duomenų praradimo, todėl organizacijaturi imtis atitinkamų saugos priemonių siekiant duomenis apsaugoti.[152] BDAR įgyvendinimas valstybėse nerėse privertė organizacijas iš naujo įvertinti savo asmens duomenų apsaugos lygį, ir taip pat įvertinti, kad jos atitiktų BDRA keliamus reikalavimus ir taip pat organizacija turi įvetinti ar ji yra pajėgi apsaugoti duomenis tinkamai. [153] Kibernetinio saugumo specialistai atlieka svarbų vaidmenį aiškinantis duomenų nutekėjimo priežastis bei duomenų nutekėjimo pasekmes ir imantis prevencinių priemonių, tam kad ateityje būtų išvengta duomenų nutekėjimo. [154] Neteisėta prieiga prie asmens duomenų pabrėžia informacinių sistemų pažeidžiamumą ir būtinybę laikytis griežtų saugumo protokolų, kad būtų išvengta tokio tipo duomenų pažeidimų. Reaguodama į tokius pažeidimus, VDAI pradeda tyrimus, siekdama patraukti atsakomybėn asmenis, atsakingus už didelio masto privačių duomenų nutekėjimą.

Asmens duomenų vagystė ir nutekinimas yra glaudžiai susiję, tačiau abu reiškiniai yra skirtingi. Asmens duomenų vagystė yra tyčinis veiksmas, kurio metu be duomenų subjekto leidimo yra

[152] „Kas yra duomenų sauga“, Micrisoft, žiūrėta 2024 m. balandžio 1 d. https://www.microsoft.com/lt-lt/security/business/security-101/what-is-data-security

[153] „Duomenų nutekėjimas – tik laiko klasuimas“, Verslo žinios, 2019 m. balandžio 2 d., https://www.vz.lt/verslo-sprendimai/2019/04/02/duomenu-nutekejimas--tik-laiko-klausimas

[154] „Dėl asmens duomenų nutekėjimo per gruodžio 8 d. įvykdytą kibernetinę ataką prieš KTU“, KTU, žiūrėta 2024 m. balandžio 2 d. https://ktu.edu/news/del-asmens-duomenu-nutekejimo-per-gruodzio-8-d-ivykdyta-kibernetine-ataka-pries-ktu/

pavagiami duomenys siekiant finansinės naudos ar naudojami tolimesniam sukčiavimui.[155] Asmens duomenų nutekinimas yra netyčinis duomenų valdytojo veiksmas bei netinkamas saugumo priemonių pasirinkimas, todėl dėl šių priežasčių yra parandami asmens duomenys.[156] Šie du reiškiniai yra susiję tuo, jog abu reiškiniai gali sukelti finansinius nuostolius ir kitus padarinius asmens duomenų subjektui. Asmens duomenų pažeidimai tap pat gali turėti neigemų pasėkmių duomenų valdytojams ir asmens duomenų tvarkytojams, nes jie yra atsakingi už asmens duomenų tvarkymą bei saugojimą. Įvykus pažeidimui, svarbu, kad organizacijos laikytųsi BDAR reikalavimų ir nedelsdamos praneštų VDAI apie pažeidimą. BDAR įpareigoja VDAI apie bet kokį asmens duomenų pažeidimą pranešti institucijai, siekiant užtikrinti skaidrumą ir atskaitomybę tvarkant tokius incidentus.

Lietuvoje yra įvykusi ne viena plačiai nuskambėjusi asmens duomenų vagysčių. 2021 m. vasario mėnesį iš įmonės „CityBee“ buvo pavogti 110 tūkstančių asmens duomenų, tokių kaip ardai ir pavardės, asmens kodai, telefonų numeriai, elektroninio pašto adresai, gyvenamosios vietos adresai, mokėjimo kortelės detalės, vairuotojų pažymėjimo numeriai bei užšifruoti slaptažodžiai. [157] Pavogti duomenys buvo 3 metų senumo ir paskelbti viešai internete, tačiau duomenų nespėjus panaudoti, šie buvo pašalinti. Įmonė viešai nepateikė informacijos dėl ko įvyko incidentas, tačiau kibernetinio saugumo ekspertai, teigia, jog duomenų vagystė įvyko, nes įmonė netinkamai saugojo atsargines duomenų kopijas arba pakeitus į duomenų saugojimo serverį (pavyzdžiui, atnaujinant informacinę sistemą), duomenys iš nebenaudojamo teikėjo tinkamai ištrinami.[158] Dėl šio įvykio VDAI savo iniciatyva ėmėsi tyrimo ir įmonei buvo paskirta 110 tūstančių eurų bauda ir buvo pripažinta, kad duomenų tvarkytojas pažeidė BDAR 32 str. ir neužtikrino duomenų saugumo. [159] Šis įvykis parodė, jog įmonė netinkamai saugojo duomenis ir taip pažeidė BDAR. Už šiuos pažeidimus įmonei buvo paskirta 110 tūks. eur. bauda. Kitas žymus įvykis Lietuvoje, 2017 metų asmenys „įsilaužė“ į „grožio chirurgijos“ klinikos saugomų duomenų baze. Šio incidento metu, buvo pavogti klientų asmens duomenys ir nuotraukos prieš plastines operacijas ir po jų. Dėl šių duomenų asmenys pavogę duomenis reikalavo 500 tūkstančių eurų „bitcoin“ kriptovaliuta. Klinika teigė, jog buvo

[155] Darius Štitiis ir kt. „Tpatybės vagystė elektroninėje erdvėje: socilainai elektroninio verslo ir teisinio reguliavimo aspektai“, (Vilnius: Mykolo Romerio Universitetas, 2011) https://cris.mruni.eu/cris/bitstream/007/16821/1/9789955193753.pdf?sequence=1&isAllowed=y

[156] „Kas yra duomenų nutekinimas? Data leak ir Data breach skirtumai“, Vnpgidas, žiūrėta 2024 m. balandžio 1 d. https://www.vpngidas.lt/saugus-internetas/kibernetiniai-nusikaltimai/duomenu-nutekinimas-data-leak-data-breach/

[157] Adomas Rutkauskas, „Interviu su „CityBee“ klientų duomenis pavogusiu programišiumi: „Man gaila žmonių, bet kaltos yra įmonės“, Lrytas, žiūrėta 2024 m. balandžio 3 d. https://www.lrytas.lt/it/ismanyk/2021/02/17/news/interviu-su-citybee-klientu-duomenis-pavogusiu-programisiumi-man-gaila-zmoniu-bet-kaltos-yra-imones--18317291

[158] Patricija Kirilova, Kibernetinio saugumo ekspertai apie tai, kas ir kodėl atsitiko su „CityBee“: tiek slaptažodžių, tiek duomenų apsauga išties labai silpna”, LRT, 2021 m. vasario 17 d., https://www.lrt.lt/naujienos/mokslas-ir-it/11/1347303/kibernetinio-saugumo-ekspertai-apie-tai-kas-ir-kodel-atsitiko-su-citybee-tiek-slaptazodziu-tiek-duomenu-apsauga-isties-labai-silpna

[159] Rūta Balčiūnienė, „CityBee“ skirta 110.000 Eur bauda už BDAR pažeidimus”, Verslo žinios, žiūrėta 2021 m. lapkričio 30 d. . https://www.vz.lt/rinkodara/2021/11/30/citybee-skirta-110000-eur-bauda-uz-bdar-pazeidimus

pavogti 22 tūkstančių klientų duomenys. [160] VDAI atlikus tyrimą buvo nustatyta, kad į klinikos duomenų bazę buvo įsilaužta duomenų bazę buvo įsilaužta naudojant buvusio klinikos darbuotojo prisijungimo duomenis.[161] Dėl šio įvykio informacijos, kad įmonė būtų nubausta nėra, tačiau buvo sulaikyti asmenys neteisėtai prisijungę prie įmonės duomenų bazės ir iš ten pavogę klientų duomenis. Šie įvykiai parodo, jog duomenų vagystė yra aktuali tema ir šių įvykių metu paveikiami dideli kiekiai duomenų subjektų, todėl yra svarbu išanalizuoti priežastis dėl kurių įvyksta asmens duomenų vagystės ar yra paviešinami asmens duomenys.

LVAT nagrinėjo administracinę bylą Nr. eA-2483-822/2021, kurioje į teismą kreipėsi sodininkų bendrija „Žalgiris-2“ su skundu kuriame prašė panaikinti VDAI sprendimo dalį, kuria V. B. skundas dėl V. B. telefono numerio perdavimo savivaldybės „Vilniaus atliekų sistemos administratorius“.[162] Byloje nustatyta, kad gavo VDAI gavo V. B. skundą, kuriame buvo nurodyta, jog pareiškėjas telefonu kreipėsi į Vilniaus atliekų sistemos administratorių dėl bendrų konteinerių sodų bendrijoje. Atliekų sistemos administratorius V. B. telefono numerį perdavė bendrijos pirmininkei, o ši sužinojusi telefono numerį administratoriui atskleidė V. B. vardą, pavardę, unikalų numerį. Bendrijos pirmininkė susirinkimo metu paviešino, kad V. B. kreipėsi į atliekų sistemos administratorių, dėl bendrų bendrijos konteinerių.[163] VDAI nustatė, kad pagal LR ADTĮ 27 straipsnio 1 dalies 4 punktu, 29 straipsnio 1 dalies 2 punktu ir 4 dalimi, 31 straipsnio 1 dalies 1 ir 2 punktais, BDAR 5 straipsnio 1 dalies a punktu, 58 straipsnio 2 dalies b punktu, priėmė sprendimą kuriuo nusprendė, kad skundo dalį dėl susirinkimo metu atskleistų duomenų nutraukti, taip pat nutraukti V. B. skundo dalį dėl duomenų apie sklypo numerį, kurį atskleidė atliekų sistemos administratorių. Tačiau dėl administratoriaus paviešinto pareiškėjo numerio sodų bendrijos pirmininkei laikė pagrįstu ir bendrijai skyrė papeikimą. [164]Viso teismo proceso metu V. B. teigė, jog nedavė sutikimo viešinti jo duomenų. Teismas konstatavo, kad V. B. nedavė sutikimo bendrijai tvarkyti jo asmens duomenų. Dėl šių duomenų atkleidimo teismas nustatė, kad bendrijos pirmininkė pažeidė BDAR 5 str. 1 d. a p., nes V. B. duomenys buvo tvarkomi neteisėtai ir pirmininkė šioje byloje buvo duomenų valdytoja, todėl bendrijai duotas papeikimas dėl netinkamų asmens duomenų tvarkymo. Dėl atliekų administratoriaus veiksmų, teismas nurodė, kad atliekų sistemos administratorius nurodęs bendrijos

[160] Ingrida Stenulienė, “Baigta byla dėl duomenų vagystės iš „Grožio chirurgijos“ klinikos”, 15min, 2018 m. rugsėjo 17 d. https://www.15min.lt/naujiena/aktualu/nusikaltimaiirnelaimes/baigta-byla-del-duomenu-vagystes-is-grozio-chirurgijos-klinikos-59-1030942?utm_medium=copied
[161] „10 garsiausių asmens duomenų vagysčių Lietuvoje“, 15min, 2021 m. spalio 12 d. https://www.15min.lt/verslas/naujiena/mokslas-it/10-garsiausiu-asmens-duomenu-vagysciu-lietuvoje-1290-1579640?utm_medium=copied
[162] „Administracinė byla Nr. eA-2483-822/2021, Lietuvos vyriausissis administracinis teismas sprendimas“, Infolex, žiūrėta 2024 m. balandžio 4 d. https://www-infolex-lt.skaitykla.mruni.eu/tp/2049327#B_0
[163] *Ibid.*
[164] *Ibid.*

pirmininkei numerį taip pat padarė BDAR 5 str. 1 d. a p. pažeidimą.[165] Bendrijos pirmininkė yra vadovė, kuri turėtų turėti išsamesnes žinias apie asmens duomenų saugojimą. Šioje byloje atkleidžiama problema, jog dėl nepakankamo supratimo apie asmens duomenų saugojimą ir BDAR nuostatų dėl atskleidimo, kyla pavojus asmens duomenų saugumui ir tokių incidentų pasikartojimui ateityje.

Vilniaus apygardos administracinis teismas nagrinėjo administracinę bylą Nr. eI2-7048-1114/2022, kurioje A. Š. kreipėsi į teismą dėl Vilniaus rajono savivaldybės ir Valstybinės teritorijų planavimo ir statybos inspekcijos prie Aplinkos ministerijos (toliau – VTPSI) dėl asmens duomenų paviešinimo tokių kaip: vardas pavardė, gyvenamosios vietos adresas, telefono numeris, elektroninis paštas. A. Š. kreipėsi į Vilniaus rajono savivaldybę, dėl valdomo žemės sklypo paskirties pakeitimo.[166] Dėl šios paslaugos pareiškėja parašė prašymą, kuriame nurodė anksčiau savo asmens duomenis. Kiek vėliau A. Š. sužinojo, kad jos asmens duomenys yra paskelbti viešai ir visiems prieinami. „Google“ paieškos sistemoje įrašiusi savo inicialus, paieškos rezultatuose, svetainėje www.tpdris.lt buvo paskelbtas pareiškėjos prašymas su jos asmens duomenimis.[167] Pamačiusi pažeidimą pareiškėja VDAI pranešė apie pažeidimą ir parašė skundą. Savivaldybė susižinojusi apie incidentą dokumentą nuasmenino. VDAI atlikusi tyrimą nustatė, kad Savivaldybė į Lietuvos Respublikos teritorijų planavimo dokumentų rengimo ir teritorijų planavimo proceso valstybinės priežiūros informacinę sistemą (toliau – ir TPDRIS) įkėlė nenuasmenintą pranešėjos bylą su visais jos asmens duomenimis ir taip pažeidė BDAR 5 straipsnio 1 dalies f punktą ir asmens duomenys turėjo būti ištrinti. [168] Teismas iš gautų paaiškinimų nustatė kad savivaldybės vyriausioji specialistė dėl žmogiškosios klaidos į sistemą įkėlė nenuasmenintą bylą. Teismas konstatavo, kad savivaldybė nesiėmė visu būtinų priemonių, kad būtų išvengta tokio incidento, todėl savivaldybė pažeidė BDAR 5 str. 1 d. f p., taip pat buvo pažeistas BDAR 5 str. 1 d., atskaitomybės principas ir BDAR 24 str. 1 d. [169] Šioje byloje asmens duomenų pažeidimą lėmė tai, kad dėl darbuotojos nepakankamos kvalifikacijos buvo padarytas asmens duomenų pažeidimas ir atskleisti bei paviešinti asmens duomenys.

Vilniaus apygardos administracinis teismas nagrinėjo administracinę bylą Nr. Nr. I2-870-789/2021, kurioje į teismą su skundu kreipėsi J. J., kuris prašo panaikinti VDAI sprendimą. J.J. nurodė, kad raštu kreipėsi į VDA dėl viešosios įstaigos Respublikinės Kauno ligoninės, kurioje

[165] *Ibid.*
[166] „Administracinė byla Nr. eI2-7048-1114/2022, Vilniaus apygardos administracinis teismas sprendimas“, Infolex, žiūrėta 2024 m. balandžio 4 d. https://www-infolex-lt.skaitykla.mruni.eu/tp/2139919
[167] „Administracinė byla Nr. eI2-7048-1114/2022, Vilniaus apygardos administracinis teismas sprendimas“, *supra note,* 163.
[168] *Ibid.*
[169] *Ibid.*

pareiškėjo nuomone sūnaus epikrizėje buvo neteisėtai paviešinti duomenys apie pareiškėja bei jo šeimą.[170] Pradžioje pareiškėjas kreipėsi į VDAI ir išdėstė skundo esmę, tačiau VADI į minėtą ligoninę kreipėsi po 29 d. J.J. mano, kad VDAI vilkino nagrinėti pareiškėjo skundą. VDAI sprendimą priėmė tik po kiek daugiau nei po 4 mėnesių. Pareiškėjui VDAI išaiškino, jog skundas gali būti išnagrinėjamas per 4 mėnesius nuo skundo gavimo dienos, o esant sudėtingais atvejais pratęsiamas dar 2 mėnesiams. [171] Pareiškėjas nesulaukęs atsakymo iš VDAI su skundu kreipėsi į gydimo įstaigą ir nelaukiant VDAI išvadų uždrausti naudoti epikrizę ir įpareigoti apie tai pranešti suinteresuotiems asmenims. J. J. Nurodo, kad be jo sutikimo duomenys sūnaus epikrizėje buvo perduoti Generolo Jono Žemaičio Lietuvos karo akademijai. Pareiškėjas skundą išsiuntė paštu. Ligoninė atsakė pareiškėjui raštu, kad norint, jog skundas būtų nagrinėjamas skundo teikėjas su skundu turi pateikti asmens dokumentą arba dokumento kopiją [172] Teismas išnagrinėjęs pateiktus faktus byloje konstatuoja, jo nustatyta, kad Lietuvos kariuomenės dr. Jono Basanavičiaus karo medicinos tarnybos centro gydytojas psichiatras pareiškėjo sūnų siuntė detalesniam ištyrimui į kitą gydimo įstaigą. Teismas konstatavo, jog gydimo įstaiga prašydama skundo teikėjo asmens dokumento nieko nepažeidė. Taip pat teismas nustatė, kad pagal BDAR 6 straipsnį duomenų tvarkymas teisėta, kai duomenų subjektas duoda sutikimą, kad jo asmens duomenys būtų tvarkomi sutikime nurodytu būdų. Tačiau anamnezės tyrimo metodas yra remiantis šeimos ligos istorija, tačiau tai ir turi apimti tik šeimos ligos istoriją. Kiti duomenys yra pertekliniai, tokie kaip šeimyninė padėtis, gyvenamosios vietos adresas, darbovietė ir kt. [173] Šioje byloje pastebima problema dėl per ilgai užsitęsusio VDAI tyrimo, taip įžvelgiama problema, jog gydymo įstaiga duomenis apie šeimos narius nustatant ligos istoriją naudoja perteklinius duomenis.

Taip pat svarbu atlikti bylų analizę kurios yra susijusios su asmens duomenų pažeidimai. LVAT nagrinėjo administracinę bylą Nr. TA-458-821/2023, kurioje A. D. Alytaus administracijos pataisos namuose užpildė prašymą gauti savo asmeninius daiktus į patisos namų vidų, tačiau daiktų negavo ir šį sprendimą apskundė. Gavus atsakymą į skundą paaiškėjo, jog Kalėjimų departamento prie Lietuvos Respublikos teisingumo ministerijos negavo prašymo, todėl prašymas su A. D. duomenimis buvo prarastas. [174] Asmuo savo skundą motyvavo BDAR 5 str. 1 d. (asmens duomenys tvarkomi

[170] „Administracinė byla Nr. I2-870-789/2021, Vilniaus apygardos administracinis teismas sprendimas“, Infolex, žiūrėta 2024 m. balandžio 4 d. https://www-infolex-lt.skaitykla.mruni.eu/tp/2065401
[171] „Administracinė byla Nr. I2-870-789/2021, Vilniaus apygardos administracinis teismas sprendimas“, *supra note,* 167.
[172] *Ibid.*
[173] *Ibid.*
[174] „Administracinė byla Nr. TA-458-821/2023, Lietuvos vyriausiasis administracinis teismas nutartis“, Infolex, žiūrėta 2024 m. balandžio 4 d. https://www-infolex-lt.skaitykla.mruni.eu/tp/2166238#pa4

teisėtai ir sąžiningai). [175] A. D. teigia, jog patyrė 5000 eur. neturtinę žalą.[176] Šis atvejis yra susijęs su asmens duomenų pažeidimu, nes Kalėjimų departamento prie Lietuvos Respublikos teisingumo ministerijos, leido, jog asmens duomenys būtų A. D. duomenys. LVAT skundą atmetė, motyvuodamas, kad byloje nėra duomenų, kad asmeniui dėl duomenų praradimo būtų kilęs didelis pavojus, taip pat byloje nėra duomenų, kad A. D. būtų patyręs didelius emocinius išgyvenimus. Pirmosios instancijos teismas nustatė, kad Alytaus pataisos namai pažeidė BDAR 4 str. 12 p., tačiau reikalavimą dėl neturtinės žalos atlyginimo atmetė, nes, buvo nustatyta, jog A. D. nepatyrė žalos.[177] LVAT atmetė A.D. apeliacinį skundą, nes byloje nebuvo nustatyta, jog šis įvykis būtų A.D. sukėlęs stiprius emocinius išgyvenimus, todėl tai neatitiko Lietuvos Respublikos civilinio kodekso 6.250 str. 1 d. [178] Šioje byloje pastebima, kad asmens duomenų pažeidimas įvyko dėl Alytaus pataisos namų darbuotojų sąmoningumo iš atsakomybės bei aplaidumo tvarkant gautus prašymus. Šis byla atskleidžia, jog organizacija negeba užtikrinti tinkamo asmens duomenų tvarkymo, o tinkamas duomenų tvarkymas yra pagrindinis duomenų apsaugos elementas.

Regionų administracinis teismas nagrinėjo administracinę bylą Nr. eI2-588-816/2024, kurioje pareiškėjas Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos, skundu kreipėsi į teismą ir prašo panaikinti VDAI priimtą sprendimą, jog Nacionalinis visuomenės sveikatos centras pažeidė BDAR 5, 13, 24, 32, 35 ir 58 straipsnio 2 dalies f punkto reikalavimus. Sveikatos centrui paskirta 12 tūkstančių eurų bauda.[179] Covid-19 pandemijos metu buvo paskelbta ekstremali situacija dėl viruso plitimo ir Lietuvos respublikos sveikatos apsaugos ministerija pavedė Nacionalinės sveikatos centro direktoriui vykdyti programėlės „Karantinas“ įsigijimą, su programėle turėjo būti tvarkomi asmens duomenys. Nacionalinis visuomenės sveikatos centras kreipėsi į įmone UAB „IT sprendimai sėkmei“ ir kartu kūrė minėtą programėlę. Sukūrus programėlę Nacionalinis visuomenės sveikatos centras organizavo programėlės testavimą, ir ji buvo atsakinga už asmens duomenų tvarkymą, kaip viena iš programos valdytojų. Sveikatos centras gavęs leidimą iš VDAI atliko programėlės bandymą. Tačiau bandymo rezultatų nepateikė VDAI ir sveikatos centras naudodamas programą pažeidė asmens duomenų apsaugos reikalavimus, nes programos tvarkymas neatitiko BDAR reikalavimų. [180]Teismas konstatavo kad programėlėje buvo renkami tokie duomenys kaip: „ID numeris, koordinatės platumos ir ilgumos, šalis, miestas, savivaldybė, pašto kodas, gatvės pavadinimas, namo numeris, vardas, pavardė, asmens kodas, telefono numeris, adresas, 2-asis

[175] BDAR
[176] „Administracinė byla Nr. I1-9212-422/2022, Regionų apygardos administracinis teismas sprendimas“, Infolex, žiūrėta 2024 m. balandžio 6 d. https://www-infolex-lt.skaitykla.mruni.eu/tp/2167137#pa4
[177] *Ibid.*
[178] „Administracinė byla Nr. TA-458-821/2023, Lietuvos vyriausiasis administracinis teismas nutartis“, *op. cit.*
[179] „Administracinė byla Nr. eI2-588-816/2024, Regiaonų administracinis teismas sprendimas“, Infolex, žiūrėta 2024 m. balandžio 6 d. https://www-infolex-lt.skaitykla.mruni.eu/tp/2239974
[180] „Administracinė byla Nr. eI2-588-816/2024, Regiaonų administracinis teismas sprendimas“, *Supra note,* 164.

adresas, ar vieta deklaruota Lietuvoje, ar privalo asmuo izoliuotis, ar pasižymėjo, ar nuotrauka reikalinga, universalus unikalus ID, vartotojo ID, kada sutikimas priimtas, kada sukurtas, kada modifikuotas, kada pasižymėjo, kada nuotrauka reikalaujama, iki kada nuotrauka reikalinga ir kada paskutinį kartą pasižymėjo.“[181] VDAI atlikus vertinimą buvo nustatyta, kad Nacionalinis visuomenės sveikatos centras BDAR 5, 13, 24, 32, 35 ir 58 straipsnio 2 dalies f punkto reikalavimus, kuriais pripažino, jog sveikatos centras duomenis rinko bei tvarkė neatitinkant BDAR reikalavimų. Teismui išnagrinėjus visas bylos aplinkybes pripažino, jog VDAI teisingai atliko vertinimą ir nustatė duomenų apsaugos pažeidimus.[182] Iš šios bylos analizės galima pastebėti, jog viena iš asmens duomenų saugumo problemų yra tai, jog programos veikimas nebuvo suderintas su BDRA nuostatomis, kas rodo, jog buvo pažeidžiamos asmens duomenų saugumas.

Atlikus bylų analizę, galima išskirti kelias pagrindines problemas, kurios įtakoja asmens duomenų pažeidimus. 1. Daugelyje bylų pastebima, jog asmens duomenų pažeidimai įvyksta dėl žmogiškųjų klaidų, kurias lemia organizacijų darbuotojų sąmoningumo ir kvalifikacijos trūkumas. 2. Teismų praktika atskleidžia, jog organizacijos nepasirenka tinkamos duomenų apsaugos, ko pasekoje įvyksta duomenų pažeidimai. 3. Analizė atskleidžia, jog organizacijos vėluoja, vengia pranešti priežiūros institucijai apie duomenų pažeidimus. 4. Analizės metu nustatyta, jog nacionaliniai teisės aktai nėra suderinti su tarptautinėje teisėje įvirtintais teisės aktais. 5. Organizacijos pasirenka netinkamas duomenų apsaugos priemones, kurios neužtikrina asmens duomenų saugumo. 6. Nepakankama VDAI kontrolė ir priežiūra gali lemti aplaidumą tvarkant asmens duomenis.

Šios problemos parodo, kad asmens duomenų apsauga yra sudėtingas procesas, kuris reikalauja daug resursų, reikalaujančios daug dėmesio ir atidumo, pradedant nuo organizacijų, baigiant pačiomis priežiūros institucijomis, kurios turi vykdyti asmens duomenų kontrolę ir atlikti patikrinimus siekiant apsaugoti duomenis. Tačiau viskas priklauso ne vien tik nuo priežiūros institucijos tačiau ir nuo pačios organizacijos ir jos darbuotojų sąmoningumo bei kibernetinio raštingumo. Duomenų apsauga turi būti organizacijų prioritetas norint užkirsti kelią duomenų paradimui ir išvengti potencialių pavojų.

3.2. Asmens duomenų praradimo atsakomybė juridiniams asmenims

Išanalizavus dėl kokių priežasčių įvyksta asmens duomenų pažeidimai svarbu aptarti, kokios priemonės yra naudojamos siekiant atgrasyti įmones nuo netinkamo asmens duomenų tvarkymo ir

[181] *Ibid.*
[182] „Administracinė byla Nr. eI2-588-816/2024, Regiaonų administracinis teismas sprendimas“, *Supra note,* 164.

BDAR pažeidimų. LVAT nagrinėjo administracinę bylą Nr. A-222-261/2022, kurioje į teismą skundu kreipėsi Vilniaus lopšelis-darželis „Gudrutis“ ir prašo panaikinti VDAI sprendimą.[183] VDAI atliko planinį patikrinimą minėtame darželyje ir VDAI nustatė, jog ugdymo įstaiga be visų duomenų papildomai renka duomenis apie tėvų darbovietę, faktus, kada vaikas buvo ir lankėsi gydymo įstaigoje, rinkdami tokius duomenis pažeidė tikslo apribojimo ir duomenų kiekio mažinimo principus, kurie įtvirtinti ir apibrėžti BDAR. Ir priėmė sprendimą, kuriuo ugdymo įstaiga turėtų nutraukti tokių duomenų rinkimą ir po papildomo patikrinimo jei bus nustatytas pakartotinis pažeidimas ikimokyklinės įstaigos vadovui pradės administracinio nusižengimo teiseną.[184] Ugdymo įstaiga nurodė, jog duomenis apie darželio nelankymą renka tam, kad apskaičiuotų mokėtino mokesčio už ugdymo įstaigą dydį. Lopšelis-darželis „Gudrutis“ tokius duomenis renka motyvuodama tuo, kad Vilniaus miesto savivaldybės tarybos aprašu, tokius duomenis turi rinkti.[185] Bylos nagrinėjime dalyvavo ir trečioji suinteresuota šalis t.y. Vilniaus miesto savivaldybė, kuri nurodė, jog aprašas nurodantis rinkti duomenis apie vaikų nelankymą ir jų priežastį yra privalomas ir galioja visoms mieste esančioms ikimokyklinėms įstaigoms. Kitu atveju, jei lopšelio-darželio „Gudrutis“, vadovas nevykdys savivaldybės priimto aprašo nuostatų, jis pažeis minėtą Vilniaus savivaldybės aprašą. LVAT konstatavo, kad *„asmens duomenų tvarkymas laikomas teisėtu tik tuo atveju, jeigu atitinka BDAR 5 ir 6 straipsnių nuostatas. BDAR 5 straipsnio 1 dalies b punkte nustatyta, kad duomenys renkami nustatytais, aiškiai apibrėžtais bei teisėtais tikslais ir toliau netvarkomi su tais tikslais nesuderinamu būdu (tikslo apribojimo principas); c punkte – kad asmens duomenys turi būti adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie tvarkomi (duomenų kiekio mažinimo principas). Pagal BDAR 6 straipsnio 1 dalį asmens duomenų tvarkymas yra teisėtas tik tuo atveju, jeigu taikoma bent viena iš šio straipsnio 1 dalyje nustatytų sąlygų. BDAR 5 straipsnio 2 dalyje įtvirtinta, jog duomenų valdytojas yra atsakingas už tai, kad būtų laikomasi šio straipsnio 1 dalies, ir turi sugebėti įrodyti, kad jos laikomasi (atskaitomybės principas).“*.[186] Taip pat LVAT nurodė, kad Europos Sąjungos Teisingumo teismas yra konstatavęs, kad BDAR yra tiesiogiai taikomas valstybės narėse, teisės viršenybės principas.[187] Iš šios bylos analizės, galima pastebėti, kad pasitaiko atvejų kai nacionaliniai teisė aktai nėra suderinti su tarptautiniais teisės aktais. Dėl teisės aktų nesuderinimo kyla pavojus, jog asmens duomenų rinkimas gali pažeisti tikslo ribojimo ir duomenų kiekio mažinimo principas. Taip pat šia byla yra primenamas teisės viršenybės principas.

[183] „Administracinė byla Nr. A-3301-968/2022, Lietuvos vyriausiais administracinis teismas nutartis“, Infolex, žiūrėta 2024 m. balandžio 9 d. https://www-infolex-lt.skaitykla.mruni.eu/tp/2131457
[184] *Ibid.*
[185] *Ibid.*
.[186] „Administracinė byla Nr. A-3301-968/2022, Lietuvos vyriausiais administracinis teismas nutartis“, *op.cit.*.
[187] “ES teisės viršenybė”, EUR-Lex, žiūrėta 2024 m. balandžio 10 d. https://eur-lex.europa.eu/LT/legal-content/glossary/primacy-of-eu-law-precedence-supremacy.html

Taip pat būtina aptari kokia atsakomybė kyla juridiniams asmenis dėl asmens duomenų pažeidimų ir kokiomis priemonėmis yra siekiama atgrasyti organizacijas nuo asmens duomenų pažeidimų. BDAR 82 str. nurodyta, kad bet kuris asmuo patyręs materialinę ar nematerialinę žala dėl BDAR pažeidimo, turi teisę gauti kompensaciją už patirtą žalą. [188] Taip pat reglamentas numato, jog duomenų valdytojas atsako tik tuo atveju jei žala asmens duomenims padaroma duomenis tvarkant pažeidžiant BDAR. [189] Tačiau jeigu duomenų valdytojas gali įrodyti, jog nėra atsakingas už įvyki dėl kurio įvyko pažeidimas duomenų valdytojas gali būti atleidžiamas nuo atsakomybės ir neatlyginti žalos padarytos duomenų subjektui. Jei organizacijos duomenų tvarkyme dalyvauja daugiau nei vienas duomenų valdytojas ar tvarkytojas, ir nustačius pažeidimą visi asmenys prisidėję prie duomenų tvarkymo už padarytą žalą atsako vienodai. [190] VDAI yra išaiškinusi, jog pažeidus BDAR nuostatas gali būti skiriamos administracinės baudos. Skiriant baudas yra atsižvelgimą į kiekvienos organizacijos pajamų dydį, taip pat kiekvienu atveju yra sprendžiama, kad bauda būtų veiksminga, proporcinga padarytam pažeidimui ir atgrasančios nuo kitų pažeidimų.[191] Jei pažeidimas nedidelis, organizacijai skiriamas įspėjimas. [192] Baudų sistema pagal paskirtį turėtų duomenų valdytojus ir tvarkytojus atgrasyti nuo asmens duomenų pažeidimų.

LVAT administracinėje byloje Nr. eA-745-261/2021, išaiškino, kaip yra skiriamos baudos. Teismas išaiškino, jog BDAR 83 str. 1 d. nurodyta, kad VDAI pagal nurodytą straipsnį, skiria baudas už 4, 5 ir 6 dalis, paskaičiuoja baudą, kuri būtų veiksminga, atgrasanti ir veiksminga organizacijai kuri pažeidžia šį tarptautinį dokumentą. Teismas nurodo, kad BDAR 83 str. 2 d., yra numatyta, kad administracinės baudos, skiriamos kartu su 58 str. 2 d. a-h p. ir j p. įtvirtintomis priemonėmis. Skiriant baudas turi būti atsižvelgiama į šiuos punktus: 1. Pažeidimo pobūdį, pažeidimo sunkumą ir trukme bei paveiktų subjektų skaičių; 2. Kaip padarytas pažeidimas, tyčia ar dėl neatsargumo; 3. Ko ėmėsi duomenų valdytojas siekdamas sumažinti padaryto pažeidimo mastą; 4. Duomenų valdytojo ar tvarkytojo atsakomybės dydį ir kaip buvo įgyvendinamos techninės ir organizacinės priemonės; 5. Kokie buvo ankstesni duomenų valdytojo ar tvarkytojo padaryti pažeidimai; 6. Ar buvo pranešta VDAI apie įvykį; 7. Kokios asmens duomenų kategorijos yra pažeistos; 8. Ar anksčiau buvo skirtos 58 str. 2 d. priemonės ir kaip jų buvo laikomasi; 9. Ar laikomasi 40 str. ir 42 str. 9. Ar yra sunkinančių

[188] „82 straipsnis BDAR. Teisė į kompensaciją ir atsakomybė“, Gdpr-text, žiūrėta 2024 m. balandžio 12 d. https://gdpr-text.com/lt/read/article-82/
[189] *Ibid.*
[190] *Ibid.*
[191] „Valstybinė duomenų apsugos inspekcija, baudos ir kitos sankcijos“, LRV, žiūrėta 2024 d. balandžio 14 d. https://vdai.lrv.lt/lt/naudinga-informacija/2018-m-duomenu-apsaugos-reforma-1/baudos-ir-kitos-sankcijos/
[192] „2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB ”, *supra note*, 32.

ir lengvinančių aplinkybių. [193] Visi šie teismo išaiškinti punktai apima priemonių paskyrimą kartu su administracine bauda. Taip pat teismas išaiškino, kad pagal BDAR 83 str. 5 d., jog pažeidus nuostatas pagal 2 dalį gali būti paskirtos baudos iki 20 000 000 eur. arba įmonės atveju iki 4 proc. įmonės ankstesnių finansinių metų bendros pasaulinės apyvartos.[194] Skaičiuojant baudos dydį yra atsižvelgiama į duomenų subjekto teises, ar duomenys buvo perduodami į trečiąsias šalis, ar laikosi duomenų valdytojo ar tvarkytojo prievolių. Nacionaliniu lygiu už netinkamą duomenų tvarkymą juridiniai asmenys yra baudžiami pagal Lietuvos Respublikos administracinių nusižengimų kodekso 83 str., kuriame yra įvirtinta dispozicija dėl asmens duomenų pažeidimų.[195]

Aptartos visos teismo išaiškintos taisyklės ir punktai į kuriuos turima atsižvelgti paskiriant administracinę baudą. Žinoma, jei juridinis asmuo vydo nuskalstamą veiką, gali būti patraukimas baudžiamojon atsakomybėn kurią taip pat reglamentuoja BDAR, tačiau praktikoje tokie atvejai pasitaiko retai. Organizacijai pažeidus BDAR nuostatas, gali patirti finansinių nuostolių, nes už pažeidimus gali būti paskiriama administracinė bauda. Taip pat gali tekti atlyginti žalą asmenims, kurių asmens duomenys gali būti paveikti. Dėl netinkamo asmens duomenų tvarkymo gali būti pradedamas VADI tyrimas. Dėl netinkamo asmens duomenų tvarkymo ar net duomenų praradimo gali būti padaryta neigiama įtaka reputacijai, dėl ko gali būti prarasti nuolatinai įmonės klientai, kurių netekus įmonė gali nukentėti finansiškai.

[193] „Administracinė byla Nr. eA-745-261/2021, Lietuvos vyriausisis administracinis teismas nutaris“, Infolex, žiūrėta 2024 m. balandžio 20 d. https://www-infolex-lt.skaitykla.mruni.eu/tp/2008056
[194] *Ibid.*
[195] „Lietuvos Respublikos administracinių nusižengimų kodeksas“, Infolex, žiūrėta 2024 m. balandžio 26 d. https://www.infolex.lt/ta/336765:str83

IŠVADOS

1. Atlikus teisės aktų analizę nustatyta, kad asmens duomenų apsaugą tiesiogiai nacionaliniu lygiu reglamentuoja Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymas, kuris yra suderintas, tarptautiniu lygiu asmens duomenų apsaugą reglamentuojančiu Bendruoju duomenų apsaugos reglamentu (BDAR). Nacionaliniu lygiu Lietuvos Respublikos kibernetinio saugumo įstatymas užtikrina saugią kibernetinę aplinką, kurioje saugomi ir tvarkomi asmens duomenys. BDAR yra pagrindinis tarptautinis asmens duomenų apsaugos dokumentas, kuris numato, kaip asmens duomenys turi būti saugojami, nustato duomenų tvarkymo tikslus.
2. Išnagrinėjus asmens duomenų pareigūno (DAP) veiklą reglamentuojančius teisės aktus, nustatyta, kad DAP tiesiogiai neprisideda prie asmens duomenų kontrolės tačiau, aktyviai dalyvauja organizacijos vidinėje politikoje siekiant užtikrinti asmens duomenų saugumą.
3. Atlikus Valstybinės duomenų apsaugos institucijos (VDAI) 2023 metų statistikos analizę nustatyta, kad: 1. organizacijos įgyvendindamos asmens duomenų apsaugą pasirenka netinkamas technines priemones dėl kurių kyla pavojus duomenų saugumui; 2. dėl darbuotojų nepakankamos kvalifikacijos ir aplaidumo tvarkant asmens duomenis yra pažeidžiamos asmens duomenų teisės; 3. organizacijų nepakankamas kibernetinis saugumo lygis, neužtikrina tinkamos duomenų apsaugos. 4. organizacijos netinkamai nustato serverio parinktis dėl kurių duomenys nėra apsaugoti nuo neleistinos prieigos. Visi šie veiksniai kelia pavojų asmens duomenų saugumui.
4. Teismų praktikos analizė, parodė, kad dauguma asmens duomenų pažeidimų įvyksta dėl žmogiškosios klaidos, nes asmenys dirbantys su asmens duomenimis nėra pakankamai kvalifikuoti ir duomenis tvarko neatsakingai. Dėl asmens duomenų pažeidimų įmonėms yra skiriamos administracinės baudos, kurios yra paskiriamos įvertinus rizikos veiksnius ir padarytos žalos mastą.

LITERATŪROS SĄRAŠAS

Teisės aktai:

1. Lietuvos Respublikos konstitucija“. LRS. Žiūrėta 2024 m. kovo 5 d. https://www.lrs.lt/home/Konstitucija/Konstitucija20220522.htm
2. „Visuotinė žmogaus teisių deklaracija“. LRS. Žiūrėta 2024 m. Vasario 15 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.278385
3. „Europos žmogaus teisių konvencija“. ECHR. Žiūrėta 2024 m. kovo 1 d. https://www.echr.coe.int/documents/d/echr/convention_lit
4. „Europos Sąjungos pagrindinių teisių chartija“. Europa.eu. Žiūrėta 2024 m. kovo 1d. https://eur-lex.europa.eu/LT/legal-content/summary/charter-of-fundamental-rights-of-the-european-union.html
5. „Europos parlamento ir tarybos reglamentas (ES) 2016/679 2016 m. balandžio 27 d. dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas)“, EUR-Lex, žiūrėta 2024 m. sausio 2 d. https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex%3A32016R0679
6. „Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas“. LRS. Žiūrėta 2024 m. kovo 6 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.29193/asr
7. „Lietuvos Respublikos kibernetinio saugumo įstatymas“. TAR. Žiūrėta 2024 m. kovo 6 d. https://www.e-tar.lt/portal/lt/legalAct/5468a25089ef11e4a98a9f2247652cf4/asr?fbclid=IwAR1o5bF8eM01wwhQ_ye6ZxqFVIqoOa5hxOoIUCm6XbGetm8RJiCO9FO1PWM\
8. „Lietuvos Respublikos administracinių nusižengimų kodeksas“. Infolex. Žiūrėta 2024 m. balandžio 26 d. https://www.infolex.lt/ta/336765:str83
9. „Dėl Lietuvos Respublikos administracinių teisės pažeidimų kodekso 40 straipsnio pripažinimo netekusiu galios ir 251 straipsnio pakeitimo įstatymo 1 ir 2 straipsnių, Lietuvos Respublikos mokesčių administravimo įstatymo 27 straipsnio 5 dalies, 50 straipsnio 3 ir 9 dalių atitikties Lietuvos Respublikos Konstitucijai“. LRS. Žiūrėta 2024 m. kovo 15 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.115172
10. 29 straipsnio duomenų apsaugos darbo grupė „nuomonė 4/2007 dėl asmens duomenų sąvokos“, Europa.eu. Žiūrėta 2024 m. vasario 15 d., https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_lt.pdf

11. EDPB „Gairės Nr. 04/2020 dėl buvimo vietos duomenų ir sąlytį turėjusių asmenų išaiškinimo priemonių naudojimo COVID- 19 protrūkio aplinkybėmis“. Europa.eu. Žiūrėta 2024 m. vasario 20 d. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_lt.pdf
12. EDPB, „Gairės 05/2020 dėl sutikimo pagal Reglamentą 2016/679“. Europa.eu. Žiūrėta 2024 m. vasario 27 d. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_lt
13. „Pasiūlymas tarybos sprendimas kuriuo, atsižvelgiant į Europos Sąjungos interesus, valstybės narės įgaliojamos ratifikuoti Protokolą, kuriuo iš dalies keičiama Europos Tarybos konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108)“, Eur-lex, žiūrėta 2024 m. kovo 3 d. https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A52018PC0451
14. „29 straipsnio duomenų apsaugos darbo grupė gairės dėl pranešimo apie asmens duomenų saugumo pažeidimą pagal Reglamentą (ES) 2016/679“. Europa.eu. Žiūrėta 2024 m. Kovo 12 d. https://ec.europa.eu/newsroom/article29/items/612048

Moksliniai šaltiniai:

1. Andrijauskas, Raimondas. „Asmens Duomenų Viešas Skelbimas Ir Asmens Duomenų Apsauga: Suderinamumo Klausimas". Lietuvos Teisė: esminiai Pokyčiai (2022): 161-174. https://cris.mruni.eu/server/api/core/bitstreams/22bb8d59-ead8-429b-937d-0f37064136f5/content
2. Jagminaitė, Klaudija. „Asmens Duomenų Apsaugos Pažeidimai Socialiniuose Tinkluose Pagal ES Bendrąjį Duomenų Apsaugos Reglamentą“, Teisinės minties šventė, studentų mokslinių straipsnių rinkinys, (2022): 217-226. https://cris.mruni.eu/server/api/core/bitstreams/03ef4924-f9c7-46d3-86b1-786095a904ae/content
3. Malinauskaitė-van De Castel, Inga. „Duomenų Subjekto Teisės Virtualiuose Socialiniuose Tinkluose“. Daktaro disertacija, Mykolo Romerio Universitetas, 2017. https://talpykla.elaba.lt/elaba-fedora/objects/elaba:23456482/datastreams/MAIN/content
4. Mažeikaitė, Justė. „Asmens duomenų rinkimas ir naudojimas elektroninėje erdvėje: probleminiai aspektai“, (magistro darbas, Vilniaus Universitetas, 2017), 31-32 https://talpykla.elaba.lt/elaba-fedora/objects/elaba:35437133/datastreams/MAIN/content
5. Petraitytė, Ilona. „Asmens Duomenų Apsauga Ir Teisė į Privatų Gyvenimą“. Teisė 80, (2011): 163-174. https://www.lituanistika.lt/content/33625

6. Rastenis, Justinas. „Duomenų viliojimo elektroniniais laiškai atakų tyrimas“. Daktaro disertacija, Vilniaus Gedimino technikos universitetas, 2022. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiKwtnoguOFAxUILRAIHbtzAQ0QFnoECA8QAQ&url=https%3A%2F%2Fvb.vgtu.lt%2Fobject%2Felaba%3A136466537%2F136466537.pdf&usg=AOvVaw00JARoXDxiUl52VspivzhF&opi=89978449
7. Solove, Daniel J. Understanding Privacy. The George Washington University Law School, Public law and legal theory working paper, No. 420, 2008, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1127888
8. Šidlauskas, Aurimas. „The Role and Significance of the Data Protection Officer in the Organization.“. Socialiniai tyrimai 44, (2021), 8-28. https://etalpykla.lituanistika.lt/fedora/objects/LT-LDB-0001:J.04~2021~1662652990611/datastreams/DS.002.1.01.ARTIC/content
9. Westin Alan F., Privacy and Freedom. Washington and Lee Law Review, Vol. 25, 1968. https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20/

Specialioji literatūra:

1. „Kibernetinių atakų atpažinimas“. VU. Žiūrėta 2024 m. kovo 19 d. https://cyberphish.knf.vu.lt/upload/lm/59a44v1ZnWpJ9nBFOgX5im6KcGOHX7EllXV82d6b.pdf
2. Birmonaitė, Toma, Egidijus Jarašiūnas, Egidijus Kūris, Mindaugas Maksimaitis, Gediminas Mesonis, Augustinas Normantas, Alvydas Pumputis, Elena Vaitiekienė, Saulė Vidrinskaitė ir Juozas Žilys. Lietuvos konstitucinė teisė. Vilnius: Lietuvos teisės universitetas, 2002. https://cris.mruni.eu/server/api/core/bitstreams/3058e0ba-7737-445b-8208-a076edd9d2f2/content
3. Civilika, Mindaugas. „Europos Sąjungos asmens duomenų apsaugos teisinis reguliavimas interneto kontekste“. Iš Europos Sąjungos teisė ir Lietuva, Vilenas Vadapalas, Vilnius : Justitia, 2002), 226-260.
4. Kavoliūnaitė-Ragauskienė, Eglė. Teisė į Privatumą, Asmens Duomenų Apsauga Ir Dirbtinis Intelektas: Teisinio Reguliavimo Iššūkiai Lietuvoje Ir Europoje. Lietuvos Socialinių Mokslų Centro Teisės Institutas, 2023. https://teise.org/wp-content/uploads/2023/05/Teise_i_privatuma.pdf
5. Solving privacy paradox, „Asmens duomenų apsaugos gairės smulkiajam ir vidutiniam verslui“. LRV. Žiūrėta 2024 m. vasario 26 d. https://vdai.lrv.lt/uploads/vdai/documents/files/01_%20SolPriPa%20Asmens%20duomenu

%20apsaugos%20gaires%20SMULKIAJAM%20IR%20VIDUTINIAM%20VERSLUI%202019-11-08.pdf

6. Štitis, Darius, Paulius Pakutinskas, Marius Laurinaitis ir Inga Dauparė. „Tapatybės vagystė elektroninėje erdvėje: socialiniai elektroninio verslo ir teisinio reguliavimo aspektai“. Vilnius: Mykolo Romerio Universitetas, 2011. https://cris.mruni.eu/cris/bitstream/007/16821/1/9789955193753.pdf?sequence=1&isAllowed=y
7. Valstybinė duomenų apsaugos inspekcija, „Viešoji konsultacija dėl pareigos paskirti duomenų apsaugos pareigūną“. LRV. Žiūrėta 2024 m. kovo 13 d. https://vdai.lrv.lt/uploads/vdai/documents/files/Viesoji%20-%20dap_2017.pdf
8. Zaleskis, Julius. Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Vilnius: VĮ Registrų centras, 2019.

Teismų praktika:

1. „Administracinė byla Nr. A-3301-968/2022, Lietuvos vyriausiais administracinis teismas nutartis“, Infolex, žiūrėta 2024 m. balandžio 9 d. https://www-infolex-lt.skaitykla.mruni.eu/tp/2131457
2. „Administracinė byla Nr. eA-2483-822/2021, Lietuvos vyriausiasis administracinis teismas sprendimas“, Infolex, žiūrėta 2024 m. balandžio 4 d. https://www-infolex-lt.skaitykla.mruni.eu/tp/2049327#B_0
3. „Administracinė byla Nr. eI2-588-816/2024, Regionų administracinis teismas sprendimas“. Infolex. Žiūrėta 2024 m. balandžio 6 d. https://www-infolex-lt.skaitykla.mruni.eu/tp/2239974
4. „Administracinė byla Nr. eI2-7048-1114/2022, Vilniaus apygardos administracinis teismas sprendimas“, Infolex, žiūrėta 2024 m. balandžio 4 d. https://www-infolex-lt.skaitykla.mruni.eu/tp/2139919
5. „Administracinė byla Nr. TA-458-821/2023, Lietuvos vyriausiasis administracinis teismas nutartis“. Infolex. Žiūrėta 2024 m. balandžio 4 d. https://www-infolex-lt.skaitykla.mruni.eu/tp/2166238#pa4
6. Administracinė byla Nr. I2-870-789/2021, Vilniaus apygardos administracinis teismas sprendimas“, Infolex, žiūrėta 2024 m. balandžio 4 d. https://www-infolex-lt.skaitykla.mruni.eu/tp/2065401
7. Judment of the court „Patrick Breyer vs Bundesrepublik Deutschland“. Europa.eu. Žiūrėta 2024 m. vasario 20 d. https://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1075747

Internetiniai šaltiniai:

1. “ES teisės viršenybė”. EUR-Lex. Žiūrėta 2024 m. balandžio 10 d. https://eur-lex.europa.eu/LT/legal-content/glossary/primacy-of-eu-law-precedence-supremacy.html
2. „82 straipsnis BDAR. Teisė į kompensaciją ir atsakomybė“. Gdpr-text. Žiūrėta 2024 m balandžio 12 d. https://gdpr-text.com/lt/read/article-82/
3. „Atsarginės duomenų kopijos: kokių taisyklių reikėtų laikytis?“. 15min, 2022 m. balandžio 15 d. https://www.15min.lt/verslas/naujiena/mokslas-it/atsargines-duomenu-kopijos-kokiu-taisykliu-reiketu-laikytis-1290-1667486
4. „Dėl asmens duomenų nutekėjimo per gruodžio 8 d. įvykdytą kibernetinę ataką prieš KTU“, KTU, žiūrėta 2024 m. balandžio 2 d. https://ktu.edu/news/del-asmens-duomenu-nutekejimo-per-gruodzio-8-d-ivykdyta-kibernetine-ataka-pries-ktu/
5. „Kas yra asmens duomenys?“, Europos komisija, žiūrėta. 2024 m. sausio 10 d. https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_lt
6. „Kas yra duomenų nutekinimas? Data leak ir Data breach skirtumai“. Vnpgidas. Žiūrėta balandžio 1 d. https://www.vpngidas.lt/saugus-internetas/kibernetiniai-nusikaltimai/duomenu-nutekinimas-data-leak-data-breach/
7. „Kibernetinio saugumo mokymai darbuotojams: kas yra tikrasis laimėtojas?“. Verslo žinios. 2021 m. gegužės 03d. https://www.vz.lt/verslo-sprendimai/2021/05/03/kibernetinio-saugumo-mokymai-darbuotojams-kas-yra-tikrasis-laimetojas
8. „Praktinis bendrojo duomenų apsaugos reglamento taikymas“. LRV. Žiūrėta 2024 m. kovo 9 d. https://aad.lrv.lt/uploads/aad/documents/files/Darbuotojams/Praktinis%20BDAR%20taikymas.pdf
9. „Tiksinti bomba: įmonę paliekantis darbuotojas išsineša slaptažodžius, banko duomenis – apie virtualų saugumą nepagalvoja net pusė darbdavių“. Delfi, 2022 m. rugpjūčio 4 d. https://www.delfi.lt/darbas/patarimai/tiksinti-bomba-imone-paliekantis-darbuotojas-issinesa-slaptazodzius-banko-duomenis-apie-virtualu-sauguma-nepagalvoja-net-puse-darbdaviu-90885973
10. „Valstybinė duomenų apsaugos inspekcija, 2022 m. I pusmečio pranešimų apie asmens duomenų saugumo pažeidimus apžvalga“. LRV. Žiūrėta 2024 m. kovo 28 d. https://vdai.lrv.lt/lt/naujienos/2022-m-i-pusmecio-pranesimu-apie-asmens-duomenu-saugumo-pazeidimus-apzvalga/

11. „Valstybinė duomenų apsaugos inspekcija, baudos ir kitos sankcijos“, LRV, žiūrėta 2024 m. balandžio 14 d. https://vdai.lrv.lt/lt/naudinga-informacija/2018-m-duomenu-apsaugos-reforma-1/baudos-ir-kitos-sankcijos/
12. Balčiūnienė, Rūta. “„CityBee“ skirta 110.000 Eur bauda už BDAR pažeidimus”. Verslo žinios, 2021 m. lapkričio 30 d. https://www.vz.lt/rinkodara/2021/11/30/citybee-skirta-110000-eur-bauda-uz-bdar-pazeidimus
13. Your Europe, „Duomenų apsauga pagal BDAR“. Europa.eu. Žiūrėta 2024 m. vasario 20 d. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_lt.htm
14. Kirilova, Patricija. “Kibernetinio saugumo ekspertai apie tai, kas ir kodėl atsitiko su „CityBee“: tiek slaptažodžių, tiek duomenų apsauga išties labai silpna”. LRT, 2021 m. vasario 18 d. https://www.lrt.lt/naujienos/mokslas-ir-it/11/1347303/kibernetinio-saugumo-ekspertai-apie-tai-kas-ir-kodel-atsitiko-su-citybee-tiek-slaptazodziu-tiek-duomenu-apsauga-isties-labai-silpna
15. Krašto apsaugos ministerija, „Nacionalinė kibernetinio saugumo būklės ataskaita“. LRV. Žiūrėta 2024 m. kovo 6 d. https://vdai.lrv.lt/uploads/vdai/documents/files/2020%20m_%20Nacionalinio%20kibernetinio%20saugumo%20būklės%20ataskaita%20el_%20versija.pdf
16. Lietuvos Respublikos teisingumo ministerija, „ Europos Sąjungos reikalų koordinavimas“. LRV. Žiūrėta 2024 m. kovo 3 d. https://tm.lrv.lt/lt/veiklos-sritys-1/es-reikalu-koordinavimas/
17. Nacionalinis kibernetinio saugumo centras. „Kibernetinis saugumas ir verslas. Ką turėtų žinoti kiekvienas įmonės vadovas 2020“. NKSC. Žiūrėta 2024 m. kovo 19 d. https://www.nksc.lt/doc/Kibernetinio_saugumo_vadovas_verslui_2020.pdf
18. Stenulienė, Ingrida.“Baigta byla dėl duomenų vagystės iš „Grožio chirurgijos“ klinikos”. 15min, 2018 m. rugsėjo 17 d. https://www.15min.lt/naujiena/aktualu/nusikaltimaiirnelaimes/baigta-byla-del-duomenu-vagystes-is-grozio-chirurgijos-klinikos-59-1030942?utm_medium=copied
19. Valstybinė duomenų apsaugos inspekcija „2022 metų asmens duomenų apsaugos priežiūros Lietuvoje apžvalga“. LRV. Žiūrėta 2024 m. kovo 16 d. https://vdai.lrv.lt/uploads/vdai/documents/files/2022%20ADA%20prieziuros%20apzvalga.pdf
20. Valstybinė duomenų apsaugos inspekcija, „Rekomendacija dėl asmens duomenų saugumo pažeidimų nustatymo, tyrimo, pranešimo apie juos ir dokumentavimo tvarkos“, LRV, žiūrėta 2024 m. kovo 16 d. https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomend_ADSP_2018.pdf

21. Valstybinė duomenų apsaugos inspekcija, „Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams“, LRV, žiūrėta 2024 m. kovo 19 d. https://vdai.lrv.lt/uploads/vdai/documents/files/VDAI_saugumo_priemoniu_gaires-2020-06-18.pdf
22. Valstybinė duomenų apsaugos inspekcija. „Asmens duomenų saugumo pažeidimai Lietuvoje 2023 m.“. LRV. Žiūrėta 2024 m. kovo 16 d. https://vdai.lrv.lt/media/viesa/saugykla/2024/1/Mdb7Qax9xsk.pdf
23. Valstybinė duomenų apsaugos inspekcija. „Duomenų apsaugos pareigūnas“. LRV. Žiūrėta 2024 m. kovo 15 d. https://vdai.lrv.lt/lt/adsp-ir-dap/duomenu-apsaugos-pareigunas/
24. Vilkišienė, Agnė. „Asmens duomenų saugumo pažeidimai Lietuvoje 2023 m. I pusmetį“. B1. Žiūrėta 2024 m. kovo 20 d. https://www.b1.lt/wiki/asmens-duomenu-saugumo-pazeidimai-lietuvoje-2023-m-i-pusmeti-3789
25. Žalimas, Dainius. „Visuotinė žmogaus teisių deklaracija – svarus ginklas kovojant dėl visų žmonių laisvės, lygybės ir orumo“. LRKT. Žiūrėta 2024 m. vasario 27 d. https://lrkt.lt/lt/dainius-zalimas-visuotine-zmogaus-teisiu-deklaracija-svarus-ginklas-kovojant-del-visu-zmoniu-laisves-lygybes-ir-orumo/1207

SANTRAUKA

Magistro baigiamojo **darbo tema** - „Asmens duomenų apsaugos kontrolės įgyvendinimo probleminiai aspektai“. Šio darbo pagrindinis **tikslas**, nustatyti ir įvertinti asmens duomenų apsaugos kontrolės sistemų efektyvumą organizacijose, identifikuoti kylančius iššūkius, su kuriais jos susiduria. Taip pat išnagrinėti teisinius, technologinius, organizacinius, komunikacijos ir privatumo aspektus, išanalizuoti sąveiką ir nustatyti, kaip sistemos atitinka teisinius reikalavimus, siekiant užtikrinti asmens duomenų saugumą bei privatumą.

Siekiant įgyvendinti išsikeltą tikslą, **buvo išsikeliami šie uždaviniai: i**šnagrinėti asmens duomenų apsaugos reglamentavimą nacionaliniu ir tarptautiniu lygmeniu. Identifikuoti asmens duomenų apsaugos kontrolės įgyvendinimo iššūkius. Išanalizuoti duomenų apsaugos funkciją ir kaip pareigūnas dalyvauja asmens duomenų kontrolės procese. Išnagrinėti teismų praktiką dėl asmens duomenų pažeidimų, nustatyti kokia yra atsakomybė asmenims už duomenų pažeidimus bei identifikuoti pagrindines organizacijose esančias problemas dėl kurių įvyksta minėti veiksniai, bei kokia atsakomybė yra už asmens duomenų pažeidimus.

Šiame darbe tiriami mokslinės literatūros šaltiniai, nacionaliniai teisės aktai, tarptautiniai teisės aktai, moksliniai straipsniai ir specialioji literatūra, teismų praktika.

Magistro darbą sudaro įvadas, trys skyriai. Pirmajame skyriuje analizuojama asmens duomenų apsaugos teoriniai aspektai, pateiktos asmens duomenų, duomenų apsaugos pareigūno instituto sampratos ir jų turinio elementai, analizuotos asmens duomenų teisės ir asmens teisės į privatumą sąsajos, apibrėžti teisėtam duomenų tvarkymui keliami reikalavimai ir taikomi principai. Antrajame skyriuje išsamiai analizuojamas asmens duomenų surinkimo, tvarkymo ir saugojimo procesas organizacijose, nagrinėjami iššūkiai, su kuriais organizacijos susiduria įgyvendindamos efektyvias asmens duomenų apsaugos kontrolės sistemas. Trečiame skyriuje išnagrinėta teismų praktika susijusi su asmens duomenų pažeidimais. Nagrinėjamos organizacijų patirtys ir iššūkiai, su kuriais jos susiduria įgyvendindamos asmens duomenų apsaugos priemones, bei kokia atsakomybė kyla dėl asmens duomenų pažeidimų.

Išgarinėjus mokslinius šaltinius, galima teigti, kad: 1. organizacijos įgyvendindamos asmens duomenų apsaugą pasirenka netinkamas technines priemones dėl kurių kyla pavojus duomenų saugumui; 2. dėl darbuotojų nepakankamos kvalifikacijos ir aplaidumo tvarkant asmens duomenis yra pažeidžiamos asmens duomenų teisės; 3. organizacijų nepakankamas kibernetinis saugumo lygis, neužtikrina tinkamos duomenų apsaugos. 4. organizacijos netinkamai nustato serverio parinktis dėl kurių duomenys nėra apsaugoti nuo neleistinos prieigos. Visi šie veiksniai kelia pavojų asmens duomenų saugumui.

SUMMARY

The topic of the master's thesis is "Problematic aspects of the implementation of personal data protection control". **The main goal of this work** is to determine and evaluate the effectiveness of personal data protection control systems in organizations, to identify emerging challenges they face. Also examine legal, technological, organizational, communication and privacy aspects, analyze interactions and determine how systems meet legal requirements in order to ensure personal data security and privacy.

In order to realize the set goal, **the following tasks were set:** to examine the regulation of personal data protection at the national and international level. Identify the challenges of implementing personal data protection control. Analyze the function of data protection and how the officer participates in the personal data control process. To examine the court practice regarding personal data violations, to determine the responsibility of individuals for data violations, and to identify the main problems in organizations that cause the aforementioned factors to occur, as well as the accountability for personal data violations.

This work examines sources of scientific literature, national legal acts, international legal acts, scientific articles and special literature, court practice.

The master's thesis consists of an introduction and three chapters. The first chapter analyzes the theoretical aspects of personal data protection, presents the concepts of personal data, the data protection officer institute and their content elements, analyzes the interfaces between the right to personal data and the right to privacy, defines the requirements for legal data processing and the applicable principles. The second chapter analyzes in detail the process of collecting, processing and storing personal data in organizations, and examines the challenges that organizations face when implementing effective personal data protection control systems. In the third chapter, the case law examined is related to the violation of personal data. The experiences of organizations and the challenges they face when implementing personal data protection measures are examined, as well as what liability arises from personal data violations.

After analyzing the scientific sources, it can be stated that: 1. when implementing the protection of personal data, organizations choose inappropriate technical measures that put data security at risk; 2. personal data rights are violated due to insufficient qualification and negligence of employees in handling personal data; 3. insufficient cyber security level of organizations, does not ensure adequate data protection. 4. Organizations do not properly set server options, as a result of which data is not protected from unauthorized access. All these factors pose a risk to the security of personal data.