MYKOLO ROMERIO UNIVERSITETAS
VIEŠOJO VALDYMO IR VERSLO FAKULTETAS

AGNĖ SIPAVIČIŪTĖ

BENDROJO DUOMENŲ APSAUGOS REGLAMENTO TAIKYMO STRATEGIJOS KŪRIMAS ORGANIZACIJOJE

Magistro baigiamasis darbas

Vadovas
Prof. dr. Tadas Limba

VILNIUS, 2021

MYKOLO ROMERIO UNIVERSITETAS
VIEŠOJO VALDYMO IR VERSLO FAKULTETAS

BENDROJO DUOMENŲ APSAUGOS REGLAMENTO TAIKYMO STRATEGIJOS KŪRIMAS ORGANIZACIJOJE

Kibernetinio saugumo valdymo magistro baigiamasis darbas

Studijų programa 6211LX066

Vadovas
Prof. dr. Tadas Limba
2021

Recenzentas
2021

Atliko:
KSVvmis19-1 stud.
A. Sipavičiūtė
2021

VILNIUS, 2021

TURINYS

ĮVADAS ... **8**
1. ASMENS DUOMENŲ APSAUGOS TEORINIAI ASPEKTAI ... **11**
1.1. Teisės į privatumą ir asmens duomenų apsaugos sąvokų sąsaja bei raida ... 11
1.2. BDAR juridinių aspektų analizė ... 16
1.3. BDAR įtvirtintų reikalavimų taikymo organizacijoje strategijos elementų analizė ... 28
1.4. BDAR taikymo strategijos kūrimo probleminiai aspektai ... 35
2. BDAR TAIKYMO STRATEGIJOS KŪRIMO TYRIMO METODOLOGIJA ... **37**
2.1. Tyrimo metodiniai aspektai ... 37
2.2. Tyrimo metodikos pagrindimas ... 40
3. BDAR TAIKYMO STARTEGIJOS KŪRIMO TYRIMO REZULTATŲ ANALIZĖ ... **42**
3.1. Asmens duomenų apsaugos pažeidimų Europoje analizė ... 42
3.2. Ekspertinio vertinimo rezultatų analizė ... 50
4. BDAR TAIKYMO STRATEGIJOS ORGANIZACIJOJE MODELIO KŪRIMAS ... **61**
4.1. Modeliavimo metodologija ... 61
4.2. Modelio analizė ... 63
IŠVADOS IR REKOMENDACIJOS ... **67**
LITERATŪRA ... **69**
ANOTACIJA ... **76**
ANNOTATION ... **77**
SANTRAUKA ... **78**
SUMMARY ... **79**
PRIEDAI ... **80**
1 PRIEDAS. Veiklų, dėl kurių turi būti atliekamas poveikio duomenų apsaugai vertinimas, sąrašas ... 80
2 PRIEDAS. Ekspertinio tyrimo anketa ... 81
3 PRIEDAS. Tyrime dalyvaujančių šalių sąrašas ... 83
4 PRIEDAS. BDAR straipsnių pažeidimų dažnis Europoje 2018 – 2021 metais ... 84
5 PRIEDAS. Darbe analizuojamų BDAR straipsnių sąrašas ... 86

LENTELĖS

1 lentelė. Asmens duomenų sąvokos apibrėžimai 13
2 lentelė. Asmens duomenų tvarkymo principai 17
3 lentelė. Duomenų valdytojo ir duomenų tvarkytojo bendrosios prievolės 29
4 lentelė. BDAR taikymo strategijos kūrimo probleminiai aspektai 36
5 lentelė. Didžiausios 2020 metais už BDAR pažeidimus skirtos baudos 43
6 lentelė. Asmens duomenų saugumo pažeidimų kategorijos 45
7 lentelė. 10 šalių, kurioms buvo skirtas didžiausias baudų kiekis 48
8 lentelė. Ekspertų nurodytos papildomos kliūtys, su kuriomis dažniausiai susiduria organizacijos siekdamos užtikrinti tinkamą asmens duomenų apsaugą 53
9 lentelė. Ekspertų nurodytos papildomos priežastys, lemiančios asmens duomenų apsaugos pažeidimus organizacijoje 54
10 lentelė. Ekspertų nurodytos papildomos priemonės, skirtos pakankamam duomenų subjekto informavimui bei jo teisių įgyvendinimo užtikrinimui 56

PAVEIKSLAI

1 pav. Magistro baigiamojo darbo struktūros loginė schema 10
2 pav. CIA triada: informacijos saugumo valdymo modelis 15
3 pav. Specialių kategorijų asmens duomenų tvarkymo išimtys 19
4 pav. Sutikimo tvarkyti asmens duomenis sąlygos 20
5 pav. Duomenų subjekto teisės 21
6 pav. Gerosios kibernetinio saugumo praktikos pavyzdžių rinkinys 31
7 pav. Pasirengimo taikyti BDAR organizacijoje žingsniai 33
8 pav. Pagrindiniai BDAR taikymo strategijos organizacijoje elementai 34
9 pav. Ekspertų vertinimų standartinio nuokrypio priklausomybė nuo ekspertų skaičiaus 38
10 pav. Empirinio tyrimo loginė eiga 39
11 pav. 2018-2021 m. baudų, skirtų už asmens duomenų apsaugos pažeidimus pagal BDAR, dinamika kiekine išraiška 42
12 pav. 2018-2021 m. baudų, skirtų už asmens duomenų apsaugos pažeidimus pagal BDAR, dinamika pinigine išraiška 43
13 pav. Asmens duomenų apsaugos pažeidimų pasiskirstymas pagal kategorijas, proc. 46
14 pav. Pažeistų BDAR straipsnių dažnis , vnt. 47
15 pav. Asmens duomenų apsaugos pažeidimų pasiskirstymas pagal vykdomos veiklos rūšį, proc. ... 48
16 pav. Konkordancijos koeficiento apskaičiavimas 51
17 pav. Ekspertų nuomonė apie tai, ar BDAR taikymo strategijos kūrimas yra prioritetinis organizacijos uždavinys 51
18 pav. Ekspertų nuomonė apie tai, ar BDAR taikymo strategijos kūrimas organizacijoje yra sudėtingas uždavinys 52
19 pav. Ekspertų nuomonė apie tai, su kokiomis kliūtimis dažniausiai susiduria organizacijos siekdamos užtikrinti tinkamą asmens duomenų apsaugą, proc. 52
20 pav. Ekspertų nuomonė apie tai, kokios priežastys pagrinde lemia asmens duomenų apsaugos pažeidimus organizacijoje, proc. 54
21 pav. Ekspertų nuomonė apie tai, kiek svarbios yra organizacijoje galimai disponuotinos priemonės, skirtos pakankamam duomenų subjekto informavimui bei jo teisių įgyvendinimo užtikrinimui, proc. 55
22 pav. Ekspertų nuomonė apie tai, kiek svarbios yra organizacijoje galimai disponuotinos priemonės skirtos tinkamai įvykdyti pranešimo apie asmens duomenų saugos pažeidimą įsipareigojimą, proc.... 57
23 pav. Ekspertų nuomonė apie tai, ar konkrečiam sektoriui pritaikytų BDAR elgesio kodeksų diegimas yra veiksminga priemonė, padedanti organizacijai laikytis asmens duomenų valdytojo atskaitomybės principo, vnt. 58

24 pav. Ekspertų nuomonė apie tai, ar atitikties BDAR reikalavimams sertifikato įgijimas yra veiksminga priemonė padedanti organizacijai tinkamai vykdyti BDAR įtvirtintus reikalavimus, vnt. 59
25 pav. Ekspertų nuomonė apie tai, ar asmens duomenų saugumo pažeidimų, įvykusių kitose organizacijose, stebėjimas bei analizė yra veiksminga profilaktinė priemonė siekiant tinkamai vykdyti BDAR įtvirtintus reikalavimus savo organizacijoje, vnt. 60
26 pav. Klasikinis sprendimų priėmimo procesas 61
27 pav. Bendroji strategija: strategija ir taktika 62
28 pav. IPO modelis 62
29 pav. BDAR taikymo strategijos organizacijoje modelis 64

SANTRUMPOS

ADTAĮ	Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas
AEPD	Ispanijos duomenų apsaugos agentūra
angl.	angliškai
BDAR	Bendrasis duomenų apsaugos reglamentas
Direktyva 95/46/EB	Europos Parlamento ir Tarybos Direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo
EDAPP	Europos duomenų apsaugos priežiūros pareigūnas
EDAV	Europos duomenų apsaugos valdyba
EEE	Europos ekonominė erdvė
ENISA	Europos Sąjungos kibernetinio saugumo agentūra
ERĮ	Lietuvos Respublikos elektroninių ryšių įstatymas
ES	Europos Sąjunga
ESTT	Europos Sąjungos Teisingumo Teismas
ET	Europos Taryba
ISO standartai	Tarptautinės standartų organizacijos kokybės vadybos sistemų standartai
LRK	Lietuvos Respublikos Konstitucija
NIST	National Institute of Standards and Technology
NKCS	Nacionalinio kibernetinio saugumo centras
PDAV	Poveikio duomenų apsaugai vertinimas
VDAI	Valstybinė duomenų apsaugos inspekcija
ŽEIT	Žurnalistų etikos inspektoriaus tarnyba

ĮVADAS

Temos naujumas ir aktualumas. Kiekvienas asmuo turi teisę į savo asmens duomenų apsaugą, tad fizinių asmenų apsauga tvarkant jų asmens duomenis bei užtikrinant laisvą tokių duomenų judėjimą yra pagrindinė jų teisė. Siekiant reglamentuoti bei užtikrinti asmens duomenų apsaugą, 2016 metais buvo priimtas Bendrasis duomenų apsaugos reglamentas (toliau - BDAR). Tai teisės aktas tiek Lietuvoje, tiek ir kitose Europos Sąjungos valstybėse narėse pradėtas taikyti 2018 m. gegužės 25 d. bei sukėlęs nemažą pokyčių bangą organizacijose. Tai – esminė asmens duomenų apsaugos reforma, kuri palietė visas įmones: duomenų valdytojus ir tvarkytojus.

Organizacijų pasirengimas reglamento taikymui, pridėtinė vertė verslui jį įgyvendinus ir organizacijų sąmoningumas šioje srityje yra nagrinėjami dar tik kelis metus. Politou, E. ir kt. (2018), analizuodami BDAR įgyvendinimo iššūkius ir galimus sprendimus, priėjo prie išvados, kad tai nėra paprastas uždavinys. Teigiama, jog įstatymų leidėjai, apibrėždami tik funkcinius BDAR įgyvendinimo reikalavimus, sąmoningai vengė rekomenduoti konkrečius techninius bei organizacinius privatumo užtikrinimo būdus įgyvendinant BDAR teisinius reikalavimus. Pagrindinis šio požiūrio tikslas buvo leisti BDAR pritaikyti prie būsimų techninių naujovių. Mense, A. ir Blobel, B. (2017) parengė ir išleido gaires, kuriose pateikiamas saugumo ir privatumo standartų bei komponentų naudojimas padeda organizacijoms tinkamai įgyvendinti BDAR reikalavimus. Chiara, A. ir Kutar, M. (2018) Jungtinėje Karalystėje atliktas tyrimas apie įmonių pasirengimą įgyvendinti BDAR reikalavimus parodė, kad žemas informuotumo apie BDAR įgyvendinimą lygis reiškia bendrą žemą reglamento įgyvendinimo lygį. Taip pat paaiškėjo, kad kai kurioms organizacijoms nepavyko susidoroti su BDAR įgyvendinimu ir jos visiškai paliko rinką. Li, H. ir bendraautoriai (2019) pabrėžė tinkamų priemonių, skirtų teisės „būti pamirštam“ bei duomenų subjekto teisės susipažinti su tvarkomais duomenimis įgyvendinimui, svarbą. Pasak Andrijausko, R. ir Morkūnienės, D. (2020), duomenų apsaugos pareigūno, padedančio organizacijoms laikytis BDAR reikalavimų, paskyrimas yra atitikties BDAR reikalavimams garantas bei sėkmingo bendradarbiavimo su nacionalinėmis asmens duomenų apsaugos institucijomis pagrindas.

Nepaisant mokslininkų ir už asmens duomenų apsaugą atsakingų priežiūros institucijų teikiamų ir viešai publikuojamų gairių bei rekomendacijų dėl BDAR įtvirtintų reikalavimų taikymo, baudų, skiriamų už asmens duomenų saugumo pažeidimus, augantis kiekis ir jų dydis (pinigine išraiška) rodo, kad daugelis organizacijų, vykdydamos savo veiklą, vis dar neišvengia BDAR pažeidimų. Po BDAR įsigaliojimo „Google Inc.“ (Prancūzija), „H&M“ (Vokietija), „TIM“ (Italija), „British Airways“ (Jungtinė Karalystė), „Caixabank S.A.“ (Ispanija) ir kt. pasauliniu mastu žinomoms įmonėms skirtos milijoninės baudos už asmens duomenų saugumo pažeidimus, taip pat ir Lietuvoje dar šių metų pirmąjį ketvirtį Valstybinės duomenų apsaugos inspekcijos pradėti tyrimai dėl „CityBee“, „Orakulas“ ir

pažinčių portalo „Darnipora.lt“ vartotojų asmens duomenų saugumo tik dar labiau pabrėžia šios temos aktualumą.

Mokslinė problema. BDAR apibrėžti tik funkciniai reglamento įgyvendinimo reikalavimai neužtikrina veiksmingo BDAR strategijos taikymo organizacijoje. Mokslo šaltiniuose (Politou, E. ir kt. (2018), Andrijauskas, R. ir Morkūnienė, D. (2020), Mense, A. ir Blobel, B. (2017), Tamavičiūtė, V. (2019), Sirur, S. ir kt. (2018) ir kt.), analizuojančiuose BDAR įtvirtintų reikalavimų taikymą organizacijoje, nėra išskirti ir pakankamai išsamiai išanalizuoti standartizuoti BDAR įtvirtintų reikalavimų taikymo organizacijoje strategijos modeliavimo kriterijai ir elementai.

Tyrimo objektas. BDAR įtvirtintų reikalavimų taikymas organizacijoje.

Tyrimo tikslas. Sukonstruoti BDAR taikymo strategijos organizacijoje modelį.

Pagrindiniai uždaviniai:

1. Išanalizuoti asmens duomenų apsaugos teorinius aspektus.
2. Sukonstruoti BDAR taikymo strategijos kūrimo tyrimo organizavimo metodologiją.
3. Atlikti asmens duomenų apsaugos pažeidimų analizę ir ekspertinį vertinimą, kuriuo siekiama išsiaiškinti BDAR taikymo strategijos optimizavimo galimybes, bei pateikti tyrimo rezultatus.
4. Remiantis teorinės ir praktinės analizės rezultatais, sukonstruoti BDAR taikymo strategijos organizacijoje modelį.

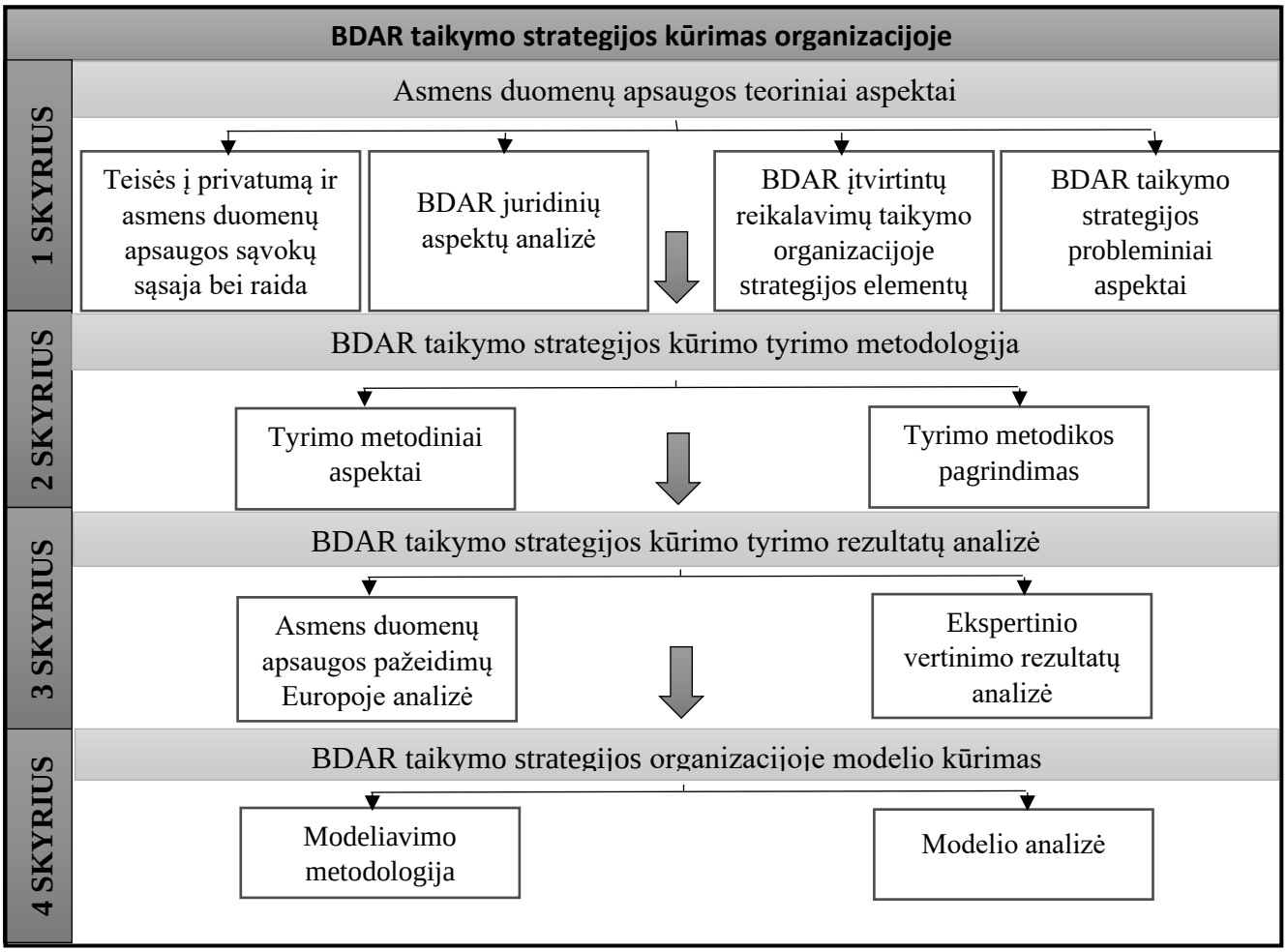
Darbo metodika ir šaltiniai. Analizuojant asmens duomenų apsaugos teorinius bei juridinius aspektus buvo taikomi mokslinės literatūros ir juridinių dokumentų analizės metodai. Mokslinės literatūros šaltiniai ir juridiniai dokumentai buvo tikrinami kokybinio turinio analizės metodu siekiant nustatyti ir apibrėžti teksto kategorijas. Juridinis analizės pagrindas – BDAR. Baigiamajame darbe pagrinde remiamasi Addis, C. ir Kutar, M. (2018), Bygrave, A. L. (2017), Cvilikos, M. ir Šlapimaitės, L. (2015), Ferrara, P. ir Spoto, F. (2018), Li, H., Yu, L. ir He, W. (2019) ir kitų autorių moksliniais darbais. Atliekant asmens duomenų apsaugos pažeidimų Europoje analizę buvo naudojami antrinių statistinių duomenų ir lyginamosios analizės metodai. Siekiant suformuluoti praktines rekomendacijas dėl BDAR taikymo strategijos modelio kūrimo organizacijoje, buvo atliekamas ekspertinis vertinimas ir taikomas anketinės apklausos metodas. Tyrimo metu buvo apklausta specialiai parinkta žmonių grupė, kurią sudarė 9 ekspertai turintys žinių asmens duomenų apsaugos srityje. Remiantis trianguliacijos metodu atlikto tyrimo rezultatais konstruojamas BDAR taikymo strategijos organizacijoje modelis.

Darbo struktūra. Baigiamąjį darbą sudaro 4 pagrindinės dalys (žr. 1 pav.). Pirmojoje dalyje yra konceptualizuojamos privatumo ir asmens duomenų apsaugos sampratos bei jų raida, analizuojami pagrindiniai BDAR įtvirtinti reikalavimai. Antrojoje dalyje yra pristatoma ir pagrindžiama empirinio tyrimo metodologija. Trečiojoje dalyje yra atliekami asmens duomenų apsaugos pažeidimų Europoje

analizė ir ekspertinis vertinimas siekiant išsiaiškinti BDAR taikymo strategijos optimizavimo galimybes. Ketvirtojoje dalyje yra konstruojamas BDAR taikymo strategijos organizacijoje modelis.

Darbo praktinis reikšmingumas. Kiekviena organizacija, siekdama išlikti sparčiai kintančioje verslo aplinkoje, privalo vykdyti savo veiklą pagal tuo metu šalyje galiojančius teisės aktus. BDAR yra visa apimtimi privalomas ir tiesiogiai taikomas organizacijoms, valdančioms ir tvarkančioms asmens duomenis ES ir ne tik. Organizacijai siekiant atitikti ir veiksmingai vykdyti BDAR reikalavimus yra svarbu turėti sistemišką reglamento taikymo strategijos modelį. Tyrimo metu sukonstruotas BDAR taikymo strategijos organizacijoje modelis gali padėti organizacijoms lengviau prisitaikyti prie duomenų apsaugos reguliavimo pokyčių bei užtikrinti tinkamas technines ir organizacines priemones duomenų apsaugai, ko pasėkoje būtų sumažinama asmens duomenų apsaugos pažeidimų įvykių tikimybė.

Tyrimo ribotumas. Tyrimo pabaigoje nėra įmanoma įvertinti sukonstruoto BDAR taikymo strategijos organizacijoje modelio veiksmingumo. Modelio veiksmingumo įvertinimui yra reikalinga konkrečių atvejų (organizacijų) veikos rezultatų stebėsena prieš ir po modelio įdiegimo.



Šaltinis: parengta darbo autorės

1 pav. Magistro baigiamojo darbo struktūros loginė schema

1. ASMENS DUOMENŲ APSAUGOS TEORINIAI ASPEKTAI

Siekiant išsamiai ir visapusiškai ištirti BDAR įtvirtintų reikalavimų taikymo strategiją organizacijoje, pirmiausia yra būtina išanalizuoti bendruosius privatumo aspektus, asmens duomenų apsaugos sampratą bei šios srities teisinį reguliavimą. Atsižvelgiant į tai, pirmajame šio darbo poskyryje yra analizuojamas teisės į privatų gyvenimą ir asmens duomenų apsaugos teisinis reguliavimas, atskleidžiamos privatumo bei asmens duomenų sąvokos bei jų raida.

1.1. Teisės į privatumą ir asmens duomenų apsaugos sąvokų sąsaja bei raida

Privatumo sąvokos oficialus apibrėžimas tarptautinėje bendruomenėje pirmą kartą buvo įtvirtintas 1948 metais priimtoje ir paskelbtoje Visuotinės žmogaus teisių deklaracijoje. Šios deklaracijos 12 straipsnyje yra skelbiama, jog „niekas neturi patirti savavališko kišimosi į jo privatumą, šeimos gyvenimą, buitį ar susirašinėjimą arba kėsinimosi į jo garbę ir reputaciją. Kiekvienas turi teisę į įstatymo apsaugą nuo tokio kišimosi arba kėsinimosi“ (Visuotinė žmogaus teisių deklaracija, 1948, 12 straipsnis).

Žinoma, kad šios sąvokos turinys, tiek prieš, tiek ir po jos oficialaus apibrėžimo atsiradimo tarptautinėje bendruomenėje, buvo nagrinėjamas daugelio mokslininkų. Pasak mokslininkų, vienų iš pirmųjų išskyrusių teisę į privatumą, besiplečianti teisės į gyvenimą sąvoka tapo teise džiaugtis gyvenimu – teise būti paliktam vienam (Warren ir Brandeis, 1890). W. Prosser 1960 metais, cituojama pagal Petraitytę, 2011, šią teisę susiejo su asmens apsauga nuo trikdančios informacijos ir iškreiptų faktų apie asmenį paviešinimo (Petraitytė, I. (2011) *Asmens duomenų apsauga ir teisė į privatų gyvenimą.* Vilnius: Teisė). Westin, A. F. (1967), Kolumbijos universiteto viešosios teisės ir vyriausybės emerito profesorius, apibūdindamas privatumą teigė, kad tai yra asmens galimybė nuspręsti, kada, kokiu būdu ir kokios apimties informacija apie jį bendraujant gali būti pateikiama kitiems.

1950 metais Europos Tarybos (toliau – ET) narės – vyriausybės, atsižvelgdamos į Jungtinių Tautų Generalinės Asamblėjos 1948 metų gruodžio 10 dieną paskelbtą Visuotinę žmogaus teisių deklaraciją bei į tai, kad ET tikslas yra siekti didesnės savo narių vienybės, ir į tai, kad vienas iš būdų siekti šio tikslo yra žmogaus teisių ir pagrindinių laisvių apsauga bei plėtojimas, priėmė Žmogaus teisių ir pagrindinių laisvių apsaugos konvenciją (Europos Žmogaus teisių konvencija, 2010). Šios konvencijos 8 straipsnyje „Teisė į privataus ir šeimos gyvenimo gerbimą“ yra numatyta, kad kiekvienas turi teisę į tai, kad būtų gerbiamas jo privatus ir šeimos gyvenimas, būsto neliečiamybė ir susirašinėjimo slaptumas, ir kad valstybės institucijos neturi teisės apriboti naudojimosi šiomis teisėmis, išskyrus įstatymų nustatytus atvejus ir, kai tai būtina demokratinėje visuomenėje valstybės saugumo, visuomenės saugos ar šalies ekonominės gerovės interesams, siekiant užkirsti kelią viešos tvarkos pažeidimams ar nusikaltimams, taip pat žmonių sveikatai ar moralei arba kitų asmenų teisėms ir laisvėms apsaugoti.

Pasak Petraitytės (2011), šios garantijos turinys plačiau yra atskleidžiamas Europos žmogaus teisių teismo sprendimuose. Teismas yra pažymėjęs, kad privataus gyvenimo sąvoka apima asmenybės raidą asmens santykiuose su kitais asmenimis, asmens fizinį ir moralinį vientisumą, seksualinę orientaciją ir lytinį gyvenimą, informaciją apie asmenį ir kita.

Nagrinėjant asmens teisės į privatų gyvenimą pripažinimą Lietuvoje, svarbus žingsnis buvo žengtas 1992 metais, priėmus Lietuvos Respublikos Konstituciją (toliau – LRK). 22 antrajame LRK straipsnyje buvo įtvirtinta, kad:

- Žmogaus privatus gyvenimas neliečiamas.
- Asmens susirašinėjimas, pokalbiai telefonu, telegrafo pranešimai ir kitoks susižinojimas neliečiami.
- Informacija apie privatų asmens gyvenimą gali būti renkama tik motyvuotu teismo sprendimu ir tik pagal įstatymą.
- Įstatymas ir teismas saugo, kad niekas nepatirtų savavališko ar neteisėto kišimosi į jo asmeninį ir šeimyninį gyvenimą, kėsinimosi į jo garbę ir orumą (Lietuvos Respublikos Konstitucija, 1992).

Analizuojant tiek įvairiuose teisės aktuose įtvirtintas, tiek mokslininkų plėtojamas teisės į privatų gyvenimą sampratas matyti, jog viena iš asmens teisės į privatų gyvenimą sudedamųjų dalių yra informacijos apie asmenį apsauga. Yra įprasta šią informaciją vadinti **asmens duomenimis**. Galima teigti, kad asmens duomenų apsauga yra neatsiejamas teisės į privatų gyvenimą elementas.

Siekiant apsaugoti fizinių asmenų pagrindines teises ir laisves, o ypač jų privatumo teisę **tvarkant asmens duomenis**, bei nevaržomo ir nedraudžiamo laisvo asmens duomenų judėjimo tarp valstybių narių dėl priežasčių, susijusių su apsauga, 1995 metais spalio 24 dieną buvo priimta Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (toliau - direktyva 95/46/EB) (Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, 1995).

Siekiant sureguliuoti asmens duomenų tvarkymą Lietuvoje, o kartu užtikrinti šių duomenų apsaugą, 1996 metais buvo priimtas Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymas. Pažymėtina, kad šio įstatymo nuostatos buvo suformuluotos į Lietuvos nacionalinę teisę perkeliant didžiąją dalį 1995 metais patvirtintos Duomenų apsaugos direktyvos 95/46/EB nuostatų. Šis įstatymas reguliuoja santykius, atsirandančius renkant, kaupiant, apdorojant, saugant, naudojant ir teikiant duomenis apie fizinius asmenis valstybės kompiuterizuotosioms informacinėms sistemoms, tarp jų ir valstybiniams registrams. Įstatymo tikslas – nustatyti duomenų subjektų teises ir šių teisių apsaugos tvarką, teisių į duomenis bei duomenų apsaugos garantijas tvarkant asmens duomenis informacinėse sistemose (Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymas, 1996). Siekiant įtvirtinti

visus pakeitimus, susijusius su BDAR įgyvendinimu ir vykdymu šalyje, šis įstatymas paskutinį kartą buvo atnaujintas 2018 metų birželio mėnesį, vėluojant tai atlikti iki BDAR įsigaliojimo. Anot Cvilikos ir Šlapimaitės (2015), „Duomenų apsaugos direktyvos rengėjai vylėsi sukurti dokumentą, įtvirtinantį ilgaamžį asmens duomenų apsaugos režimą. Vis dėlto duomenų apsaugos režimui būdinga duomenų subjektų ir duomenų valdytojų interesų pusiausvyra nusistovi socialinėje tikrovėje, o ne formaliose teisės normose“. Dėl šios priežasties praėjus beveik dvidešimčiai metų po priėmimo, 2012 metais, Europos Komisija revizavo Duomenų apsaugos direktyvą mėgindama statutinės teisės įrankiais apdoroti neapibrėžtą socialinę realybę (Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation, 2012). Šis pasiūlymas buvo esminės asmens duomenų apsaugos reformos pradžia. Kaip jau minėta anksčiau, 2016 metais buvo priimtas BDAR, o pats teisės aktas buvo pradėtas taikyti 2018 metais. Kaip teigia Ferrara, P. ir Spoto, F. (2018), per pastaruosius dešimtmečius Europoje įvairios šalys patvirtino ir vykdė daugelį skirtingų taisyklių, susijusių su asmens duomenų apsauga. ES BDAR yra pripažįstama kaip pirmoji pastanga suvienodinti šias skirtingas taisykles ir įstatymus.

Pastaraisiais dešimtmečiais yra matomas suaktyvėjęs visuomenės susirūpinimas asmens tapatumu, privatumu bei duomenų saugumu internete. Kaip matyti iš atliktos teisės į privatumą ir asmens duomenų apsaugos koncepcijos analizės, asmens duomenų samprata išgyvena reikšmingus pokyčius. Analizuojant regioninius ir nacionalinius juridinius dokumentus matyti, kad asmens duomenų sąvokos samprata kito:

1 lentelė. Asmens duomenų sąvokos apibrėžimai

	Asmens duomenų sąvoka	Šaltinis, metai
1.	**Asmens duomenys** reiškia bet kurią informaciją, susijusią su asmeniu (duomenų subjektu), kurio tapatybė yra nustatyta arba gali būti nustatyta; asmuo, kurio tapatybė gali būti nustatyta, yra tas asmuo, kurio tapatybė gali būti nustatyta tiesiogiai ar netiesiogiai, ypač pasinaudojus nurodytu asmens identifikavimo kodu arba vienu ar keliais to asmens fizinei, fiziologinei, protinei, ekonominei, kultūrinei ar socialinei tapatybei būdingais veiksniais.	1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (1995)
2.	**Asmens duomenys** – duomenys apie konkretų arba iš duomenų nustatomą fizinį asmenį, jo dalykinius santykius ir išvados apie asmenį, padarytos remiantis šiais duomenimis.	Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymas (1996)

1 lentelės tęsinys

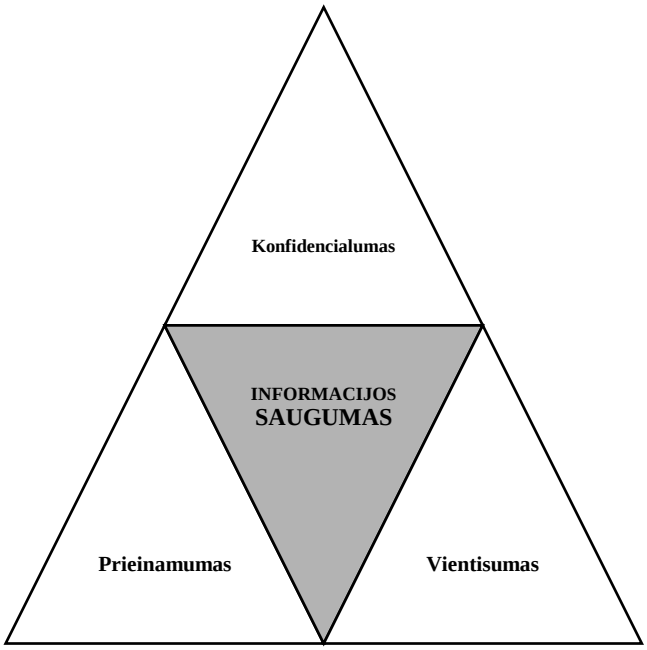
	Asmens duomenų sąvoka	Šaltinis, metai
3.	**Asmens duomenys** – bet kuri informacija, susijusi su fiziniu asmeniu – duomenų subjektu, kurio tapatybė yra žinoma arba gali būti tiesiogiai ar netiesiogiai nustatyta pasinaudojant tokiais duomenimis kaip asmens kodas, vienas arba keli asmeniui būdingi fizinio, fiziologinio, psichologinio, ekonominio, kultūrinio ar socialinio pobūdžio požymiai.	Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas (2000)
4.	**Asmens duomenys** – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (duomenų subjektas); fizinis asmuo, kurio tapatybę galima nustatyti, yra asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti, visų pirma pagal identifikatorių, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius.	Europos parlamento ir tarybos reglamentas (ES) 2016/679 (Bendrasis duomenų apsaugos reglamentas) (2016)

Šaltinis: parengta autorės, remiantis išnagrinėtais juridiniais dokumentais

Iš pateiktos lentelės matyti, kad asmens duomenų sąvoka plačiausiai yra apibrėžiama BDAR. Sąvokos apibrėžtis BDAR, palyginti su sąvokos apibrėžtimi Duomenų apsaugos direktyvoje, yra papildyta šiais informacijos apie fizinį asmenį nustatymo požymiais: asmens vardas ir pavardė, asmens buvimo vietos duomenys, interneto identifikatorius, asmens genetinės ar psichinės tapatybės požymiai. Apibrėžiant asmens duomenų sąvoką Asmens duomenų teisinės apsaugos įstatyme, kuris buvo kuriamas remiantis direktyva 95/46/EB, buvo pasirinktas gana trumpas ir neišsamus (palyginti su direktyva 95/46/EB) sąvokos apibrėžimas: duomenys apie konkretų asmenį ir išvados apie asmenį, padarytos remiantis tais duomenimis. Pasak Štareikės, E. ir Kausteklytės-Tunkevičienės, S. (2018), įvertinus teisės doktrinoje pateikiamus apibrėžimus, duomenų apsaugos teisė suprantama kaip teisės sritis, kuri skirta apsaugoti fizinius asmenis nuo žalos, kuri gali kilti dėl tam tikros informacijos apie juos tvarkymo.

Yra būtina pabrėžti, kad visa informacija apie asmenį (asmens duomenys) buvo apibrėžiama tam, kad būtų užtikrintas jų saugumas, ir būtų nustatyta, kurie asmens duomenų komponentai yra teisiškai reguliuojami. Viena iš priežasčių, dėl kurios buvo priimtas BDAR, buvo įvardinta kaip būtinybė užtikrinti tinklo ir informacijos saugumą atliekant asmens duomenų tvarkymą, tai yra užtikrinti tinklo ar informacinės sistemos nustatyto patikimumo laipsnio atsparumą trikdžiams arba neteisėtiems ar tyčiniams veiksmams, kuriais pažeidžiamas saugomų ar persiunčiamų **asmens duomenų prieinamumas**, **autentiškumas, vientisumas ir konfidencialumas** (BDAR, 2016).

Prieinamumas (angl. availability), vientisumas (angl. integrity) ir konfidencialumas (angl. confidentiality) yra trys pagrindiniai informacijos saugumo tikslai (CIA triada):



Šaltinis: parengta autorės, remiantis išanalizuota moksline literatūra

2 pav. CIA triada: informacijos saugumo valdymo modelis

- **Konfidencialumas** suprantamas kaip informacijos slaptumas, tai yra, kad tik įgalioti vartotojai turėtų galimybę prieiti prie informacijos ar ją modifikuoti.
- **Vientisumas -** informacija ir jos šaltinis turi būti apsaugoti nuo bet kokio klaidingo ar nesankcionuoto pakeitimo.
- **Prieinamumas -** įgaliotiems vartotojams turėtų būti suteikta galimybė pasiekti informaciją, kai tik reikia (Fruhlinger, J., 2020).

Skirtingai nuo daugelio pamatinių informacijos saugumo modelių – koncepcijų, panašu, kad būtent CIA triada neturi vieno autoriaus ar šalininko. CIA triada pirmą kartą buvo paminėta NIST (National Institute of Standards and Technology) publikacijoje „Post-processing audit tools and techniques“ 1977 metais, kur dar tuomet ji buvo įvardijama kaip „kompiuterių sauga“ – sistemos duomenų ir išteklių apsauga nuo atsitiktinių ir apgalvotų grėsmių konfidencialumui, vientisumui ir prieinamumui (Neumann, A. J., Statland, N. ir Webb, R. D. (1977), Post-processing audit tools and techniques). Vėliau, remiantis šiais pagrindiniais trimis tikslais, daugiau nei dvidešimtmetį buvo ir vis dar yra analizuojama bei plėtojama informacijos saugumo apibrėžtis.

Informacijos saugumas yra neatsiejama asmens duomenų apsaugos dalis, tad kiekvienai organizacijai yra labai svarbu įgyvendinti tinkamas tiek technines, tiek organizacines priemones, kad būtų išvengta galimų duomenų apsaugos pažeidimų, kurie šiuo metu yra teisiškai reguliuojami pagrinde remiantis BDAR. Viena iš organizacinių asmens duomenų apsaugos priemonių ir yra BDAR strategijos

kūrimas bei taikymas organizacijoje, tad toliau šiame darbe ir yra nagrinėjami esminiai reglamento aspektai bei strategijos taikymo koncepcija.

1.2. BDAR juridinių aspektų analizė

2018 metai, be abejo, buvo pagrindiniai privatumo metai - ne tik ES, bet ir visame pasaulyje dėl BDAR teritorinės taikymo srities. Daugelis šalių praneša apie padidėjusį privatumo reguliavimo institucijoms teikiamų skundų ir jų (institucijų) nustatytų asmens duomenų apsaugos pažeidimų skaičių. Asmenys, kurių asmens duomenys yra valdomi ar tvarkomi, bei organizacijos, valdančios ar tvarkančios klientų asmens duomenis, vis labiau suvokia asmens duomenų apsaugos užtikrinimo svarbą, tačiau klausimai, susiję su asmens duomenų apsauga ir įvairiais pažeidimais, ir toliau skamba antraštėse.

Bendruoju duomenų apsaugos reglamentu buvo ir yra siekiama užbaigti kurti laisvės, saugumo ir teisingumo erdvę ir ekonominę sąjungą, skatinti ekonominę ir socialinę pažangą, stiprinti valstybių narių ekonomiką ir siekti jų ekonomikos konvergencijos vidaus rinkoje ir fizinių asmenų gerovės. Nors direktyvos 95/46/EB, galiojusios iki BDAR įgyvendinimo, tikslai ir principai buvo ir tebėra laikomi pagrįstais, matyti, kad ši direktyva neužkirto kelio suskaidytam ir skirtingam asmens duomenų apsaugos įgyvendinimui atskirose šalyse, teisiniam netikrumui ar plačiai paplitusiai viešajai nuomonei, kad fizinių asmenų apsaugai kyla didelių pavojų. Sparti technologinė plėtra ir globalizacija lėmė ženklų asmens duomenų rinkimo ir keitimosi jais masto išaugimą, o to pasėkoje, atsirado nemažai naujų sunkumų, susijusių su asmens duomenų apsauga. Priimant šį reglamentą buvo siekiama užtikrinti, kad fizinių asmenų duomenys būtų tvarkomi nuosekliai ir laikantis vienodų taisyklių.

BDAR turi **materialinę** ir **teritorinę** taikymo sritis:

- Pagal **materialinę taikymo sritį** reglamentas taikomas asmens duomenų tvarkymui, visiškai arba iš dalies atliekamam automatizuotomis priemonėmis, ir asmens duomenų, kurie sudaro susisteminto rinkinio dalį ar yra skirti ją sudaryti, tvarkymui ne automatizuotomis priemonėmis.
- Pagal **teritorinę taikymo sritį** reglamentas taikomas asmens duomenų tvarkymui, kai asmens duomenis Sąjungoje tvarko duomenų valdytojo arba duomenų tvarkytojo buveinė, vykdydama savo veiklą, neatsižvelgiant į tai, ar duomenys tvarkomi Sąjungoje, ar ne (Europos parlamento ir tarybos reglamentas (ES) 2016/679).

Pagrindiniai **BDAR** išskiriami su asmens duomenų tvarkymu susiję **principai** yra šie:

2 lentelė. Asmens duomenų tvarkymo principai

	Principas	Principo esmė
1.	**Teisėtumo, sąžiningumo ir skaidrumo**	Duomenų subjekto atžvilgiu duomenys yra tvarkomi teisėtu, sąžiningu ir skaidriu būdu.
2.	**Tikslo apribojimo**	Duomenys yra renkami nustatytais, aiškiai apibrėžtais bei teisėtais tikslais ir toliau netvarkomi su tais tikslais nesuderinamu būdu.
3.	**Duomenų kiekio mažinimo**	Yra renkami adekvatūs, tinkami ir tik tokie duomenys, kurių reikia siekiant tikslų, dėl kurių jie tvarkomi.
4.	**Tikslumo**	Renkami tikslūs duomenys ir prireikus jie yra atnaujinami; turi būti imamasi visų pagrįstų priemonių užtikrinti, kad asmens duomenys, kurie nėra tikslūs, atsižvelgiant į jų tvarkymo tikslus, būtų nedelsiant ištrinami arba ištaisomi.
5.	**Saugojimo trukmės apribojimo**	Duomenys yra laikomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, nei tai yra būtina tais tikslais, kuriais asmens duomenys yra tvarkomi; asmens duomenis galima saugoti ilgesnius laikotarpius, jeigu asmens duomenys bus tvarkomi tik archyvavimo tikslais viešojo intereso labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais pagal BDAR 89 straipsnio 1 dalį, įgyvendinus atitinkamas technines ir organizacines priemones, kurių reikalaujama šiuo reglamentu siekiant apsaugoti duomenų subjekto teises ir laisves.
6.	**Vientisumo ir konfidencialumo**	Duomenys yra tvarkomi tokiu būdu, kad taikant atitinkamas technines ar organizacines priemones būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo.

Šaltinis: parengta autorės, remiantis išnagrinėtais juridiniais dokumentais

Lūkestis, kad organizacijos yra teisingos, skaidrios ir teisėtai tvarko asmens duomenis, galiausiai veda link organizacijų **atskaitomybės**, kuri yra jų savidrausmės pagrindas. Atsakomybė įrodyti, kad laikomasi pagrindinių BDAR principų, visada tenka duomenų valdytojui. Tai reiškia, kad organizacijos turėtų būti atsakingos už veiksmus, susijusius su asmens duomenų tvarkymu, prisiimti atsakomybę už tai, ką daro, ir pateikti visų sprendimų, priimtų asmens duomenų tvarkymo kontekste, įrodymus.

Pasak Falk, T.T. (2016), „duomenų privatumo atskaitomybė organizacijoje yra įtvirtinta tada, kai yra taikomi šie trys komponentai:

- **Atsakomybė:** organizacijoje yra vykdoma privatumo valdymo veikla ir ji yra nuolat palaikoma.
- **Nuosavybė:** privatumo valdymo veikla yra įdiegta visoje organizacijoje (įskaitant kiekvieną organizacijos atliekamą funkciją ar verslo padalinį, kuris tvarko asmens duomenis).
- **Įrodymai:** pateikiama privatumo valdymo veiklos dokumentacija. Šie dokumentai gali būti naudojami kaip atskaitomybės ir atitikties įrodymai.“

Apibendrinant galima teigti, kad BDAR reikalavimai yra pagrįsti principais. Šie principai yra sutelkti į atskaitomybės ir teisėto, sąžiningo bei skaidraus duomenų tvarkymo sąvokas. Pabrėžtina, kad visuomet yra svarbu užtikrinti asmens duomenų vientisumą ir konfidencialumą.

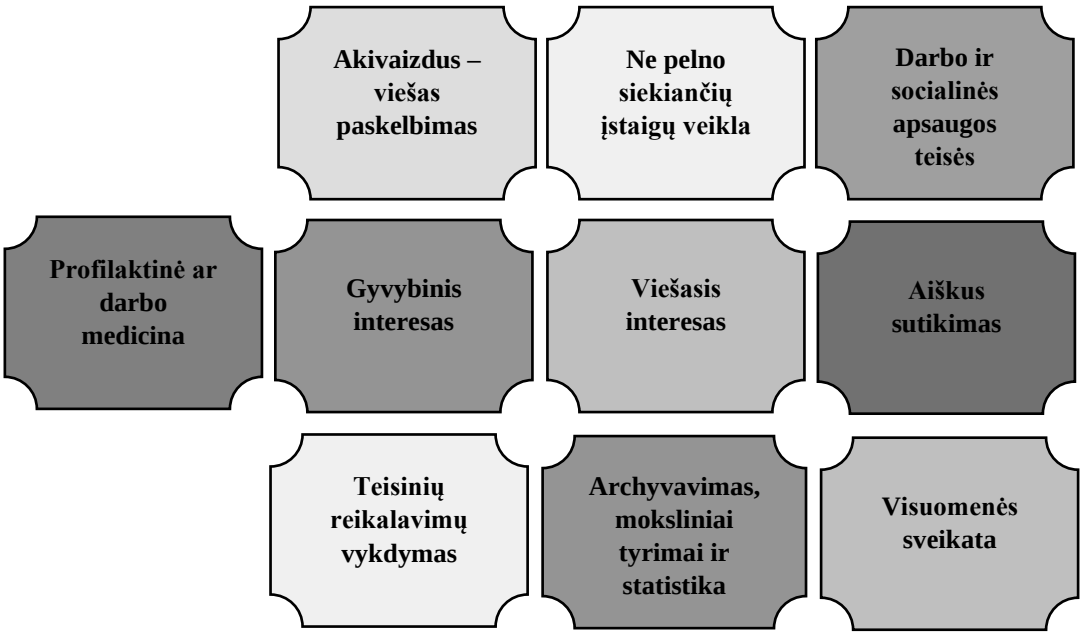
Analizuojant esmines BDAR nuostatas, yra būtina pabrėžti, kad asmens duomenų tvarkymas yra teisėtas tik tuo atveju, jeigu taikoma bent viena iš šių sąlygų, ir tik tokiu mastu, kokiu ji yra taikoma:

- duomenų **subjektas davė sutikimą**, kad jo asmens duomenys būtų tvarkomi vienu ar keliais konkrečiais tikslais;
- tvarkyti duomenis būtina **siekiant įvykdyti sutartį**, kurios šalis yra duomenų subjektas, arba siekiant imtis veiksmų duomenų subjekto prašymu prieš sudarant sutartį;
- tvarkyti duomenis būtina, kad būtų įvykdyta duomenų valdytojui **taikoma teisinė prievolė**;
- tvarkyti duomenis būtina **siekiant apsaugoti gyvybinius duomenų subjekto** ar kito fizinio asmens **interesus**;
- tvarkyti duomenis būtina **siekiant atlikti užduotį, vykdomą viešojo intereso labui** arba vykdant duomenų valdytojui **pavestas viešosios valdžios funkcijas**;
- tvarkyti duomenis būtina **siekiant teisėtų duomenų valdytojo arba trečiosios šalies interesų**, išskyrus atvejus, kai tokie duomenų subjekto interesai arba pagrindinės teisės ir laisvės, dėl kurių būtina užtikrinti asmens duomenų apsaugą, yra už juos viršesni, ypač kai duomenų subjektas yra vaikas. Šis punktas netaikomas duomenų tvarkymui, kurį valdžios institucijos atlieka vykdydamos savo užduotis (Europos parlamento ir tarybos reglamentas (ES) 2016/679).

Yra tam tikros rūšies duomenys, kuriuos BDAR laiko neskelbtinais asmens duomenimis, todėl juos priskiria **specialiajai asmens duomenų kategorijai**. Draudžiama tvarkyti asmens duomenis, atskleidžiančius:

- rasinę ar etninę kilmę;
- politines pažiūras;
- religinius ar filosofinius įsitikinimus;
- narystę profesinėse sąjungose;
- genetinius ar biometrinius duomenis, siekiant konkrečiai nustatyti fizinio asmens tapatybę;
- sveikatos duomenis arba duomenis apie fizinio asmens lytinį gyvenimą ir lytinę orientaciją (Europos parlamento ir tarybos reglamentas (ES) 2016/679).

Draudimas tvarkyti aukščiau išvardintus specialiajai asmens duomenų kategorijai priskiriamus duomenis yra netaikomas, jei duomenų tvarkymas yra būtinas dėl bent vienos iš šių priežasčių (sąlygų):



Šaltinis: parengta autorės, remiantis „Sensitive personal data - special category under the GDPR", (2020)

3 pav. Specialių kategorijų asmens duomenų tvarkymo išimtys

Ne visa informacija yra laikoma asmens duomenimis, tad BDAR yra apibrėžiama, kas yra laikoma asmens duomenimis: bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti. Tai reiškia, kad asmens duomenys leidžia tiesiogiai ar netiesiogiai identifikuoti duomenų subjektą pagal vardą, identifikavimo numerį, vietos duomenis, internetinį identifikatorių arba to fizinio asmens fizinę, fiziologinę, genetinę, psichinę, ekonominę, kultūrinę ar socialinę tapatybę. Terminas „asmens duomenys" yra vartojamas gana plačiai ir gali apimti mažiau specifinę informaciją, pavyzdžiui, IP adresą.

Anot Irwin, L. (2019), gana dažnai tarp organizacijų pasitaikantis neteisingas BDAR reikalavimų vykdymo supratimas yra tai, jog organizacijos mano, kad norint tvarkyti asmens duomenis yra būtina gauti duomenų subjekto sutikimą, o griežtos taisyklės, apibrėžiančios teisėtą duomenų tvarkymo sutikimo gavimą, rodo, kad šis duomenų tvarkymo pagrindas paprastai yra mažiausiai organizacijų mėgiamas būdas. Tiesą sakant, duomenų subjekto sutikimas yra tik vienas iš šešių aukščiau paminėtų teisėtų asmens duomenų tvarkymo pagrindų, tačiau kartais duomenų subjekto sutikimas yra tinkamiausias pagrindas tvarkyti asmens duomenis, tad organizacijos privalo žinoti, kada joms yra reikalinga gauti duomenų subjekto aiškų sutikimą tvarkyti neskelbtinus asmens duomenis. Duomenų apsaugos specialistas Irwin, L. (2019) teigia, kad „bet kuri organizacija, neskyrusi laiko išsamiai

išnagrinėti savo atitikties BDAR reikalavimams, gali nukentėti. Tai gali sukelti ilgalaikę žalą, tokią kaip veiklos apribojimus, baudas už BDAR pažeidimus, blogą reputaciją ir klientų praradimą".

Plačiau kalbant apie asmens duomenų tvarkymą remiantis duomenų subjekto sutikimu, yra verta paminėti, kad duomenų valdytojas privalo galėti įrodyti, kad duomenų subjektas yra davęs minimą sutikimą tvarkyti jo asmens duomenis. BDAR yra apibrėžiamos **sutikimo sąlygos**:

SUTIKIMO SĄLYGOS	Prašymas duoti sutikimą yra aiškiai atskirtas nuo kitų klausimų
	Prašymas duoti sutikimą yra pateikiamas suprantama ir lengvai prieinama forma
	Prašymas duoti sutikimą yra pateikiamas aiškia ir paprasta kalba

Šaltinis: parengta autorės, remiantis „Europos parlamento ir tarybos reglamentas (ES) 2016/679"

4 pav. Sutikimo tvarkyti asmens duomenis sąlygos

Išskirtinės sąlygos sutikimui yra taikomos tuo atveju, kai informacinės visuomenės paslaugos yra siūlomos vaikui. BDAR įtvirtintuose reikalavimuose yra nurodoma, kad „vaiko asmens duomenų tvarkymas yra teisėtas tik tuo atveju, jei vaikas yra bent 16 metų amžiaus. Kai vaikas yra jaunesnis nei 16 metų, toks tvarkymas yra teisėtas tik tuo atveju, jeigu tą sutikimą davė arba tvarkyti duomenis leido vaiko tėvų pareigų turėtojas, ir tik tokiu mastu, kokiu duotas toks sutikimas ar leidimas" (Europos parlamento ir tarybos reglamentas (ES) 2016/679).

Toliau kalbant apie duomenų subjekto sutikimą tvarkyti jo asmens duomenis, yra verta paminėti ir pačių duomenų subjektų klaidingą supratimą apie BDAR įtvirtintų reikalavimų vykdymą. Vienas iš pavyzdžių yra Lietuvos Valstybinės duomenų apsaugos inspekcijos (toliau - VDAI) parengtoje metodinėje informacijoje apie dažniausiai pasitaikančius atvejus, kai VDAI pateikti skundai pripažįstami nepagrįstais, minimas atvejis, jog vienas iš dažniausių atvejų, kai yra skundžiamasi VDAI dėl asmens duomenų apsaugos pažeidimų, yra skundai dėl gaunamos **tiesioginės rinkodaros**. Nemaža dalis besikreipiančių asmenų klaidingai mano, kad po 2018 metų gegužės 25 dienos, įsigaliojus BDAR, tiesioginės rinkodaros siuntėjai turi pakartotinai prašyti asmenų jų sutikimo siųsti tiesioginės rinkodaros pasiūlymus. Nuo 2018 metų gegužės 25 dienos Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme (toliau - ADTAĮ) nebeliko specialaus tiesioginės rinkodaros reguliavimo, todėl tiesioginei rinkodarai taikomi bendri asmens duomenų tvarkymo reikalavimai, numatyti BDAR. Tiesioginę rinkodarą, vykdomą elektroninių ryšių priemonėmis, reguliuoja ir Lietuvos Respublikos elektroninių ryšių įstatymas (toliau - ERĮ), kurio nuostatos dėl tiesioginės rinkodaros nebuvo pakeistos, pradėjus taikyti BDAR. Vadovaujantis ERĮ 69 straipsnio 1 dalimi, naudoti elektroninių ryšių paslaugas, įskaitant elektroninio pašto pranešimų siuntimą, tiesioginės rinkodaros tikslu leidžiama tik gavus

išankstinį abonento ar registruoto elektroninių ryšių paslaugų naudotojo sutikimą. Pažymėtina, kad BDAR nenumato pareigos duomenų valdytojui pakartotinai gauti duomenų subjekto sutikimą tvarkyti jo asmens duomenis tiesioginės rinkodaros tikslais, jei toks sutikimas jau buvo duotas iki BDAR įsigaliojimo (Dažniausiai pasitaikantys atvejai, kai Valstybinei duomenų apsaugos inspekcijai pateikti skundai pripažįstami nepagrįstais, VDAI, 2019).

Duomenų subjekto asmeninių duomenų tvarkymas neapsiriboja vien tik duomenų subjekto sutikimo tvarkyti duomenis gavimu. Duomenų subjektas turi ir kitų teisių, susijusių su jo asmeninių duomenų tvarkymu:

DUOMENŲ SUBJEKTO TEISĖS	Teisė susipažinti su duomenimis
	Teisė reikalauti ištaisyti duomenis
	Teisė reikalauti ištrinti duomenis („teisė būti pamirštam“)
	Teisė apriboti duomenų tvarkymą
	Teisė į duomenų perkeliamumą
	Teisė nesutikti

Šaltinis: parengta autorės, remiantis „Europos parlamento ir tarybos reglamentas (ES) 2016/679”

5 pav. Duomenų subjekto teisės

Duomenų valdytojui pateikus patvirtinimą, kad su duomenų subjektu susiję duomenys yra tvarkomi, duomenų subjektas turi teisę susipažinti su tvarkomais asmeniniais duomenimis ir kita informacija, tokia kaip: duomenų tvarkymo tikslai, asmens duomenų kategorijos, duomenų gavėjai, numatomas asmens duomenų saugojimo laikotarpis, informacija apie duomenų gavimo šaltinius, kai duomenys yra renkami ne iš paties duomenų subjekto ir kita su asmens duomenų valdymu susijusi informacija. Susipažinus su aukščiau išvardinta informacija ir nustačius, kad ji yra neteisinga ar neišsami, duomenų subjektas turi teisę reikalauti duomenų valdytojo nepagrįstai nedelsiant ištaisyti netikslius su duomenų subjektu susijusius duomenis ar juos papildyti, jei jie yra neišsamūs. Duomenų subjektui užginčijus duomenų tikslumą ar nustačius, kad duomenų tvarkymas yra neteisėtas, atsiranda duomenų subjekto teisė apriboti su juo susijusių duomenų tvarkymą. Ribojimas tvarkyti asmens duomenis yra taikomas tol, kol duomenų valdytojas patikrina asmens duomenų tikslumą, ar esant neteisėtam duomenų tvarkymui duomenų subjektas nesutinka su jų ištrynimu, o vietoje to reikalauja apriboti tų duomenų naudojimą. Duomenų subjektas turi teisę ne tik pats gauti su juo susijusius asmens duomenis iš duomenų valdytojo įprastai naudojamu ar kompiuterio skaitomu formatu, bet ir teisę persiųsti iš duomenų valdytojo gautus asmens duomenis kitam duomenų valdytojui, kai tai yra techniškai įmanoma. Duomenų subjektas taip pat turi teisę nesutikti, kad su juo susiję duomenys būtų tvarkomi. Tokiu atveju duomenų valdytojas nebetvarko asmens duomenų, išskyrus atvejus, kai duomenų

valdytojas įrodo, kad duomenys tvarkomi dėl įtikinamų teisėtų priežasčių, kurios yra viršesnės už duomenų subjekto interesus, teises ir laisves, arba siekiant pareikšti, vykdyti ar apginti teisinius reikalavimus. Taip pat duomenų subjektas turi teisę, kad jau nebūtų taikomas tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiamas sprendimas, dėl kurio jam kyla teisinės pasekmės arba kuris jam panašiu būdu daro didelį poveikį. Apibendrinant, duomenų subjekto teisės, kuriomis duomenų subjektai gali naudotis, yra tos pačios kaip ir pagal Direktyvą 95/46/EB, tačiau yra keli patobulinimai. Teisė į duomenų perkeliamumą yra nauja. Tai yra patobulinta duomenų subjekto teisės susipažinti su savo asmens duomenimis forma.

Paskutinė iš aukščiau paminėtų duomenų subjekto teisių – teisė reikalauti ištrinti duomenis ar kitaip „teisė būti pamirštam“ - šiai dienai yra gana dažnai girdima ir duomenų subjektų naudojama teisė. Pagal BDAR įtvirtintus reikalavimus, duomenų subjektas turi teisę reikalauti, kad duomenų valdytojas nepagrįstai nedelsdamas ištrintų su juo susijusius asmens duomenis, jei tai galima pagrįsti viena iš šių priežasčių:

- asmens duomenys nebėra reikalingi, kad būtų pasiekti tikslai, kuriais jie buvo renkami arba kitaip tvarkomi;
- asmens duomenų subjektas atšaukia sutikimą, kuriuo grindžiamas duomenų tvarkymas, ir nėra jokio kito teisinio pagrindo tvarkyti duomenis;
- asmens duomenų subjektas nesutinka su duomenų tvarkymu ir nėra viršesnių teisėtų priežasčių tvarkyti duomenis;
- asmens duomenys buvo tvarkomi neteisėtai;
- asmens duomenys turi būti ištrinti laikantis Sąjungos arba valstybės narės teisėje, kuri taikoma duomenų valdytojui, nustatytos teisinės prievolės;
- asmens duomenys buvo surinkti apie jaunesnį nei 16 metų vaiką informacinės visuomenės paslaugų siūlymo kontekste (Europos parlamento ir tarybos reglamentas (ES) 2016/679).

„Teise būti pamirštam” Europos Sąjungoje buvo galima pasinaudoti dar prieš šią teisę įtvirtinant BDAR. Kalbant apie šios teisės panaudojimo galimybės atsiradimą ES, būtina aptarti Europos Sąjungos Teisingumo Teismo (toliau – ESTT) vaidmenį ir indėlį šiame procese.

2010 metais Ispanijos pilietis M. Costeja González kreipėsi į Ispanijos duomenų apsaugos agentūrą (toliau – AEPD) su skundu dėl La Vanguardia dienraščio ir Google Spain bei Google Inc. veiksmų. M. Costeja González nurodė, kad atlikus M. Costeja González asmenvardžio paiešką per Google grupės paieškos variklį (toliau – Google Search), kaip paieškos rezultatas yra pateikiamos nuorodos į 1998 metų sausio ir kovo mėnesių. dienraščio La Vanguardia puslapius, kuriuose skelbiama informacija apie areštuoto nekilnojamojo turto pardavimo aukcioną, vykdytą išieškant M. Costeja González nesumokėtą socialinės apsaugos srities skolą. Skunde M. Costeja González prašė įpareigoti

La Vanguardia arba panaikinti šiuos puslapius, arba pakeisti (kad juose nebeliktų jo asmens duomenų), arba panaudoti tam tikrus paieškos variklių teikiamus šių duomenų apsaugos įrankius. M. Costeja González taip pat prašė įpareigoti Google Spain arba Google Inc. pašalinti arba paslėpti jo asmens duomenis, kad šie nebūtų pateikiami paieškos rezultatų sąraše ir nuorodose į La Vanguardia. M. Costeja González tvirtino, kad visa skola, dėl kurios jam taikytas areštas, sumokėta jau prieš daug metų ir nebėra poreikio tai toliau minėti. (Europos Sąjungos teisingumo teismo praktikos apžvalga (2014 m. gegužės 1d. – 2014 m. birželio 30 d.)). Ieškovas, prašydamas pašalinti su juo susijusius asmens duomenis iš internetinės erdvės, naudojosi Direktyvos 95/46/EB suteikiama teise duomenų subjektui prašyti pašalinti „neadekvačią, ne(be)reikšmingą arba perteklinę“ informaciją.

AEPD išnagrinėjus skundą ir Google Spain bei Google Inc. nesutikus su įpareigojimu imtis priemonių, kad ieškovo skunde minimi duomenys būtų pašalinti iš rodyklės ir padaryti neprieinami, buvo kreiptasi į ESTT. ESTT įpareigojo paieškos variklius, tokius kaip „Google“, „Yahoo“ ar „Bing“, tenkinant fizinio asmens prašymą iš rezultatų sąrašo, rodomo atlikus paiešką pagal jo vardą ir pavardę, ištrinti nuorodas į tinklalapius, kuriuose pateikiami su juo susiję asmens duomenys, jei ši informacija, pasak ESTT, tapo „neadekvati, ne(be)reikšminga arba perteklinė“.

Anot Tamavičiūtės (2019), ESTT, įtvirtindamas asmens teisę reikalauti pašalinti savo asmeninius duomenis internete, atsižvelgė į radikalius išmaniųjų technologijų ir interneto vystymosi, visuomenės bendravimo pokyčius. Suteikdamas asmenims galimybę „būti pamirštiems“ ir kontroliuoti savo asmens duomenų naudojimą, ESTT siekė pakeisti paieškos variklių, tokių kaip „Google“, „Yahoo“ ar „Bing“, požiūrį į asmens privatumą ir bent iš dalies grąžino asmenims jų privatumo kontrolę.

Nepaisant to, asmens duomenų apsaugos specialistai ESTT sprendime įžvelgė ir spragų, tokių kaip:

- paieškos varikliams suteikta teisė savo nuožiūra vertinti kiekvieną atvejį atskirai, tai yra nuspręsti, kokia informacija yra laikoma neadekvačia, ne(be)reikšminga ar pertekline;
- teisės reikalauti ištrinti duomenis taikymas teritoriniu atžvilgiu: nėra konkrečiai nurodoma, ar ši teisė privalo būti taikoma lokaliu, regioniniu ar globaliu mastu.

Anot Tamavičiūtės (2019), ESTT eliminavo galimybę „teisę būti pamirštam“ taikyti globaliai – paieškos varikliai privalo pašalinti nuorodas tik iš savo sistemos versijų, apimančių visas valstybes nares, tai yra Europos Sąjungos mastu. Drauge ESTT nurodė, kad „nuorodų pašalinimas iš visų paieškos sistemos versijų nėra draudžiamas“ ir kad valstybės narės priežiūros arba teisminė institucija, atsižvelgdama į nacionalinius pagrindinių teisių apsaugos standartus, išlaiko kompetenciją prireikus įpareigoti paieškų variklį pašalinti nuorodas globaliai, tokiu būdu **atverdamas duris skirtingam asmens duomenų apsaugos standartui** plėtotis atskirose valstybėse narėse.

Apibendrinant galima teigti, kad „teisė būti pamirštam“ nėra absoliuti. Esant viršesnėms teisėtoms priežastims tvarkyti duomenis ar esant teisėtam visuomenės interesui turėti prieigą prie šios informacijos, ši teisė nėra taikoma. Visgi, esant prievolei šią teisę vykdyti, Li, H., Yu, L. ir He, W. (2019) rekomenduoja pagalvoti apie tinkamas priemones tiek teisės „būti pamirštam“, tiek duomenų subjekto teisės susipažinti su tvarkomais duomenimis įgyvendinimui. Organizacijai siekiant patenkinti klientų ar darbuotojų prašymą susipažinti su savo asmens duomenimis ir esant poreikiui efektyviai juos pašalinti iš sistemos gali tekti patobulinti arba iš naujo sukurti savo naudojamas platformas ir sistemas. Pirmiausia, organizacija turi nustatyti visus šaltinius, kurie yra susiję su konkretaus kliento tvarkomais asmens duomenimis: santykių su klientais valdymo sistemos, žmogiškųjų išteklių valdymo sistemos, duomenų bazės ir archyvai. Antra, organizacija turi įdiegti holistinius paieškos įrankius, galinčius ieškoti reikiamos informacijos visose technologijų platformose, sistemose, archyvuose ir architektūrose, kad būtų galima nustatyti ir išgauti asmens duomenis, susijusius su konkrečiu. Be holistinių paieškos įrankių nebus garantijos, kad organizacijos galės užtikrinti, jog visi asmens duomenys, susiję su konkrečiu klientu ar darbuotoju, yra tinkamai tvarkomi ir esant poreikiui bus ištrinti.

Analizuojant BDAR įtvirtintus asmens duomenų apsaugos reikalavimus neišvengiamai yra susiduriama su duomenų valdytojo ir duomenų tvarkytojo sąvokomis. Besiruošiant BDAR įgyvendinimui šalyse, buvo pastebėta, kad organizacijos dažnai painiojo šias sąvokas, kas lėmė ir iki šio lemia klaidas, organizacijoms derintis dėl duomenų tvarkymo taisyklių su verslo partneriais. Visoms organizacijoms yra ypatingai svarbu teisingai nustatyti, kas yra duomenų valdytojas, o kas yra duomenų tvarkytojas verslo santykiuose, ir kokios atsakomybės duomenų apsaugos srityje tenka kiekvienam iš jų.

BDAR šios sąvokos yra apibrėžiamos taip:

Duomenų valdytojas – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuris vienas ar drauge su kitais nustato duomenų tvarkymo tikslus ir priemones; kai tokio duomenų tvarkymo tikslai ir priemonės nustatyti Sąjungos arba valstybės narės teisės, duomenų valdytojas arba konkretūs jo skyrimo kriterijai gali būti nustatyti Sąjungos arba valstybės narės teise (Europos parlamento ir tarybos reglamentas (ES) 2016/679).

BDAR duomenų valdytojo atsakomybė yra apibrėžiama taip: „atsižvelgdamas į duomenų tvarkymo pobūdį, aprėptį, kontekstą bei tikslus, taip pat į įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas įgyvendina tinkamas **technines** ir **organizacines priemones**, kad užtikrintų ir galėtų įrodyti, kad duomenys tvarkomi laikantis šio reglamento. Tos priemonės prireikus peržiūrimos ir atnaujinamos”.

Duomenų tvarkytojas – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri duomenų valdytojo vardu tvarko asmens duomenis (Europos parlamento ir tarybos reglamentas (ES) 2016/679).

Apibendrinant šias dvi sąvokas, galima teigti, kad duomenų valdytojas – tai subjektas, kuris nustato **asmens duomenų tvarkymo tikslus ir priemones**, o tuo tarpu **duomenų tvarkytojas asmens duomenis tvarko duomenų valdytojo vardu**, vadovaudamasis pastarojo nurodymais. Jeigu du ar daugiau duomenų valdytojų duomenų tvarkymo tikslus ir priemones nustato drauge, tuomet tokie subjektai, vadovaujantis BDAR, laikomi **bendraisiais duomenų valdytojais**. Kaip Europos parlamento ir tarybos reglamente (ES) 2016/679 yra nurodoma, „jie (bendrieji duomenų valdytojai) tarpusavio susitarimu skaidriu būdu nustato savo atitinkamą atsakomybę už pagal šį reglamentą nustatytų prievolių, visų pirma susijusių su duomenų subjekto naudojimusi savo teisėmis ir jų atitinkamomis pareigomis pateikti 13 ir 14 straipsniuose nurodytą informaciją, vykdymą, išskyrus atvejus, kai atitinkama duomenų valdytojų atsakomybė yra nustatyta Sąjungos arba valstybės narės teisėje, kuri yra taikoma duomenų valdytojams, ir tokiu mastu, kokiu ji yra nustatyta“.

Iš pirmo žvilgsnio viskas atrodo labai paprasta, tačiau praktika rodo, kad organizacijos labai dažnai klysta vertindamos, kurie jų verslo partneriai bei tiekėjai yra asmens duomenų tvarkytojai, o su kuriais jos veikia yra vertinama kaip bendrųjų duomenų valdytojų. Dėl šios priežasties 2020 metų rugsėjo mėnesį Europos duomenų apsaugos valdyba (toliau - EDAV) paskelbė organizacijoms labai reikšmingas gaires dėl duomenų valdytojo ir duomenų tvarkytojo sąvokos, teigdama, kad: „duomenų valdytojo, bendrojo duomenų valdytojo ir duomenų tvarkytojo sąvokos vaidina ypatingai svarbų vaidmenį taikant BDAR, nes jos nustato, kas bus atsakingas už skirtingų duomenų apsaugos taisyklių laikymąsi ir kaip duomenų subjektai gali naudotis savo teisėmis praktikoje“ (Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 2020).

Yra būtina paminėti, kad šios EDAV paskelbtos gairės nepakeitė nei duomenų tvarkytojo, nei duomenų valdytojo sąvokos ir kriterijų, kuriais vadovaujantis yra atskiriamas duomenų valdytojas nuo duomenų tvarkytojo. Paskelbtose gairėse yra pakankamai aiškiai ir detaliai pateikiami atsakymai į verslo subjektams iki šiol praktikoje kylantiems klausimams, tokiems kaip: kas yra duomenų valdytojas ir tvarkytojas; kodėl svarbu atskirti duomenų valdytoją nuo tvarkytojo; kodėl turi būti pasirašomos papildomos sutartys ir susitarimai su duomenų tvarkytoju; ar yra tinkama standartinė duomenų tvarkytojo naudojama asmens duomenų tvarkymo sutartis; ar privalome sutartyje aptarti visus šiuos techninius reikalavimus. Pirmojoje šių gairių dalyje detaliai aprašomos duomenų valdytojo, bendrų duomenų valdytojų, tvarkytojo ir trečiųjų asmenų ir gavėjų sąvokos bei jų išaiškinimo būdai. Antrojoje dalyje aptariamos teisinės pasekmės, kylančios duomenų valdytojui, bendriems duomenų valdytojams ir duomenų tvarkytojui tvarkant asmens duomenis. Taip pat pakankamai išsamiai aprašomas duomenų valdytojo ir duomenų tvarkytojo tarpusavio ryšys, ypatingas dėmesys atkreipiamas į tinkamo duomenų tvarkytojo pasirinkimą, duomenų tvarkymo sutarties formą, jos turinį, duomenų tvarkytojo teisę nustatyti duomenų tvarkymo tikslus ir priemones.

Šios gairės taps puikiu atspirties tašku, siekiant įsivertinti, ar asmenys, tvarkantys asmens duomenis, teisingai prisiskyrė sau taikytinas atsakomybes ir tinkamai identifikavo ir apsibrėžė santykį su bet kuriomis trečiosiomis šalimis, dalyvaujančiomis asmens duomenų tvarkymo veikloje. Žinoma, kad taikytinos atsakomybės nėra paliekamos tik pačių organizacijų savikontrolei, kadangi visą veiklą, susijusią su asmens duomenų valdymu ar tvarkymu, prižiūri ir atitinkamos valstybinės institucijos.

Duomenų valdytojas yra atsakingas už tinkamų techninių ir organizacinių priemonių įgyvendinimą, kuriomis užtikrinama asmens duomenų apsauga. Duomenų valdytojams ir duomenų tvarkytojams privalu laikytis BDAR 25 straipsnyje numatytų **pritaikytosios ir standartizuotosios duomenų apsaugos** reikalavimų:

- **Pritaikytoji duomenų apsauga** reiškia, kad privatumo ir duomenų apsaugos principai bei duomenų privatumą užtikrinančios technologijos yra įgyvendinamos jau ankstyvuosiuose duomenų tvarkymo operacijų rengimo etapuose.
- **Standartizuotoji duomenų apsauga** reiškia užtikrinimą, kad standartizuotai būtų tvarkomi tik tie asmens duomenys, kurie yra būtini kiekvienam konkrečiam duomenų tvarkymo tikslui. Standartizuotoji duomenų apsauga yra principas, apimantis renkamų duomenų kiekį, tvarkymo mastą, saugojimo laikotarpį ir prieinamumą (Europos parlamento ir tarybos reglamentas (ES) 2016/679).

Anot Bygrave, A. L. (2017), BDAR 25 straipsnio nuostatos yra vienos iš novatoriškiausių ir ambicingiausių naujai reformuoto ES duomenų apsaugos režimo normų. Jos iš esmės yra skirtos informacinių sistemų plėtrai, siekiant užtikrinti, kad per sistemų plėtros vystymosi bei gyvavimo ciklą būtų tinkamai atsižvelgta į su privatumu susijusius interesus.

Lietuvoje yra dvi Bendrojo duomenų apsaugos reglamento priežiūros institucijos. Viena iš jų yra Valstybinė duomenų apsaugos inspekcija (toliau – VDAI). Ši institucija atlieka tiek konsultuojančios, tiek prižiūrinčios institucijos funkcijas. Lietuvos VDAI yra atsakinga už:

- Prevencinius organizacijų tikrinimus;
- Išankstines konsultacijas;
- Auditus;
- Skundų nagrinėjimus;
- Duomenų saugumo pažeidimus;
- Tarptautinį bendradarbiavimą;
- Visuomenės informavimą (Valstybinė duomenų apsaugos inspekcija – Veiklos sritys, 2020).

VDAI taip pat yra atsakinga už nuobaudų skyrimą organizacijoms, nesilaikančioms BDAR įtvirtintų reikalavimų.

Žurnalistų etikos inspektoriaus tarnyba (toliau – ŽEIT) – antroji Bendrojo duomenų apsaugos reglamento priežiūros institucija Lietuvoje. Pagrindinė ŽEIT funkcija – neturtinių žmogaus teisių (garbės ir orumo, privatumo, asmens duomenų apsaugos) gynimas visuomenės informavimo srityje. Pagal Lietuvoje galiojantį teisinį reguliavimą, žurnalistų etikos inspektoriui priskirta funkcija – stebėti, kaip taikomas Reglamentas ir užtikrinti, kad jis būtų taikomas, kai asmens duomenys tvarkomi žurnalistikos tikslais ir akademinės, meninės ar literatūrinės saviraiškos tikslais. (Žurnalistų etikos inspektoriaus tarnybos veiklos sritys, 2021).

Regioniniu mastu už nuoseklų duomenų apsaugos taisyklių taikymą ES yra atsakinga EDAV. EDAV, įsteigta BDAR, yra nepriklausoma Europos institucija, kurią sudaro nacionalinių duomenų apsaugos institucijų atstovai ir Europos duomenų apsaugos priežiūros pareigūnas (toliau - EDAPP). Šios institucijos pagrindinės funkcijos yra:

- teikti bendrąsias gaires (įskaitant gaires, rekomendacijas ir gerąją patirtį), teisės aktams išaiškinti;
- konsultuoti Europos Komisiją bet kokiais klausimais, susijusiais su asmens duomenų apsauga ir naujais siūlomais teisės aktais ES;
- priimti išvadas dėl nuoseklumo tarpvalstybiniais duomenų apsaugos atvejais;
- skatinti nacionalinių priežiūros institucijų bendradarbiavimą ir veiksmingus informacijos ir gerosios patirties mainus. (Europos duomenų apsaugos valdyba. Apie EDAV, 2021)

Nuoseklus BDAR taikymas yra svarbus visoms valstybėms. Kaip jau minėta anksčiau, konceptualizuojant privatumo ir asmens duomenų apsaugos sampratas, Lietuva pavėlavo tinkamai pasirengti reglamento taikymui šalyje laiku nepriėmusi privalomų pagrindinio šiuo metu galiojančio Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo pakeitimų. Dėl šios priežasties Lietuva kartu su dar septyniomis ES šalimis buvo įvardinta kaip šalis, laiku nepasiruošusi naujajame reglamente įtvirtintų reikalavimų vykdymui.

Nepaisant to, kad ES šalys turėjo net 2 metus pasiruošti BDAR įgyvendinimui, Belgija, Bulgarija, Kipras, Čekijos Respublika, Graikija, Vengrija, Slovėnija ir Lietuva laiku neatnaujino savo vidaus teisės aktų, susijusių su asmens duomenų apsauga. Pasak Nielsen (2018), analizavusio ES šalių pasirengimą BDAR įgyvendinimui, vidinių teisės aktų atnaujinimas yra būtinas norint užtikrinti, kad nacionalinės valdžios institucijos turėtų reikiamus įrankius sankcijų už reglamente įtvirtintų reikalavimų nesilaikymą taikymui organizacijoms. Šiuo klausimu jam antrino ir ES teisingumo komisarė V. Jaurova, teigdama, kad dėl laiku neatnaujintų teisės aktų neišvengiamai kils tam tikras teisinis neapibrėžtumas, o dėl to ji kaltino šalių aplaidumą ir per ilgai užsitęsusias buitines diskusijas šalyse (Four days until GDPR D-Day: Only seven EU states ready, 2019).

Apibendrinant išanalizuotus BDAR juridinius aspektus galima teigti, kad reglamente pateikiami reikalavimai yra griežti, didelės apimties ir ypatingai svarbūs, tad siekiant tinkamai įgyvendinti BDAR įtvirtintus reikalavimus valstybėje, yra būtinas tiek valstybinių institucijų, prižiūrinčių asmens duomenų apsaugą, tiek organizacijų, vykdančių su tuo susijusią veiklą, tiek ir valstybės pagrindinių vykdomosios ir įstatymų leidimo institucijų bendradarbiavimas. Faktas, kad Lietuva buvo viena iš šalių, laiku nepasiruošusi naujojo reglamento taikymui dėl vidaus teisės aktų neatnaujinimo, tik įrodo, kad organizacijoms, besiruošusioms reglamento taikymui savo vykdomoje veikloje, Vyriausybė nebuvo geras pavyzdys. Daugeliui organizacijų šis uždavinys buvo ir vis dar yra gana didelis iššūkis, kadangi neišvengiama klaidų ir pažeidimų, tad BDAR strategijos taikymo organizacijoje sukūrimas yra viena iš pagrindinių užduočių, padedančių tinkamai vykdyti BDAR keliamus reikalavimus ir sumažinti su tuo susijusių galimų patirti rizikų poveikį.

1.3. BDAR įtvirtintų reikalavimų taikymo organizacijoje strategijos elementų analizė

BDAR – tiesioginio taikymo teisės akto Europos Sąjungoje įsigaliojimas lėmė organizacijų poreikį iš esmės peržiūrėti savo asmens duomenų apsaugos ir jų tvarkymo procesus, adaptuoti ir transformuoti savo veiklą bei veiklos **strategiją**, siekiant užtikrinti valdomų asmens duomenų saugumą bei duomenų subjektų teisių įgyvendinimą.

Pasak Svetiko, K. Ž. ir Arimavičiūtės, M. (2012), strategija reiškia mąstymą apie ateitį ir veiksmų krypties išplėtojimą, kad būtų galima pasiekti tikslus ir uždavinius. Anot Raksha, N. (2015), įmonės strategija yra ilgalaikis planas, leidžiantis verslui sėkmingai veikti rinkoje, tenkinant klientų poreikius geriau nei konkurentai. Kaip teigia Lawrence, S. (2013), strategijos poreikis iškyla kiekvieną kartą, kai kelias į numatytą tikslą nėra paprastas, arba kai reikia spręsti tam tikslui pasiekti reikalingų išteklių pasirinkimą, veiksmingą jų taikymo planą ir tinkamą jų seką.

Bendrą organizacijos verslo strategiją gali ir turi sudaryti atskiros strategijos, skirtos konkrečių organizacijos tikslų įgyvendinimui ir skirtingų klausimų sprendimui. Šiomis dienomis vienas iš svarbiausių organizacijų tikslų bei uždavinių ir yra – tinkamas BDAR įtvirtintų reikalavimų vykdymas, todėl BDAR taikymo strategijos organizacijoje poreikis yra neabejotinas.

Siekiant išanalizuoti ir susisteminti BDAR taikymo strategijos organizacijoje esminius aspektus, yra remiamasi BDAR įtvirtintais reikalavimais duomenų tvarkytojams ir valdytojams, atsakingų už duomenų apsaugą priežiūros institucijų bei mokslininkų bei šios srities specialistų teikiamomis rekomendacijomis.

BDAR yra nurodomos šios duomenų valdytojui ir duomenų tvarkytojui galiojančios bendrosios prievolės:

3 lentelė. Duomenų valdytojo ir duomenų tvarkytojo bendrosios prievolės

	Bendroji prievolė	**Prievolės išaiškinimas**
1.	**Duomenų tvarkymo veiklos įrašai**	Prievolė tvarkyti veiklos įrašus, susijusius su asmeniniais duomenimis, apima toliau nurodytos informacijos pateikimą: duomenų valdytojo ir duomenų apsaugos pareigūno, jei taikoma, vardas bei pavardė ir kontaktiniai duomenys; duomenų tvarkymo tikslai; duomenų subjektų kategorijų ir asmens duomenų kategorijų aprašymas; duomenų gavėjų kategorijos; kai taikoma, asmens duomenų perdavimai į trečiąją valstybę ar tarptautinei organizacijai; kai įmanoma, numatomi įvairių kategorijų duomenų ištrynimo terminai; kai įmanoma, techninių ir organizacinių saugumo priemonių aprašymas.
2.	**Bendradarbiavimas su priežiūros institucija**	Duomenų valdytojas ir duomenų tvarkytojas, gavę prašymą bendradarbiauja su priežiūros institucija jai vykdant savo užduotis.
3.	**Duomenų tvarkymo saugumas**	Duomenų valdytojas ir duomenų tvarkytojas įgyvendina tinkamas technines ir organizacines priemones, kad būtų užtikrintas pavojų atitinkančio lygio saugumas.
4.	**Pranešimas priežiūros institucijai apie asmens duomenų saugumo pažeidimą**	Asmens duomenų saugumo pažeidimo atveju duomenų valdytojas pagrįstai nedelsdamas ir, jei įmanoma, praėjus ne daugiau kaip 72 valandoms nuo tada, kai jis sužino apie asmens duomenų saugumo pažeidimą, apie tai praneša priežiūros institucijai.
5.	**Pranešimas duomenų subjektui apie asmens duomenų pažeidimą**	Kai dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus duomenų fizinių asmenų teisėms ir laisvėms, duomenų valdytojas, pagrįstai nedelsdamas praneša apie asmens duomenų saugumo pažeidimą duomenų subjektui.
6.	**Poveikio duomenų apsaugai vertinimas**	Tais atvejais, kai dėl duomenų tvarkymo rūšies, visų pirma, kai naudojamos naujos technologijos, ir atsižvelgiant į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, fizinių asmenų teisėms bei laisvėms gali kilti didelis pavojus, duomenų valdytojas, prieš pradėdamas tvarkyti duomenis, atlieka numatytų duomenų tvarkymo operacijų poveikio asmens duomenų apsaugai vertinimą (toliau – PDAV).
7.	**Išankstinės konsultacijos su priežiūros institucija**	Duomenų valdytojas, prieš pradėdamas tvarkyti duomenis, konsultuojasi su priežiūros institucija, jeigu PDAV nurodyta, kad tvarkant duomenis kiltų didelis pavojus, jei duomenų valdytojas nesiimtų priemonių pavojui sumažinti.

3 lentelės tęsinys

	Bendroji prievolė	Prievolės išaiškinimas
8.	**Duomenų apsaugos pareigūno skyrimas**	Duomenų valdytojas ir duomenų tvarkytojas paskiria duomenų apsaugos pareigūną, kai: • duomenis tvarko valdžios institucija arba įstaiga, išskyrus teismus, kai jie vykdo savo teismines funkcijas; • duomenų valdytojo arba duomenų tvarkytojo pagrindinė veikla yra duomenų tvarkymo operacijos, dėl kurių pobūdžio, aprėpties ir (arba) tikslų būtina reguliariai ir sistemingai dideliu mastu stebėti duomenų subjektus; • duomenų valdytojo arba duomenų tvarkytojo pagrindinė veikla yra specialių kategorijų duomenų tvarkymas dideliu mastu pagal BDAR 9 straipsnį ir 10 straipsnyje nurodytų asmens duomenų apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas tvarkymas dideliu mastu.
9.	**Elgesio kodeksų patvirtinimas ir stebėsena**	Valstybės narės, priežiūros institucijos, EDAV ir EK skatina parengti elgesio kodeksus, kuriais būtų siekiama padėti tinkamai taikyti BDAR, atsižvelgiant į konkrečius įvairių su duomenų tvarkymu susijusių sektorių ypatumus ir į konkrečius labai mažų, mažųjų ir vidutinių įmonių poreikius. Asociacijos ir kitos įstaigos, atstovaujančios įvairių kategorijų duomenų valdytojams arba duomenų tvarkytojams, gali parengti elgesio kodeksus arba iš dalies pakeisti ar išplėsti tokius kodeksus siekdamos nustatyti, kaip turi būti taikomas šis reglamentas. Elgesio kodekso laikymosi stebėseną gali atlikti įstaiga, turinti tinkamo lygio ekspertinių žinių kodekso dalyko srityje ir tuo tikslu akredituota kompetentingos priežiūros institucijos.

Šaltinis: parengta autorės, remiantis „Europos parlamento ir tarybos reglamentas (ES) 2016/679”

Apibendrinant aukščiau išvardintas duomenų valdytojo ir duomenų tvarkytojo bendrąsias prievoles, verta akcentuoti, kad pirmoji prievolė nėra taikoma įmonei ar organizacijai, kurioje dirba mažiau kaip 250 darbuotojų, išskyrus atvejus, kai dėl jos vykdomo duomenų tvarkymo gali kilti pavojus duomenų subjektų teisėms ir laisvėms, duomenų tvarkymas nėra reguliarus arba duomenų tvarkymas apima specialių kategorijų, kurios yra nurodytos šio darbo 2.1. poskyryje, 17 puslapyje, asmens duomenis.

Išsamiau analizuojant duomenų valdytojo ir duomenų tvarkytojo prievolę užtikrinti duomenų tvarkymo saugumą, būtina pabrėžti, kad įmonės ir organizacijos privalo užtikrinti reguliarų techninių ir organizacinių priemonių, kuriomis užtikrinamas duomenų tvarkymo saugumas, tikrinimo,

vertinimo ir veiksmingumo vertinimo procesą. Prie organizacinių priemonių, kuriomis yra užtikrinamas duomenų tvarkymo saugumas, yra priskiriamas ir tarptautinės standartų organizacijos (angl. International Standard Organization) kokybės vadybos sistemų (toliau – ISO standartai) standartų laikymasis – atitiktis Projekto „Kurk Lietuvai" dalyviai, bendradarbiaudami su Nacionalinio kibernetinio saugumo centru prie Krašto apsaugos ministerijos (toliau – NKSC), parengė ir viešai paskelbė ISO standartų, kuriuos rekomenduotina taikyti įmonės veikloje, siekiant teisingai taikyti rizikų vertinimo metodologijas ir susipažinti su gerosiomis užsienio kibernetinio ir informacijos saugumo praktikomis, sąrašą:

- tarptautinis ISO 27000 šeimos informacijos apsaugos sistemos standartas;
- tarptautinis ISO 22301 standartas ir verslo tęstinumo valdymo sistema;
- tarptautinis ISO 20000 standartas ir paslaugų valdymo principai;
- tarptautinis ISO 27031 standartas, kuriame pateikiami saugumo užtikrinimo metodai bei informacinių ir komunikacinių technologijų pasirengimo verslo tęstinumui gairės *(*Kibernetinis saugumas ir verslas. Ką turėtų žinoti kiekvienas įmonės vadovas, 2020).

Taip pat rekomenduojama taikyti ENISA rekomendacijose nurodomas organizacines ir technines asmens duomenų saugumo priemones.

Kadangi kibernetinio saugumo užtikrinimas organizacijoje yra neatsiejama BDAR įtvirtintų reikalavimų vykdymo dalis, verta susipažinti su NKSC rekomenduojamais atlikti veiksmais, didinančiais organizacijos kibernetinį atsparumą bei padedančiais suprasti, kaip apsaugoti organizacijos informaciją ir informacines technologijas nuo labiausiai paplitusių kibernetinių grėsmių:

KIBERNETINIO SAUGUMO PRAKTIKA	Slaptažodžių politika (saugus kūrimas ir naudojimas)
	Kelių žingsnių autentifikacija
	Antivirusinių programų naudojimas
	Savalaikis automatinių atnaujinimų įdiegimas
	Atsarginių duomenų kopijų kūrimas
	Prieigos kontrolė
	Darbuotojų mokymai
	Darbo ir asmeninių prietaisų atskyrimas
	Ugniasienės naudojimas
	Bevielio tinklo saugumo užtikrinimas

Šaltinis: parengta autorės, remiantis "Kibernetinis saugumas ir verslas. Ką turėtų žinoti kiekvienas įmonės vadovas, 2020"

6 pav. Gerosios kibernetinio saugumo praktikos pavyzdžių rinkinys

Lietuvos įmonės ir organizacijos, vykdančios prievolę pranešti priežiūros institucijai apie asmens duomenų saugumo pažeidimą, šį pranešimą adresuoja VDAI. Tuo tarpu duomenų tvarkytojas,

sužinojęs apie asmens duomenų apsaugos pažeidimą, apie tai praneša duomenų valdytojui. Įmonių ir organizacijų veiklos praktikoje yra laikomasi taisyklės, kad duomenų tvarkytojas apie asmens duomenų apsaugos pažeidimą informuoja duomenų valdytoją anksčiau nei praėjus 72 valandoms nuo tada, kai jis sužino apie pažeidimą, tam, kad duomenų valdytojas galėtų laiku įvykdyti savo prievolę pranešti priežiūros institucijai apie asmens duomenų apsaugos pažeidimą. Pranešimas apie asmens duomenų pažeidimą duomenų subjektui turi būti pateikiamas aiškia ir paprasta kalba, pranešime turi būti aprašomas asmens duomenų saugumo pažeidimo pobūdis, tikėtinos pažeidimo pasekmės ir priemonės, kurių ėmėsi duomenų valdytojas, kad būtų pašalintas pažeidimas, ar kad būtų sumažintos galimos neigiamos pasekmės, kilusios dėl šio pažeidimo. Visos šios išvardintos sąlygos galioja ir pranešimui apie asmens duomenų saugumo pažeidimą priežiūros institucijai.

Konkretizuojant prievolę atlikti PDAV, būtina paminėti, kad vertinimas visų pirma turi būti atliekamas, kai yra vykdomas:

- sistemingas ir išsamus su fiziniais asmenimis susijusių asmeninių aspektų vertinimas, kuris yra grindžiamas automatizuotu tvarkymu, įskaitant profiliavimą, ir kuriuo remiantis priimami sprendimai, kuriais padaromas su fiziniu asmeniu susijęs teisinis poveikis arba kurie daro panašų didelį poveikį fiziniam asmeniui;
- specialių kategorijų duomenų arba asmens duomenų apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas tvarkymas dideliu mastu;
- sistemingas viešos vietos stebėjimas dideliu mastu kontekste (Europos parlamento ir tarybos reglamentas (ES) 2016/679).

Institucija, vykdanti BDAR taikymo priežiūrą šalyje, sudaro ir viešai paskelbia tų rūšių duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti PDAV, sąrašą. Lietuvoje šis sąrašas paskutinį kartą buvo patikslintas ir patvirtintas buvo patvirtintas 2019 metų kovo mėnesį (žr. 1 priedą). Pasak VDAI direktoriaus Andrijausko (2019), šis sąrašas buvo laukiamas ne tik verslo, bet ir valstybinių institucijų, nes jis suteikė daugiau aiškumo, kokiais atvejais tvarkant asmens duomenis reikės atlikti PDAV. VDAI direktorius tuo pačiu atkreipė dėmesį, kad šis sąrašas nėra baigtinis. Jis nurodė, kad pasitaikys atvejų, kai organizacijos, atsižvelgdamos į BDAR reikalavimus, turės atlikti PDAV.

Pasak Andrijausko, R. ir Morkūnienės, D. (2020), duomenų apsaugos pareigūnas gali įmonėms ar organizacijoms padėti laikytis BDAR reikalavimų ir siekti organizacijos strateginių tikslų stebėdamas, kaip įmonė ar organizacija tvarko asmens duomenis, patarti galinčių kilti rizikų klausimais ir kitais su asmens duomenų tvarkymu ar duomenų subjekto teisių įgyvendinimu susijusiais klausimais. Šio pareigūno įtraukimas į organizacijoje vykdomus ar planuojamus vykdyti procesus (konsultavimas dėl PDAV, darbuotojų konsultavimas duomenų apsaugos klausimais, dalyvavimas nagrinėjant asmens duomenų saugumo pažeidimus) yra atitikties BDAR reikalavimams garantas bei sėkmingo bendradarbiavimo su VDAI pagrindas.

Duomenų tvarkytojas ir duomenų valdytojas privalo laikytis ne tik aukščiau išvardintų BDAR įtvirtintų bendrųjų prievolių, bet ir užtikrinti, jei tai yra aktualu, tinkamą asmens duomenų perdavimą į trečiąsias valstybes arba tarptautinėms organizacijoms, remiantis sprendimu dėl tinkamumo, tai yra, kai užtikrinama tinkamo lygio asmens duomenų apsauga (Europos parlamento ir tarybos reglamentas (ES) 2016/679).

VDAI, apibendrindama ir susistemindama organizacijoms reikalingus atlikti veiksmus, besiruošiant BDAR įgyvendinimui, pateikė šią metodinę informaciją, apimančią 12 žingsnių:

PASIRENGIMO TAIKYTI BDAR ŽINGSNIAI	Organizacijos darbuotojų sąmoningumo ugdymas
	Informacijos (tvarkomų asmens duomenų) analizė
	Informacijos apie privatumą pateikimas
	Duomenų subjektų teisių užtikrinimas
	Subjekto prašymų dėl teisės susipažinti įgyvendinimas
	Asmens duomenų tvarkymo teisinis pagrindimas
	Sutikimo tvarkyti asmens duomenis gavimas
	Vaikų asmens duomenų tvarkymas
	Asmens duomenų saugumo pažeidimų valdymas
	Pritaikytosios duomenų apsaugos ir poveikio duomenų apsaugai vertinimas
	Duomenų apsaugos pareigūno paskyrimas
	Bendradarbiavimas su duomenų apsaugos priežiūros institucija

Šaltinis: parengta autorės, remiantis ”Pasiruošimas taikyti Bendrąjį duomenų apsaugos reglamentą (ES) 2016/679”, 2017

7 pav. Pasirengimo taikyti BDAR organizacijoje žingsniai

Anot Sirur, S., Nurce, J. R.C. ir Webb, H. (2018), analizavusių organizacijų pasiruošimą BDAR įtvirtintų reikalavimų taikymo atitikčiai, BDAR taikymo sritis yra kiek beprecedentė: ji reguliuoja kiekvieną asmens duomenų tvarkymo aspektą, apima nemažas galimas nuobaudas už reglamento nesilaikymą ir gali bet kurią pasaulio bendrovę, kuri tvarko ES piliečių duomenis, patraukti baudžiamojon atsakomybėn už asmens duomenų apsaugos pažeidimus.

Kiekviena nacionalinė priežiūros institucija, remdamasi BDAR, turi įgaliojimus ne tik nurodyti ištaisyti arba ištrinti asmens duomenis arba apriboti jų tvarkymą organizacijoje, bet ir skirti administracinę baudą organizacijai, pažeidusiai reglamente įtvirtintus reikalavimus. Duomenų apsaugos priežiūros institucija privalo užtikrinti, kad skiriamos administracinės baudos už reglamento pažeidimus kiekvienu konkrečiu atveju būtų veiksmingos, proporcingos ir atgrasomos. Pagal BDAR, organizacijai už asmens duomenų saugumo pažeidimus skiriama administracinė bauda gali siekti net 20 000 000 eurų arba, įmonės atveju – iki 4 % jos ankstesnių finansinių metų bendros metinės pasaulinės apyvartos sumą, atsižvelgiant į tai, kuri suma yra didesnė (Europos parlamento ir tarybos reglamentas (ES) 2016/679).

Galimos skirti administracinės baudos sumos dydis tik dar kartą įrodo, kaip yra svarbu organizacijoms užtikrinti sistemingą techninių, organizacinių ir teisinių priemonių taikymą visuose vykdomos veiklos procesuose bei laiku tas priemones peržiūrėti ir atnaujinti.

Apibendrinant BDAR įtvirtintas bendrąsias prievoles, taikomas duomenų valdytojui ar duomenų tvarkytojui, VDAI pateikiamas rekomendacijas dėl pasiruošimo BDAR įtvirtintų reikalavimų taikymui bei kibernetinio saugumo specialistų teikiamas rekomendacijas dėl organizacijos informacijos apsaugos, BDAR taikymo strategiją organizacijoje galima suskirstyti į 3 pagrindinius elementus:



Šaltinis: parengta autorės, remiantis juridiniais dokumentais bei priežiūros institucijų teikiamomis rekomendacijomis

8 pav. Pagrindiniai BDAR taikymo strategijos organizacijoje elementai

Bendrai teigiant, strategijos procesas apima 2 etapus: strategijos formavimą ir strategijos įgyvendinimą. Šie etapai nėra izoliuoti vienas nuo kito kaip atskiros stadijos ar tarpsniai, bet atvirkščiai,

jie yra stipriai susiję ir persidengiantys vienas su kitu. Kaip Drucker (2004) akcentavo - strategija reikalauja analizuoti esamą padėtį ir prireikus ją keisti. Remiantis tuo galima teigti, kad BDAR taikymo strategijos organizacijoje periodiška peržiūra ir atnaujinimas yra privalomas. Kontrolės sistemų, skirtų BDAR taikymo strategijos organizacijoje įgyvendinimo užtikrinimui, sukūrimas galimas įvardinti kaip vienas iš pagrindinių kriterijų siekiant strategijos veiksmingumo.

BDAR taikymo strategijos organizacijoje peržiūros periodiškumą gali lemti: teisės aktų tiek nacionaliniu, tiek regioniniu mastu, pasikeitimas; įmonės ar organizacijos veiklos ar jos procesų pasikeitimas; pokyčiai informacinių technologijų srityje; duomenų apsaugos priežiūros institucijų naujų (aktualių organizacijos vykdomai veiklai) rekomendacijų ar gairių paskelbimas; kibernetinio saugumo specialistų naujai teikiamos rekomendacijos, padedančios užtikrinti informacijos saugą bei įmonės informacinės sistemos suderinimą su reikalavimais ir normomis informacijos saugumo srityje; gerosios praktikos, stebint organizacijų veiklą duomenų apsaugos srityje tarptautiniu mastu, pritaikymo poreikis savo organizacijoje; asmens duomenų saugos pažeidimų analizė tiek nacionaliniu, tiek regioniniu mastu.

Kaip teigia Buttarelli, G. (2016), mokslininkai netiki, kad BDAR galutinis rezultatas yra tobulas, o tam tikru požiūriu jis yra toli nuo idealo. Nepaisant to, mokslininkai tiki, jog ši reforma yra iki šiol įvykusi ambicingiausia pastanga apsaugoti duomenų subjektų teises skaitmeninėje erdvėje.

Asmens duomenų saugos pažeidimų specifikos analizė padėtų identifikuoti BDAR įtvirtintų reikalavimų taikymo strategijos organizacijoje silpniausias sritis. Atliktos analizės rezultatai galėtų pasitarnauti optimizuojant organizacijos BDAR taikymo strategiją.

1.4. BDAR taikymo strategijos kūrimo probleminiai aspektai

Apibendrinant asmens duomenų apsaugos teorinių aspektų analizės rezultatus galima teigti, jog internetui, išmaniosioms technologijoms, bendravimui socialiniuose tinkluose ir informacijos paieškai „Google“ tapus neatsiejama kasdienio gyvenimo dalimi, išaugo ne tik asmens duomenų viešinimo, rinkimo ir keitimosi jais mastas, bet ir prieigos prie šių duomenų galimybės. To pasėkoje BDAR taikymo strategijos kūrimas organizacijoje, laikantis saugumo reikalavimų ir atsižvelgiant į techninių naujovių perspektyvą, tapo viena iš svarbiausių organizacijos užduočių. Siekiant įvykdyti šią užduotį, yra susiduriama ir su problemomis.

Organizacijos privalo skaidriai ir efektyviai įgyvendinti keliamus reikalavimus, tad verslo aplinkoje taikomų techninių metodų bei naudojamų sistemų, įgyvendinant visišką asmens duomenų kontrolę, silpnųjų ir stipriųjų pusių išryškinimas bei mokslinių - praktinių rekomendacijų pateikimas yra ypatingai svarbus. Atlikus asmens duomenų apsaugos teorinių aspektų analizę yra naudinga išskirti ir pabrėžti pagrindinius BDAR taikymo strategijos organizacijoje kūrimo probleminius aspektus (žr. 4 lent.).

4 lentelė. BDAR taikymo strategijos kūrimo probleminiai aspektai

	Probleminis aspektas	**Aspekto išaiškinimas**
1.	**Duomenų valdytojo ir duomenų tvarkytojo įsipareigojimų atskirtis**	Labai dažnai praktikoje yra susiduriama su problema, kad duomenų valdytojai ir duomenų tvarkytojai negeba atskirti jiems privalomų vykdyti įsipareigojimų, siekiant užtikrinti asmens duomenų apsaugą savo vykdomoje veikloje.
2.	**Kintančios technologijos**	BDAR taikymo strategiją organizacijoje yra būtina periodiškai peržiūrėti ir priimti tam tikrus jos atnaujinimo sprendimus siekiant pritaikyti pačią strategiją prie atsinaujinusių – pakitusių technologijų.
3.	**Teisės „būti pamirštam“ nebuvimas absoliučia**	Esant viršesnėms teisėtoms priežastims tvarkyti duomenis ar esant teisėtam visuomenės interesui turėti prieigą prie asmens informacijos, ši teisė nėra taikoma. Yra susiduriama su problema nusprendžiant, ar teisė „būti pamirštam“ privalo būti taikoma konkrečiu atveju.
4.	**Skirtingas asmens duomenų apsaugos standarto plėtojimas atskirose valstybėse**	Teismų asmens duomenų apsaugos pažeidimų srityje praktika rodo, kad atskirose valstybėse yra priimami skirtingi sprendimai.
5.	**Tik funkcinių BDAR įgyvendinimo reikalavimų apibrėžimas**	Organizacijos susiduria su konkrečių organizacinių ir techninių priemonių, kurios yra taikomos siekiant užtikrinti tinkamą asmens duomenų apsaugą, apibrėžimo trūkumu.
6.	**Darbuotojų kompetencija ir sąmoningumas**	Netinkami darbuotojų veiksmai ir kompetencijos asmens duomenų apsaugos srityje trūkumas dažniausiai lemia asmens duomenų apsaugos pažeidimus organizacijoje.

Šaltinis: parengta autorės remiantis išanalizuota moksline literatūra ir juridiniais dokumentais

Taip pat yra reikšminga paminėti, kad asmens duomenų apsauga yra neatsiejama kibernetinio saugumo dalis. Kibernetinis saugumas ir asmens duomenų apsauga nėra sinonimai, tačiau kibernetinės saugos principų ignoravimas gali lemti ir BDAR pažeidimus, o kartu ir dideles skiriamas baudas, kurios turėtų būti reikšmingas signalas įmonėms, tik deklaratyviai įgyvendinančioms šio teisės akto nuostatas. BDAR įpareigojimai nėra vien tik teisinio ar techninio pobūdžio reikalavimai. BDAR nuostatomis siekiama, kad kiekviena įmonė kasdieninėje savo veikloje galvotų apie tai, kaip įmonėje vykstantys procesai veikia asmens duomenų tvarkymą, o kartu – siekiama kelti asmens duomenų apsaugos kultūrą versle ir ne tik.

2. BDAR TAIKYMO STRATEGIJOS KŪRIMO TYRIMO METODOLOGIJA

2.1. Tyrimo metodiniai aspektai

Tyrimo tikslingumo pagrindimas ir problematika. Mokslinės literatūros analizė (Politou ir bendraautoriai (2018), Addis ir Kutar (2018), Mense ir Blobel (2017), Petraitytė (2011), Cvilika ir Šlapimaitė (2015), Falk (2016), Irwin (2019), Tamavičiūtė (2019), Lawrence (2013), Andrijauskas ir Morkūnienė (2020), Sirur, Nurce, ir Webb (2018) ir kt.), atliepianti BDAR įtvirtintų reikalavimų įgyvendinimo ypatumus, atskleidė, kad reglamento taikymo strategijos kūrimas organizacijoje nėra paprastas uždavinys, o atvirkščiai, tai yra sudėtingas daugialypis procesas, kuris apima ne tik strategijos sukūrimą ir jos įgyvendinimą, bet taip pat reikalauja jos periodiškos peržiūros ir atnaujinimo bei pačios strategijos įgyvendinimo kontrolės sistemų taikymo. Nepaisant to, kad juridiniuose dokumentuose (BDAR (2016), Europos Parlamento ir Tarybos direktyva (95/46/EB) (1995), LRADTAĮ (2018) ir kt.) yra konkrečiai apibrėžiami funkciniai BDAR įgyvendinimo reikalavimai, pasigendama rekomendacijų dėl techninių bei organizacinių priemonių, skirtų privatumo užtikrinimui įgyvendinant BDAR teisinius reikalavimus, taikymo organizacijos veikloje.

Teorinis - juridinis pagrindas, padėjęs metodologiškai pasirengti konstruojant tyrimą, yra 2016 metais Europos parlamento ir tarybos priimtas BDAR, kuris tiek Lietuvoje, tiek ir kitose Europos Sąjungos valstybėse narėse pradėtas taikyti 2018 metų gegužės 25 dieną.

Tyrimo tikslas – išanalizavus asmens duomenų saugumo pažeidimus Europoje per apibrėžtą laikotarpį (2018 – 2021 m.) bei atlikus ekspertinį vertinimą, pasiūlyti BDAR taikymo strategijos organizacijoje modelį.

Atvejų analizės laikotarpis (2018 – 2021 m.) grindžiamas tuo, kad šiuo laikotarpiu fiksuoti asmens duomenų saugumo pažeidimai Europoje įvyko dėl BDAR įtvirtintų reikalavimų nevykdymo.

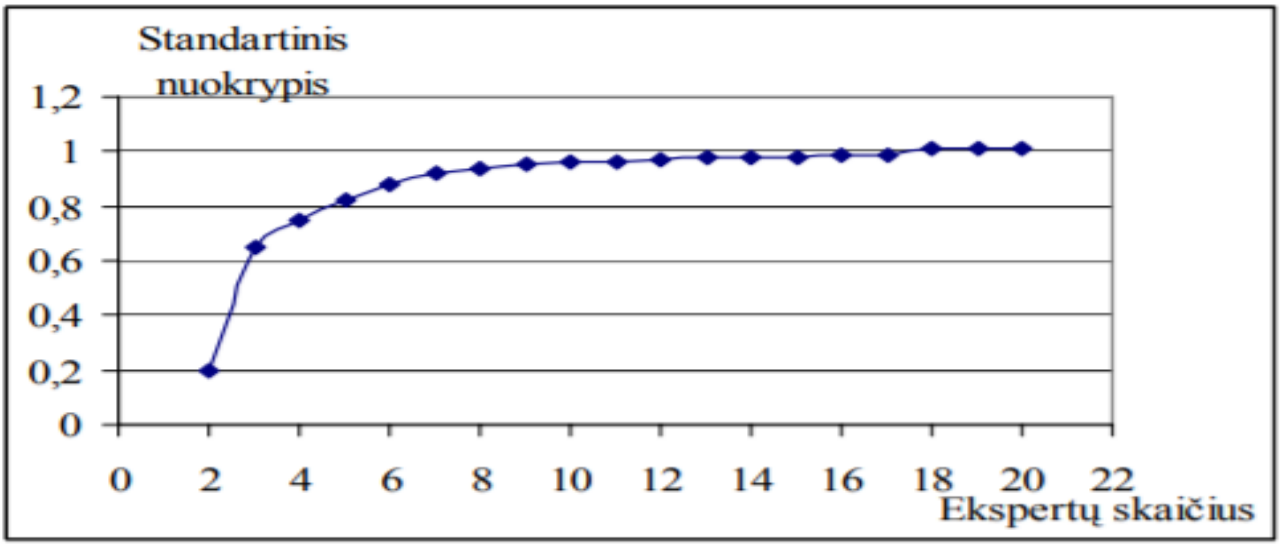
Tyrimo uždaviniai:

1. Išanalizuoti asmens duomenų apsaugos pažeidimus Europoje per apibrėžtą laikotarpį.
2. Identifikuoti dažniausiai BDAR pažeidžiamus straipsnius.
3. Remiantis atliktos analizės rezultatais, atlikti ekspertinį vertinimą BDAR taikymo strategijos kūrimo organizacijoje tema.

Tyrimo metodika: BDAR taikymo strategijos organizacijoje modelio konstravimui pasirinktas **trianguliacijos metodas** (kombinuotas tyrimas**)**. Pirmiausiai yra atliekamas kiekybinis tyrimas – asmens duomenų apsaugos pažeidimų analizė, pagrinde taikomas antrinių statistinių duomenų analizės metodas. Remiantis kiekybinio tyrimo rezultatais yra formuojami ekspertinio vertinimo apklausos klausimai ir atliekamas kokybinis tyrimas, taikomi ekspertinio vertinimo ir anketinės apklausos metodai.

Kaip nurodo Valackienė A. ir Mikėnė, S. (2007), kiekybiniu tyrimu galima apibrėžti tokį empirinį tyrimą, kurio duomenys pateikiami skaičiais (kiekybine išraiška) ir apdorojami statistiniais metodais, o kokybinio tyrimo atveju tiriama nedidelė aibė (keli atvejai), tačiau analizuojama daug kintamųjų. Vienas iš kokybinio tyrimo metodų ir yra ekspertinis vertinimas.

Tyrime dalyvaujančių ekspertų skaičiaus nustatymas. Tyrimo metu buvo apklausti 9 ekspertai. Kaip nurodo Blashfield, R. K. ir Libby R. (1978), nustatant priimtiną ekspertų skaičių, yra vadovaujamasi metodologinėmis prielaidomis, suformuluotomis klasikinėje testų teorijoje, kurioje yra teigiama, jog agreguotų sprendimų patikimumą ir priimančių sprendimą skaičių sieja greitai gęstantis netiesinis ryšys (žr. 9 pav.). Anot mokslininkų, yra įrodyta, kad agreguotų ekspertinių vertinimų moduliuose su vienodais svoriais nedidelės ekspertų grupės sprendimų ir vertinimų tikslumas nenusileidžia didelės ekspertų grupės sprendimų ir vertinimų tikslumui.



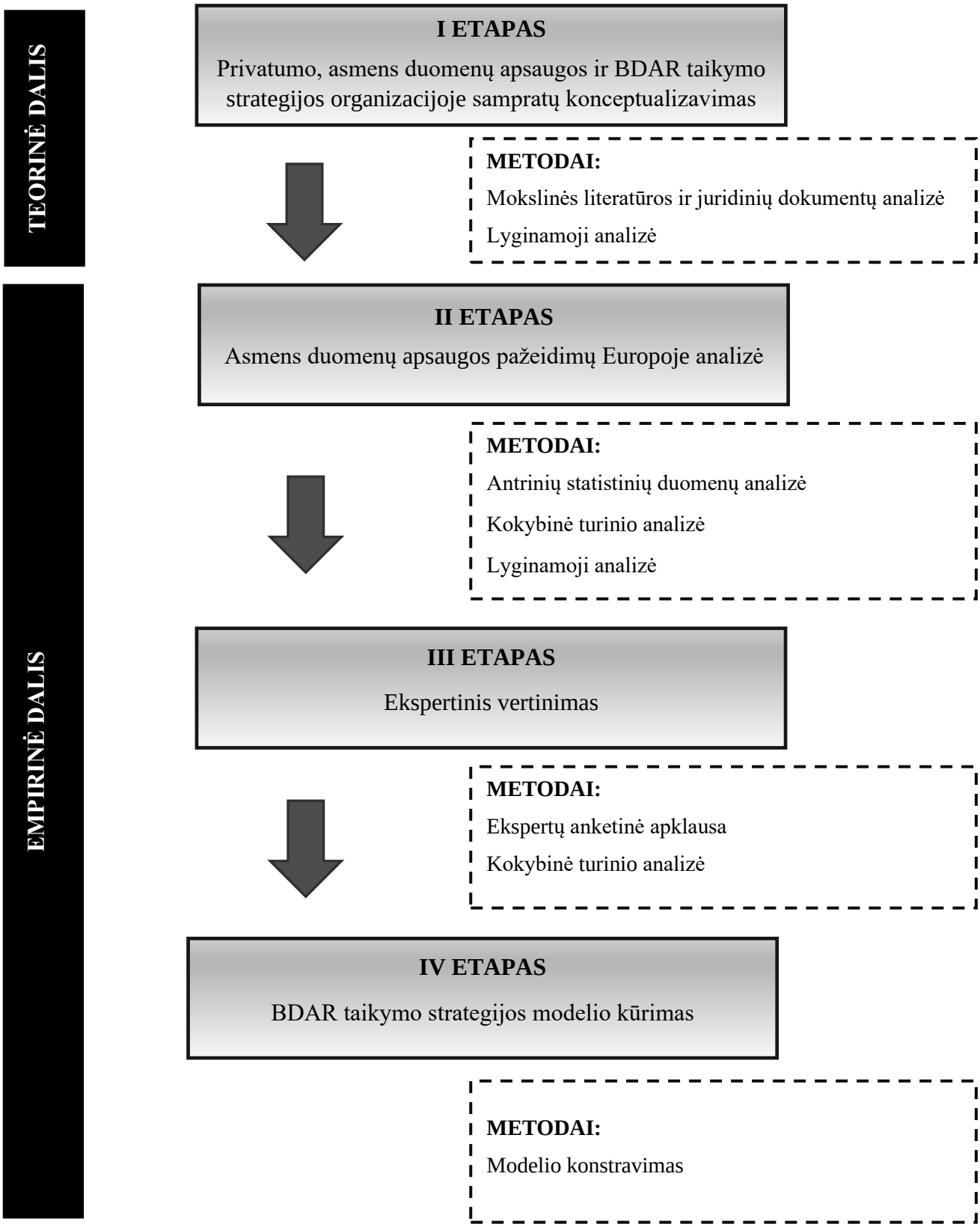
Šaltinis: Baležentis, A. ir Žalimaitė, M. (2011).

9 pav. Ekspertų vertinimų standartinio nuokrypio priklausomybė nuo ekspertų skaičiaus

Iš paveiksle pateiktos informacijos matyti, jog tyrime dalyvaujant 9 ekspertams, jų pateiktų nuomonių bei vertinimų tikslumas yra gana didelis: standartinis nuokrypis yra didesnis nei 0,8. Tad galima teigti, kad tyrime dalyvavusių ekspertų skaičius yra pakankamas tiksliai ir reikšmingai informacijai gauti.

Pasak Kardelio (2017), metodologija suprantama kaip tyrimo proceso visuma, siejanti teorinę ir empirinę šio proceso dalis, aiškinanti nagrinėjamus reiškinius. Tačiau planuojant tyrimą labiau įprasta laikytis mokslinio tyrimo metodologijos, aiškinančios pagrindinius tyrimo proceso žingsnius.

Tyrimo loginė eiga: siekiant sėkmingo tyrimo įgyvendinimo ir užsibrėžto tikslo pasiekimo, sudaroma tyrimo loginė schema, nurodanti tyrėjo veiksmų eiliškumą bei metodologinį tyrimo pagrįstumą (žr. 10 pav.).



Šaltinis: sudaryta darbo autorės

10 pav. Empirinio tyrimo loginė eiga

I etapas. Siekiant konceptualizuoti privatumo, asmens duomenų apsaugos ir BDAR taikymo strategijos organizacijoje sampratas buvo atlikta juridinių dokumentų, mokslinės lietuvių ir užsienio

autorių literatūros bei srities specialistų teikiamų rekomendacijų ir gairių analizė. Atlikta analizė leido suprasti bendruosius privatumo aspektus, teisės į privatų gyvenimą ir asmens duomenų apsaugos teisinio reguliavimo dinamiką bei jos priežastis. Kaip vienos iš pagrindinių priežasčių yra įvardijamos informacinių technologijų plėtra bei duomenų keitimosi (judėjimo) poreikio masto išaugimas. Šiame etape buvo išskirti pagrindiniai BDAR įtvirtinti reikalavimai bei 2 pagrindiniai strategijos proceso etapai: strategijos formavimas ir strategijos įgyvendinimas bei pabrėžta strategijos peržiūrėjimo periodiškumo svarba. Taip pat buvo nustatyti 3 pagrindiniai BDAR taikymo strategijos organizacijoje elementai: procesas, technologijos ir darbuotojai.

II etapas. Siekiant identifikuoti dažniausiai BDAR pažeidžiamus straipsnius, buvo atlikta asmens duomenų saugumo pažeidimų Europoje per apibrėžtą laikotarpį (2018 – 2021 m.) analizė. Atlikta analizė leido nustatyti BDAR taikymo strategijos organizacijoje problemines sritis.

III etapas. Remiantis III etape atliktos analizės rezultatais buvo atliktas ekspertinis vertinimas. Ekspertinis vertinimas buvo atliekamas siekiant sukonstruoti BDAR taikymo strategijos organizacijoje modelį. Atliekant vertinimą, buvo apklausiami ekspertai, turintys specifinių žinių, susijusių su tiriamuoju reiškiniu, ir dirbantys asmens duomenų apsaugos srityje. Ekspertiniam vertinimui atlikti naudotas instrumentas (anketa) yra pateikiamas šio darbo 2-ame priede.

IV etapas. Remiantis II ir III etapo metu atliktais tyrimų rezultatais konstruojamas BDAR taikymo strategijos organizacijoje modelis.

2.2. Tyrimo metodikos pagrindimas

Kaip matyti iš 10-tame paveiksle pateikiamos empirinio tyrimo loginės eigos, tyrimui atlikti buvo pasirinkti keli metodai:

Kokybinė turinio (ang. Content) analizė. Anot Kansteiner, K. ir König, S. (2020) šis metodas yra pagrindinis ne skaitmeninių duomenų analizės metodas. Pasak Kardelio (2017), šis metodas gali suteikti objektyvios informacijos nagrinėjant tyrėjui aktualų klausimą. Šio atlikto tyrimo atveju, šis metodas buvo pasirinktas siekiant išanalizuoti ir susisteminti ekspertinio vertinimo metu surinką informaciją bei atliekant asmens duomenų apsaugos pažeidimų analizę, siekiant nustatyti BDAR taikymo strategijos organizacijoje problemines sritis.

Lyginamoji analizė. Morkevičiaus V. (2008) požiūriu, lyginimas yra esminis mokslo logikos principas: dviejų ar didesnio skaičiaus objektų požymių (charakteristikų) reikšmių (variantų) gretinimas. Anot autoriaus, lyginamasis metodas - ryšių ir priežastinių sąryšių tarp reiškinių analizės metodas, kuris remiasi alternatyvių hipotezių apie priežastinius - pasekminius ryšius tikrinimu pasitelkiant empirinius įrodymus. Tyrime šis metodas taikytas siekiant išanalizuoti asmens duomenų sąvokos kitimą laike bei asmens duomenų apsaugos pažeidimų dinamiką.

Antrinių statistinių duomenų analizė. Anot Valackienė A. ir Mikėnė, S. (2007) statistinės analizės tikslas – apibendrintų duomenų gavimas ir siekimas atskleisti reiškinių bendrąsias savybes pagal tam tikrus kintamuosius (vietos, laiko, gamybinius, demografinius, socialinius požymius ir sąlygas). Pasak Voblevičiaus, V. (2017), tyrimuose yra būtina naudoti 2 statistinės analizės metodus: aprašomąjį (duomenų rinkimas, sisteminimas, pateikimas) ir inferencinį, tai yra išvadų (statistiškai pagrįstų išvadų darymas). Aprašomosios statistikos metodai dažnai laikomi mažiau įdomiais ar svarbiais nei išvadų statistikos metodai, tačiau Voblevičiaus, V. nuomone, tai klaidingas požiūris. Neatlikus kvalifikuotos ir nuodugnios aprašomosios duomenų analizės, yra sunku tikėtis patikimų statistinio tyrimo išvadų. Tyrime šis metodas buvo naudojamas asmens duomenų apsaugos pažeidimų ES analizei atlikti, siekiant aprašyti asmens duomenų apsaugos pažeidimų dinamiką bei nustatyti BDAR taikymo organizacijose problemines sritis: naudojami tiek aprašomasis, tiek išvadų statistinės analizės metodai.

Ekspertų apklausa. Kaip Kardelis, K. (2017) teigia, naudojant apklausos metodą yra bandoma įvertinti tiriamų asmenų nuomones, požiūrius į tam tikrus reiškinius, elgsenos ypatumus ir su elgsena susijusius veiksnius. Nurodoma, kas ekspertų apklausa yra specifinės rūšies apklausa, kurios metu apklausiama specialiai parinkta žmonių grupė, turinti kurios nors srities žinių. Siekiant rasti tyrime iškeltos problemos sprendinius, buvo atlikta ekspertų anketinė apklausa.

Pasak Kardelio (2017), tyrimo rezultatų analizė yra vienas svarbiausių mokslinio darbo skyrių, kadangi čia pateikiami konkretaus tyrimo duomenys. Yra išskiriamos 2 pagrindinės šio etapo dalys: tyrimo rezultatai (konstatuojamojo pobūdžio dalis) ir rezultatų aptarimas, kurioje išryškėja autoriaus erudicija, gebėjimas analizuoti ir sintetinti tyrimo rezultatus. Remiantis tuo, šio darbo pabaigoje ir yra konstatuojami bei apibendrinami atlikto tyrimo rezultatai, pateikiamos darbo išvados bei siūlymai.

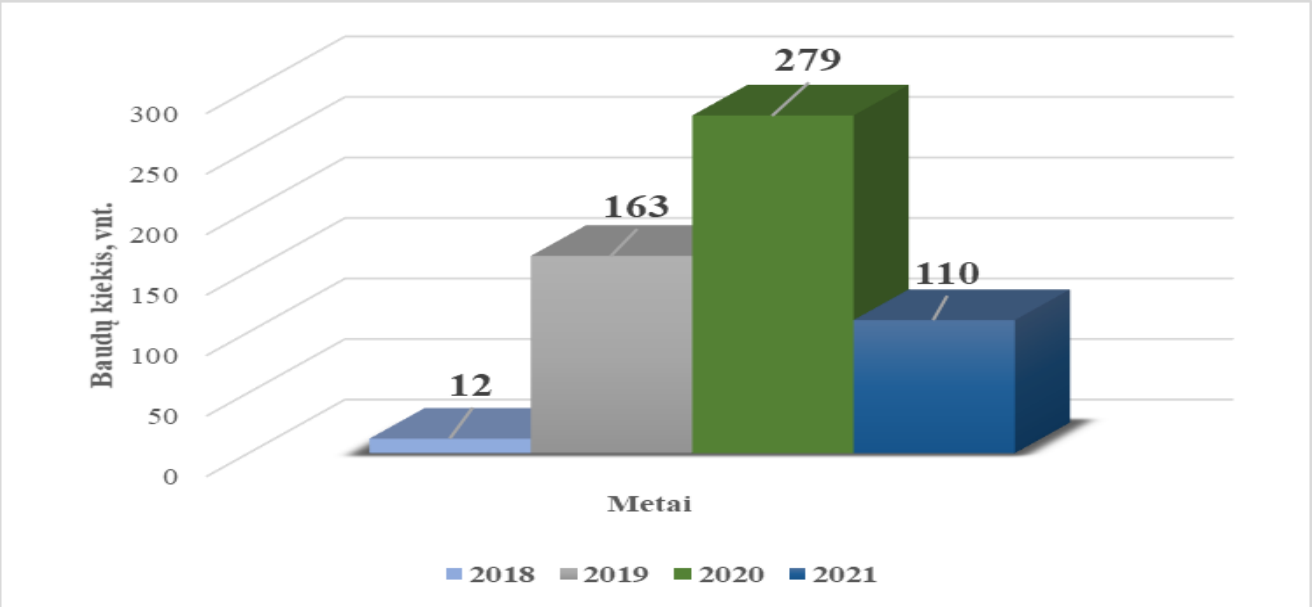
3. BDAR TAIKYMO STARTEGIJOS KŪRIMO TYRIMO REZULTATŲ ANALIZĖ

3.1. Asmens duomenų apsaugos pažeidimų Europoje analizė

Po BDAR priėmimo ir įsigaliojimo asmens duomenų apsauga ne tik kad neprarado savo svarbos, bet tapo dar labiau aktualesnė. Asmens duomenų apsaugos teisėje yra numatytas tinkamų duomenų subjektų teisių gynimas, o tai įrodo organizacijoms skiriamų baudų už asmens duomenų saugumo pažeidimus skaičius bei dydis (pinigine išraiška). Baudų skyrimas yra viena iš rimčiausių organizacijoms taikomų poveikio priemonių už asmens duomenų apsaugos pažeidimų, be šios priemonės organizacijoms gali būti teikiamos rekomendacijos dėl duomenų saugumo užtikrinimo, skiriami papeikimai ar nurodymai.

Kaip jau minėta anksčiau, nacionalinės asmens duomenų apsaugos priežiūros institucijos ES mastu nėra teisiškai įpareigotos viešai skelbti ar EDAV teikti informaciją apie visus įvykusius asmens duomenų apsaugos pažeidimus, tad šiame poskyryje yra analizuojami tik „CMS International“ advokatų kontoros oficialioje baudų už BDAR reikalavimų pažeidimus suvestinėje pateikiami atvejai. Duomenys yra patalpinti internetinėje svetainėje, šiuo adresu: https://www.enforcementtracker.com/ (žiūrėta 2021-03-05). Šios empirinio **tyrimo** dalies **imtis yra 581 atvejis**. Laikoma, kad tyrimo **imtis yra reprezentatyvi**, kadangi į tyrimą yra įtraukiami visi galimi analizuoti (viešai publikuojami) atvejai. Tyrime dalyvaujančių 28 šalių sąrašas yra pateikiamas 3 priede.

Pastaruoju laikotarpiu asmens duomenų apsaugos pažeidimų skaičius auga (žr. 11 pav.).

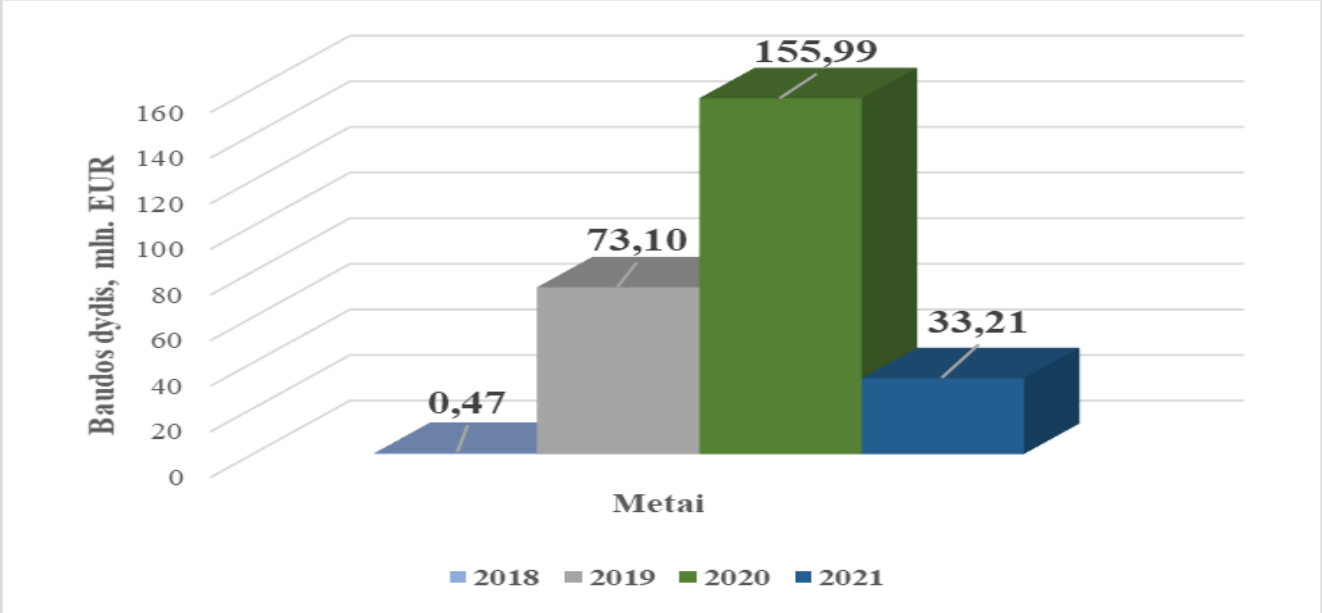


Šaltinis: sudaryta autorės, remiantis CMS International Fines Database: GDPR Enforcement Tracker, 2021

11 pav. 2018-2021 m. baudų, skirtų už asmens duomenų apsaugos pažeidimus pagal BDAR, dinamika kiekine išraiška

Išanalizavus 11 paveiksle pateiktus duomenis (į baudų dinamikos analizę nebuvo įtraukti 17 atvejų, kadangi duomenų šaltinyje nėra nurodoma tiksli jų skyrimo data) galima daryti išvadą, kad baudų kiekis per analizuojamą laikotarpį sparčiai augo. 2018 metais fiksuotų baudų skaičius yra pateikiamas tik laikotarpyje nuo BDAR įsigaliojimo iki metų pabaigos, tad reikšmingas išvadas galima daryti įvertinus skirtų baudų dinamiką 2019 - 2020 metais. 2019 metais skirtų baudų kiekį palyginus su 2020 metų laikotarpiu, nustatyta, kad baudų kiekis išaugo daugiau nei 71 %. Per nepilną pirmąjį 2021 metų ketvirtį jau buvo užfiksuoti 110 asmens duomenų apsaugos pažeidimų, už kuriuos buvo skirtos baudos, o tai sudaro beveik 40 % per 2020 metus skirtų baudų kiekio. Stebint tokį baudų augimo tempą, galima manyti, kad 2021 metų pabaigoje bus matomas ženklus baudų kiekio padidėjimas 2020 metus palyginti su 2021 metais.

Analizuojant baudų, skirtų už asmens duomenų apsaugos pažeidimus pagal BDAR, dydį (pinigine išraiška) taip pat stebima neigiama tendencija (žr. 12 pav.).



Šaltinis: sudaryta autorės, remiantis CMS International Fines Database: GDPR Enforcement Tracker, 2021

12 pav. 2018-2021 m. baudų, skirtų už asmens duomenų apsaugos pažeidimus pagal BDAR, dinamika pinigine išraiška

Kaip matoma iš 12 paveikslo (į baudų dinamikos analizę nebuvo įtraukti 18 atvejų, kadangi duomenų šaltinyje nėra nurodoma tiksli jų suma), baudų dydis išaugo daugiau nei 113 % 2019 metus palyginti su 2020 metais. Šiam ženkliam pokyčiui įtakos turėjo tiek išaugęs asmens duomenų apsaugos pažeidimų kiekis, tiek skirtų baudų dydis:

5 lentelė. Didžiausios 2020 metais už BDAR pažeidimus skirtos baudos

Įmonės pavadinimas	Šalis	Baudos dydis, mln. EUR
H&M Hennes & Mauritz Online Shop A.B. & Co.	Vokietija	35,26
TIM (telecommunications operator)	Italija	27,80

5 lentelės tęsinys

Įmonės pavadinimas	Šalis	Baudos dydis, mln. EUR
British Airways	Jungtinė Karalystė	22,05
Marriott International, Inc	Jungtinė Karalystė	20,45
Wind Tre S.p.A.	Italija	16,70
Vodafone Italia S.p.A.	Italija	12,25

Šaltinis: sudaryta autorės, remiantis CMS International Fines Database: GDPR Enforcement Tracker, 2021

Iš 5 lentelėje pateiktų duomenų matyti, kad 6 per 2020 metus paskirtų didžiausių baudų suma sudaro 133,79 mln. eurų, o tai yra beveik 86 % visos per 2020 metus paskirtų baudų sumos. Šis faktas leidžia teigti, kad likusios 273 per 2020 metus paskirtos baudos buvo santykinai nedidelės, tai reiškia, kad pažeidimas buvo mažiau reikšmingas arba mažesnio masto.

Didžiausia per 2020 metus skirta bauda (35,26 mln. eurų) už asmens duomenų apsaugos pažeidimą buvo paskirta H&M (viena iš drabužių mažmenininko dukterinių bendrovių)įmonei, savo veiklą vykdžiusiai Vokietijoje. Baudą skyrė Vokietijos (Hamburgo) duomenų apsaugos inspekcija. Minimai įmonei bauda buvo skirta už perteklinį kelių šimtų darbuotojų asmens duomenų rinkimą: darbuotojams grįžus į darbą po nedarbingumo dėl ligos ar atostogų, pokalbių metu buvo renkama, įrašoma ir skaitmeniniu būdu saugoma informacija apie darbuotojų atostogų patirtį, ligos simptomus ir diagnozes, šeimos problemas ir religinius įsitikinimus. Ši informacija vėliau buvo naudojama įmonės vadovų, atliekant darbuotojų vertinimus bei priimant sprendimus dėl darbuotojų tinkamumo dirbti įmonėje. Prieigą prie šios informacijos turėjo iki 50 įmonės darbuotojų (vadovų). Ši informacija per klaidą, dėl įmonės sistemų konfigūracijos klaidos, 2019 metų spalio mėnesį kelioms valandoms tapo prieinama visiems įmonėms darbuotojams.

Nors ši skirta bauda ir buvo didžiausia per visą BDAR galiojimo laikotarpį, pasak prof. Dr. Johannes Caspar – Hamburgo duomenų apsaugos inspekcijos specialisto, paskirtos baudos dydis buvo tinkamas ir efektyvus, o taip yra siekiama atgrasyti kitas įmones nuo darbuotojų asmens duomenų saugumo pažeidimų (Schemm, M. (2020). *35,3 Millionen Euro Bußgeld wegen Datenschutzverstößen im Servicecenter von H&M.*).

Anot Jaeger, J. (2020), atitikties specialistės, po šio įvykio H&M pristatė ir pradėjo įgyvendinti išsamų veiksmų planą, skirtą vidaus audito praktikos tobulinimui bei duomenų privatumo saugos užtikrinimui: personalo pokyčiai (vadovų lygmenyje); papildomi vadovų mokymai apie duomenų saugą ir darbo teisę; patikslintos vadovų instrukcijos; naujos pareigybės, susijusios su asmens duomenų apsaugos užtikrinimu, įsteigimas; patobulinti IT sprendimai duomenų valdymui bei saugojimui.

Už asmens duomenų apsaugos pažeidimus taikomos vienos iš poveikių priemonių, tai yra baudų skyrimo, analizė kiekine ir pinigine išraiška leidžia tik susidaryti bendrą vaizdą, kaip dažnai yra pažeidžiami BDAR įtvirtinti reikalavimai, ir kokios sankcijos laukia organizacijų už šių reikalavimų nevykdymą. Siekiant identifikuoti dažniausiai pažeidžiamus BDAR straipsnius ir nustatyti organizacijų BDAR taikymo strategijos problemines sritis, toliau darbe yra atliekama asmens duomenų apsaugos pažeidimų analizė skirtingais pjūviais: pagal pažeidimo rūšį, pagal organizacijos vykdomos veiklos sritį (sektorių) ir pagal šalį.

Pradžioje visi analizuojami asmens duomenų apsaugos pažeidimų atvejai buvo suskirstyti į atskiras kategorijas pagal pažeidžiamą BDAR straipsnį:

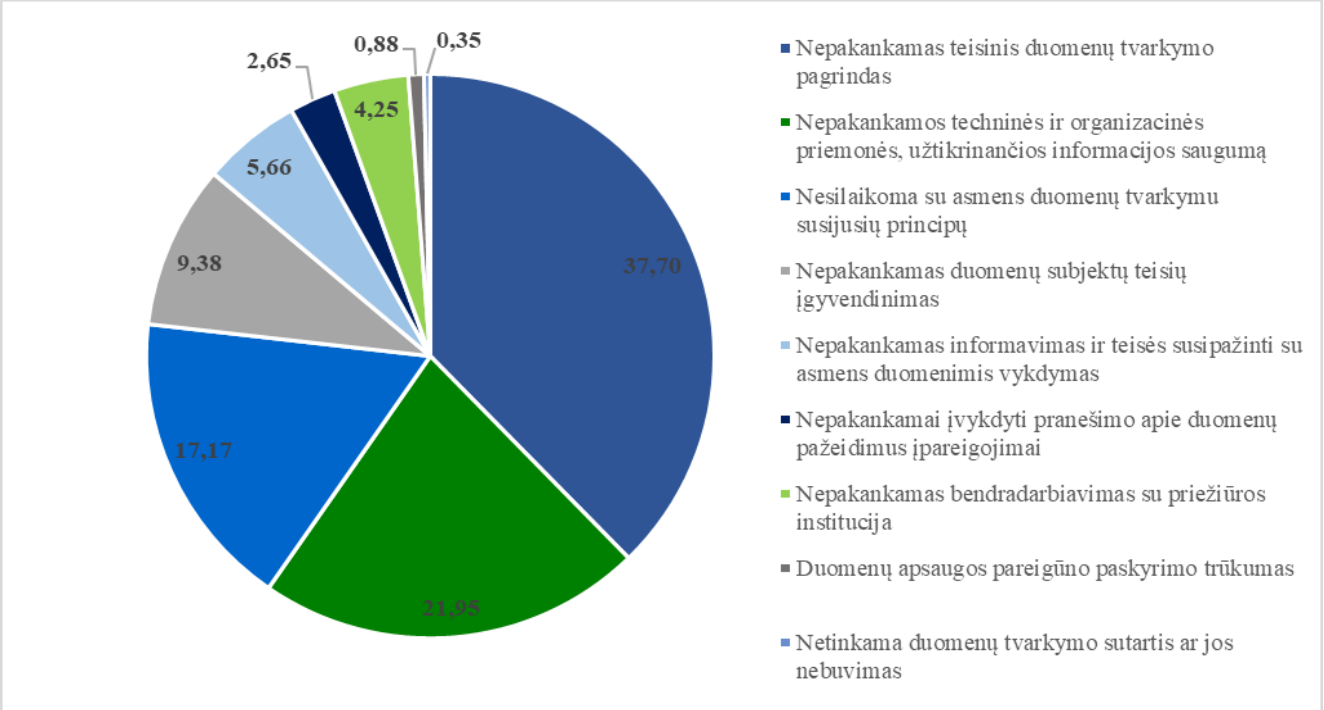
6 lentelė. Asmens duomenų saugumo pažeidimų kategorijos

	Kategorija	**Pagrindinis BDAR str.**	**Papildomas BDAR str.**
1.	Nepakankamas teisinis duomenų tvarkymo pagrindas	**6, 5**	**7, 9, 36**
2.	Nepakankamos techninės ir organizacinės priemonės, užtikrinančios informacijos saugumą	**32, 5**	
3.	Nesilaikoma su asmens duomenų tvarkymu susijusių principų	**5**	**8, 24, 25, 29, 30, 35**
4.	Nepakankamas duomenų subjektų teisių įgyvendinimas	**12, 15, 17, 21**	**16, 18**
5.	Nepakankamas informavimas ir teisės susipažinti su asmens duomenimis vykdymas	**13, 14**	**58,83**
6.	Nepakankamai įvykdyti pranešimo apie duomenų pažeidimus įpareigojimai	**33, 44**	**31, 58**
7.	Duomenų apsaugos pareigūno paskyrimo trūkumas	**37**	
8.	Nepakankamas bendradarbiavimas su priežiūros institucija	**31, 58**	
9.	Netinkama duomenų tvarkymo sutartis ar jos nebuvimas	**28**	

Šaltinis: sudaryta autorės (žr. 4 ir 5 priedus), remiantis CMS International Fines Database: GDPR Enforcement Tracker (2021) ir „Europos parlamento ir tarybos reglamentas (ES) 2016/679”

Asmens duomenų saugumo pažeidimų analizė, suskirstant asmens duomenų apsaugos pažeidimus į atskiras 9 kategorijas pagal BDAR pažeidžiamą straipsnį, leido identifikuoti BDAR įtvirtintų reikalavimų taikymo organizacijoje problemines sritis, kurioms turėtų būti skiriamas didesnis dėmesys organizacijoje planuojant ir diegiant tinkamas organizacines ir technines priemonės siekiant užtikrinti tinkamą asmens duomenų apsaugą valdant ir tvarkant duomenų subjektų duomenis. Asmens duomenų apsaugos pažeidimus skirstant į atskiras kategorijas, kategorijoms buvo priskirti pagrindiniai ir papildomi, mažesnės reikšmės pažeidimui turėję, BDAR straipsniai.

Atlikus asmens duomenų apsaugos pažeidimų analizę Europoje 2018 – 2021 metais pagal nurodytas kategorijas, nustatyta:

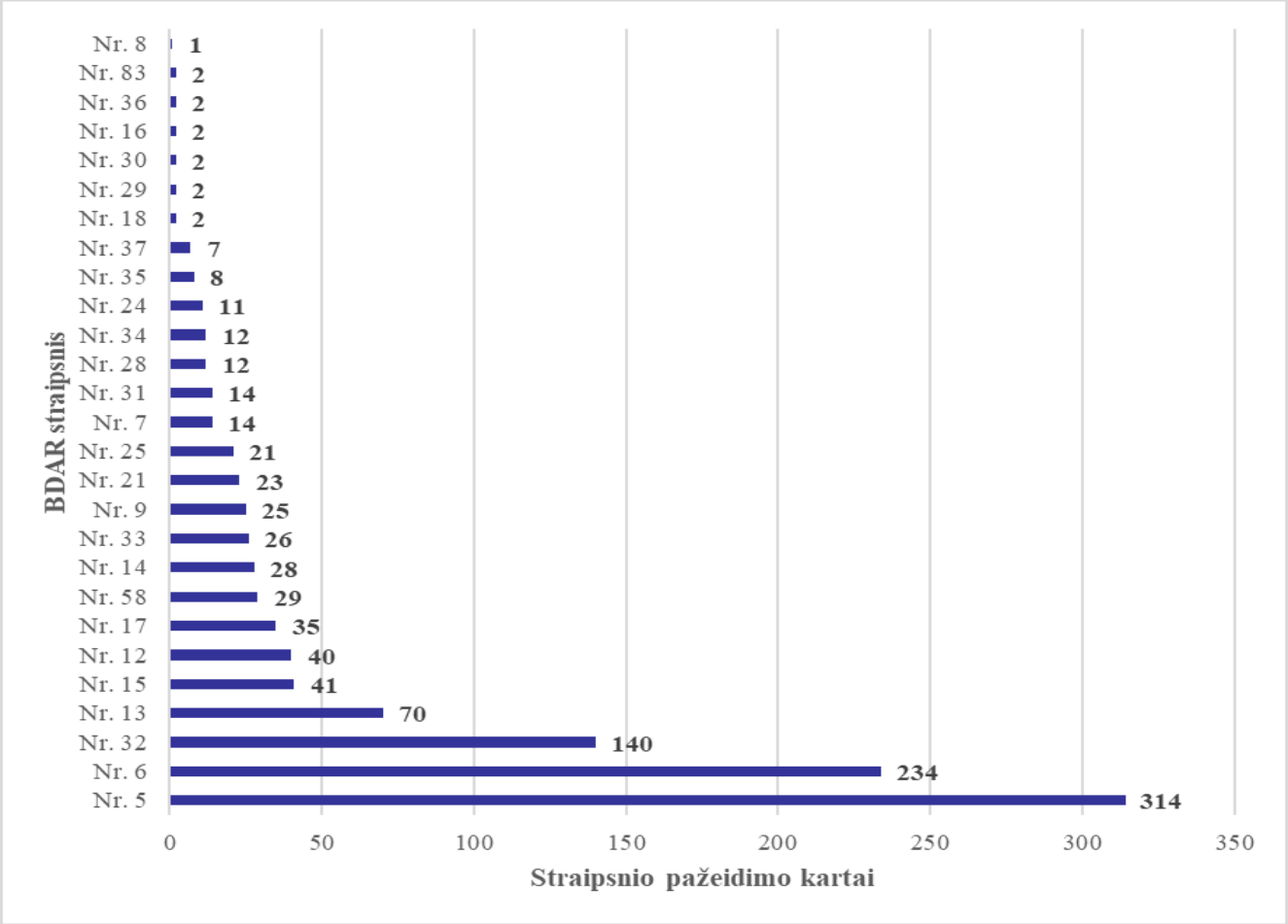


Šaltinis: sudaryta autorės, remiantis CMS International Fines Database: GDPR Enforcement Tracker (2021) ir „Europos parlamento ir tarybos reglamentas (ES) 2016/679"

13 pav. Asmens duomenų apsaugos pažeidimų pasiskirstymas pagal kategorijas, proc.

Dažniausiai nustatoma asmens duomenų apsaugos pažeidimų priežastis yra nepakankamas teisinis duomenų tvarkymo pagrindas, ši kategorija sudaro beveik 38 % visų analizuotų pažeidimų. Ši kategorija pagrinde grindžiama BDAR 6 straipsnio „Tvarkymo teisėtumas" pažeidimu. Antroji pagal dažnumą pasitaikanti priežastis yra nepakankamas techninių ir organizacinių priemonių, užtikrinančių informacijos saugumą, taikymas organizacijoje, ši kategorija sudaro beveik 22 % visų analizuotų pažeidimų. Ši kategorija pagrinde grindžiama BDAR 32 straipsnio „Duomenų tvarkymo saugumas", už kurio įgyvendinimą yra atsakingi duomenų valdytojas ir duomenų tvarkytojas, pažeidimu. Nesilaikymas su asmens duomenų tvarkymu susijusių principų, pagrinde pažeidžiant BDAR 5 straipsnį „Su asmens duomenų tvarkymu susiję principai", yra trečioji pagal dažnumą pasitaikanti asmens duomenų saugumo pažeidimų priežastis, sudaranti 17,17 % visų analizuotų pažeidimų. Dėl šių 3 įvardintų asmens duomenų saugumo pažeidimų priežasčių įvyko daugiau nei 77 % visų analizuotų pažeidimų. Taip pat nustatyta, kad rečiau pasitaikančios, tačiau ne mažiau svarbios, pažeidimų priežastys yra: nepakankamas duomenų subjektų teisių įgyvendinimas (9,38 %), nepakankamas informavimas ir teisės susipažinti su asmens duomenimis vykdymas (5,66 %), nepakankamas bendradarbiavimas su priežiūros institucija (4.25 %) ir nepakankamai įvykdyti pranešimo apie duomenų pažeidimus įpareigojimai (2,65 %).

Siekiant labiau detalizuoti asmens duomenų apsaugos pažeidimų analizės pagal nurodytas kategorijas rezultatus, buvo atlikta atskirų BDAR straipsnių pažeidimų dažnio analizė (žr. 14 pav.).



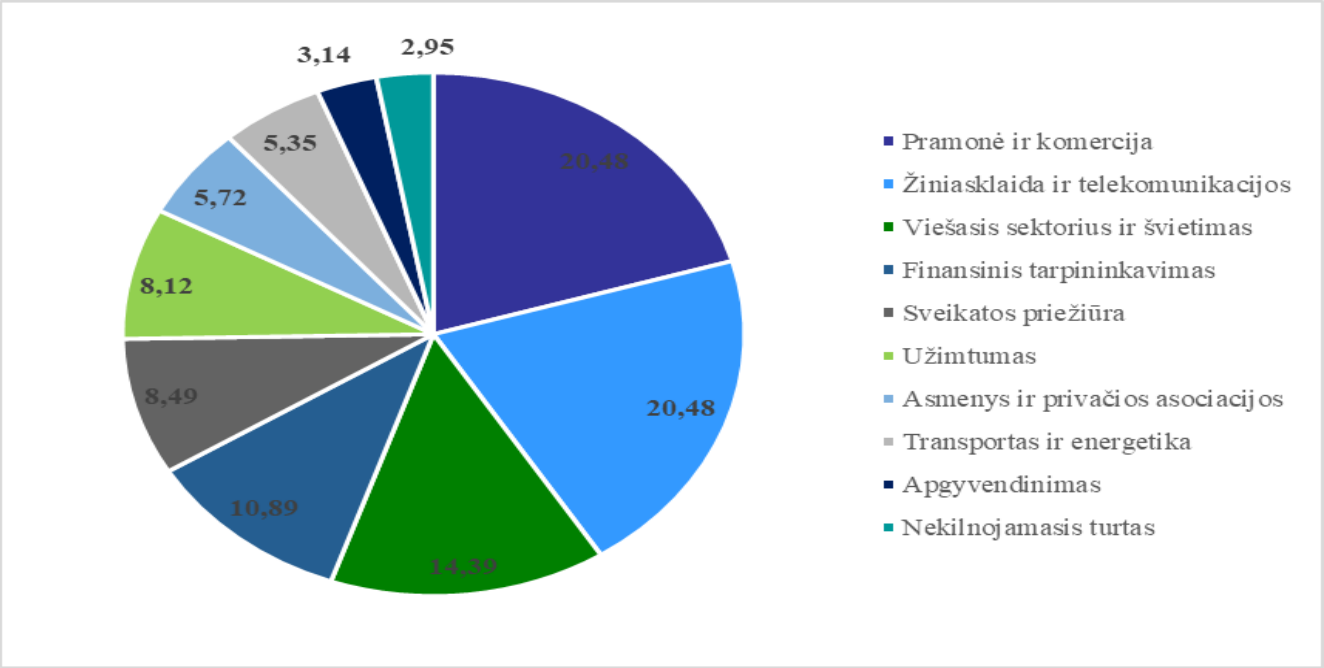
Šaltinis: sudaryta autorės (žr. 4 priedą), remiantis CMS International Fines Database: GDPR Enforcement Tracker (2021)

14 pav. Pažeistų BDAR straipsnių dažnis , vnt.

14 paveiksle pateiktų duomenų analizė atskleidė, kad per visą analizuojamą laikotarpį dažniausiai buvo pažeidžiamas 5 BDAR straipsnis, reglamentuojantis su asmens duomenų tvarkymu susijusių principų laikymąsi. Šis straipsnis kelerių metų laikotarpyje buvo pažeistas 314 kartų. Antrasis pagal dažnumą pažeidžiamas straipsnis yra 6 BDAR straipsnis – „Tvarkymo teisėtumas“ (pažeistas 234 kartus). Trečioje vietoje pagal pažeidžiamumo dažnį yra 32 BDAR straipsnis - „Duomenų tvarkymo saugumas“, kuris per visą analizuojamą laikotarpį buvo pažeistas 140 kartų. Duomenų subjekto teisė į tinkamą informavimą ir teisė susipažinti su asmens duomenimis buvo netinkamai vykdoma 70 kartų pažeidžiant 13 BDAR straipsnį ir 28 kartus pažeidžiant 14 BDAR straipsnį. Tinkamas duomenų subjekto teisių įgyvendinimas nebuvo vykdomas 41 kartą pažeidžiant 15, 40 kartų pažeidžiant 12, 35 kartus pažeidžiant 17 ir 23 kartus pažeidžiant 21 BDAR straipsnius. Nemažiau svarbu yra paminėti ir 58 BDAR straipsnio pažeidimų dažnį: per analizuojamą laikotarpį 29 kartus buvo neužtikrintas pakankamas bendradarbiavimas su priežiūros institucijomis ir jų įgaliojimų vykdymas.

Šie rezultatai leidžia teigti, kad probleminės tinkamo BDAR įtvirtintų reikalavimų vykdymo sritys yra: 5, 6, 12, 13, 14, 15, 17 , 21, 32 ir 58 BDAR straipsnių įgyvendinimas.

Asmens duomenų apsaugos pažeidimai yra fiksuojami įvairias ekonominės veiklos rūšis vykdančiose organizacijose (žr. 15 pav.).



Šaltinis: sudaryta autorės, remiantis CMS International Fines Database: GDPR Enforcement Tracker (2021)

15 pav. Asmens duomenų apsaugos pažeidimų pasiskirstymas pagal vykdomos veiklos rūšį, proc.

Apibendrinant 15 paveiksle pateiktus duomenis, galima teigti, kad dažniausiai asmens duomenų apsaugos pažeidimai fiksuojami organizacijose, vykdančiose veiklą, susijusią su pramone ir komercija (20,48 %) bei su žiniasklaida ir telekomunikacijomis (20,48 %). Sekančios 3 veiklos sritys, kuriose yra fiksuojamas didžiausias asmens duomenų apsaugos pažeidimų skaičius, yra: viešasis sektorius ir švietimas (14,39 %), finansinis tarpininkavimas (10.89 %) ir sveikatos priežiūra (8.49 %).

Toliau darbe pateikiama statistika rodo, kiek baudų ir kokia baudų suma per analizuojamą laikotarpį buvo paskirta kiekvienai šaliai (žr. 7 lentelę).

7 lentelė. 10 šalių, kurioms buvo skirtas didžiausias baudų kiekis

	Šalis	Skirtų baudų skaičius, vnt.	Skirtų baudų dydis, mln. EUR
1.	Ispanija	190	16,16
2.	Italija	51	70,60
3.	Rumunija	48	0,67
4.	Vengrija	38	0,75
5.	Vokietija	29	48,89
6.	Belgija	23	0,91
7.	Lenkija	21	1,79
8.	Bulgarija	20	3,21
9.	Norvegija	20	1,13
10.	Švedija	17	12,33

Šaltinis: sudaryta autorės, remiantis CMS International Fines Database: GDPR Enforcement Tracker (2021)

Kaip matyti iš 7 lentelėje pateiktų duomenų, daugiausiai baudų, kaip poveikio priemonės už asmens duomenų apsaugos pažeidimą, per visą analizuojamą laikotarpį buvo skirta Ispanijai (190 baudų), Italijai (51 bauda) ir Rumunijai (48 baudos). Tačiau analizuojant skirtų baudų dydį matyti, jog šioje srityje pirmą vietą užima Italija, kuriai skirtų baudų suma siekia 70,60 mln. eurų. Antroje vietoje yra Vokietija, kuriai už 29 asmens duomenų saugumo pažeidimus buvo skirta baudų už 48,89 mln. eurų. Ispanija, esanti 1 vietoje pagal skirtų baudų už asmens duomenų saugumo pažeidimus kiekį, yra trečioje vietoje pagal skirtų baudų sumą, kuri siekia 16,16 mln. eurų. Šis faktas leidžia teigti, kad baudų kiekis, skirtas konkrečiai šaliai, nėra pagrindinis rodiklis, lemiantis baudų sumos dydį. Tam įtakos dažniausiai turi asmens duomenų apsaugos pažeidimo mastas ir reikšmingumas bei organizacijos, kuriai skiriama bauda, ankstesnių finansinių metų bendros metinės pasaulinės apyvartos suma, kuria remiantis ir yra skiriama administracinė nuobauda.

Įvertinus atliktos asmens duomenų apsaugos pažeidimų Europoje analizės rezultatus, galima daryti išvadą, jog tinkamas BDAR įtvirtintų reikalavimų įgyvendinimas organizacijoje yra ypatingai svarbus. Nustatytas asmens duomenų saugumo pažeidimų kiekis bei už juos skirtų sankcijų (baudų) dydis tik dar kartą įrodo, kad BDAR įtvirtintų reikalavimų taikymo strategijos tobulinimas organizacijoje yra vienas iš jos prioritetinių uždavinių, siekiant užtikrinti tinkamą asmens duomenų apsaugą bei išvengti už pažeidimus taikomų sankcijų.

Kaip teigia Lietuvos asmens duomenų apsaugos direktorius R. Andrijauskas, aptardamas VDAI 2020 metų veiklos rezultatus, 2020 metai asmens duomenų apsaugos priežiūros institucijoms bei daugeliui kitų organizacijų, buvo išskirtiniai dėl prasidėjusios pasaulinės koronaviruso COVID-19 pandemijos. Metų pradžioje prasidėjusi ir vis dar besitęsianti pandemija kėlė ir vis dar kelia daug naujų asmens duomenų tvarkymo iššūkių: daug veiklų buvo skaitmenizuojamos, daugybė žmonių, privataus ir viešojo sektoriaus organizacijų persikėlė į nuotolines bendravimo ir veiklos platformas. Dėl šios priežasties tvarkomų asmens duomenų apimtys staiga išaugo ir, tikėtina, ši nauja realybė niekuomet nesugrįš į buvusią padėtį (Valstybinės duomenų apsaugos inspekcijos 2020 metų veiklos ataskaita, (2021)).

Būtina pabrėžti, kad dėl tvarkomų asmens duomenų staigaus apimčių išaugimo kylančios rizikos privalo būti suvaldytos užtikrinant asmens duomenų apsaugos principų pritaikymą siekiant tolesnio tvaraus skaitmenizacijos procesų vystymosi, kuris yra neišvengiamas. Šiuo tikslu aktyviai veikti privalo ne tik visų ES valstybių narių priežiūros institucijos ir jas vienijanti EDAV, bet būtent ir pačios organizacijos, kurios visų pirmiausia ir yra atsakingos už tinkamą asmens duomenų valdymą bei tvarkymą.

3.2. Ekspertinio vertinimo rezultatų analizė

Remiantis atliktos asmens duomenų apsaugos pažeidimų Europoje analizės rezultatais bei teorinėje darbo dalyje išryškintais aspektais buvo suformuluoti ekspertiniam vertinimui atlikti skirti klausimai. Ekspertiniam vertinimui atlikti pasirinktas instrumentas – anketa (žr. 2 priedą). Anketoje pateiktų klausimų pagalba buvo siekiama įvertinti BDAR taikymo strategijos kūrimo svarbą organizacijoje, identifikuoti pagrindines priežastis, lemiančias asmens duomenų apsaugos pažeidimus organizacijoje, bei atsižvelgiant į ekspertų pateiktą nuomonę suformuluoti praktines rekomendacijas BDAR taikymo strategijos optimizavimui.

Tyrimo organizavimas. Tyrimas buvo atliekamas 2021 metų kovo mėnesio 22 – balandžio mėnesio 6 dienomis. Tiriamųjų imčiai pagrįsti taikytas netikimybinė tikslinės atrankos tipas. Tiriamųjų atrankos pagrindimas, bei informantų atrankos kriterijai:

- Duomenų apsaugos pareigūno paslaugą siūlančios įmonės;
- Duomenų apsaugos srityje dirbantys specialistai;
- BDAR atitikties užtikrinimo paslaugą siūlančios įmonės;
- BDAR atitikties mokymus siūlančios įmonės.

Anketinė apklausa respondentams buvo pateikiama elektroniniu būdu, tai yra, naudojant internetinį apklausų portalą www.apklausa.lt . Tiesioginė nuoroda į apklausą respondentams buvo siunčiama prieš tai su jais susisiekus telefonu bei gavus jų sutikimą dalyvauti tyrime.

Tyrimo metu buvo apklausta specialiai parinkta žmonių grupė, kurią sudarė **9 ekspertai** turintys žinių asmens duomenų apsaugos srityje. 2 iš 9 respondentų nepanoro, kad jų asmens duomenys (vardas, pavardė ar darbovietės pavadinimas) būtų atskleisti ir minimi šiame darbe, tad visi apklausti ekspertai šiame tyrime yra laikomi anoniminiais ir įvardijami kaip: Respondentas A, Respondentas B, Respondentas C, Respondentas D, Respondentas E, Respondentas F, Respondentas G, Respondentas H ir Respondentas I.

Tyrime dalyvavusių ekspertų nuomonių suderinamumas. Prieš analizuojant ekspertinio vertinimo metu gautus rezultatus yra būtina įsitikinti, kad apklausoje dalyvavusių respondentų nuomonės yra suderintos. Pasak Podvezko, V. (2005), ekspertų nuomonės ir požiūris į sprendžiamą problemą dažnai skiriasi, gali būti ir prieštaringi. Jeigu reikia priimti sprendimą ekspertų vertinimų pagrindu, būtina įvertinti ekspertų nuomonių suderinamumo laipsnį, kuris yra vertinamas konkordancijos koeficientu („W“). Konkordancijos koeficientas vertina objekto rangų sumos kvadratų nuokrypį nuo bendro vidurkio:

Ekspertizės objektas	EKSPERTAS											
	1	2	3	4	5	6	7	8	9	$\tilde{R}_i$	S_i	S_i^2
Nr. 1	2	2	2	1	2	1	1	2	3	16	-21	441
Nr. 2	2	2	1	1	2	1	1	2	3	15	-22	484
Nr. 3	2	2	2	2	2	1	3	2	2	18	-19	361
Nr. 4	2	2	1	1	2	1	1	2	3	15	-22	484
Nr. 5	2	3	1	1	2	1	1	2	4	17	-20	400
Nr. 6	2	2	2	1	2	1	1	2	2	15	-22	484
Nr. 7	2	3	3	2	2	1	3	2	2	20	-17	289
Nr. 8	2	2	2	1	2	1	1	2	2	15	-22	484
Nr. 9	2	2	2	2	2	1	2	2	3	18	-19	361
									Suma:	149		3788

$\tilde{R}$	=	37
$\tilde{S}$	=	3788
W	=	0,779

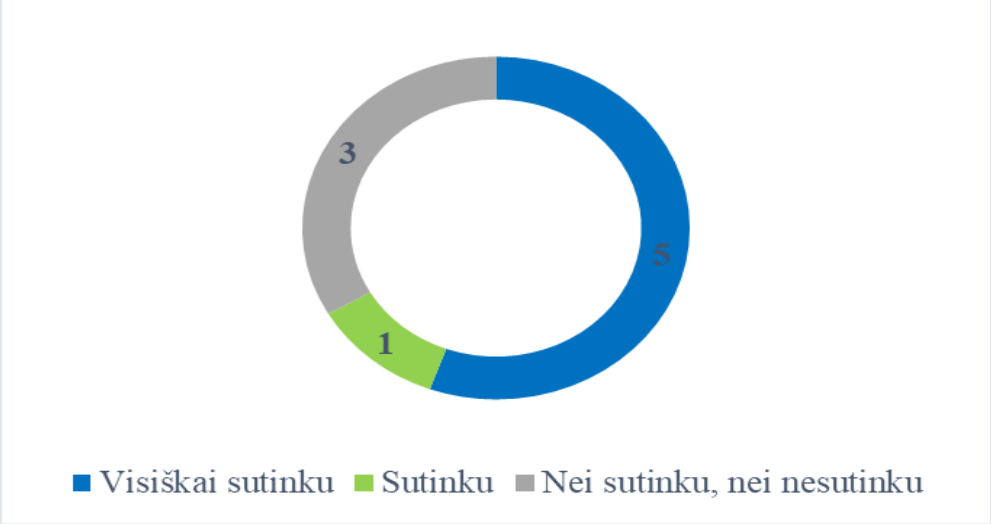
Šaltinis: sudaryta autorės, remiantis Podvezko, V. (2005).

16 pav. Konkordancijos koeficiento apskaičiavimas

Jei ekspertų nuomonės suderintos, konkordancijos koeficiento W reikšmė yra arti vieneto, jei vertinimai labai skiriasi - W reikšmė yra arti nulio. Gautas konkordancijos koeficientas „**W“ yra 0,779**, tad galima teigti, jog ekspertų nuomonės yra suderintos pakankamai ir ekspertų vertinimų rezultatus galima taikyti praktikoje.

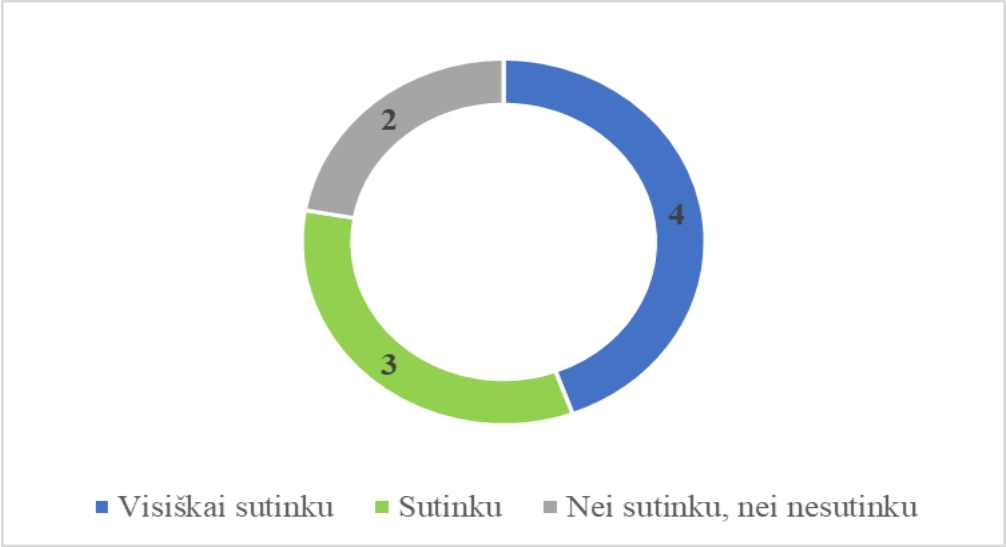
Ekspertų apklausos metu gautų duomenų apdorojimui bei grafiniam atvaizdavimui buvo pasirinktos SPSS ir Microsoft Excel programos.

Pirmuoju ekspertams pateiktu klausimu buvo siekiama nustatyti, ar ekspertai sutinka su teiginiu, jog BDAR taikymo strategijos kūrimas yra svarbus ir prioritetinis organizacijos uždavinys:



Šaltinis: sudaryta autorės, remiantis ekspertinio vertinimo rezultatais

17 pav. Ekspertų nuomonė apie tai, ar BDAR taikymo strategijos kūrimas yra prioritetinis organizacijos uždavinys

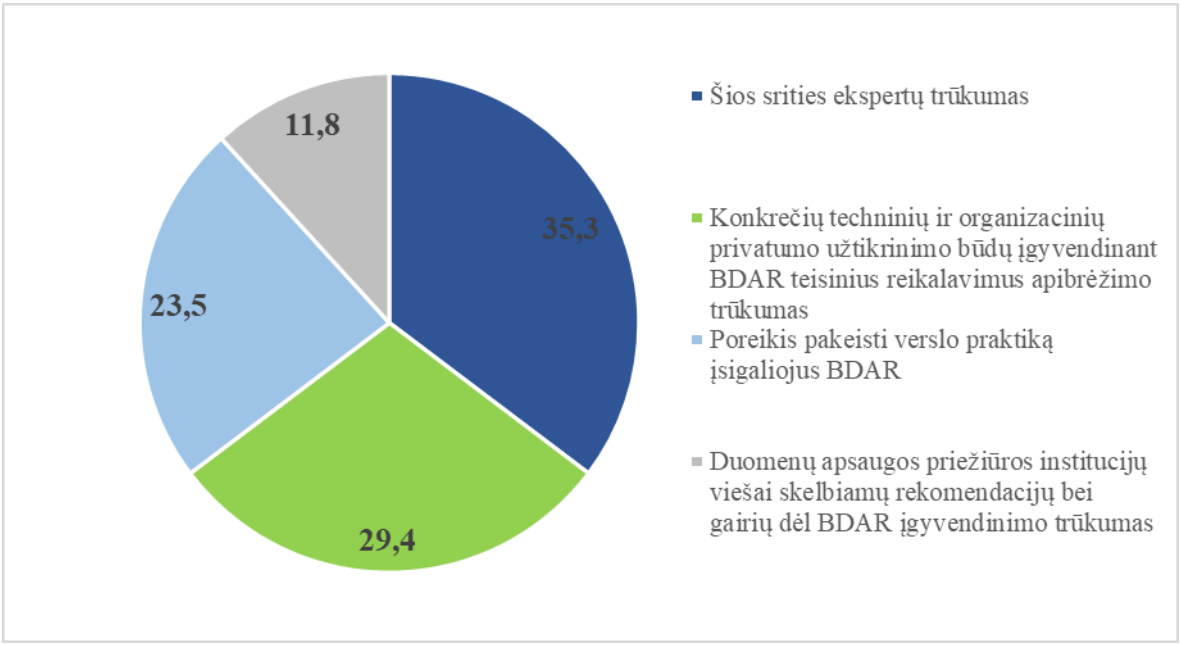


Šaltinis: sudaryta autorės, remiantis ekspertinio vertinimo rezultatais

18 pav. Ekspertų nuomonė apie tai, ar BDAR taikymo strategijos kūrimas organizacijoje yra sudėtingas uždavinys

Kaip matyti iš 17 ir 18 paveikslų, 6 ekspertai sutiko (pasirinkdami rangavimo variantus „Visiškai sutinku“ ir „Sutinku“) su teiginiu, jog BDAR taikymo strategijos kūrimas yra prioritetinis organizacijos uždavinys. 7 ekspertai sutiko (pasirinkdami rangavimo variantus „Visiškai sutinku“ ir „Sutinku“) su teiginiu, jog BDAR taikymo strategijos kūrimas organizacijoje yra sudėtingas uždavinys.

Antrame klausime ekspertų buvo prašoma nurodyti, su kokiomis kliūtimis dažniausiai susiduria organizacijos siekdamos užtikrinti tinkamą asmens duomenų apsaugą:



Šaltinis: sudaryta autorės, remiantis ekspertinio vertinimo rezultatais

19 pav. Ekspertų nuomonė apie tai, su kokiomis kliūtimis dažniausiai susiduria organizacijos siekdamos užtikrinti tinkamą asmens duomenų apsaugą, proc.

Ekspertų nuomone, dažniausiai organizacijos, siekdamos užtikrinti tinkamą asmens duomenų apsaugą, susiduria su šios srities ekspertų trūkumo problema (35,3 %). Antroji pagal dažnumą kliūtis, su kuria susiduria organizacijos, ekspertų buvo įvardinta kaip konkrečių techninių ir organizacinių privatumo užtikrinimo būdų įgyvendinant BDAR teisinius reikalavimus apibrėžimo trūkumas (29,4 %). Poreikis pakeisti verslo praktiką įsigaliojus BDAR buvo įvardintas kaip trečioji pagal dažnumą pasitaikanti kliūtis (23,5 %). Kaip rečiausiai pasitaikanti kliūtis buvo įvardinta duomenų apsaugos priežiūros institucijų viešai skelbiamų rekomendacijų bei gairių dėl BDAR įgyvendinimo trūkumas (11,8 %).

Ekspertų taip pat buvo paprašyta įvardinti papildomas kliūtis, nepaminėtas tarp antrame klausime pateiktų galimų pasirinkti variantų, su kuriomis, jų nuomone, susiduria organizacijos siekdamos užtikrinti tinkamą asmens duomenų apsaugą. Ekspertai, dalyvavę tyrime, įvardijo šias papildomas kliūtis:

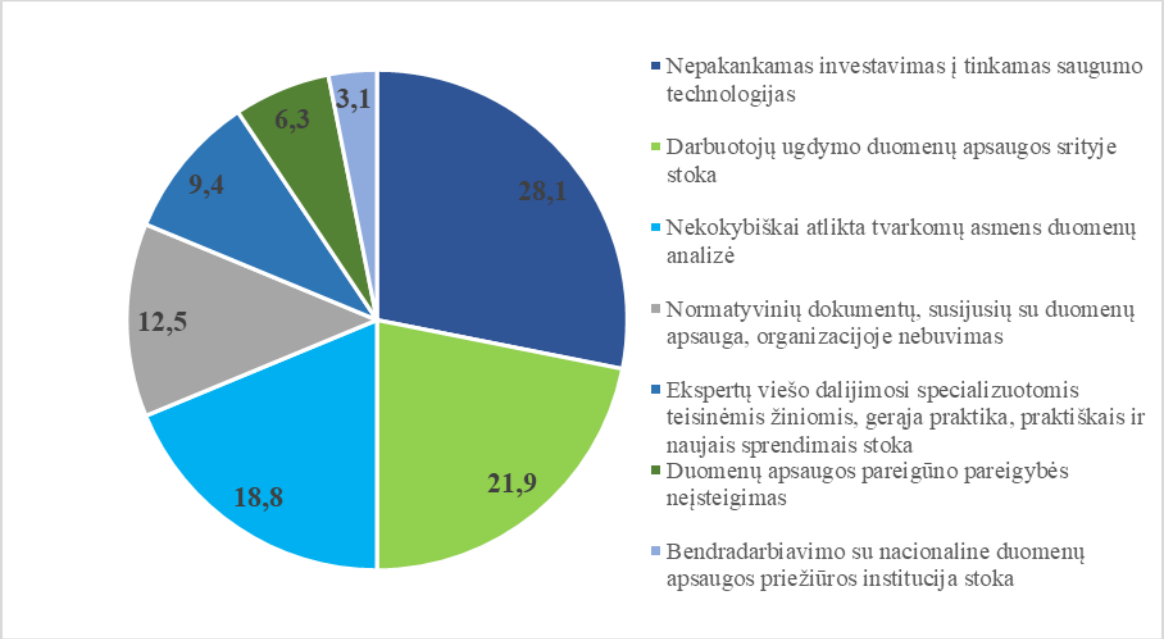
8 lentelė. Ekspertų nurodytos papildomos kliūtys, su kuriomis dažniausiai susiduria organizacijos siekdamos užtikrinti tinkamą asmens duomenų apsaugą

	Ekspertų įvardintos kliūtys
1.	Finansinių išteklių trūkumas
2.	Per daug abstrakčios BDAR taisyklės
3.	Per daug erdvės priežiūros institucijai interpretuoti BDAR taisykles
4.	Žinių trūkumas
5.	Įrankių, skirtų įvertinti organizacijoje taikomų techninių ir organizacinių priemonių duomenų apsaugos užtikrinimui pakankamumą, trūkumas
6.	Poreikis diegti naujas ir / ar papildomas technologijas bei programas

Šaltinis: sudaryta autorės, remiantis ekspertinio vertinimo rezultatais

Apibendrinant ekspertų įvardintas papildomas kliūtis, kelias kliūtis galima būtų priskirti prie klausime pateiktų galimų atsakymų variantų grupių: „Per daug abstrakčios BDAR taisyklės“ ir „Per daug erdvės priežiūros institucijai interpretuoti BDAR taisykles“ galėtų būti priskirtos prie „Konkrečių techninių ir organizacinių privatumo užtikrinimo būdų įgyvendinant BDAR teisinius reikalavimus apibrėžimo trūkumo“ kliūties. Tokiu atveju ši kliūtis įgyja dar didesnį svarbą. Dar viena ekspertų įvardinta kliūtis „Žinių trūkumas“ taip pat galėtų būti priskirta prie „Šios srities ekspertų trūkumo“ kategorijos.

Ekspertų buvo paprašyta nurodyti priežastis (leidžiant pasirinkti kelis variantus), pagrinde lemiančias asmens duomenų apsaugos pažeidimus organizacijoje:



Šaltinis: sudaryta autorės, remiantis ekspertinio vertinimo rezultatais

20 pav. Ekspertų nuomonė apie tai, kokios priežastys pagrinde lemia asmens duomenų apsaugos pažeidimus organizacijoje, proc.

Kaip vieną iš pagrindinių priežasčių, lemiančių asmens duomenų apsaugos pažeidimus organizacijoje, ekspertai įvardijo „Nepakankamą investavimą į tinkamas saugumo technologijas“ (28,1 %). Antra, ne ką mažiau svari priežastis nei pirmoji, buvo įvardinta kaip „Darbuotojų ugdymo duomenų apsaugos srityje stoka“ (21,9 %). „Nekokybiškai atlikta tvarkomų asmens duomenų analizė“ buvo įvardinta kaip trečioji priežastis pagrinde lemianti asmens duomenų apsaugos pažeidimus organizacijoje (18,8 %). „Bendradarbiavimo su nacionaline duomenų apsaugos priežiūros institucija stoka“, ekspertų nuomone, yra priežastis, rečiausiai lemianti asmens duomenų apsaugos pažeidimus (3,1 %).

Ekspertų buvo paprašyta įvardinti papildomas priežastis, nepaminėtas tarp trečiame klausime pateiktų galimų pasirinkti variantų, lemiančias asmens duomenų apsaugos pažeidimus organizacijoje:

9 lentelė. Ekspertų nurodytos papildomos priežastys, lemiančios asmens duomenų apsaugos pažeidimus organizacijoje

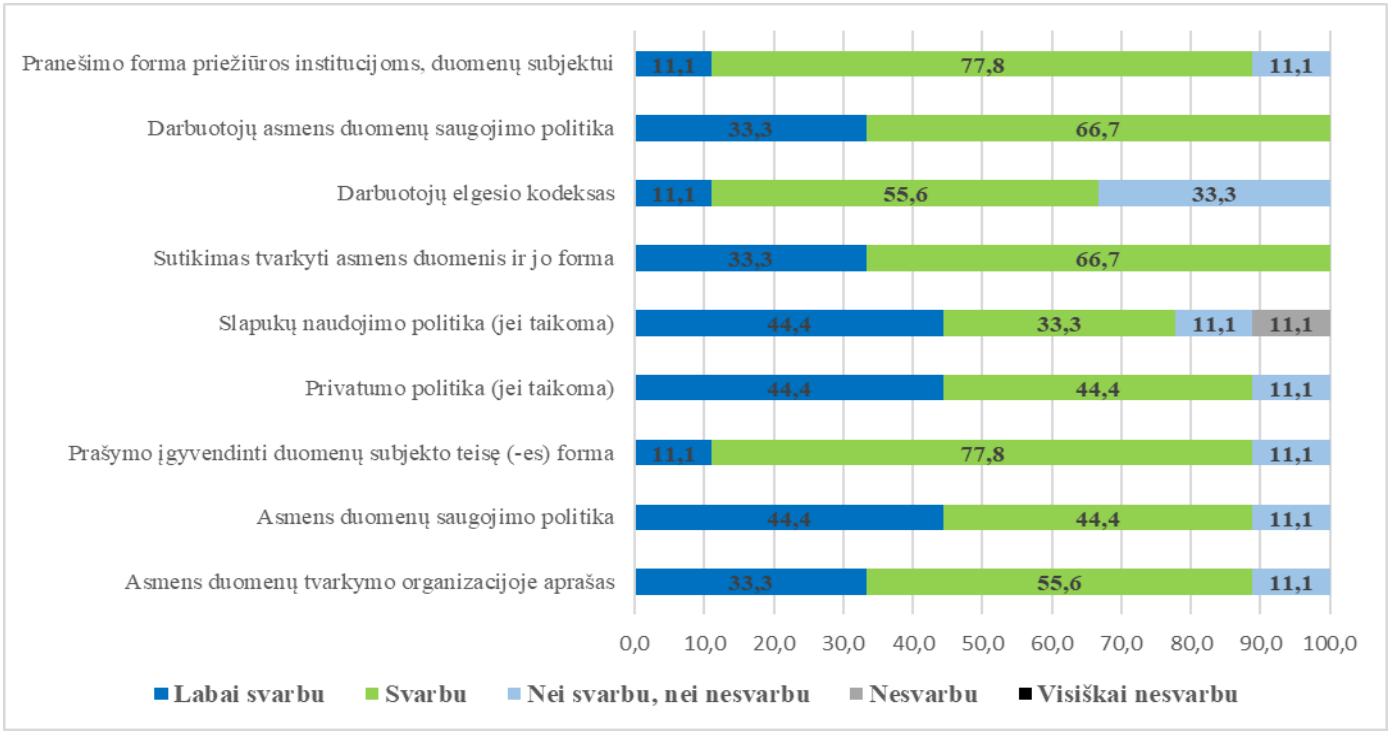
Ekspertų įvardintos priežastys	
1.	Nepakankamas mokymų duomenų apsaugos srityje rengimas
2.	Organizacijos darbuotojų suvokimo apie asmens duomenų apsaugos svarbą stoka
3.	Neaiškus atsakomybių paskirstymas tarp duomenų valdytojo ir tvarkytojo
4.	BDAR numatytų pareigų (veiklos įrašai, PDAV, ADSP) nevykdymas
5.	Nežinojimas, aplaidumas, žiūrėjimas "pro pirštus" į duomenų saugumą
6.	Per daug abstrakčios BDAR taisyklės
7.	Priežiūros institucijų priimamų sprendimų, kuriais konstatuojami pažeidimai, viešinimo stoka
8.	Neatsižvelgimas į duomenų apsaugos pareigūno nuomonę

Šaltinis: sudaryta autorės, remiantis ekspertinio vertinimo rezultatais

Apibendrinant galima teigti, kad priežastis - „Darbuotojų ugdymo duomenų apsaugos srityje stoka“ – įgyja dar didesnę svarbą, kadangi ekspertų nurodytos papildomos priežastys nr. 1, 2, 4 ir 5 galėtų būti priskiriamos būtent šios kategorijos priežasčių grupei. Ekspertinio vertinimo metu gautus rezultatus patvirtina ir kitų mokslininkų bei šios srities specialistų atliktas tyrimas (apklausa): atlikus JAV, Europos, Kinijos ir Japonijos įmonių apklausą siekiant įvertinti BDAR įtvirtintų reikalavimų taikymo progresą šalyse, net 45 % respondentų nurodė, kad aplaidus ir neatsakingas darbuotojų elgesys yra pagrindinė priežastis, dėl kurios organizacijoje įvyksta asmens duomenų apsaugos pažeidimai. (Keeping pace in the GDPR race: a global view of GDPR progress in the United States, Europe, China and Japan, (2019)).

Pasak Molony, D. ir Leemans, V. (2018), net ir taikant tinkamas priemones, ne visada pavyksta išvengti asmens duomenų apsaugos pažeidimų vykdant veiklą. Viena iš priemonių, amortizuojančių patiriamus nuostolius, įvykus pažeidimui, yra kibernetinių grėsmių draudimas. Anot mokslininkų, BDAR greičiausiai paveiks kibernetinio draudimo rinką tiek ES, tiek ir kitose šalyse. Nesvarbu, ar tai yra duomenų apsaugos pažeidimas, išpirkos reikalaujanti programinė įranga, ar asmens duomenų vagystė, vykdoma elektroninio pašto žinutėmis – įmonės susiduria su nuolat kintančiomis kibernetinėmis grėsmėmis.

Taip pat buvo svarbu įvertinti organizacijoje galimai disponuotinų priemonių, skirtų pakankamam duomenų subjekto informavimui bei jo teisių įgyvendinimo užtikrinimui, svarbą:



Šaltinis: sudaryta autorės, remiantis ekspertinio vertinimo rezultatais

21 pav. Ekspertų nuomonė apie tai, kiek svarbios yra organizacijoje galimai disponuotinos priemonės, skirtos pakankamam duomenų subjekto informavimui bei jo teisių įgyvendinimo užtikrinimui, proc.

Svarbiausios priemonės, skirtos pakankamam duomenų subjekto informavimui bei jo teisių įgyvendinimo užtikrinimui, ekspertų nuomone, yra: duomenų subjekto sutikimas tvarkyti jo asmens duomenis bei to sutikimo forma; darbuotojų asmens duomenų saugojimo politika; privatumo politika bei asmens duomenų saugojimo politika.

Ekspertai taip pat nurodė papildomas priemones, kurios padėtų užtikrinti pakankamą duomenų subjekto informavimą bei jo teisių įgyvendinimą. Šios ekspertų įvardintos priemonės yra pateikiamos 10 lentelėje:

10 lentelė. Ekspertų nurodytos papildomos priemonės, skirtos pakankamam duomenų subjekto informavimui bei jo teisių įgyvendinimo užtikrinimui

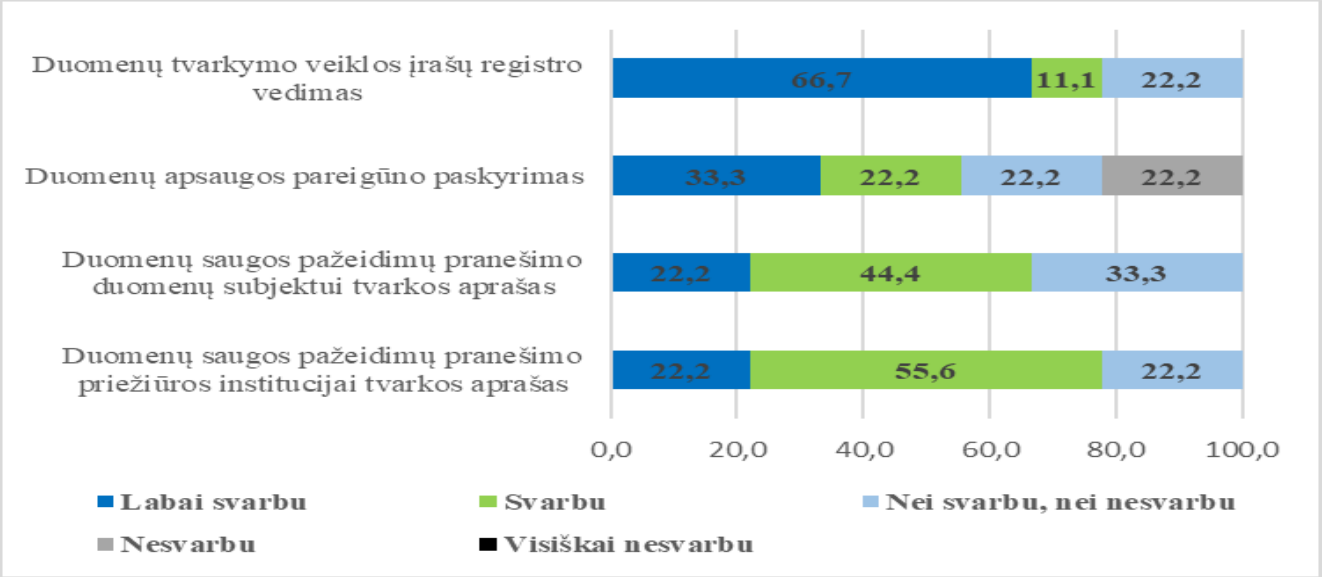
Ekspertų įvardintos priemonės	
1.	Suprantamos, fiziniams asmenims adaptuotos informacijos apie asmens duomenų tvarkymą pateikimas viešai - organizacijos interneto svetainėje, organizacijos buveinėje ir panašiai
2.	Konkrečios priežiūros institucijos gairės ir rekomendacijos
3.	Naudojimosi informacinėmis technologijomis tvarkos aprašas
4.	Duomenų apsaugos pareigūno veiksmai, kuriais jis kontroliuotų, kaip organizacijos darbuotojai laikosi asmens duomenų saugumo reikalavimų
5.	Laikytis pritaikytosios ir standartizuotosios duomenų apsaugos diegiant IT priemones

Šaltinis: sudaryta autorės, remiantis ekspertinio vertinimo rezultatais

Duomenų subjekto tinkamas teisių įgyvendinimas remiasi atskaitomybės principu. Pasak Zaleskio, J. (2017), bendrasis duomenų apsaugos reglamentas išplečia duomenų valdytojų atsakomybę užtikrinant veiksmingą duomenų apsaugos reikalavimų įgyvendinimą kasdienėje veikloje. Naujasis reguliavimas įvairiais aspektais skatina pasitikėjimą duomenų valdytojais įpareigodamas juos prisiimti daugiau atsakomybės už duomenų tvarkymą. Šiuo požiūriu didelę reikšmę turi atskaitomybės principas, kuriuo siekiama sustiprinti duomenų valdytojų vaidmenį ir sugriežtinti jų atsakomybę, paskatinti juos pasirinkti priemones atitikčiai užtikrinti.

Netinkamai vykdant BDAR įtvirtintus reikalavimus ir neužtikrinant asmens duomenų apsaugos, yra neišvengiama asmens duomenų apsaugos pažeidimų. Įvykus pažeidimui, organizacijoms yra būti imtis tinkamų veiksmų ne tik dėl pažeidimo ir su juo susijusių pasekmių pašalinimui, tačiau apie tai tinkamai informuoti tiek duomenų apsaugos priežiūros instituciją bei duomenų subjektą, jei tai yra reikalinga.

Buvo svarbu nustatyti galimai disponuotinų priemonių, siekiant tinkamai įvykdyti pranešimo apie asmens duomenų saugos pažeidimą įsipareigojimą, organizacijoje svarbą:



Šaltinis: sudaryta autorės, remiantis ekspertinio vertinimo rezultatais

22 pav. Ekspertų nuomonė apie tai, kiek svarbios yra organizacijoje galimai disponuotinos priemonės skirtos tinkamai įvykdyti pranešimo apie asmens duomenų saugos pažeidimą įsipareigojimą, proc.

„Duomenų tvarkymo veiklos įrašų registro vedimas“ ekspertų nuomone yra viena iš svarbiausių priemonių, kurias turėtų naudoti organizacijos siekdamos tinkamai įvykdyti pranešimo apie asmens duomenų saugos pažeidimą įsipareigojimą. Net 6 ekspertai iš 9 nurodė, kad ši priemonė yra labai svarbi. Antra pagal svarbumą priemonė buvo įvardinta kaip „Duomenų saugos pažeidimų pranešimo priežiūros institucijai tvarkos aprašas“: 2 ekspertai nurodė, kad tai yra labai svarbi priemonė, 5 ekspertai nurodė, kad tai yra svarbi priemonė.

Ekspertų įvardintos papildomos priemonės, kurios galėtų padėti tinkamai įvykdyti pranešimo apie asmens duomenų saugos pažeidimą įsipareigojimą, yra šios:

- Glaudus organizacijos struktūrinių padalinių bendradarbiavimas;
- Duomenų saugumo incidentų atvejų tvarkos aprašas;
- Darbuotojų mokymai, pratybos, incidento simuliavimas.

Viena iš priemonių, leidžiančių tam tikros srities duomenų valdytojams susitarti dėl bendrų BDAR reikalavimus atitinkančių standartų taikymo, yra konkrečiam sektoriui pritaikytų BDAR elgesio kodeksų diegimas organizacijoje. Ekspertų buvo paprašyta nurodyti, ar jų nuomone, ši priemonė būtų veiksminga organizacijai siekiant laikytis asmens duomenų valdytojo atskaitomybės principo:

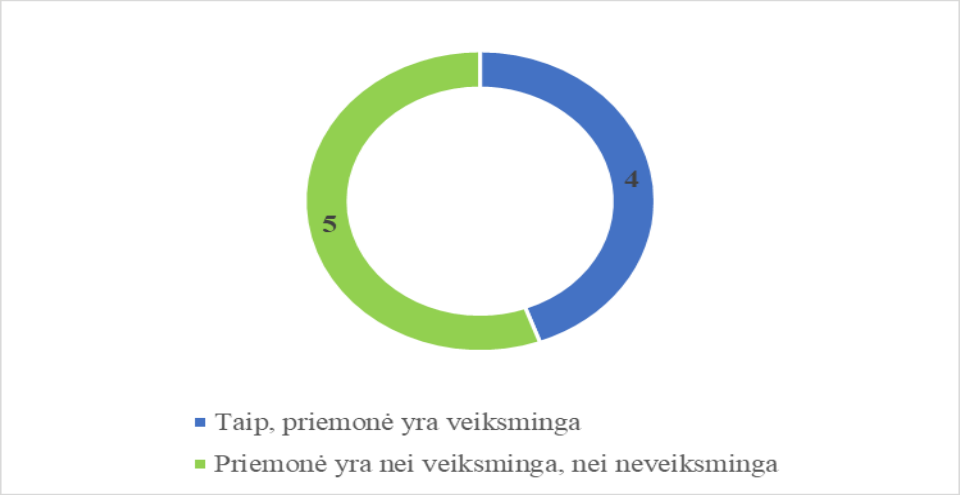


Šaltinis: sudaryta autorės, remiantis ekspertinio vertinimo rezultatais

23 pav. Ekspertų nuomonė apie tai, ar konkrečiam sektoriui pritaikytų BDAR elgesio kodeksų diegimas yra veiksminga priemonė, padedanti organizacijai laikytis asmens duomenų valdytojo atskaitomybės principo, vnt.

Daugiau nei pusė, tai yra net 6 ekspertai nurodė, kad ši priemonė yra veiksminga. Respondentas „C“, pagrįsdamas savo atsakymą į klausimą nurodė, kad „elgesio kodeksas yra savanoriška priemonė, tai labiau garantuoja norą jo laikytis, be to, elgesio kodeksas negali egzistuoti be priežiūros subjekto, kuris numatytas pačiame kodekse. Vadinasi, pati organizacija labiau suinteresuota laikytis savo paties sukurto mechanizmo, be to, tai sukuria lengvatas dėl laisvo duomenų judėjimo“. Respondentas „E“ teigia, kad „tai būtų veiksminga priemonė, nes remiantis BDAR 40 str. 5 ir 6 dalimis rengiami etikos kodeksai derinami su priežiūros institucija“. Etikos kodekso derinimas su priežiūros institucija leistų parengti konkrečias taisykles, padedančias organizacijai laikytis asmens duomenų valdytojo atskaitomybės principo. Respondentas „D“ pabrėžia standartų, diegiant elgesio kodeksus, svarbą: „standartų taikymas yra susijęs su dokumentų parengimu. Būtent dokumentai leidžia įrodyti, kad asmens duomenų valdytojas laikosi atskaitomybės principo“.

Ekspertų buvo paprašyta įvertinti ir antrąją priemonę, galimai padedančią organizacijai tinkamai vykdyti BDAR įtvirtintus reikalavimus:



Šaltinis: sudaryta autorės, remiantis ekspertinio vertinimo rezultatais

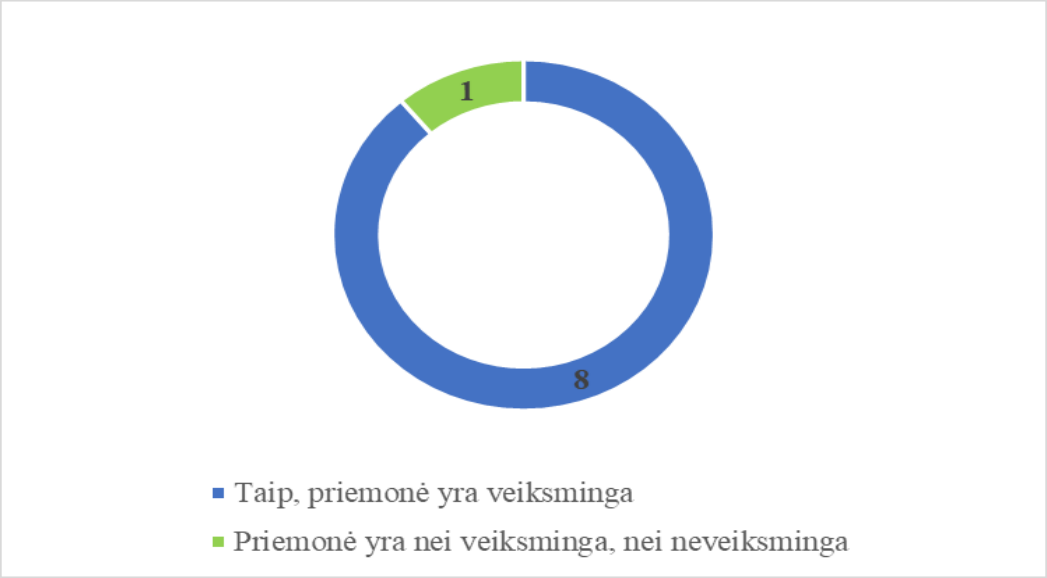
24 pav. Ekspertų nuomonė apie tai, ar atitikties BDAR reikalavimams sertifikato įgijimas yra veiksminga priemonė padedanti organizacijai tinkamai vykdyti BDAR įtvirtintus reikalavimus, vnt.

Mažiau nei pusė tyrime dalyvavusių ekspertų, tai yra 4 iš 9, sutiko su teiginiu, kad atitikties BDAR reikalavimams sertifikato įgijimas yra veiksminga priemonė padedanti organizacijai tinkamai vykdyti BDAR įtvirtintus reikalavimus. 5 iš 9 ekspertų laikėsi neutralios nuomonės, teigdami, jog ši priemonė yra nei veiksminga, nei neveiksminga.

Respondentas „C“, teigęs, jog ši priemonė yra veiksminga, nurodė, kad : „sertifikato, išduoto akredituoto subjekto, gavimas reiškia tam tikrą veiklos validumą. Vadinasi, organizacija tam tikra prasme buvo tikrinta daugeliu aspektų, reikšmingų veiklos teisėtumui deklaruoti“. Respondentas „D“, pagrįsdamas savo nuomonę dėl šios priemonės veiksmingumo, teigė, kad: „tai akivaizdu, jei įgyji sertifikatą, vadinasi organizacija tinkamai įvykdė BDAR reikalavimus“.

Respondentas „B“, pasilikęs prie neutralios nuomonės, teigia, kad: „reikalavimų laikymasis nebūtinai turi būti sertifikuotas“. Respondentas „I“, taip pat pasirinkdamas neutralią poziciją šiuo klausimu, teigia, kad: „Lietuvoje nėra patvirtintų sertifikavimo kriterijų, akredituotų sertifikavimo įstaigų. Paraiškas sertifikuoti siūlo vos 3 - 3,5 metų rinkoje veikiančios kompanijos, kas jų gebėjimą sertifikuoti kitas įmones darytų abejotinu“.

Ekspertų paprašius įvertinti trečiosios priemonės „Asmens duomenų saugumo pažeidimų, įvykusių kitose organizacijose, stebėjimas bei analizė“, galimai padedančios tinkamai vykdyti BDAR įtvirtintus reikalavimus savo organizacijoje, veiksmingumą, beveik visi laikėsi vieningos nuomonės:



Šaltinis: sudaryta autorės, remiantis ekspertinio vertinimo rezultatais

25 pav. Ekspertų nuomonė apie tai, ar asmens duomenų saugumo pažeidimų, įvykusių kitose organizacijose, stebėjimas bei analizė yra veiksminga profilaktinė priemonė siekiant tinkamai vykdyti BDAR įtvirtintus reikalavimus savo organizacijoje, vnt.

8 iš 9 ekspertų nurodė, kad ši priemonė yra veiksminga. 1 ekspertas nepaneigė šios priemonės veiksmingumo, o pasirinko neutralią poziciją, teigdamas, kad ši priemonė yra nei veiksminga, nei neveiksminga. Respondentai „D“, „E“ ir „I“ pagrįsdami savo nuomonę, kad ši priemonė yra veiksminga, teigė, jog visada yra pravartu mokytis iš kitų (svetimų) klaidų.

Respondentas „C“, teigdamas, kad ši priemonė yra veiksminga ir pagrįsdamas savo nuomonę šiuo klausimu, nurodė, jog yra būtina teisingai identifikuoti ir atskleisti priežastis, dėl kurių įvyko asmens duomenų apsaugos pažeidimas, tam, kad ši priemonė būtų veiksminga ir kitoms organizacijoms ateityje būtų galima imtis veiksmų, padedančių eliminuoti tą pačią problemą. Respondentas „F“ taip pat pritaręs, kad ši priemonė yra veiksminga, nurodė, jog: „duomenų saugumo pažeidimų stebėjimas skatina įvesti papildomas saugumo priemones organizacijoje“.

Respondentas „B“, pasirinkęs neutralią poziciją šiuo klausimu, teigia, kad ši priemonė yra „tiesiog viena iš daugelio priemonių, todėl savaime nei veiksminga, nei ne. Priemonės veiksmingumas priklauso nuo veiklos sektoriaus ir kitų dalykų“.

Apibendrinant tyrimo rezultatus galima teigti, kad didžioji tyrime dalyvavusių ekspertų dalis sutinka su teiginiu, jog BDAR taikymo strategijos kūrimas organizacijoje yra sudėtingas ir prioritetinis uždavinys. Duomenų apsaugos pareigūno pareigybės steigimas nebuvo įvardintas kaip efektyvi priemonė, padedanti išvengti asmens duomenų apsaugos pažeidimų organizacijoje. Užtikrinus pakankamą investavimą į tinkamas saugumo technologijas, tinkamą ir savalaikį darbuotojų sąmoningumo ugdymą duomenų apsaugos srityje bei kokybiškai atlikus tvarkomų asmens duomenų analizę, ekspertų nuomone, būtų sumažinama rizika įvykti asmens duomenų apsaugos pažeidimui.

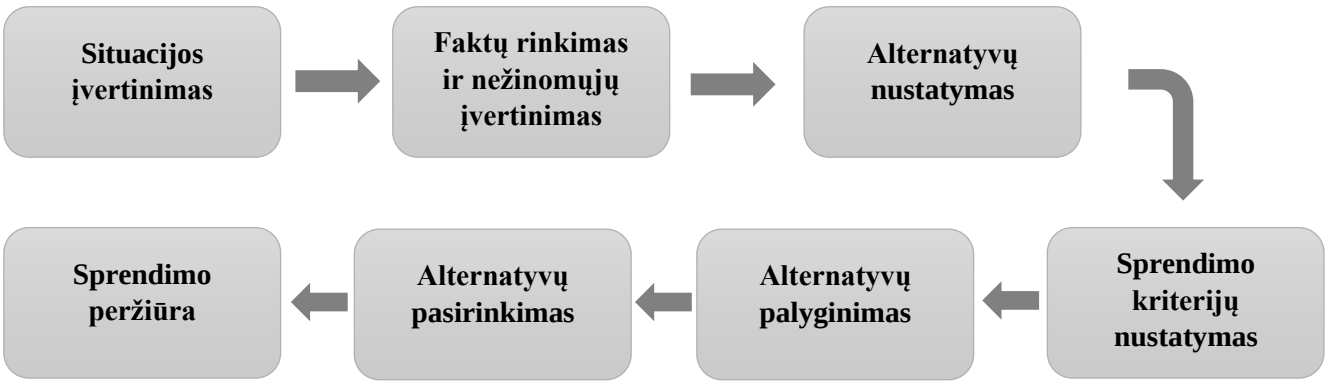
4. BDAR TAIKYMO STRATEGIJOS ORGANIZACIJOJE MODELIO KŪRIMAS

4.1. Modeliavimo metodologija

Anot Arsham, H. (2020), sprendimų priėmimas yra sėkmės esmė, nors kartais būna ir kritinių momentų, kai procesas (sprendimų priėmimas) tampa sunkus ir painus. Paprastai sprendimas apima tris veiksmus:

1. Poreikio pripažinimas;
2. Sprendimas pakeisti;
3. Sąmoningas atsidavimas sprendimo įgyvendinimui.

BDAR įsigaliojimas ir prievolė organizacijoms jį taikyti savo vykdomoje veikloje siekiant užtikrinti tinkamą asmens duomenų apsaugą – galimas įvardinti kaip aiškus poreikis adaptuoti savo veiklą pagal naująjį teisinį reguliavimą, ko pasėjoje priimamas sprendimas keisti esamus procesus ir technologijas, ir vėliau tas sprendimas yra įgyvendinamas. Tam, kad šis sprendimas būtų tinkamai įgyvendintas, yra reikalinga visuma veiksmų ir priemonių, kuriuos yra būtina atlikti:



Šaltinis: sudaryta autorės, remiantis Ahmed, A., Bwisa, H., Otieno, R. ir Karanja, K. (2014)

26 pav. Klasikinis sprendimų priėmimo procesas

Kaip Ahmed, A. ir kt. (2014) teigia, pirmiausiai yra reikalingas situacijos įvertinimas. BDAR taikymo strategijos kūrimo atveju: esamų procesų ir technologijų peržiūra ir įvertinimas bei išsami tvarkomų asmens duomenų analizė. Alternatyvų nustatymui galima prilyginti organizacijoje galimai disponuotinų priemonių, skirtų tinkamam asmens duomenų apsaugos užtikrinimui, identifikavimą. Visos identifikuotos galimos priemonės privalo būti išanalizuojamos ir įvertinamos siekiant nustatyti, kurios iš identifikuotų priemonių yra privalomos ir reikalingos konkrečioje organizacijoje, atsižvelgiant į jos vykdomą veiklą, tvarkomų duomenų pobūdį ir kiekį, darbuotojų skaičių ir kitus aspektus.

Atsižvelgiant į analizės rezultatus, pasirenkamos priemonės – priimamas sprendimas. Rekomenduojama priimtą sprendimą dar kartą peržiūrėti siekiant įsitikinti, kad jis yra tinkamas ir vedantis link geriausio rezultato.

Strategija nurodo, kaip bus pasiektas tam tikras organizacijos tikslas, dar kitaip - kaip bus siekiama tam tikro rezultato:



Šaltinis: sudaryta autorės, remiantis Nickols, F. (2016)

27 pav. Bendroji strategija: strategija ir taktika

Pasak Nickols, F. (2016), strategija apskritai yra susijusi su santykiais tarp tikslų ir priemonių, tai yra, tarp siekiamų rezultatų ir organizacijos turimų išteklių (priemonių). Daugiausia strategija yra susijusi su turimų išteklių išdėstymu, o taktika – jau su turimų išteklių panaudojimu. Apibendrinant teigiama, kad kartu strategija ir taktika mažina atotrūkį tarp tikslų (siekiamų rezultatų) ir priemonių.

Būtina pabrėžti, kad konstruojant modelį, yra būtina numatyti, kokių rezultatų (tikslų) yra siekiama, kitaip tariant, yra būtina nustatyti **modelio rezultatų išeigą**.



Šaltinis: sudaryta autorės, remiantis Gabelloni, D., Ghezzi, A., Martini, A. ir Natalicchio, A. (2017)

28 pav. IPO modelis

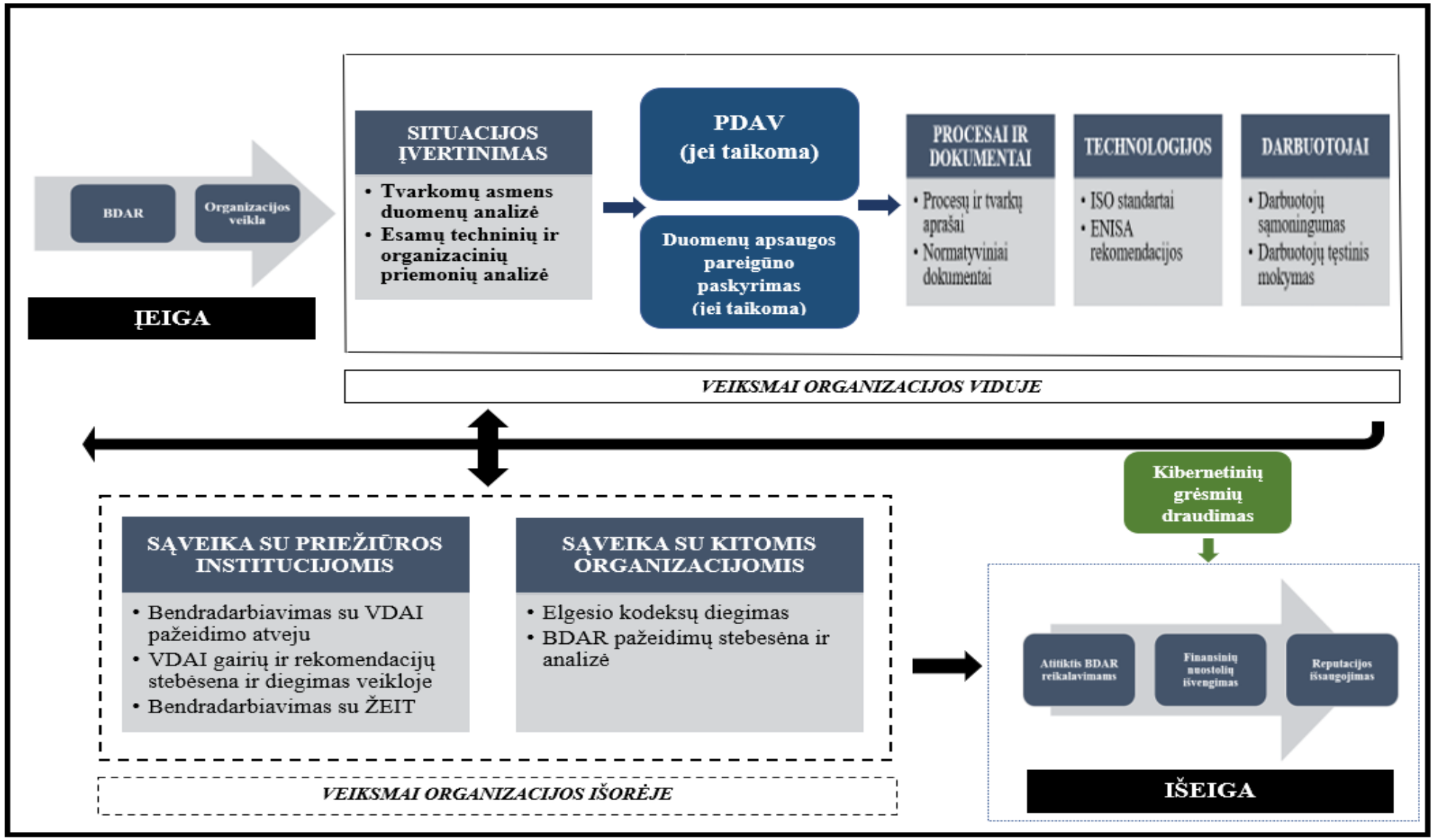
Kaip teigia Gabelloni, D. ir bendraautoriai (2017), IPO modelis susideda iš 3 pagrindinių komponentų. Pirmasis modelio komponentas yra įeiga, arba kitaip įvestis, kur yra apibrėžiama problema

ar užduotis, kuri turi būti išspręsta ar įvykdyta. Remiantis organizacijos norimos išspręsti problemos ar įvykdyti užduoties struktūra bei pobūdžiu yra nustatomi reikalingi atlikti procesai: technologijų, reikalingų užduočiai atlikti, valdymas; žmogiškųjų išteklių, dalyvaujančių užduoties atlikime, valdymas; operacijų ir veiksmų, atliekamų įgyvendinant užduotį, valdymas. Paskutinis modelio komponentas yra išeiga: problemos sprendimas ar įvykdyta užduotis.

BDAR taikymo strategijos kūrimo organizacijoje modelio konstravimo atveju modelio **įeiga** yra **BDAR įtvirtinti reikalavimai** pradėti taikyti 2018 metų gegužės 25 dieną, ir **organizacijos vykdoma veikla**. Modelio pagrindinė išeiga yra **organizacijos atitiktis BDAR įtvirtintiems reikalavimams.**

4.2. Modelio analizė

Išanalizavus mokslinę literatūrą, susijusią su asmens duomenų apsauga ir BDAR įtvirtintų reikalavimų taikymu organizacijoje, juridinius dokumentus, asmens duomenų apsaugos priežiūros institucijų teikiamas gaires ir rekomendacijas šioje srityje, asmens duomenų apsaugos pažeidimus Europoje įvykusius 2018 – 2021 metų laikotarpyje bei atlikus ekspertinį vertinimą, yra siūlomas BDAR taikymo strategijos kūrimo organizacijoje modelis (žr. 29 pav.):



Šaltinis: sudaryta autorės, remiantis tyrimo rezultatais

29 pav. BDAR taikymo strategijos organizacijoje modelis

BDAR taikymo strategijos organizacijoje modelis yra aktualus visoms įmonės valdančioms ir tvarkančioms asmens duomenis, tai yra, toms įmonėms, kurių veikla yra reglamentuojama BDAR.

Kaip matyti iš 29 paveikslo, pirmiausiai yra reikalinga atlikti esamos situacijos analizę: šio etapo metu yra identifikuojamos asmens duomenų tvarkymo operacijos, asmens duomenų ir duomenų subjektų kategorijos, duomenų teikėjai ir duomenų gavėjai. Taip pat yra identifikuojamas poreikis įgyti papildomas žinias ar kompetencijas asmens duomenų apsaugos srityje. Šiame etape yra nustatomi ir pagrindiniai reikalavimai sistemos vientisumui, konfidencialumui ir prieinamumui užtikrinti.

Toliau yra siūloma atlikti poveikio duomenų apsaugai vertinimą (PDAV) bei įsteigti asmens duomenų apsaugos pareigūno pareigybę, jei tai yra privaloma konkrečiai organizacijai. PDAV atliekamas, kai dėl duomenų tvarkymo gali kilti didelis pavojus asmenų teisėms ir laisvėms. PDAV reikalingas bent šiais trimis atvejais:

- atliekant sistemingą ir išsamų su fiziniais asmenimis susijusių asmeninių aspektų vertinimą, įskaitant profiliavimą;
- tvarkant neskelbtinus duomenis dideliu mastu;
- sistemingai stebint viešąsias erdves dideliu mastu.

Tiek PDAV atlikimas, tiek duomenų apsaugos pareigūno paskyrimas padėtų organizacijai tinkamai įvykdyti sekantį siūlomo modelio etapą: parengti procesų, susijusių su privatumo ir asmens duomenų saugumo užtikrinimu, aprašus bei tų procesų eigoje naudojamus normatyvinius dokumentus ar kitas jų formas; užtikrinti įmonės veikloje naudojamų technologijų saugumą bei atitiktį informacinių technologijų reikalavimams; užtikrinti įmonės darbuotojų sąmoningumą asmens duomenų apsaugos srityje bei vykdyti tęstinį jų mokymą. Verta pabrėžti, kad darbuotojų kompetencijos kėlimas duomenų apsaugos srityje yra viena iš svarbiausių priemonių, kuri buvo įvardinta ekspertinio vertinimo metu, padedanti tinkamai vykdyti BDAR įtvirtintus reikalavimus. Mokymai yra viena pagrindinių organizacinių asmens duomenų saugumo priemonių, padedanti užtikrinti bet kokios organizacijos atitiktį BDAR reikalavimams.

Organizacijos, siekdamos užtikrinti tinkamą asmens duomenų apsaugą, neturėtų apsiriboti tik veiksmais pačios organizacijos viduje. Kaip buvo nustatyta ekspertinio vertinimo metu, bendradarbiavimas su duomenų apsaugos priežiūros institucijomis bei jų teikiamų gairių bei rekomendacijų stebėsena ir įgyvendinimas savo vykdomoje veikloje, yra vienas iš BDAR taikymo strategijos organizacijoje etapų. Bendradarbiavimas (sąveikavimas) su kitomis organizacijomis, vykdančiomis panašią veiklą, yra taip pat įvardijama kaip veiksminga priemonė, padedanti užtikrinti asmens duomenų apsaugą. Rekomenduojama BDAR pažeidimų, įvykusių kitose organizacijose, stebėsena ir analizė bei konkrečiam sektoriui pritaikytų BDAR elgesio kodeksų diegimas, kas ekspertinio vertinimo metu buvo įvardinta kaip veiksminga priemonė, padedanti organizacijai laikytis asmens duomenų valdytojo atskaitomybės principo.

Aptartų veiksmų atlikimas tiek organizacijos viduje, tiek išorėje turėtų užtikrinti veiksmingą BDAR įtvirtintų reikalavimų taikymą organizacijoje ir išvengti neigiamų pasekmių, su kuriomis organizacija susidurtų patyrusi asmens duomenų apsaugos pažeidimus. Konkrečiau, siūlomo modelio išeiga – atitiktis BDAR įtvirtintiems reikalavimams, finansinių nuostolių išvengimas ir reputacijos (prekės ženklo) išsaugojimas. Tačiau nepaisant visų pastangų, nėra įmanoma 100 % apsisaugoti nuo visų įmanomų rizikų. Kaip teigia Štitilis, D. (2013), elektroninės erdvės globalumas sukūrė beprecedentes sąlygas daryti nusikaltimus, susijusius su svarbios elektroninės informacijos praradimu ar sugadinimu, iš bet kurio pasaulio taško, kuriame yra internetas. Todėl labai svarbu apsisaugoti nuo elektroninių nusikaltimų, vykdomų pasitelkiant internetą.

Kadangi kibernetinė rizika, kuri dažniausiai yra pastebima tik patyrus nuostolius. tampa vis plačiau paplitusiu reiškiniu, viena iš pagrindinių apsaugos priemonių nuo šios grėsmės yra draudimo sutartis. Organizacijoms, siekiančioms išvengti finansinių nuostolių bei neigiamo poveikio prekės ar paslaugos ženklui ir reputacijai yra siūloma su draudimo bendrove sudaryti kibernetinių grėsmių draudimo sutartį, apimančią draudimą nuo tokių nestandartinių rizikų kaip:

- atsakomybė, kylanti dėl informacinių tinklų saugumo ir asmens privatumo pažeidimų;
- pirmojo lygmens asmens duomenų pažeidimo išlaidos (dėl informacinių tinklų saugumo ir asmens privatumo pažeidimų atsiradusios žalos fakto nustatymas, duomenų ištaisymas ir atkūrimas; išlaidos, susijusios su reikalavimu informuoti klientus ir pasiūlyti jiems kreditų stebėsenos paslaugas; išlaidos, susijusios su krizių valdymo specialistų samdymu, atsiradus informacinių tinklų saugumo ir asmens privatumo pažeidimams);
- verslo proceso nutrūkimo, padidėjusių darbo kaštų išlaidos; valdžios institucijų atliekamų patikrinimų ir paskirtų baudų išlaidos;
- išpirkos reikalavimas.

Apibendrinant galima teigti, kad organizacijoms, siekiančioms tinkamai vykdyti BDAR įtvirtintus reikalavimus ir tinkamai užtikrinti asmens duomenų, yra rekomenduojama remtis ne tik siūlomu BDRA taikymo strategijos modeliu, bet ir pasirūpinti draudimu nuo šiais laikais dažnai pasitaikančių ir paplitusių kibernetinių grėsmių.

IŠVADOS IR REKOMENDACIJOS

1. Sprendžiant privatumo ir asmens duomenų apsaugos klausimus, laikui bėgant vis svarbesnį vaidmenį įgijo teisinė valstybės kontrolė, ko pasėkoje imperatyvus reguliavimas pakeitė šioje srityje vyravusią savireguliaciją. BDAR, pradėtas taikyti 2018 metų gegužės 25 dieną, iš esmės reformavo ankstesnę duomenų apsaugos sistemą – persvarstytos ir naujai suformuluotos asmens duomenų apsaugos priežiūros institucijų vykdomos funkcijos, išplėstas ES valstybių narių duomenų apsaugos priežiūros institucijų bendradarbiavimas, įtvirtintos naujos pareigos duomenų valdytojams ir naujos teisės duomenų subjektams. BDAR leidėjams apibrėžiant tik funkcinius BDAR įgyvendinimo reikalavimus bei sąmoningai vengiant rekomenduoti konkrečius techninius bei organizacinius privatumo užtikrinimo būdus įgyvendinant reglamentą, atsirado neužtikrintumo (praktiškai taikant BDAR) problema. Remiantis išanalizuota moksline literatūra bei juridiniais dokumentais, buvo išskirti trys pagrindiniai BDAR taikymo strategijos organizacijoje elementai: procesas, technologijos ir darbuotojai.
2. Atlikus asmens duomenų apsaugos pažeidimų Europoje analizę 2018 – 2021 metų laikotarpiu, buvo identifikuotos BDAR įtvirtintų reikalavimų taikymo organizacijoje probleminės sritys. Šios sritys buvo suskirstytos į 9 kategorijas, joms priskiriant dažniausiai pažeidžiamus BDAR straipsnius: nepakankamas teisinis duomenų tvarkymo pagrindas (5, 6 BDAR str. pažeidimai); nepakankamos techninės ir organizacinės priemonės, užtikrinančios informacijos saugumą (5, 32 BDAR str. pažeidimai); nesilaikoma su asmens duomenų tvarkymu susijusių principų (5 BDAR str. pažeidimai); nepakankamas duomenų subjektų teisių įgyvendinimas (12, 15, 17 ir 21 BDAR str. pažeidimai); nepakankamas informavimas ir teisės susipažinti su asmens duomenimis vykdymas (13, 14 BDAR str. pažeidimai); nepakankamai įvykdyti pranešimo apie duomenų pažeidimus įpareigojimai (33, 34 BDAR str. pažeidimai); duomenų apsaugos pareigūno paskyrimo trūkumas (37 BDAR str. pažeidimai); nepakankamas bendradarbiavimas su priežiūros institucija (31, 58 BDAR str. pažeidimai); netinkama duomenų tvarkymo sutartis ar jos nebuvimas (28 BDAR str. pažeidimai).
3. Remiantis atliktos analizės rezultatais atliktas ekspertinis vertinimas, kurio metu nustatyta, jog: BDAR taikymo strategijos kūrimas yra prioritetinis ir sudėtingas organizacijos uždavinys; organizacijos, siekdamos užtikrinti tinkamą asmens duomenų apsaugą, dažniausiai susiduria su šios srities ekspertų trūkumo bei finansinių išteklių trūkumo problemomis; pagrindinės priežastys, lemiančios asmens duomenų apsaugos pažeidimus organizacijoje, yra „nepakankamas investavimas į tinkamas saugumo technologijas“ ir „darbuotojų ugdymo duomenų apsaugos srityje stoka“; nustatytos organizacijoje galimai disponuotinos priemonės, skirtos pakankamam duomenų subjekto informavimui bei jo teisių įgyvendinimo užtikrinimui;

BDAR elgesio kodeksų diegimas ir asmens duomenų saugumo pažeidimų, įvykusių kitose organizacijose, stebėjimas bei analizė yra pripažintos kaip veiksmingos priemonės, padedančios organizacijai laikytis asmens duomenų valdytojo atskaitomybės principo.

4. Remiantis trianguliacijos metodu atlikto tyrimo rezultatais sukonstruotas BDAR taikymo strategijos organizacijoje modelis (žr. 29 pav.), kurio įeiga yra BDAR ir organizacijos vykdoma veikla, o išeiga: atitiktis BDAR įtvirtintiems reikalavimas, finansinių nuostolių išvengimas ir reputacijos iššsaugojimas. Modelyje išskiriamos 2 rekomenduojamų atlikti veiksmų aplinos: veiksmai organizacijos viduje ir išorėje. Prie pirmosios aplinkos veiksmų yra priskiriami: esamos situacijos įvertinimas; PDAV atlikimas; duomenų apsaugos pareigūno paskyrimas; procesų aprašų bei dokumentų parengimas; technologijų saugumo ir tinkamumo užtikrinimas; darbuotojų ugdymas. Prie veiksmų organizacijos išorėje yra priskiriama: sąveika su priežiūros institucijomis; sąveika su kitomis organizacijomis. Siekiant sumažinti modelio išeigos rizikų tikimybę, siūloma pasirūpinti draudimu nuo kibernetinių grėsmių.

Rekomendacijos:

- BDAR taikymo strategijos kūrimą pradėti nuo esamos situacijos organizacijoje išsamios analizės: įvertinti esamų techninių ir organizacinių priemonių veiksmingumą. Esant poreikiui užtikrinti pakankamą finansavimą šių priemonių atnaujinimui ar naujų įdiegimui.
- Kuriant BDAR taikymo organizacijoje strategiją, neapsiriboti tik su tuo susijusių veiksmų atlikimu organizacijos viduje. Rekomenduojama intensyvi sąveika su asmens duomenų apsaugos priežiūros institucija bei kitomis organizacijomis, vykdančiomis panašią veiklą.
- Rodyti iniciatyvą ir imtis diegti konkrečiam sektoriui pritaikytus BDAR elgesio kodeksus kartu su kitomis panašią veiklą vykdančiomis organizacijomis.
- Stebėti ir analizuoti asmens duomenų apsaugos pažeidimus, įvykusius kitose organizacijose. Stebėjimo ir analizės metu gautus rezultatus panaudoti savo organizacijos vykdomos veiklos atnaujinimui ar koregavimui siekiant užtikrinti tinkamą asmens duomenų apsaugą.
- Modelio išeigos rezultatus rekomenduojama apdrausti kibernetinių rizikų draudimu. Anot Molony, D. ir Leemans, V. (2018), tai yra viena iš priemonių, amortizuojančių patiriamus nuostolius, įvykus asmens duomenų apsaugos pažeidimui.

LITERATŪRA

Moksliniai šaltiniai:

1. Addis, C. ir Kutar, M. (2018). *The General Data Protection Regulation (GDPR), Emerging Technologies and UK Organisations: Awareness, Implementation and Readiness.* Prieiga per internetą: URL: https://aisel.aisnet.org/ukais2018/29/ .
2. Ahmed, A., Bwisa, H., Otieno, R. ir Karanja, K. (2014). *Strategic Decision Making: Process, Models, and Theories*. Business Management and Strategy, ISSN 2157-6068, Vol. 5, No. 1. Prieiga per internetą: URL: https://Strategic Decision Making Process Models and Theories .
3. Andrijauskas, R. ir Morkūnienė, D. (2020). *Asmens duomenų apsaugos priežiūros institucijos vaidmens pasikeitimai priėmus Bendrąjį duomenų apsaugos reglamentą.* Central and Eastern European Online Library. Prieiga per internetą: URL: https://www.ceeol.com/search/viewpdf?id=961558 .
4. Arsham, H. (2020). *Leadership Decision Making*. Prieiga per internetą: URL: https://www.researchgate.net/publication/344638188_Leadership_Decision_Making .
5. Baležentis, A. ir Žalimaitė, M. (2011). *Ekspertinių vertinimų taikymas inovacijų plėrtos veiksnių analizėje: Lietuvos inovatyvių įmonių vertinimas*. ISSN 1822-6760. Management theory and studies for rural business and infrastructure development. 2011. Nr. 3 (27). Research papers. Prieiga per internetą: URL: http://mts.asu.lt/mtsrbid/article/viewFile/269/298 .
6. Blashfield, R. K. ir Libby R. (1978). *Performance of a composite as a function of the number of judges.* Volume 21, Issue 2, April 1978, Pages 121-129. Prieiga per internetą: URL: https://www.sciencedirect.com/science/article/abs/pii/0030507378900442?via%3Dihub .
7. Buttarelli, G. (2016). *The EU GDPR as a clarion call for a new global digital gold standard*. International Data Privacy Law, Volume 6, Issue 2, May 2016, Pages 77–78. Prieiga per internetą: URL: https://academic.oup.com/idpl/article/6/2/77/2404469 .
8. Bygrave, A. L. (2017). *Data Protection by Design and by Default : Deciphering the EU's Legislative Requirements.* Oslo Law Review 02 / 2017 (Volum 4). Prieiga per internetą: URL: https://www.idunn.no/oslo_law_review/2017/02/data_protection_by_design_and_by_default_deciphering_the_ .
9. Cvilika, M. ir Šlapimaitė, L. (2015). *Asmens duomenų samprata elektroninėje erdvėje*. ISSN 1392-1274. TEISĖ 2015 96. Prieiga per internetą: URL: https://www.zurnalai.vu.lt/teise/article/view/8761/7647 .
10. Drucker, P.F. (2004). *Valdymo iššūkiai XXI amžiuje.* Vilnius, Rgrupė.
11. Ferrara, P. ir Spoto, F. (2018). *Static Analysis for GDPR Compliance.* Prieiga per internetą: URL: https://www.researchgate.net/profile/Pietro_Ferrara/publication/336987954_Static_Analysis_fo

r_GDPR_Compliance/links/5dbd94474585151435e1f5ac/Static-Analysis-for-GDPR-Compliance.pdf .

12. Fruhlinger, J. (2020). The CIA triad: Definition, components and examples. *CSO magazine*. Prieiga per internetą: URL: https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html.
13. Gabelloni, D., Ghezzi, A., Martini, A. ir Natalicchio, A. (2017). *Review and Suggestions for Future Research.* International Journal of Management Reviews. DOI: 10.1111/ijmr.12135 Prieiga per internetą: URL: file:///C:/Users/agess/Downloads/Ghezzietal.2017-Crowdsourcingaliteraturereviewandsuggestionsforfutureresearch-InternationalJournalofManagementReviews.pdf .
14. Kansteiner, K. ir König, S. (2020). *The Role(s) of Qualitative Content Analysis in Mixed Methods Research Designs*. Prieiga per internetą: URL: https://www.qualitative-research.net/index.php/fqs/article/view/3412/4514 .
15. Kardelis, K. (2017). *Mokslinių tyrimų metodologija ir metodai.* Vilnius: „Mokslo ir enciklopedijų leidybos centras".
16. Lawrence, S. (2013). *Strategy: A History*. Prieiga per internetą: URL: http://web.b.ebscohost.com.skaitykla.mruni.eu/ehost/ebookviewer/ebook/ZTAwMHh3d19fNjM5MzA2X19BTg2?sid=5aa0de66-960b-4899-8397-31ef978c820d@pdc-v-sessmgr02&vid=9&format=EB&rid=1 .
17. Li, H., Yu, L. ir He, W. (2019). *The Impact of GDPR on Global Technology Development*. Journal of Global Information Technology Management, Volume 22, 2019 - Issue 1. Prieiga per internetą: URL: https://www.tandfonline.com/doi/full/10.1080/1097198X.2019.1569186 .
18. Mense, A. ir Blobel, B. (2017). *HL7 Standards and Components to Support Implementation of the European General Data Protection Regulation (GDPR).* Prieiga per internetą: URL: https://www.ejbi.org/scholarly-articles/hl7-standards-and-components-to-support-implementation-ofthe-european-general-data-protection-regulation-gdpr.pdf.
19. Molony, D. ir Leemans, V. (2018). Are GDPR Fines Insurable? New York Vol. 65, Iss. 9, (Oct 2018): 28-29. Prieiga per internetą: URL: https://search.proquest.com/openview/3ce3867b9d4debe0284f41ec5675f183/1?pq-origsite=gscholar&cbl=47271 .
20. Morkevičius, V. (2008). *Kokybinė lyginamoji analizė (QCA): principai ir programinės priemonės.* Prieiga per internetą: URL: https://www.lidata.eu/index.php?file=files/mokymai/QCA_2008/QCA_2008.html&course_file=QCA_2008_1_.html .

21. Nickols, F. (2016). *Three Forms of Strategy. General, Corporate & Competitive*. Prieiga per internetą: URL: https://www.nickols.us/three_forms.pdf .
22. Neumann, A. J., Statland, N. Ir Webb, R. D. (1977). Post-processing audit tools and techniques. *US Department of Commerce, National Bureau of Standards. pp. 11-3--11-4.* Prieiga per internetą: URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nbsspecialpublication500-19.pdf.
23. Padvezko, V. (2005). Ekspertų įverčių suderinamumas. Technological and economic development of economy. ISSN 1392-8619, Vol XI, No 2, 101-107. Prieiga per internetą: URL: file:///C:/Users/agess/Downloads/Agreement_of_expert_estimates.pdf .
24. Petraitytė, I. (2011). *Asmens duomenų apsauga ir teisė į privatų gyvenimą.* ISSN 1392–1274. TEISĖ 2011 80, 163 - 174. Prieiga per internetą: URL: https://www.zurnalai.vu.lt/teise/article/view/158/124.
25. Politou, E., Alepis, E.ir Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity, 1–20.* Prieiga per internetą: URL:https://academic.oup.com/cybersecurity/article/4/1/tyy001/4954056.
26. Raksha, N. (2015). *Competitive strategies as an effective instrument of enterprise development.* Prieiga per internetą: URL: http://web.b.ebscohost.com.skaitykla.mruni.eu/ehost/detail/detail?vid=5&sid=5aa0de66-960b-4899-8397-31ef978c820d%40pdc-v-sessmgr02&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=a9h&AN=114259591 .
27. Sirur, S., Nurce, J. R.C. ir Webb, H. (2018). *Are We There Yet?: Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR).* Prieiga per internetą: URL: https://dl.acm.org/doi/abs/10.1145/3267357.3267368 .
28. Svetikas, K. Ž. ir Arimavičiūtė, M. (2012). Strateginis valdymas. Mykolo Romerio universitetas. Prieiga per internetą: URL: https://repository.mruni.eu/bitstream/handle/007/16845/9789955194255.pdf?sequence=1 .
29. Štareikė, E. ir Kausteklytė-Tunkevičienė, S. (2018). *Pagrindinės duomenų subjekto teisės ir jų užtikrinimas pagal ES Bendrąjį duomenų apsaugos reglamentą*. ISSN 2335-2035 (Online). Prieiga per internetą: URL: file:///C:/Users/agess/Downloads/5597-12825-1-PB.pdf .
30. Štitilis, D. (2013). *Kibernetinio saugumo teisinis reguliavimas: kibernetinio saugumo strategijos.* ISSN 2029-7564 (online), SOCIALINĖS TECHNOLOGIJOS, 2013, 3(1), p. 189–207. Prieiga per internętą: URL: https://core.ac.uk/download/pdf/197254465.pdf .
31. Tamavičiūtė, V. (2019). *Teisė būti (ne)pamirštam: kokias teisės ištrinti savo duomenis ribas nustato Europos Sąjungos Teisingumo Teismas?* Lietuva ir tarptautinė teisė. Prieiga per internetą: URL:

https://repository.mruni.eu/bitstream/handle/007/16261/2019%20Teise_4.3._Tamavic%CC%8Ciu%CC%84te%CC%87.pdf?sequence=1&isAllowed=y .

32. Valackienė, A. ir Mikėnė, S. (2007). *Sociologinis tyrimas: metodologija ir atlikimo metodika*. Kaunas: „Technologija‘‘.
33. Vobolevičius, V. (2017). *Statistinė duomenų analizė.* LIDA, Lietuvos HSM duomenų archyvas. Prieiga per internetą: URL: http://www.lidata.eu/index.php?file=files/mokymai/sda/sda.html&course_file=sda_I_1.3.html.
34. Warren, S. D. ir Brandeis, L D. (1890). The Right to Privacy. *Harvard Law Review, Vol. 4, No. 5 (Dec. 15, 1890), pp. 193-220.* Prieiga per internetą: URL: https://www.jstor.org/stable/pdf/1321160.pdf?refreqid=excelsior%3A8850606f501eed23936d48ad737b75eb.
35. Westin, A. (1967). Privacy and Freedom. *Ig Publishing (Politics & the English Language).* Prieiga per internetą: URL: http://www.igpub.com/privacy-and-freedom/.
36. Zaleskis, J. (2016). *ES Bendrasis duomenų apsaugos reglamentas: reikšmė duomenų apsaugos teisei.* ISSN 2424-6050 (Online) ISSN 1392-1274 (Print). TEISĖ 2017 103 Prieiga per internetą: URL: https://www.journals.vu.lt/teise/article/view/10779/8959 .

Teisės aktai:

37. 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. Prieiga per internetą: URL: https://eur-lex.europa.eu/legal-content/lt/TXT/?uri=CELEX%3A31995L0046 .
38. 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).* Prieiga per internetą: URL: https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32016R0679.
39. Europos Žmogaus teisių konvencija (iš dalies pakeista protokolais Nr. 11 ir 14; su Pirmuoju Protokolu ir papildomais protokolais Nr. 4, 6, 7, 12, 13 ir 16) (2010). *Europos Žmogaus Teisių Teismas.* Prieiga per internetą: URL: https://www.echr.coe.int/Documents/Convention_LIT.pdf.
40. Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymas, 1996 m. birželio 11 d. Nr. I-1374, Vilnius. Prieiga per internetą: URL: https://www.e-tar.lt/portal/lt/legalAct/TAR.5368B592234C.
41. Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas, 2000 m. liepos 17 d. Nr. VIII-1852, Vilnius. Prieiga per internetą: URL: https://www.e-tar.lt/portal/lt/legalAct/TAR.199366D1EF9E.

42. Lietuvos Respublikos elektroninių ryšių įstatymas, 2004 m. balandžio 15 d. Nr. IX-2135, Vilnius. Prieiga per internetą: URL: https://www.e-tar.lt/portal/lt/legalAct/TAR.82D8168D3049/hlbWSfsMOw .
43. Lietuvos Respublikos Konstitucija (1992). Prieiga per internetą: URL: https://www.lrs.lt/home/Konstitucija/Konstitucija.htm.
44. Visuotinė žmogaus teisių deklaracija (1948). Prieiga per internetą: URL: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.278385.

Kita:

45. CMS International Fines Database: GDPR Enforcement Tracker. Prieiga per internetą: URL: https://www.enforcementtracker.com/?insights.
46. *Dažniausiai pasitaikantys atvejai, kai Valstybinei duomenų apsaugos inspekcijai pateikti skundai pripažįstami nepagrįstais*. VDAI, 2019. Prieiga oer internetą: URL: https://vdai.lrv.lt/uploads/vdai/documents/files/Atvejai_kai_skundai_nepagristais_2019-05-06.pdf .
47. *Determining what is personal data.* ICO (Information Commissioner's Office), 2012. Prieiga per internetą: URL: https://ico.org.uk/media/for-organisations/documents/1554/determining-what-is-personal-data.pdf .
48. Duomenų subjekto Žodynėlis (sąvokos ir sutrumpinimai), 2020. *Lietuvos Respublikos sveikatos apsaugos ministerija.* Prieiga per internetą: URL: https://sam.lrv.lt/lt/asmens-duomenu-apsauga/duomenu-subjekto-zodynelis-savokos-ir-sutrumpinimai.
49. Europos duomenų apsaugos valdyba. Apie EDAV, 2021. Prieiga per internetą: URL: https://edpb.europa.eu/about-edpb/about-edpb_lt
50. *Europos Sąjungos teisingumo teismo praktikos apžvalga (2014 m. gegužės 1d. – 2014 m. birželio 30 d.).* Lietuvos vyriausiasis administracinis teismas. Prieiga per internetą: URL: https://www.lvat.lt/data/public/uploads/2018/01/d1_estt-praktikos-apzvalga-2014-05-01-2014-06-30.pdf .
51. Falk, T.T. (2016). *An Accountability Approach to Demonstrating Compliance*. CPO magazine. Prieiga per internetą: URL: https://www.cpomagazine.com/data-protection/accountability-approach-demonstrating-compliance/ .
52. *Four days until GDPR D-Day: Only seven EU states ready*. Decision Marketing, 2019. Prieiga per internetą: URL: https://www.decisionmarketing.co.uk/news/four-days-until-gdpr-d-day-only-seven-eu-states-ready .
53. *Guidelines 07/2020 on the concepts of controller and processor in the GDPR.* EDPB, 2020. Priega per internetą: URL:

https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf .

54. Irwin, L. (2019). *GDPR: What's the difference between personal data and sensitive data?* Prieiga per internetą: URL: https://www.itgovernance.co.uk/blog/the-gdpr-do-you-know-the-difference-between-personal-data-and-sensitive-data .
55. IT Governance privacy team (2017). *EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide.* Second edition. ISBN: 978-1-84928-946-7. https://books.google.lt/books?hl=lt&lr=&id=hnQ2DwAAQBAJ&oi=fnd&pg=PA1&dq=gdpr+implementation&ots=WiMdBzPUSo&sig=xoXqjnSL2cgFVKLQDd87_C1gxo0&redir_esc=y#v=onepage&q=gdpr%20implementation&f=false.
56. Jaeger, J. (2020). *H&M Germany fined $41.3M in one of largest GDPR penalties*. Prieiga per internetą: URL: https://www.complianceweek.com/data-privacy/handm-germany-fined-413m-in-one-of-largest-gdpr-penalties/29556.article .
57. *Keeping pace in the GDPR race: a global view of GDPR progress in the United States, Europe, China and Japan*. (2019). Ponemon Institute. Prieiga per internetą: URL: https://mcdermott-will-emery-2793.docs.contently.com/v/keeping-pace-in-the-gdpr-race-a-global-view-of-gdpr-progress-in-the-united-states-europe-china-and-japan .
58. *Kibernetinis saugumas ir verslas. Ką turėtų žinoti kiekvienas įmonės vadovas, 2020*. Nacionalinis kibernetinio saugumo centras. Prieiga per internetą: URL: file:///C:/Users/agess/Downloads/kibernetinio%20saugumo%20vadovas%20verslui%20(1).pdf.
59. Nielsen, N. (2018). *Eight countries to miss EU data protection deadline.* Euobserver – Justice & Home Affairs. Prieiga per internetą: URL: https://euobserver.com/justice/141860 .
60. *Pasiruošimas taikyti Bendrąjį duomenų apsaugos reglamentą (ES) 2016/679, 2017.* Valstybinė duomenų apsaugos inspekcija. Prieiga per internetą: URL: https://vdai.lrv.lt/uploads/vdai/documents/files/12zingsnius_BDAR_20170525.pdf .
61. Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation). COM/2012/011 final - 2012/0011 (COD). Prieiga per internetą: URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52012PC0011.
62. Schemm, M. (2020). *35,3 Millionen Euro Bußgeld wegen Datenschutzverstößen im Servicecenter von H&M.* Prieiga per internetą: URL: https://datenschutz-hamburg.de/pressemitteilungen/2020/10/2020-10-01-h-m-verfahren .

63. *Sensitive personal data - special category under the GDPR*. Data Privacy Manager, 2020. Prieiga per internetą: URL: https://dataprivacymanager.net/sensitive-personal-data-special-category-under-the-gdpr/ .
64. Valstybinės duomenų apsaugos inspekcijos 2020 metų veiklos ataskaita, (2021). Prieiga per internetą: URL: https://vdai.lrv.lt/uploads/vdai/documents/files/2020%20m_%20VDAI%20veiklos%20ataskaita%202021-02-26.pdf .
65. Valstybinė duomenų apsaugos inspekcija – Veiklos sritys. Prieiga per internetą: URL: https://vdai.lrv.lt/lt/ .
66. Valstybinės duomenų apsaugos inspekcijos direktoriaus įsakymas „Dėl Duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąrašo patvirtinimo“, 2019 m. kovo 14 d. Nr. 1T-35 (1.12.E). Prieiga per internetą: URL: https://www.e-tar.lt/portal/lt/legalAct/abb01940465511e9a221b04854b985af .
67. Veiklos, dėl kurių turės būti atliekamas poveikio duomenų apsaugai vertinimas, 2019. Valstybinė duomenų apsaugos inspekcija. Prieiga per internetą: URL: https://vdai.lrv.lt/lt/naujienos/veiklos-del-kuriu-tures-buti-atliekamas-poveikio-duomenu-apsaugai-vertinimas .
68. Žurnalistų etikos inspektoriaus tarnybos veiklos sritys. ŽEIT, 2021. Prieiga per internetą: URL: http://www.zeit.lt/lt/veiklos-sritys/417 .

Sipavičiūtė A. (2021). *Bendrojo duomenų apsaugos reglamento taikymo strategijos kūrimas organizacijoje* (magistro baigiamasis darbas). Vilnius: Mykolo Romerio universitetas

ANOTACIJA

Magistro baigiamajame darbe yra analizuojamas tiek teoriniu, tiek praktiniu požiūriu aktualus Europos Sąjungos Bendrasis duomenų apsaugos reglamentas, kuris buvo pradėtas taikyti 2018 metų gegužės 25 dieną. BDAR yra pristatomas kaip asmens duomenų apsaugos teisės reformos ES rezultatas, kadangi juo buvo panaikinamas Direktyvos 95/46/EB galiojimas. Pirmoje darbo dalyje konceptualizavus privatumo ir asmens duomenų apsaugos sampratų sąsajas ir raidą bei išanalizavus pagrindinius BDAR juridinius aspektus, išskiriami pagrindiniai BDAR taikymo strategijos organizacijoje elementai: procesas, technologijos ir darbuotojai (žmonės). Antroje darbo dalyje yra pristatoma ir pagrindžiama empirinio tyrimo metodologija, taip pat pateikiama tyrimo loginė eigos schema. Trečioje darbo dalyje yra analizuojami BDAR taikymo strategijos kūrimo organizacijoje tyrimo rezultatai. Atlikus asmens duomenų apsaugos pažeidimų Europoje analizę 2018 – 2021 metais identifikuojami dažniausiai pažeidžiami BDAR straipsniai. Remiantis atliktos analizės rezultatais suformuoti klausimai apklausai, kuria siekiama pasitelkus ekspertų žinias, įvertinti BDAR taikymo strategijos kūrimo svarbą organizacijoje bei pateikti praktines rekomendacijas strategijos optimizavimui. Įvertinus ir išanalizavus ekspertinio vertinimo metu gautus rezultatus, pasiūlytas BDAR taikymo strategijos kūrimo organizacijoje modelis.

Pagrindiniai žodžiai: Bendrasis duomenų apsaugos reglamentas, duomenų apsauga, asmens duomenys, duomenų subjektas, strategija, duomenų saugumo pažeidimas.

Sipavičiūtė A. (2021). *Development of the General Data Protection Regulation application strategy in an organization*.(master thesis). Vilnius: Mykolas Romeris University

ANNOTATION

The Master's Thesis analyzes both the theoretically and practically relevant the EU General Data Protection Regulation, which was introduced on 25 May 2018. The GDPR is presented as a result of the personal data protection law reform in the EU, since it has replaced Directive 95/46 / EC. The first part deals with conceptualization of privacy and personal data protection notions and their evolution while analyzing the principal legal aspects of the BDAR. The central elements of the GDPR application strategy in an organization are specified: the process, technologies and employees (human resources). The second part of the thesis presents and is substantiated by the methodology of the empirical research. In addition, the logical course of the research is displayed. The third part analyzes the research results of the development of application strategy of the GDPR in an organization. The analysis of personal data protection breaches in Europe in 2018-2021 identifies the weakest GDPR articles. Based on the results of the analysis, a questionnaire is developed. The aim of the questionnaire is to assess the importance of the development of application strategy of the GDPR in an organization as well as to provide practical recommendations for strategy's optimization. After evaluating and analyzing the results obtained during the expert evaluation, a model of the development of application strategy of the GDPR in an organization is proposed.

Key words: General Data Protection Regulation; data protection; personal data, data subject; strategy, data protection breach.

Sipavičiūtė A. (2021). *Bendrojo duomenų apsaugos reglamento taikymo strategijos kūrimas organizacijoje* (magistro baigiamasis darbas). Vilnius: Mykolo Romerio universitetas

SANTRAUKA

Europos Sąjungos Bendrasis duomenų apsaugos reglamentas, kuris buvo pradėtas taikyti 2018 metų gegužės 25 dieną, yra tiek teoriniu, tiek praktiniu požiūriu aktualus juridinis dokumentas kiekvienai organizacijai tvarkančiai ar valdančiai asmens duomenis. BDAR yra pristatomas kaip asmens duomenų apsaugos teisės reformos ES rezultatas, kadangi juo buvo panaikinamas Direktyvos 95/46/EB galiojimas.

Asmens duomenų apsauga apibrėžiama kaip teisinių, techninių ir organizacinių priemonių visuma, skirta apsaugoti asmens duomenis nuo neteisėto, atsitiktinio ar netinkamo asmens duomenų tvarkymo. BDAR leidėjams apibrėžiant tik funkcinius BDAR įgyvendinimo reikalavimus bei sąmoningai vengiant rekomenduoti konkrečius techninius bei organizacinius privatumo užtikrinimo būdus įgyvendinant BDAR teisinius reikalavimus (siekiant leisti BDAR pritaikyti prie būsimų techninių naujovių) atsirado neužtikrintumo praktiškai taikant BDAR įtvirtintus reikalavimus organizacijos vykdomoje veikloje problema.

Magistro baigiamajame darbe, remiantis mokslinės literatūros, juridinių dokumentų, nacionalinių priežiūros institucijų (užtikrinančių asmens duomenų apsaugą) teikiamų gairių ir rekomendacijų, asmens duomenų apsaugos pažeidimų Europoje analizės rezultatais bei pasitelkus šios srities ekspertų žinias, siūlomas BDAR taikymo strategijos organizacijoje modelis, padedantis organizacijai savo vykdomoje veikloje veiksmingai taikyti BDAR įtvirtintus reikalavimus bei išvengti galimų finansinių nuostolių (patiriamų įvykus asmens duomenų apsaugos pažeidimui) ir reputacinės žalos. Siūlomas modelis padeda užtikrinti organizacijos vykdomos veiklos atitiktį BDAR įtvirtintiems teisinimas, organizaciniams bei techniniams reikalavimams.

Baigiamąjį darbą sudaro 3 pagrindinės dalys. Pirmojoje darbo dalyje yra konceptualizuojamos privatumo ir asmens duomenų apsaugos sampratos bei jų raida, analizuojami pagrindiniai BDAR įtvirtinti reikalavimai. Antrojoje darbo dalyje yra pristatoma ir pagrindžiama empirinio tyrimo metodologija. Trečiojoje darbo dalyje yra atliekama asmens duomenų apsaugos pažeidimų Europoje analizė, ekspertinis vertinimas siekiant suformuluoti rekomendacijas dėl BDAR taikymo strategijos optimizavimo bei BDAR taikymo strategijos modelio konstravimas.

Sipavičiūtė A. (2021). *Development of the General Data Protection Regulation application strategy in an organization*.((master thesis). Vilnius: Mykolas Romeris University

SUMMARY

The General Data Protection Regulation of the European Union (GDPR), taken into effect on 25 May 2018, is a legal document both theoretically and practically relevant to every organization that handles or manages personal data. GDPR is presented as a result of personal data protection law reform in the EU as it has replaced Directive 95/46 / EC.

The protection of personal data is defined as a set of legal, technical and organizational measures designed to protect personal data against unlawful, accidental or inappropriate processing. The legislators of GDPR have created uncertainty in the practical application of GDPR requirements in the organization's activities by defining only the functional GDPR implementation requirements and consciously avoiding the recommended specific technical and organizational ways to ensure privacy in such implementations (in order to allow GDPR to adapt to future technical innovations).

This master's thesis draws on the analysis of scientific literature, legal documents, guidelines and recommendations provided by national supervisory authorities (which ensure personal data protection), personal data breaches in Europe and the expertise of the field while outlining a model of GDPR requirement application strategy in the organization. The proposed model offers an assistance in applying the GDPR requirements effectively as well as avoiding possible financial losses (occurring in the event of a personal data breach) and reputational damage. In addition, this model helps to ensure that the activities carried out by the organization comply with the legislations along with the organizational and technical requirements established by the GDPR.

This master's thesis consists of three main parts. The first part of the work conceptualizes the notiona of privacy and personal data protection and their development while analyzing the main requirements established by the GDPR. The second part of the paper displays and is substantiated by the methodology of empirical research. The third part of the thesis draws on the analysis of personal data protection violations in Europe, expert evaluation with the purpose of devising proposals for the optimization of the GDPR application strategy, and the construction of the GDPR application strategy model.

PRIEDAI

1 PRIEDAS. Veiklų, dėl kurių turi būti atliekamas poveikio duomenų apsaugai vertinimas, sąrašas

1.	Asmens duomenų tvarkymas mokslinių ar istorinių tyrimų tikslais, kai be asmens sutikimo tvarkomi specialių kategorijų asmens duomenys arba asmens duomenų tvarkymas vykdomas susiejant ar derinant duomenų rinkinius; kai tvarkomi nepilnamečių asmenų duomenys; kai tvarkomas asmens kodas.
2.	Asmens duomenų tvarkymas vykdomas dideliu mastu, kai asmens duomenys gauti ne iš asmens bei informacijos pateikimas tam tikrais atvejais yra neįmanomas arba tam reikėtų neproporcingų pastangų, arba jeigu dėl tokio informacijos pateikimo gali tapti neįmanoma arba jis gali labai sukliudyti pasiekti tvarkymo tikslus.
3.	Asmens duomenų tvarkymas, kai duomenų gavėjų, kuriems buvo atskleisti asmens duomenys, informavimas apie asmens duomenų ištaisymą, ištrynimą arba tvarkymo apribojimą nėra įmanomas arba pareikalautų neproporcingų pastangų.
4.	Biometrinių duomenų, kuriais siekiama konkrečiai nustatyti fizinio asmens tapatybę, tvarkymas asmenų stebėsenos ar kontrolės tikslais arba kai tvarkomi pažeidžiamų asmenų duomenys.
5.	Genetinių duomenų tvarkymas vykdant asmens savybių vertinimą arba balų skyrimą, įskaitant profiliavimą ir prognozavimą.
6.	Asmens vaizdo duomenų tvarkymas, kai vaizdo stebėjimas vykdomas patalpose ir (ar) teritorijose, kurios nėra duomenų valdytojo valdomos nuosavybės ar kitais teisėtais pagrindais; sveikatos priežiūros, socialinės globos, įkalinimo įstaigose ir kitose įstaigose, kuriose paslaugos yra teikiamos pažeidžiamiems asmenims; kartu su garso įrašymu.
7.	Pokalbių telefonu įrašymas.
8.	Asmens duomenų tvarkymas naudojant inovatyvias technologijas arba egzistuojančias technologijas panaudojant nauju būdu, kai tvarkomi pažeidžiamų duomenų subjektų asmens duomenys.
9.	Vaikų asmens duomenų tvarkymas tiesioginės rinkodaros tikslais, vaikų asmeninių aspektų vertinimas, kuris yra grindžiamas automatizuotu tvarkymu, įskaitant profiliavimą, arba kai vaikams tiesiogiai yra siūlomos informacinės visuomenės paslaugos.
10.	Darbuotojų asmens duomenų tvarkymas stebėsenos ar kontrolės tikslais: asmens vaizdo ir (ar) garso duomenų tvarkymas darbo vietoje ir (ar) duomenų valdytojo patalpose ar teritorijose, kuriose dirba jo darbuotojai; asmens duomenų, susijusių su darbuotojų, komunikacijos, elgesio, vietos ar judėjimo stebėsena, tvarkymas.

Šaltinis: sudaryta autorės, remiantis VDAI direktoriaus įsakymu „Dėl duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai įvertinimą, sąrašo patvirtinimo“, priimto 2019 metų kovo mėnesio 14 dieną (Nr. 1T-35 (1.12.E))

2 PRIEDAS. Ekspertinio tyrimo anketa

1. Prašom nurodyti, kiek pritariate šiems teiginiams.

	Visiškai sutinku	Sutinku	Nei sutinku, nei nesutinku	Nesutinku	Visiškai nesutinku
BDAR taikymo strategijos kūrimas yra prioritetinis organizacijos uždavinys					
BDAR taikymo strategijos kūrimas organizacijoje yra sudėtingas uždavinys					

2. Su kokiomis kliūtimis, Jūsų nuomone, dažniausiai susiduria organizacijos siekdamos užtikrinti tinkamą asmens duomenų apsaugą? (galimi keli atsakymų variantai)

   - Poreikis pakeisti verslo praktiką įsigaliojus BDAR
   - Konkrečių techninių ir organizacinių privatumo užtikrinimo būdų įgyvendinant BDAR teisinius reikalavimus apibrėžimo trūkumas
   - Šios srities ekspertų trūkumas
   - Duomenų apsaugos priežiūros institucijų viešai skelbiamų rekomendacijų bei gairių dėl BDAR įgyvendinimo trūkumas
   - Kitas variantas (įrašykite)

3. Kokios priežastys, Jūsų nuomone, pagrinde lemia asmens duomenų apsaugos pažeidimus organizacijoje? (galimi keli atsakymų variantai)

   - Duomenų apsaugos pareigūno pareigybės neįsteigimas
   - Nepakankamas investavimas į tinkamas saugumo technologijas
   - Nekokybiškai atlikta tvarkomų asmens duomenų analizė
   - Normatyvinių dokumentų, susijusių su duomenų apsauga, organizacijoje nebuvimas
   - Bendradarbiavimo su nacionaline duomenų apsaugos priežiūros institucija stoka
   - Darbuotojų ugdymo duomenų apsaugos srityje stoka
   - Ekspertų viešo dalijimosi specializuotomis teisinėmis žiniomis, geroji praktika, praktiškais ir naujais sprendimais stoka
   - Kitas variantas (įrašykite)

4. Įvertinkite, Jūsų nuomone, organizacijoje galimai disponuotinų priemonių, skirtų pakankamam duomenų subjekto informavimui bei jo teisių įgyvendinimo užtikrinimui, svarbą.

	Labai svarbu	Svarbu	Nei svarbu, nei nesvarbu	Nesvarbu	Visiškai nesvarbu
Asmens duomenų tvarkymo organizacijoje aprašas					
Asmens duomenų saugojimo politika					
Prašymo įgyvendinti duomenų subjekto teisę (-es) forma					
Privatumo politika (jei taikoma)					
Slapukų naudojimo politika (jei taikoma)					
Sutikimas tvarkyti asmens duomenis ir jo forma					
Darbuotojų elgesio kodeksas					
Darbuotojų asmens duomenų saugojimo politika					
Pranešimo forma priežiūros institucijoms, duomenų subjektui					

5. Kokios papildomos disponavimo priemonės (nepaminėtos 4 klausime), Jūsų nuomone, galėtų padėti organizacijai užtikrinti pakankamą duomenų subjekto informavimą bei jo teisių įgyvendinimą?

6. Įvertinkite, Jūsų nuomone, organizacijoje galimai disponuotinų priemonių siekiant tinkamai įvykdyti pranešimo apie asmens duomenų saugos pažeidimą įsipareigojimą svarbą.

	Labai svarbu	Svarbu	Nei svarbu, nei nesvarbu	Nesvarbu	Visiškai nesvarbu
Duomenų saugos pažeidimų pranešimo priežiūros institucijai tvarkos aprašas					
Duomenų saugos pažeidimų pranešimo duomenų subjektui tvarkos aprašas					
Duomenų apsaugos pareigūno paskyrimas					
Duomenų tvarkymo veiklos įrašų registro vedimas					

7. Kokios papildomos disponavimo priemonės (nepaminėtos 6 klausime), Jūsų nuomone, galėtų padėti organizacijai tinkamai įvykdyti pranešimo apie asmens duomenų saugos pažeidimą įsipareigojimą?

8. Kaip manote, ar konkrečiam sektoriui pritaikytų BDAR elgesio kodeksų, leidžiančių tam tikros srities duomenų valdytojams susitarti dėl bendrų BDAR reikalavimus atitinkančių standartų taikymo, diegimas yra veiksminga priemonė, padedanti organizacijai laikytis asmens duomenų valdytojo atskaitomybės principo?

   - Taip, priemonė yra veiksminga
   - Ne, priemonė yra neveiksminga
   - Priemonė yra nei veiksminga, nei neveiksminga

   Pagrįskite savo nuomonę (įrašyti).

9. Kaip manote, ar atitikties BDAR reikalavimams sertifikato įgijimas yra veiksminga priemonė padedanti organizacijai tinkamai vykdyti BDAR įtvirtintus reikalavimus?

   - Taip, priemonė yra veiksminga
   - Ne, priemonė yra neveiksminga
   - Priemonė yra nei veiksminga, nei neveiksminga

   Pagrįskite savo nuomonę (įrašyti).

10. Ar, Jūsų nuomone, asmens duomenų saugumo pažeidimų, įvykusių kitose organizacijose, stebėjimas bei analizė yra veiksminga profilaktinė priemonė siekiant tinkamai vykdyti BDAR įtvirtintus reikalavimus savo organizacijoje?

    - Taip, profilaktinė priemonė yra veiksminga
    - Ne, profilaktinė priemonė yra neveiksminga
    - Profilaktinė priemonė yra nei veiksminga, nei neveiksminga

    Pagrįskite savo nuomonę (įrašyti).

3 PRIEDAS. Tyrime dalyvaujančių šalių sąrašas

	ES valstybės narės	**Šengeno erdvei priklausančios valstybės**	**Kitos Eurpos šalys**
1.	Airija	Islandija	Jungtinė Karalystė*
2.	Austrija	Norvegija	
3.	Belgija		
4.	Bulgarija		
5.	Čekija		
6.	Danija		
7.	Estija		
8.	Graikija		
9.	Ispanija		
10.	Italija		
11.	Kipras		
12.	Kroatija		
13.	Latvija		
14.	Lenkija		
15.	Lietuva		
16.	Malta		
17.	Nyderlandai		
18.	Portugalija		
19.	Prancūzija		
20.	Rumunija		
21.	Slovakija		
22.	Suomija		
23.	Švedija		
24.	Vengrija		
25.	Vokietija		

Šaltinis: sudaryta autorės, remiantis CMS International Fines Database: GDPR Enforcement Tracker, 2021

Tyrime nedalyvaujančios ES valstybės narės: Liuksemburgas, Slovėnija

* Įskaitant Meino Salą

4 PRIEDAS. BDAR straipsnių pažeidimų dažnis Europoje 2018 – 2021 metais

METAI	2018																										
BDAR straipsnis	**5**	**6**	**7**	**8**	**9**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**21**	**24**	**25**	**28**	**29**	**30**	**31**	**32**	**33**	**34**	**35**	**36**	**37**	**58**	**83**
AIRIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AUSTRIJA	3	2	0	0	0	0	3	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
BELGIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
BULGARIJA	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ČEKIJA	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DANIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ESTIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
GRAIKIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ISLANDIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ISPANIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ITALIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
JUNGTINĖ KARALYSTĖ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
KIPRAS	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
KROATIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
LATVIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
LENKIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
LIETUVA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MALTA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
NYDERLANDAI	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
NORVEGIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PORTUGALIJA	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
PRANCŪZIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
RUMUNIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SLOVAIKIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SUOMIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ŠVEDIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
VENGRIJA	0	0	0	0	0	1	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
VOKIETIJA	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	1	1	0	0	0	0	1
IŠ VISO:	**5**	**4**	**0**	**0**	**0**	**1**	**4**	**1**	**2**	**0**	**0**	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**2**	**1**	**1**	**0**	**0**	**0**	**0**	**1**

METAI	2019																										
BDAR straipsnis	**5**	**6**	**7**	**8**	**9**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**21**	**24**	**25**	**28**	**29**	**30**	**31**	**32**	**33**	**34**	**35**	**36**	**37**	**58**	**83**
AIRIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AUSTRIJA	1	2	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
BELGIJA	2	4	0	0	0	2	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
BULGARIJA	5	9	0	0	1	2	0	0	3	0	0	0	0	0	2	0	0	0	1	2	0	0	0	0	0	1	1
ČEKIJA	2	3	1	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0
DANIJA	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ESTIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
GRAIKIJA	3	2	0	0	0	0	1	1	0	0	0	0	2	0	2	0	0	0	0	1	0	0	0	0	0	0	0
ISLANDIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ISPANIJA	14	11	1	0	0	0	4	0	0	1	0	0	0	0	0	0	0	0	1	5	0	0	0	0	0	0	0
ITALIJA	2	2	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	2	0	0	0	0	0	0	0
JUNGTINĖ KARALYSTĖ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
KIPRAS	1	5	0	0	3	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
KROATIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
LATVIJA	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
LENKIJA	2	1	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0
LIETUVA	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0
MALTA	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
NYDERLANDAI	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0
NORVEGIJA	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0
PORTUGALIJA	0	0	0	0	0	0	2	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PRANCŪZIJA	3	2	0	0	0	1	3	2	0	0	0	0	1	0	0	0	0	0	0	3	0	0	0	0	0	0	0
RUMUNIJA	7	6	3	0	1	2	1	0	1	0	17	0	1	0	2	0	0	0	0	11	2	0	0	0	0	3	0
SLOVAIKIJA	3	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0
SUOMIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ŠVEDIJA	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0
VENGRIJA	14	12	0	0	0	1	5	1	2	0	2	1	1	2	2	0	0	0	0	1	4	1	0	0	0	0	0
VOKIETIJA	7	5	0	0	0	0	0	0	2	0	1	0	2	0	0	1	0	0	0	4	1	1	0	0	2	0	0
IŠ VISO:	**72**	**67**	**5**	**0**	**6**	**8**	**18**	**6**	**13**	**1**	**23**	**1**	**8**	**2**	**8**	**2**	**0**	**0**	**2**	**43**	**8**	**2**	**1**	**1**	**3**	**4**	**1**

4 priedo tęsinys

METAI	2020																									
BDAR straipsnis	**5**	**6**	**7**	**8**	**9**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**21**	**24**	**25**	**28**	**29**	**30**	**31**	**32**	**33**	**34**	**35**	**36**	**37**	**58**	**83**
AIRIJA	4	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	3	0	0	0	0	0	0
AUSTRIJA	3	2	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
BELGIJA	8	11	1	0	0	4	1	3	2	0	2	0	2	2	1	0	0	1	2	0	0	0	0	0	2	1	0
BULGARIJA	0	3	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	2	0	0	0	0	0	0	0
ČEKIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DANIJA	5	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	3	1	1	0	0	0	0	0
ESTIJA	4	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
GRAIKIJA	3	0	0	0	0	1	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
ISLANDIJA	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0
ISPANIJA	84	63	3	1	0	4	21	10	1	0	0	0	5	0	0	0	0	0	2	10	1		0	0	2	8	0
ITALIJA	37	24	3	0	7	6	10	3	5	1	3	0	2	2	3	5	1	1	0	9	1	0	1	0	0	0	0
JUNGTINĖ KARALYSTĖ	2	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0
KIPRAS	2	2	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	3	1	0	0	0	0	0	0
KROATIJA	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
LATVIJA	1	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
LENKIJA	4	1	0	0	1	0	0	0	0	0	0	0	0	0	2	0	0	0	5	3	2	2	0	0	0	5	0
LIETUVA	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MALTA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
NYDERLANDAI	2	1	0	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
NORVEGIJA	5	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	1	0	0	0	0
PORTUGALIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PRANCŪZIJA	4	0	0	0	0	1	2	2	1	0	1	0	2	0	0	1	0	0	0	3	3	1	0	0	0	0	0
RUMUNIJA	5	4	1	0	1	2	1	0	1	0	2	0	1	0	1	0	0	0	2	16	1	0	0	0	0	5	0
SLOVAIKIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SUOMIJA	3	3	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0
ŠVEDIJA	14	5	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	9	1	1	1	1	0	0	0
VENGRIJA	9	7	0	0	2	6	2	0	5	0	2	0	0	1	2	0	0	0	0	4	0	1	0	0	0	0	0
VOKIETIJA	2	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0
IŠ VISO:	**204**	**141**	**8**	**1**	**13**	**27**	**40**	**19**	**24**	**1**	**11**	**0**	**12**	**5**	**11**	**6**	**1**	**2**	**11**	**78**	**14**	**6**	**5**	**1**	**4**	**20**	**0**

METAI	2021																									
BDAR straipsnis	**5**	**6**	**7**	**8**	**9**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**21**	**24**	**25**	**28**	**29**	**30**	**31**	**32**	**33**	**34**	**35**	**36**	**37**	**58**	**83**
AIRIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AUSTRIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
BELGIJA	2	2	1	0	0	1	1	0	0	0	0	0	1	2	1	1	0	0	0	1	1	1	0	0	0	0	0
BULGARIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ČEKIJA	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DANIJA	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ESTIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
GRAIKIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ISLANDIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ISPANIJA	9	7	0	0	0	0	4	1	0	0	1	0	2	0	0	1	0	0	0	0	0	0	0	0	0	1	0
ITALIJA	6	1	0	0	5	1	0	0	1	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0
JUNGTINĖ KARALYSTĖ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
KIPRAS	1	1	0	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	1	2	1	0	0	0	0	1	0
KROATIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
LATVIJA	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
LENKIJA	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	1	2	0	0	0	1	0
LIETUVA	2	0	0	0	0	0	2	0	0	0	0	0	0	2	0	0	0	0	0	3	0	0	2	0	0	2	0
MALTA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
NYDERLANDAI	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
NORVEGIJA	8	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PORTUGALIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PRANCŪZIJA	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0
RUMUNIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0
SLOVAIKIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
SUOMIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ŠVEDIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
VENGRIJA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
VOKIETIJA	3	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0
IŠ VISO:	**33**	**22**	**1**	**0**	**6**	**4**	**8**	**2**	**2**	**0**	**1**	**0**	**3**	**4**	**2**	**3**	**1**	**0**	**1**	**17**	**3**	**3**	**2**	**0**	**0**	**5**	**0**

Šaltinis: sudaryta autorės, remiantis CMS International Fines Database: GDPR Enforcement Tracker, 2021

5 PRIEDAS. Darbe analizuojamų BDAR straipsnių sąrašas

Straipsnio nr.	**Straipsnio pavadinimas**	**Skyrius**	**Skyriaus pavadinimas**	**Skyriaus skirsnio pavadinimas**
5	Su asmens duomenų tvarkymu susiję principai	II	Principai	Nėra
6	Tvarkymo teisėtumas	II	Principai	Nėra
7	Sutikimo sąlygos	II	Principai	Nėra
8	Sąlygos, taikomos vaiko, kuriam siūlomos informacinės visuomenės paslaugos, sutikimui	II	Principai	Nėra
9	Specialių kategorijų asmens duomenų tvarkymas	II	Principai	Nėra
12	Skaidrus informavimas, pranešimas ir duomenų subjekto naudojimosi savo teisėmis sąlygos	III	Duomenų subjekto teisės	Skaidrumas ir sąlygos
13	Informacija, kuri turi būti pateikta, kai asmens duomenys renkami iš duomenų subjekto	III	Duomenų subjekto teisės	Informavimas ir teisė susipažinti su asmens duomenimis
14	Informacija, kuri turi būti pateikta, kai asmens duomenys yra gauti ne iš duomenų subjekto	III	Duomenų subjekto teisės	Informavimas ir teisė susipažinti su asmens duomenimis
15	Duomenų subjekto teisė susipažinti su duomenimis	III	Duomenų subjekto teisės	Informavimas ir teisė susipažinti su asmens duomenimis
16	Teisė reikalauti ištaisyti duomenis	III	Duomenų subjekto teisės	Duomenų ištaisymas ir ištrynimas
17	Teisė reikalauti ištrinti duomenis („teisė būti pamirštam“)	III	Duomenų subjekto teisės	Duomenų ištaisymas ir ištrynimas
18	Teisė apriboti duomenų tvarkymą	III	Duomenų subjekto teisės	Duomenų ištaisymas ir ištrynimas
21	Teisė nesutikti	III	Duomenų subjekto teisės	Teisė nesutikti ir automatizuotas atskirų sprendimų priėmimas
24	Duomenų valdytojo atsakomybė	IV	Duomenų valdytojas ir duomenų tvarkytojas	Bendrosios prievolės
25	Pritaikytoji duomenų apsauga ir standartizuotoji duomenų apsauga	IV	Duomenų valdytojas ir duomenų tvarkytojas	Bendrosios prievolės
28	Duomenų tvarkytojas	IV	Duomenų valdytojas ir duomenų tvarkytojas	Bendrosios prievolės
29	Duomenų valdytojui ar duomenų tvarkytojui pavaldžių asmenų atliekamas duomenų tvarkymas	IV	Duomenų valdytojas ir duomenų tvarkytojas	Bendrosios prievolės
30	Duomenų tvarkymo veiklos įrašai	IV	Duomenų valdytojas ir duomenų tvarkytojas	Bendrosios prievolės

5 priedo tęsinys

31	Bendradarbiavimas su priežiūros institucija	IV	Duomenų valdytojas ir duomenų tvarkytojas	Bendrosios prievolės
32	Duomenų tvarkymo saugumas	IV	Duomenų valdytojas ir duomenų tvarkytojas	Asmens duomenų saugumas
33	Pranešimas priežiūros institucijai apie asmens duomenų saugumo pažeidimą	IV	Duomenų valdytojas ir duomenų tvarkytojas	Asmens duomenų saugumas
34	Pranešimas duomenų subjektui apie asmens duomenų saugumo pažeidimą	IV	Duomenų valdytojas ir duomenų tvarkytojas	Asmens duomenų saugumas
35	Poveikio duomenų apsaugai vertinimas	IV	Duomenų valdytojas ir duomenų tvarkytojas	Poveikio duomenų apsaugai vertinimas ir išankstinės konsultacijos
36	Išankstinės konsultacijos	IV	Duomenų valdytojas ir duomenų tvarkytojas	Poveikio duomenų apsaugai vertinimas ir išankstinės konsultacijos
37	Duomenų apsaugos pareigūno skyrimas	IV	Duomenų valdytojas ir duomenų tvarkytojas	Duomenų apsaugos pareigūnas
58	Įgaliojimai	VI	Nepriklausomos priežiūros institucijos	Kompetencija, užduotys ir įgaliojimai
83	Bendrosios administracinių baudų skyrimo sąlygos	VIII	Teisių gynimo priemonės, atsakomybė ir sankcijos	Nėra

Šaltinis: sudaryta autorės, remiantis „Europos parlamento ir tarybos reglamentas (ES) 2016/679”

PATVIRTINIMAS APIE ATLIKTO DARBO SAVARANKIŠKUMĄ

2021-04-28

Vilnius

Aš, Mykolo Romerio universiteto (toliau – Universitetas),

____Viešojo valdymo ir verslo fakulteto, kibernetinio saugumo valdymo_____

(fakulteto / instituto, programos pavadinimas)

Studentas (-ė)_____Agnė Sipavičiūtė_____,

(vardas, pavardė)

patvirtinu, kad šis magistro baigiamasis darbas

„Bendrojo duomenų apsaugos reglamento taikymo strategijos kūrimas organizacijoje“:_____

(*baigiamojo darbo pavadinimas*)

1. Yra atliktas savarankiškai ir sąžiningai;
2. Nebuvo pristatytas ir gintas kitoje mokslo įstaigoje Lietuvoje ar užsienyje;
3. Yra parašytas remiantis akademinio rašymo principais ir susipažinus su rašto darbų metodiniais nurodymais.

Man žinoma, kad už sąžiningos konkurencijos principo pažeidimą – plagijavimą studentas gali būti šalinamas iš Universiteto kaip už šiurkštų akademinės etikos pažeidimą.

_____ _____Agnė Sipavičiūtė_____

(parašas) *(vardas, pavardė)*