Vilniaus universiteto Teisės fakulteto

Privatinės teisės katedra

Dianos Lauros Ločinskos

V kurso, Europos Sąjungos

verslo teisės studijų šakos

studentės

Magistro darbas

Duomenų apsaugos pareigūno ir duomenų valdytojo atsakomybės už atitiktį duomenų apsaugos teisei santykis

Vadovas: asist. dr. Julius Zaleskis

Recenzentas: doc. dr. Laurynas Didžiulis

Vilnius

2020

TURINYS

ĮVADAS

Temos aktualumas. Vis didėjantis gyvenimo tempas, progresuojančios technologijų galimybės verčia teisę taip pat prisitaikyti prie aktyvios ir vis modernėjančios visuomenės bei pasiruošti priimti naujus iššūkius. Vis labiau klesti internetinė prekyba, atostogų rezervacijos, transporto nuoma ir kt. Visos šios ir kitos verslo platformos apima duomenų srauto apdorojimo operacijas, kad būtų teikiamos rinkai siūlomos paslaugos. Tai sudaro prielaidą vis sparčiau vystyti vienos iš verslo varomųjų jėgų – duomenų, apsaugos sistemą. 2018 m. gegužės 25 d. įsigaliojęs 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (toliau – BDAR) padėjo atskaitos tašką verslo pokyčiams iš pagrindų. Prof. dr. D. Žalimas pažymi jog, istoriniu duomenų apsaugos teisės pamatu laikytina asmens teisė į privatų gyvenimą, įtvirtinta 1948 m. Visuotinėje žmogaus teisių deklaracijoje, 1950 m. Europos žmogaus teisių ir pagrindinių laisvių konvencijoje (toliau – EŽTK), o taip pat 1966 m. Tarptautiniame pilietinių ir politinių teisių pakte bei Lietuvos Respublikos Konstitucijoje[1]. Savarankiškos asmens duomenų apsaugos teisės pirmųjų nacionalinės teisės aktų ištakos randamos Vakarų Europos valstybėse[2]. Rengiant 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvą 1995/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (toliau – Direktyva 95/46/EB) stengtasi sukurti ilgaamžį asmens duomenų apsaugos režimą[3], tačiau Prof. dr. D. Žalimo nuomone, naujasis šios teisės šakos raidos etapas prasidėjo 2018 m. gegužės 25 d., pradėjus taikyti BDAR[4]. Be BDAR teisė į duomenų apsaugą įtvirtinta Europos Sąjungos pagrindinių teisių chartijoje, Konvencijoje dėl asmens duomenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) (toliau – Konvencija Nr. 108) bei Sutarties dėl Europos Sąjungos suvestinėje redakcijoje (toliau – SESV).

Iš visų BDAR naujojo reguliavimo pateiktų naujovių, duomenų apsaugos ekspertų bei verslo subjektų dėmesį prikaustė duomenų valdytojo atsakomybės raida bei duomenų

[1] ZALESKIS, Julius. *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: Registrų centras, 2019, p. 8.
[2] *Ibidem.*
[3] CIVILKA, Mindaugas; ŠLAPIMAITĖ, Lina. *Asmens duomenų samprata elektroninėje erdvėje*. Teisė, 2015, t. 96, p. 126- 148 [interaktyvu. Žiūrėta vasario 30 d.]. Prieiga per internetą: < https://www.zurnalai.vu.lt/teise/article/view/8761/7647>.
[4] ZALESKIS, Julius. *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: Registrų centras, 2019, p. 8.

apsaugos pareigūno institutas. Iki šiol išlieka neaiškus šių dviejų subjektų ryšys, o tuo labiau vis daugiau klausimų kelia atsakomybės ribos už tinkamą duomenų apsaugos reikalavimų įgyvendinimą. Nepateikiamas aiškus atribojimas, kur baigiasi duomenų valdytojo ir kur prasideda duomenų apsaugos pareigūno atsakomybė, kas atsako už atitiktį, o kaip pasiskirsto atsakomybė atsiradus žalai dėl netinkamai vykdyto duomenų apsaugos reikalavimų įgyvendinimo. Dėl savo abstraktaus pobūdžio pagrindinis duomenų apsaugą reguliuojantis teisės aktas – BDAR, nepateikia reikiamų atsakymų, dėl ko plečiant šią teisės sritį atsiranda vis daugiau spragų bei vis įvairesnių interpretacijų siekiant rasti sprendimą. Taip pat šis klausimas nėra nagrinėtas teismų praktikoje, pateikiant eksplicitinį vertinimą. Visą tai sąlygoja aplinkybes, kurioms esant sudėtinga rasti balansą ir nubrėžti aiškią ribą tarp kompetencijų sąlygotos atsakomybės.

Tyrimo objektas – teisės normos nustatančios duomenų valdytojo ir duomenų apsaugos pareigūno teisinę atsakomybę apibrėžiant ją kaip, teisinį įpareigojimą teisės subjektams garantuoti naudojimąsi savo teisėmis atitinkamų pareigų vykdymu nurodant, kad tokių pareigų nevykdymas, virs atitinkamų teisių praradimu.[5] Tiriamas duomenų valdytojo ir duomenų apsaugos pareigūno teisinės atsakomybės santykis, vertinant tiek atsakomybę už netinkamą duomenų tvarkymo politiką, tiek už tokios politikos sąlygotus pažeidimus.

Tyrimo dalykas – tarptautinės, ES bei nacionalinės teisės nuostatos, reglamentuojančios reikalavimus keliamus duomenų valdytojo atliekamiems asmens duomenų tvarkymo procesams bei nustatančios asmens duomenų apsaugos standartus bei duomenų valdytojo ir duomenų apsaugos pareigūno atsakomybę.

Tyrimo tikslas – nustatyti duomenų valdytojo ir duomenų apsaugos pareigūno atsakomybės santykį, užtikrinant atitiktį duomenų apsaugos teisės normų reikalavimams bei atsakant už įvykusius teisės pažeidimus.

Tyrimo uždaviniai:

1. Įvertinti duomenų valdytoją, kaip vieną svarbiausių asmens duomenų apsaugos teisės subjektų, atlikti apibrėžties analizę, įvertinti jam paskirtas pareigas bei pagrindinius reikalavimus vykdomai veiklai;
2. Atlikti detalią sąvokos „duomenų apsaugos pareigūnas“ analizę, įvertinant pagrindines pareigas, funkcijas, suteikiamą statusą ir vietą, kurią subjektas užima duomenų apsaugos teisės grandinėje;

[5] VAIŠVILA, Alfonsas. Teisės teorija: vadovėlis. Vilnius: Justitia, 2000, p. 350.

3. Įvertinti duomenų valdytojo ir duomenų apsaugos pareigūno atsakomybės santykį už atitiktį duomenų apsaugos teisės reguliavimui bei aiškiai atskirti kiekvieno subjekto atsakomybės atsiradimo bei pasibaigimo momentą;
4. Įvertinti duomenų valdytojo ir duomenų apsaugos pareigūno atsakomybės santykį už nustatytus duomenų apsaugos pažeidimus, nustatant, kuris subjektas turi plačiausias atsakomybės ribas bei didesnę įtaką pažeidimų atsiradimui.

Tyrimo metodai – iškeltiems tyrimo uždaviniams įgyvendinti pasirinkti:

1. *Lyginamasis metodas* – jo pagalba analizuojamos bei lyginamos tarptautinės bei Lietuvos teisės normos, įtvirtinančios asmens duomenų apsaugos reikalavimus ir svarbiausius principus.
2. *Apibendrinimo metodas* – jo pagalba vertinama surinkta informacija siekiant suformuluoti išvadas ir apibendrinti atsakymus į pagrindinę tyrimo problematiką.
3. *Teisinių dokumentų analizės metodas* – šio metodo pagalba tiriami, analizuojami teisės aktai, atskleidžiami trūkumai bei įgyvendinimo problemos.

Darbo originalumas – teisės doktrinoje pakankamai plačiai spėta išnagrinėti skirtingus asmens duomenų apsaugos teisės aspektus. I. Petraitytė kaip ir jos užsienio kolegos J. Kokott ir C. Sobotta[6], atliko duomenų apsaugos teisės ir teisės į asmens privatų gyvenimą koreliacijos analizę[7] bei apžvelgė duomenų teisinės apsaugos principus[8]. Duomenų apsaugos teisės ypatumus elektroninėje erdvėje vertino M. Civilka ir L. Šlapimaitė[9]. Tuo tarpu praktinius sveikatos duomenų tvarkymo aspektus pateikė Prof. J. Januševičienė[10]. Pagrindines BDAR naujoves apžvelgė Dr. J. Zaleskis[11], o taip pat pateikė duomenų

[6] KOKOTT, Juliane; SOBOTTA, Christoph. The distinction between privacy amd data protection in the jurisprudence CJEU and the ECtHR. *International Data Privacy Law*, 2013, Vol. 3, No. 4 p. 222-228 [interaktyvu. Žiūrėta 2020 m. balandžio 5 d.] Prieiga per internetą:https://watermark.silverchair.com/ipt017.pdf

[7] PETRAITYTĖ, Ilona, *Asmens duomenų apsauga ir teisė į privatų gyvenimą*. Teisė, 2011, t. 80; [interaktyvu. Žiūrėta 2020 m. balandžio 5d.] Prieiga per internetą: < http://www.journals.vu.lt/teise/article/view/158/124>.

[8] PETRAITYTĖ, Ilona, *Asmens duomenų teisinės apsaugos principai*: daktaro disertacija. Vilnius: Vilniaus universitetas, 2013. [interaktyvu. Žiūrėta 2020 m. balandžio 5 d.] Prieiga per internetą: <http://www.tf.vu.lt/wp-content/uploads/2016/08/Ilona-Petraityt%C4%97_Asmens-duomen%C5%B3-teisin%C4%97s-apsaugos-principai-.pdf>

[9] CIVILKA, M. IR ŠLAPIMAITĖ, L. *Asmens duomenų samprata elektroninėje erdvėje*. Teisė. 2015. t. 95; [interaktyvu. Žiūrėta 2020 m. balandžio 5 d.] Prieiga per internetą: <https://www.zurnalai.vu.lt/teise/article/view/8761/7647 >

[10] JANUŠEVIČIENĖ, Justina. *Praktiniai asmens sveikatos duomenų tvarkymo aspektai pagal bendrąjį asmens duomenų apsaugos reglamentą*. Teisė. 2018. T. 107; [interaktyvu. Žiūrėta 2020 m. balandžio 5 d.] Prieiga per internetą: <https://www.zurnalai.vu.lt/teise/article/view/11674/10258>

[11] ZALESKIS, Julius, ES bendrasis duomenų apsaugos reglamentas: reikšmė duomenų apsaugos teisei. Teisė, 2017, t. 103., p. 45- 54. [interaktyvu. Žiūrėta 2020 m. balandžio 5 d.] Prieiga per internetą: http://www.zurnalai.vu.lt/teise/article/view/10779/8959

apsaugos pareigūno instituto analizę[12]. Vertinant šį duomenų apsaugos teisės subjektą, duomenų apsaugos pareigūno sertifikavimo klausimo analizę atliko užsienio autorius E. Lachaud[13]. O atsakomybės klausimais pasisakė Brendon Van Alsenoy pateikdamas duomenų valdytojo atsakomybės vertinimą[14]. Tačiau doktrinoje nėra išnagrinėtas, duomenų apsaugos pareigūno atsakomybės santykis su duomenų valdytoju, nors šie du duomenų apsaugos teisės subjektai yra vieni svarbiausių. Šiame darbe detaliai vertinamas šių dviejų asmens duomenų apsaugos teisės subjektų santykis. Atliekama išsami duomenų valdytojui ir duomenų apsaugos pareigūnui kylančios atsakomybės analizė. Darbas gali būti reikšmingas siekiant tiek teoriniu, tiek praktiniu lygiu aiškiai apibrėžti duomenų valdytojo ir duomenų apsaugos pareigūno atsakomybės ribas užtikrinant organizacijos atitiktį duomenų apsaugos teisės normoms ar atsiradus duomenų apsaugos teisės pažeidimui.

Svarbiausi šaltiniai – pagrindiniu tyrimo šaltiniu buvo BDAR bei Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas. Taip pat naudojamasi *soft law* šaltiniais ES 29 straipsnio duomenų apsaugos darbo grupės gairėmis bei Europos duomenų apsaugos valdybos gairėmis bei nuomonėmis, pateikiančiomis BDAR normų išaiškinimus, taip pat nacionalinės priežiūros institucijos – Valstybinės duomenų apsaugos inspekcijos rekomendacijomis. Remtasi papildomai teisine doktrina bei nacionalinių teismų, Europos Žmogaus Teisių Teismo ir Europos Sąjungos Teisingumo Teismo praktika.

[12] ZALESKIS, Julius, Duomenų apsaugos pareigūno veiklos pagrindai pagal ES bendrąjį duomenų apsaugos reglamentą. Teisė, 2017, t. 104. Prieiga per internetą: <http://www.zurnalai.vu.lt/teise/article/view/10851/8986>

[13] Lachaud, Eric. Should the DPO be certified? International Data Privacy Law, 2014, Vol. 4, No. 3, p. 189-202 [interaktyvus. Žiūrėta balandžio 5 d.] Prieiga per internetą: <https://www.scribd.com/document/350068564/Should-the-DPO-Be-Certified>.

[14] VAN ALSENOY, Brendan. Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation, 7. 2016. JIPITEC 271 para 15, p. 276 [interaktyvu. Žiūrėta 2020 m. balandžio 18 d.]. Prieiga per internetą: < https://www.jipitec.eu/issues/jipitec-7-3-2016/4506/van_alsenoy_liability_under_eu_data_protection_law_jiptec_7_3_2016_271.pdf>.

1. DUOMENŲ VALDYTOJO ATSAKOMYBĖ UŽ ATITIKTĮ ASMENS DUOMENŲ APSAUGOS REGULIAVIMUI

1.1. Duomenų valdytojo samprata

Asmens duomenų apsaugos teisės normos, kaip ir bet kurios kitos teisės šakos normos yra teisinio reguliavimo priemonės, visuomenės santykio modelis[15], orientuotas į duomenų apsaugos santykio reguliavimą. Prof. A. Vaišvilos teigimu[16], gyvenant visuomenėje susidaro galimybė ne tik tinkamiau apsaugoti ir įgyvendinti savo interesus, bet ir vienam asmeniui ar socialinei grupei išnaudoti kitus, nes čia atsiranda vienų asmenų priklausomybė nuo kitų. Vertinant santykį duomenų apsaugos apimtyje, tai santykis tarp fizinio asmens ir fizinio ar juridinio vieneto, atsirandantis ryšium su duomenų tvarkymo veiksmais. Fizinis asmuo, kurio duomenys yra tvarkomi, duomenų apsaugos teisėje tapatinamas su duomenų subjektu – tai asmuo, kuris gali būti tiesiogiai ar netiesiogiai identifikuojamas, pasinaudojant jam priklausančiais asmens duomenimis, tokiais kaip, vardas, pavardė, identifikavimo numeris, buvimo vieta, fizinės, fiziologinės savybės ir kt., ši sąvoka išplaukia iš BDAR 4 str., nurodomos asmens duomenų apibrėžties. Duomenų subjektu gali būti bet kuris asmuo, kurio asmens duomenų tvarkymą atlieka duomenų valdytojas, tai tiek patys organizacijos darbuotojai, tiek klientai, pacientai, interesantai ar asmenys patekę į vaizdo stebėjimo zoną. Tuo tarpu, vertinant fizinio ar juridinio subjekto, atliekančio duomenų tvarkymo veiksmus, vietą duomenų apsaugos teisėje, jis identifikuojamas kaip duomenų valdytojas ir tokiam subjektui reglamentas pateikia konkrečią apibrėžtį, remiantis asmens duomenų apsaugos teisės aktais duomenų valdytoju laikomas: „*fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, vienas ar su kitais, nustatantys duomenų tvarkymo tikslus ir priemones*“. Tokią apibrėžtį pateikia tiek BDAR 4 str., tiek Konvencijos Nr. 108 2 str. Papildomai Konvencijoje Nr. 108 pažymima, jog duomenų valdytojas yra kompetentingas priimti sprendimus, susijusius su duomenų saugojimo klausimais[17], ši nuostata leidžia konkretizuoti duomenų valdytojo kompetencijos apimtį.

Duomenų valdytoju laikoma visa organizacija, niekaip neatskiriant nei jos vadovo, nei bet kurių darbuotojų, kurie darbo funkcijoms įgyvendinti atlieka duomenų tvarkymą. Šis aspektas itin reikšmingas priskiriant už duomenų tvarkymą tenkančią atsakomybę.

[15] VAIŠVILA, Alfonsas. Teisės teorija: vadovėlis. Vilnius: Justitia, 2000, p. 27
[16] *ibidem.*
[17] Europos duomenų apsaugos vadovas. 2014 m. p. 49 [interaktyvu. Žiūrėta 2020 m. vasario 29 d.]. Prieiga per internetą: <https://www.echr.coe.int/Documents/Handbook_data_protection_LIT.pdf>.

Remiantis asmens duomenų apsaugos teise duomenų valdytojui tenka visa atsakomybė už tinkamą nustatytų reikalavimų įgyvendinimą. Jam yra taikomas BDAR 5 str., 2 d., atskaitomybės principas, ir tik jis pats atsakingas už tai, kad būtų laikomasi reikalavimų bei už įrodymus, kuriuos turėtų pateikti siekiant pagrįsti, kad jų realiai laikomasi[18]. Dr. J. Zaleskis savo monografijoje[19] atkreipia dėmesį į tai, kad: „*duomenų valdytoju pripažįstamas subjektas, kuris nustato duomenų tvarkymo tikslus ir priemones, bet nebūtinai pats atlieka faktinį duomenų tvarkymą*.“ Autoriaus nuomone, duomenų valdytojo statusas gali būti nulemtas teisės aktų pagrindu suteikta kompetencija atlikti duomenų tvarkymo veiksmus. Tokia nuomonė pateikiama ir 29 straipsnio darbo grupės, kuri teigia, jog[20]: „ *„Duomenų valdytojas“ yra praktinė sąvoka, kurios paskirtis – priskirti atsakomybę tam, kas turi tikrąją įtaką, taigi atsakomybė priskiriama remiantis ne formalių aspektų, o konkrečių faktų analize*.“. Šiai nuomonei antrina ES Teisingumo Teismo (toliau – Teisingumo Teismas) praktika. Darbo grupė teigia, kad svarbiausia yra nustatyti „subjektą priimantį sprendimus“ ir tai siūlo daryti tiek pagal faktines, tiek pagal teisines aplinkybes, kurios leistų nustatyti subjekto įtaką. Todėl tokį vertinimą siūlo daryti nagrinėjant tris kategorijas.

Pirmoji kategorija būtų „*duomenų valdymas pagal aiškią teisinę kompetenciją“* – tai atvejai, kuomet norminiais aktais yra aiškiai nustatomas duomenų valdytojas, tai gali būti ir valstybės institucijos, atsakingos už duomenų tvarkymą, tačiau tokie konkretizuoti atvejai yra pakankamai reti, todėl esminga atlikti kitų duomenų valdytojo įsipareigojimų priskyrimo kategorijų analizę.

Antroji kategorija pagal 29 straipsnio darbo grupę yra *„numanoma duomenų valdytojo kompetencija“* – į šią kategoriją priskirtini atvejai, kuomet teisinio pagrindo tiesiogiai nurodančio organizacijos kaip duomenų valdytojo pritaikyti negalima būtų, tačiau šis statusas savaime įgyjamas pagal įvairių sričių teisinę praktiką, pvz.: darbdavys tampa darbuotojų duomenų valdytoju. Taigi šiuo aspektu, duomenų valdytojo statusas priklauso tik nuo organizacijos praktinės veiklos vykdymo, kas savaime suponuoja ir atsakomybės taikymą.

Trečioji analizuotina kategorija – „*duomenų valdymas turint tikrąją galią*“. Ši kategorija leidžia paskirstyti atsakomybę sudėtingomis aplinkybėmis, kuomet duomenų tvarkymas

---

[18] ZALESKIS, Julius. *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: Registrų centras, 2019, p. 99.

[19] *ibidem*

[20] ES 29 str. darbo grupės 2010 m. vasario 16 d. *Nuomonė Nr. 1/2010 dėl sąvokų „duomenų valdytojas“ ir „duomenų tvarkytojas“* Nr. WP169, p. 9 [interaktyvus. Žiūrėta 2020 m. vasario 27 d.]. Prieiga per internetą: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_lt.pdf>.

atliekamas kelių šalių sutartinių santykių pagrindu. Sutarties sąlygos negali būti visais atvejais lemiamas veiksnys, itin lemiamas momentas gali būti tai, jog subjektas priima sprendimus dėl duomenų tvarkymo. Tokiu atveju, jis turi tikrąją galią, jis laikytinas duomenų valdytoju bei jam tenka atsakomybė susijusi su duomenų tvarkymu. Tam, kad nebūtų kliudoma efektyviai taikyti asmens duomenų apsaugos teisę, turi būti labai konkrečiai nustatomas duomenų valdytojas, kadangi su šiuo subjektu tiesiogiai siejama atsakomybė atsirandanti dėl duomenų tvarkymo.

Pirmos dvi kategorijos leidžia nustatyti duomenų valdytojo statusą patikimiau nei trečioji kategorija, kuriai reikalinga išsamesnė aplinkybių ir faktų analizė, kadangi reikšminga bus tik tikroji subjekto įtaka duomenų tvarkymo procesams. Šią nuostatą patvirtina Teisingumo Teismo praktika[21], teismas pažymi, kad fizinis ar juridinis asmuo, kuris siekdamas savo tikslų daro įtaką asmens duomenų tvarkymui ir dėl to nustato duomenų tvarkymo tikslus ir būdus, gali būti laikomas duomenų valdytoju. Tokią poziciją palaiko 29 straipsnio darbo grupė, jos nuomone, bendrąja prasme duomenų valdytoju *a priori* negali būti laikomas subjektas, kuris neturi nei teisėtos, nei tikrosios įtakos asmens duomenų tvarkymo procesams[22]. Šie išaiškinimai reikšmingi tiek senosios Direktyvos 95/46/EB, tiek naujojo BDAR kontekste. BDAR, kaip naujasis asmens duomenų apsaugos teisės pagrindas orientuotas į duomenų apsaugos standartų įdiegimą į kiekvieną organizaciją. Ir vienos efektyviausių priemonių siekiant užtikrinti, jog atitinkamų veiksmų bus imtasi yra atsakomybė ir sankcijos. Būtent todėl, atskaitomybės principas viena duomenų valdytojų padėtį iš esmės pakeitusių naujovių. Ši naujovė išplečia duomenų valdytojų atsakomybės ribas, šiems užtikrinant tinkamą duomenų apsaugos teisės reikalavimų integravimą į organizacijos kasdienį darbą. Atskaitomybės principas įtvirtina ne tik duomenų apsaugos reikalavimų laikymąsi, tačiau ir įrodymus, kurie patvirtintų reikalavimų tinkamo įgyvendinimo faktą.

Vertinant atsakomybės ribas, atkreiptinas dėmesys į duomenų valdytojo apibrėžtyje esantį žodžių junginį „*vienas ar drauge su kitais*“ tai svarbus momentas, nustatantis atvejus, kuomet duomenų valdytojo atsakomybė nėra vienareikšmiškai aiški. Tai atvejai, kuomet duomenų tvarkymą vykdo keli fiziniai ar juridiniai asmenys reglamente vadinami bendrais duomenų valdytojais. Šie atvejai priklauso nuo veiklos rūšių, kurioms reikalinga vykdyti duomenų tvarkymą. BDAR 26 str., numato šios kategorijos ypatybes – tai du ar daugiau

[21] Europos Sąjungos Teisingumo Teismo 2018 m. liepos 10 d. sprendimas byloje C-25/17 *Jehovan todistajat*, EU:C:2018:551, 68 parag. [interaktyvu. Žiūrėta 2020 m. balandžio 6 d.]. Prieiga per internetą: < http://curia.europa.eu/juris/document/document.jsf?text=&docid=203822&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=4876877>.
[22] *ibidem* p. 9 – 11.

duomenų valdytojų, kartu nustatantys duomenų tvarkymo tikslus ir priemones. Tačiau šiuo aspektu nereikėtų apsigauti, tai jog pagal apibrėžimą šalys kartu nusprendžia duomenų tvarkymo sąlygas, jokiu būdu nereiškia, jog valdytojai yra lygiaverčiai. Taip pat neturėtų būti painiojami atvejai, kuomet vykdomas paprastas, atitinkamu pagrindu pagrįstas duomenų judėjimas, vykdant bendradarbiavimą – tai gali būti santykiai su duomenų tvarkytoju, su duomenų gavėju ar atskiru duomenų valdytoju. Šiuo atveju reikšmingas aspektas yra bendro tikslo turėjimas ir nustatymas priemonių, kuriomis siekiamas bendras tikslas. Būtent dėl to siekiant sureguliuoti bendradarbiavimą ir įtraukti aiškumą bendri valdytojai sudaro tarpusavio susitarimą, kuriame nustatomos atsakomybės ribos, funkcijos, santykiai su duomenų subjektais, pagrindinis informacijos teikimo punktas. Reglamentas nereikalauja turėti sutarties, tačiau numato, jog turi būti sudarytas skaidrus susitarimas.[23] Nepaisant daugelio dalykų, kurie aptariami šiame susitarime, vis dėl to, pagrindinis dalykas yra atsakomybės pasidalinimas, tai reikšmingas klausimas veikiant vienam valdytojui, ir jo reikšmė išauga, kai valdytojų yra keli, todėl sprendžiant šiuos klausimus, aptariami subjektai turi vadovautis išimtinai skaidrumo principu. Turi būti priimti sprendimai tiek prievolių vykdymo aspektu, tiek dėl pareigos teikti pilnos apimties informaciją duomenų subjektui, tiek įgyvendinti duomenų subjektų teises pagal reglamentą. Tačiau pažymėtina tai, kad duomenų subjektas, remiantis BDAR 26 str., 3 d., gali kreiptis į bet kurį jam žinomą duomenų valdytoją. Vienintelė galima išimtis, kuomet susitarimas dėl atsakomybės nėra reikalingas ar galintis ką nors pakeisti, remiantis BDAR 26 str., 1 d., yra kuomet atsakomybė jau yra nustatyta tiek Sąjungos, tiek nacionaliniais teisės aktais. Visais kitais atvejais atsakomybės klausimai turi būti sprendžiami pirmiausia, siekiant išvengti neaiškumų, kadangi valdytojas atsako pilna apimtimi už bet kokius pažeidimus, o duomenų subjektas pirmiausiai kreipsis į jam artimą duomenų valdytoją. Vertindamas bendros atsakomybės aspektą Teisingumo Teismas pažymi[24], kad bendros atsakomybės buvimas nebūtinai reiškia, kad įvairių su asmens duomenų tvarkymu susijusių ūkio subjektų atsakomybė yra lygiavertė. Teismo teigimu, situacija turėtų būti vertinama priešingai, šie subjektai gali dalyvauti tvarkant duomenis skirtinguose etapuose ir skirtingu mastu, todėl kiekvieno jų atsakomybės lygis turi būti įvertintas atsižvelgiant į visas reikšmingas konkretaus atvejo aplinkybes.

---

[23] Europos Sąjungos Teisingumo Teismo 2018 m. birželio 5 d. sprendimas byloje C-210/*16 Wirtschaftsakademie Schleswig-Holstein*, EU:C:2018:388, 43 pastr. [interaktyvus. Žiūrėta kovo 15 d.]. Prieiga per internetą: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=4877022>.

Duomenų valdytoju laikomas fizinis ar juridinis asmuo, kuris turi galios nustatyti duomenų tvarkymo tikslus ir priemones, kuriomis tų tikslų bus siekiama. Duomenų valdytojas yra reikšminga duomenų apsaugos teisės figūra, kadangi jis sudaro terpę, duomenų apsaugos reguliavimui veikti, jam keliami reikalavimai duomenų apsaugos normų atitikties įgyvendinimui bei jam taikoma pilnos apimties atsakomybė, vertinant atliekamą duomenų tvarkymą.

1.2. Duomenų valdytojo pareiga įgyvendinti duomenų apsaugos principus

Duomenų subjektų duomenų tvarkymo veiksmai įprastai atneša duomenų valdytojui pelną. Dažnu atveju, jei subjektas kvalifikuojamas, kaip duomenų valdytojas, tuomet vertinami verslo santykiai. Pavyzdžiui viešbutis – negalėdamas tvarkyti klientų asmens duomenų, jis negalės tinkamai vykdyti savo veiklos, atitinkamai nebus gaunamas joks pelnas. Todėl šiame santykyje duomenų subjektas yra silpnesnioji šalis ir siekiant išlaikyti balansą duomenų valdytojui kyla atitinkamos pareigos duomenų subjektų atžvilgiu, kurias būtina vykdyti. Pagrindinis tikslas yra užtikrinti atitiktį asmens duomenų apsaugos teisės aktų reikalavimams. Kadangi pagrindinės normos yra labai abstraktaus pobūdžio ir paliekama duomenų valdytojo interpretacijai, pagrindiniai bet kurios teisinės sistemos pamatai, kuriais turi būti vadovaujamasi tai teisės principai.

Visų pirma, duomenų valdytojui kyla pareiga užtikrinti tinkamą asmens duomenų tvarkymo principų turinio įgyvendinimą. Šaltiniai, kuriuose šie principai numatomi yra Konvencija Nr. 108 ir BDAR. BDAR 5 str., principai formuluojami platesne apimtimi bei šiek tiek papildomi. Remiantis šia norma, asmens duomenys turi būti tvarkomi remiantis teisėtumo, sąžiningumo ir skaidrumo, tikslo apribojimo, duomenų kiekio mažinimo, tikslumo, saugojimo trukmės apribojimo, vientisumo ir konfidencialumo bei atskaitomybės principais.

Teisėtumo, sąžiningumo ir skaidrumo principų turinys jungiamas į vieną bendrą reiškiantį, jog duomenų valdytojui taikoma pareiga duomenų subjekto duomenis tvarkyti remiantis teisėtais pagrindais, sąžiningai bei skaidriai, nors kiekvienas iš jų atskirai turi labai didelę svarbą. Teisėtumo principas – neturi jokios kitos prasmės, jis vienareikšmiškai nustato, jog duomenys turi būti tvarkomi griežtai teisėtais duomenų tvarkymo pagrindais ir būdais. Šis principas reiškia, jog turi būti laikomasi teisės aktais nustatytų reikalavimų, kad duomenų tvarkymas būtų teisėtas. Sąžiningumas suponuoja tai, jog duomenų valdytojo veiksmai turėtų būti vertinami per vertybių prizmę. Bendrais bruožais, šio principo turinys pasižymi atidumu, rūpestingumu bei draudimu piktnaudžiauti teise, tik veikiantis

rūpestingai ir teisingai asmuo, gali būti laikomas iš tikrųjų sąžiningu[25]. Duomenų valdytojo pareiga vadovautis sąžiningumo principu atliekant bet kokius duomenų tvarkymo veiksmus tiek santykyje su kitais duomenų valdytojais, tiek santykyje su duomenų subjektu, tiek santykyje su Valstybine duomenų apsaugos inspekcija[26]. Nuo šio principo neatsiejamu laikytinas skaidrumo principas. Tai, jog vykdomas duomenų tvarkymo procesas, nereiškia, jog nutrūksta ryšys tarp duomenų subjekto ir jo asmens duomenų, priešingai, duomenų subjektas išlaiko interesą žinoti kam, kiek ir kokiu būdu tvarkomi jo duomenys ir valdyti duomenų sklaidą[27]. Duomenų valdytojo pareiga laikytis skaidrumo principo, leidžia duomenų subjektams kontroliuoti savo asmens duomenis ir užtikrinti veiksmingą duomenų apsaugą[28].

Tikslo apribojimo principas įpareigoja duomenų valdytoją duomenis tvarkyti tik konkrečiais nustatytais tikslais ir netvarkyti gautų duomenų subjekto duomenų kitiems tikslams, apie kuriuos duomenų subjektas nėra informuotas ir su kurių tvarkymo sąlygomis nėra supažindintas. Pagrindinė duomenų valdytojo užduotis – nustatyti duomenų tvarkymo ribas ir jų neperžengti, taip užtikrinant duomenų subjektų apsaugą[29]. Lietuvos vyriausiojo administracinio teismo praktikoje[30] išskiriama situacija, kai asmuo nesilaikydamas tikslo apribojimo principo pripažintas kaltu padaręs Lietuvos Respublikos administracinių teisės pažeidimų kodekso 214^{14} str., 1 d., numatytą pažeidimą ir jam skirta piniginė bauda. Tai labai svarbus principas, nes pirmiausia nustatomas tikslas, dėl kurio yra būtina tvarkyti asmens duomenis ir siekiant to tikslo įgyvendinimo vyksta sekantys duomenų tvarkymo procesai.

Duomenų kiekio mažinimo principas apriboja duomenų valdytoją, nurodant, jog jam tenka pareiga tvarkyti griežtai tik tokius duomenis, kurie yra būtini nustatytiems tikslams pasiekti, kitaip tariant turi būti vengiama tvarkyti papildomus duomenis, be kurių duomenų valdytojas gali išsiversti. Šį principą galima būtų iliustruoti pavyzdžiu, kuomet tiesioginės rinkodaros vykdymui yra būtina pateikti tik elektroninio pašto adresą, kitaip nėra galimybės teikti asmeniui rinkodaros pasiūlymų, o duomenų valdytojas nusprendžia privalomai rinkti elektroninio pašto adresą, asmens vardą, pavardę ir gyvenamąjį adresą, teigdamas, jog šių

---

[25] PETRAITYTĖ, Ilona. *Asmens duomenų teisinės apsaugos principai: daktaro disertacija*. Socialiniai mokslai, teisė (01S). Vilnius: Vilniaus universitetas, 2013, p. 109. [interaktyvus. Žiūrėta kovo 2 d.]. Prieiga per internetą: <https://aleph.library.lt/F?func=findb&request=000074137&find_code=SYS&local_base=LITLI>.
[26] *ibidem*, p. 112.
[27] *ibidem*, p. 130.
[28] *ibidem*, p. 132.
[29] ZALESKIS, Julius. *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: Registrų centras, 2019, p.117.
[30] Lietuvos vyriausiojo administracinio teismo 2011 m. balandžio 15 d., nutarimas byloje Nr. N62-939/2011.[interaktyvus. Žiūrėta kovo 2 d.]. Prieiga per internetą: < https://eteismai.lt/byla/97187080245856/N-62-939-11>.

duomenų jam gali prireikti ateityje, šiuo atveju tai būtų duomenų kiekio mažinimo principo pažeidimas, kadangi tiesioginės rinkodaros vykdymui yra pakankama tvarkyti tik asmens elektroninio pašto adresą į kurį jis gaus jam adresuotus pasiūlymus. Šis principas gali būti tinkamai užtikrinamas tik tuo atveju, jeigu bus palaikomas tinkamas santykis tarp duomenų tvarkymo tikslų ir duomenų apimties[31].

Ketvirtasis yra *tikslumo* principas, remiantis šiuo principu, duomenų valdytojas įpareigojamas tvarkyti visuomet tik tikslius ir atnaujintus duomenų subjekto asmens duomenis. Jeigu duomenų valdytojas turi šio principo turinio neatitinkančius duomenis, jie nedelsiant privalo būti ištrinami arba ištaisomi. Šis principas iš visų išsiskiria tuo, jog duomenų valdytojas savarankiškai negali jo įgyvendinti pilna apimtimi. Reikšmingas yra pačių duomenų subjektų atsakingumas ir sąmoningumas. Su šiuo principu taip pat susijęs *saugojimo trukmės apribojimo* principas – duomenys turi būti laikomi tik tiek, kiek tai yra būtina siekiant nustatyti asmens tapatybę, remiantis duomenų tvarkymo tikslais. Galimi atvejai, kuomet duomenų saugojimo trukmė yra numatyta nacionalinės teisės normomis, tuomet turi būti remiamasi nustatytais terminais, tačiau taip pat ne reti atvejai, kuomet duomenų saugojimo terminai nėra nustatyti jokiomis normomis ir tuo atveju duomenų saugojimo terminų nustatymas tenka duomenų valdytojui, kuris atsižvelgiant į duomenų tvarkymo tikslus vidaus tvarkomis nustato duomenų saugojimo terminą. Šiais atvejais nustatyti terminai turi būti proporcingi duomenų tvarkymo tikslams ir negali būti saugomi ilgiau nei būtina tikslams pasiekti. Pats BDAR jokio saugojimo termino nenumato bei nepateikia konkrečių išaiškinimu, kas yra tinkamai nustatyti terminai, tačiau preambulėje numato, jog terminai turi būti tikrai labai minimalūs.

Vientisumo ir konfidencialumo principas, sąlygoja aplinkybes, kai duomenų valdytojas turi imtis atitinkamų priemonių siekiant užtikrinti tinkamo lygio asmens duomenų saugumą, įskaitant atvejus, kai duomenys tvarkomi neturint tam leidimo, ar duomenys prarandami ar sunaikinami. Šis principas labiausiai skirtinas techninėmis priemonėmis vykdomam duomenų tvarkymui, kadangi šiuo atveju reikalinga užtikrinti tinkamo techninių galimybių išsivystymo lygio apsaugą.

Paskutinysis principas numatomas BDAR 5 str., 2 d., ir tai yra svarbiausias principas, kurio turinys pajungia visus šio straipsnio 1 dalyje nurodytus principus – *atskaitomybės* principas. 29 straipsnio darbo grupė pažymi, kad iš esmės atskaitomybė yra tiesioginė duomenų valdytojo pareiga nustatyti priemones, kurios užtikrins atitiktį duomenų apsaugos

[31] ZALESKIS, Julius. *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: Registrų centras, 2019, p. 121.

taisyklėms ir turėti parengtus dokumentus, kurie būtų tiesioginiai įrodymai, jog imtasi tinkamų priemonių atitikties užtikrinimui[32].

Atskaitomybės principas, suponuoja duomenų valdytojo atsakomybę už bet kokį jo arba jo vardu atliekamą duomenų tvarkymą[33]. Remiantis šiuo principu duomenų valdytojas yra pilnai atsakingas už visų principų įgyvendinimą bei įrodymus, kurie patvirtintų, jog principų iš tiesų yra tinkamai laikomasi ir visi duomenų tvarkymo procesai remiasi BDAR 5 str., 1 d., turiniu. Aptariamo principo turinys yra labai platus, jis apima bet kokias duomenų valdytojo pareigas ar įsipareigojimus pagal asmens duomenų apsaugos reguliavimą.

Tačiau duomenų tvarkymo principų įgyvendinimu duomenų valdytojo pareigos nėra apribojamos, taip pat jam tenka pareiga užtikrinti, jog duomenų tvarkymas būtų vykdomas teisėtai. Tam, kad duomenų tvarkymas būtų laikomas teisėtu, jis turi atitikti vieną iš BDAR 6 str., 1 d., nurodomų duomenų tvarkymo pagrindų.

Pirmasis duomenų tvarkymo pagrindas – *sutikimas (BDAR 6 str., 1d., a) p.).* Pagal BDAR 4 str., 1d., 11 p., pateikiamą apibrėžtį, sutikimas, tai: „bet koks laisva valia duotas, konkretus ir nedviprasmiškas tinkamai informuoto duomenų subjekto valios išreiškimas pareiškimu arba vienareikšmiais veiksmais kuriais jis sutinka, kad būtų tvarkomi su juo susiję asmens duomenys“. Šį pagrindą detalizuoja taip pat BDAR 7 str., ir nacionalinės teisės normos – LR Elektroninių ryšių įstatymas, nurodant sutikimo gavimo sąlygas. Pagrindinės teisėto sutikimo sudedamosios dalys yra duomenų valdytojo suteikiama informacija apie asmens duomenų tvarkymo tikslus, apimtis, būdus, duomenų subjekto valia, laisvė pasirinkti be spaudimo, neigiamų pasekmių netaikymas. Sutikimas turi būti išreikštas tokia forma, kad vėliau būtų galima įrodyti laisvą subjekto valią ir galimybę gauti visą su duomenų tvarkymu susijusią informaciją sutikimo davimo momentu. Teisingumo Teismas savo praktikoje[34] atkreipia dėmesį, kad sutikimas turi būti išreikštas aktyviais veiksmais ir susijęs būtent su atitinkamu duomenų tvarkymu, o taip pat atkreipia dėmesį į BDAR nuostatas, kuriose numatoma, kad teisėtu sutikimu nelaikoma tyla ar iš anksto sužymėti laukeliai. Šis duomenų tvarkymo pagrindas gali būti gana keblus atvejais, kai duomenų subjektas yra darbuotojas. Šiuo atveju, dėl galios disbalanso, sudėtinga užtikrinti

[32] Europos duomenų apsaugos vadovas. 2014 m. p. 77 [interaktyvu. Žiūrėta 2020 m. kovo 30 d.]. Prieiga per internetą: <https://www.echr.coe.int/Documents/Handbook_data_protection_LIT.pdf>.
[33] ZALESKIS, Julius. *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė.* Vilnius: Registrų centras, 2019, p.135
[34] Europos Sąjungos Teisingumo Teismas. 2019 m. spalio 1 d. sprendimas *Planet49 GmbH* C-673/17, EU:C:2019:801 [interaktyvus. Žiūrėta 2020 m. kovo 5 d.]. Prieiga per internetą: <http://curia.europa.eu/juris/document/document.jsf;jsessionid=B542D71188C4C1DA290A6EE2BAA843F3?text=&docid=218462&pageIndex=0&doclang=LT&mode=req&dir=&occ=first&part=1&cid=1821361>.

laisvos valios išraišką, nes įprastai darbuotojas silpnesnioji darbo santykių šalis, dėl ko sutinka su bet kokiais darbdavio pasiūlymais. Siekiant gauti sutikimą iš darbuotojo darbdavys turi pareigą sudaryti sąlygas asmeniui suprasti, jog jis turi galimybę rinktis ir jo sprendimas neturės jokios neigiamos įtakos tolesniems darbo santykiams. Sutikimo pagrindas taip pat laikytinas nepatikimu dėl dar vienos priežasties, duomenų subjektas turi teisę, remiantis BDAR 7 str., 3 d., bet kuriuo metu atšaukti duotą sutikimą ir duomenų valdytojas turi pareigą įgyvendinti šią subjekto teisę bei nutraukti duomenų tvarkymo veiksmus.

Antrasis duomenų tvarkymo teisinis pagrindas – *sutartis (BDAR 6 str., 1d., b) p.)*. Šis pagrindas leidžia tvarkyti duomenis siekiant sudaryti sutartį bei siekiant toliau ją vykdyti. Duomenys yra tvarkomi sutarties, kurią duomenų valdytojas pasirašė su duomenų subjektu pagrindu. Tačiau kaip galime matyti iš Lietuvos vyriausiojo administracinio teismo praktikos[35], nepaisant to, kad sudaroma sutartis, kurioje įtvirtinamas šalių susitarimas apimantis asmens duomenų tvarkymą, jos nuostatos negali prieštarauti teisės aktų nustatytoms asmens duomenų tvarkymo taisyklėms.

Trečiasis duomenų tvarkymo pagrindas – *teisinė prievolė (BDAR 6 str., 1d., c) p.)*. Tai atvejai, kuomet duomenų subjekto duomenų tvarkymas duomenų valdytojui yra privalomas nacionalinės teisės normų pagrindu. Šis duomenų tvarkymo pagrindas yra teigiamas tuo, jog yra imperatyvus ir apibrėžtas, nėra vietos subjektyviai interpretacijai, o taip pat įprastai teisine prievole grįstas duomenų tvarkymas, turi teisine norma įtvirtintą saugojimo terminą, kas palengvina duomenų valdytojo veiklą bei atsakomybę, kadangi jam telieka laikytis nustatytų terminų.

Be abejonės įvertinama ir tai, jog tam tikrais itin skubiais atvejais, laikytis formalumų yra itin sudėtinga ar net neįmanoma, tokiu atveju galėtų būti naudojamasi duomenų tvarkymo pagrindu, kuris leidžia *tvarkyti duomenis siekiant apsaugoti gyvybinius duomenų subjekto ar kito fizinio asmens interesus (BDAR 6 str., 1d., d) p.)*. Remiantis BDAR preambulės 46 punktu šis duomenų tvarkymo pagrindas galimas tik tais atvejais, kai akivaizdžiai negali būti taikomas joks kitas teisinis pagrindas. Svarbus momentas yra tai, jog šis pagrindas taip pat turi būti remiamas duomenų tvarkymo principais ir jeigu vis dėl to gyvybiniai interesai gali būti apsaugoti netvarkant jokių fizinio asmens duomenų, tokiu atveju šio pagrindo, kaip ir bet kurio kito, taikymas nebūtų laikomas pagrįstu[36].

---

[35] Lietuvos vyriausiojo administracinio teismo 2013 m. gegužės 23 d. nutartis byloje Nr. A822-1173-13 UAB „Init“ prieš Valstybinę duomenų apsaugos inspekciją. [interaktyvus. Žiūrėta kovo 5 d.]. Prieiga per internetą: < https://eteismai.lt/byla/245492016270101/A-822-1173-13?word=init>.

[36] ZALESKIS, Julius. *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: Registrų centras, 2019, p.155

Neįprastas ir sekantis duomenų tvarkymo pagrindas – *tvarkyti duomenis būtina siekiant atlikti užduotį, vykdomą viešojo intereso labui arba vykdant duomenų valdytojui pavestas viešosios valdžios funkcijas (BDAR 6 str., 1d., e) p.)*. Šio duomenų tvarkymo pagrindo nereikėtų painioti su teisine prievole. Tai atvejai, kai duomenų valdytojas yra oficialiai įpareigojamas ar veikia viešojo intereso labui[37].

Paskutinysis duomenų tvarkymo pagrindas – *teisėtas duomenų valdytojo arba trečiosios šalies interesas (BDAR 6 str., 1d., f) p.)*. Tai komplikuotas duomenų tvarkymo pagrindas turint omenyje duomenų valdytojo ir duomenų subjekto nelygiavertę padėtį, kadangi leidžia duomenų valdytojui tvarkyti subjekto asmens duomenis, jei jis turi įtikinamų teisėtų interesų vykdyti duomenų tvarkymo procesą neparemtą jokiu kitu teisiniu pagrindu. Tačiau, atliekant šio pagrindo analizę pirmiausia reikšminga paminėti, jog jis remiasi į pusiausvyros nustatymą. Duomenų valdytojas prieš atliekant duomenų tvarkymą šiuo pagrindu, privalo įvertinti ar duomenų subjekto teisės ir laisvės nėra viršesnės už jo deklaruojamą teisėtą interesą. Kadangi nėra pateikiamo jokio sąrašo ar aprašymo koks interesas gali būti laikomas pagrįstu, tik pusiausvyros kriterijaus gautas rezultatas lemia, ar gali būti taikomas teisėto intereso pagrindas, ar ne. Įprastai šiuo pagrindu grindžiamas duomenų tvarkymas atliekamas su subjektais, su kuriais jau yra sukurtas atitinkamas santykis, pvz.: duomenų subjektas yra darbuotojas[38]. Vertinimo metu svarbu ne tik įvertinti pusiausvyrą tarp duomenų subjekto teisių ir duomenų valdytojo interesų, bet ir atsižvelgti į jau sukurtus santykius bei įvertinti duomenų subjekto lūkesčius dėl jo asmens duomenų tvarkymo. Tikėtina, jog duomenų subjekto interesai ir pagrindinės teisės bus viršesnės už valdytojo interesą vien dėl to, kad duomenų subjektas nesitiki bet kokio tolesnio duomenų tvarkymo[39].

Asmens duomenų tvarkymo principų ir teisėtų duomenų tvarkymo pagrindų laikymasis yra pamatinės duomenų valdytojo pareigos, sąlygojančios atsakomybę, kadangi bet kurie tolesni duomenų tvarkymo veiksmai turi remtis nustatytais principais. Siekiant tinkamai įgyvendinti principų turinį duomenų valdytojas turi užtikrinti tinkamą kitų pareigų vykdymą.

1.3. Duomenų valdytojo pareiga paskirti duomenų apsaugos pareigūną

Ne visais atvejais duomenų valdytojas gali susitvarkyti su duomenų tvarkymo procesais be tinkamos specialisto pagalbos, todėl reglamentas numatė duomenų valdytojui pareigą

[37] *ibidem*, p.155
[38] *ibidem*. P.160
[39] BDAR preambulės 47 punktas

paskirti duomenų apsaugos pareigūną[40]. Jeigu apie pareigas užtikrinti asmens duomenų apsaugos principų įgyvendinimą bei teisiniais pagrindais grįsti duomenų tvarkymo procesus galima buvo rasti normų tiek Konvencijoje Nr. 108, tiek Direktyvoje 95/46/EB, tai duomenų apsaugos pareigūno paskyrimo pareiga BDAR yra visiškai nauja norma. Duomenų apsaugos paskyrimą reglamentuoja BDAR 37 str., kuris numato imperatyvius atvejus, kuomet duomenų apsaugos pareigūnas privalo būti paskirtas. Privalomų sąlygų sąrašas suponuoja tai, jog daliai duomenų valdytojų, neatitinkančių nurodytų aplinkybių, ši pareiga nėra aktuali. Tam, kad suprasti ar ši pareiga duomenų valdytojui taikoma, pirmiausia jis turi atlikti išsamią vidinių duomenų tvarkymo procesų analizę, kurios rezultatai leis pasitikrinti ar duomenų valdytojo vykdoma duomenų tvarkymo veikla atitinka bent vieną iš BDAR 37 str., nurodomų aplinkybių, kurių yra tik trys.

Visų pirma duomenų apsaugos pareigūnas paskiriamas, jei duomenų valdytojas yra *valdžios institucija ar įstaiga, išskyrus teismus, kai jie vykdo savo teismines funkcijas* (*BDAR 37 str., 1 d., a) p.).* Šiuo atveju, jeigu duomenų valdytojas veikia kaip viešojo sektoriaus atstovas, plačios analizės atlikti jam nereikės, pakanka įvertinti veiklos pobūdį. Sąvokas atskleisti padeda nacionalinė teisė – Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo 2 str., 2d., kurioje detalizuojama valdžios institucijų ir įstaigų apibrėžtis, nurodant, kad tai: „valstybės ir savivaldybių institucijos ir įstaigos, įmonės ir viešosios įstaigos, finansuojamos iš valstybės ar savivaldybių biudžetų bei valstybės pinigų fondų ir Lietuvos Respublikos viešojo administravimo įstatymo nustatyta tvarka įgaliotos atlikti viešąjį administravimą arba teikiančios asmenims viešąsias ar administracines paslaugas ar vykdančios kitas viešąsias funkcijas“. Remiantis pateikiamu apibrėžimu duomenų valdytojui lengviau identifikuoti savo priskyrimą šiai kategorijai.

Antras atvejis, kuomet būtina paskirti duomenų apsaugos pareigūną yra, kai *pagrindinė veikla yra duomenų tvarkymo operacijos, dėl kurių pobūdžio, aprėpties ir (arba) tikslų būtina reguliariai ir sistemingai dideliu mastu stebėti duomenų subjektus* (*BDAR 37 str., 1 d., b) p.*). Reglamentas nedetalizuoja normų ar papildomų sąvokų, todėl siekiant tinkamai atskleisti normos prasmę, turi būti žvelgiama į atskiras jos sudedamąsias dalis. Pirmiausiai tai „pagrindinė veikla“ – tai svarbiausios operacijos duomenų tvarkytojo tikslams pasiekti, sudarančios neatskiriamą vykdomos veiklos dalį.[41] Tai reiškia, kad be duomenų tvarkymo duomenų valdytojas negalėtų vykdyti savo veiklos ar teikti atitinkamų paslaugų. Sekanti svarbi normos dalis, tai „reguliariai ir sistemingai“ – 29 straipsnio darbo grupės vertinimu,

[40] BDAR 37 straipsnis

[41] ES 29 str. darbo grupės 2017 m. balandžio 5 d. *Duomenų apsaugos pareigūnų gairės* Nr. WP 243, p. 23 [interaktyvus. Žiūrėta kovo 10 d.]. Prieiga per internetą: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048>.

„reguliarus“, tai vykstantis tam tikrais intervalais ir (ar) pasikartojantis[42]. Tuo tarpu „sistemingas“, tai vykdomas kaip plano dalis, iš anksto suplanuotas ir ar vykstantis pagal tam tikrą sistemą[43]. Trečioji sudedamoji normos dalis – „dideliu mastu“. Šis matas nustatomas tik įvertinus duomenų subjektų skaičių, tvarkomų duomenų kiekį bei geografinę veiklos aprėptį[44]. Svarbu suprasti, kokią dalį atitinkamos rinkos, kurioje veikiama apima duomenų valdytojo atliekamas duomenų tvarkymas, pvz.: pacientų duomenų tvarkymas respublikinio dydžio ligoninėje ir pacientų duomenų tvarkymas gydytojo odontologo privačiame kabinete. Pavyzdys puikiai iliustruoja masto skirtumą, ir būtent tokią visų aplinkybių analizę ir turėtų atlikti duomenų valdytojas.

Trečiasis atvejis, kuomet duomenų valdytojui kyla pareiga paskirti duomenų apsaugos pareigūną yra tuomet, kai – *duomenų valdytojo pagrindinė veikla yra specialiųjų kategorijų asmens duomenų tvarkymas dideliu mastu ir asmens duomenų apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas tvarkymas dideliu mastu (BDAR 37 str., 1 d., c) p.*). Šiuo atveju, kaip ir prieš tai vertintuoju, visų pirma duomenų valdytojas turi įvertinti duomenų tvarkymo apimtis, tačiau jau ne bendrąja prasme, o būtent tvarkant specialiuosius duomenis[45] arba duomenis apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas[46]. Remiantis paties BDAR preambulės 91 punktu, tai toks duomenų tvarkymas, kuris dėl didelio kiekio ir duomenų jautrumo gali kelti pavojų duomenų subjektams, kurie patenka į šias operacijas.

Atlikus tinkamą analizę ir įvertinus atitiktį pateikiamiems kriterijams galima nustatyti poreikį paskirti duomenų apsaugos pareigūną, kuris pagal ekspertų vertinimą laikytinas centrine duomenų apsaugos teisės reguliavimo dalimi. Duomenų valdytojui ne tik privalomais atvejais, bet ir savanoriškai labai naudinga paskirti duomenų apsaugos pareigūną. Duomenų apsaugos pareigūnas turi tinkamą kompetenciją, leisiančią jam atskleisti reikalavimų duomenų valdytojui turinį ir užtikrinti tinkamą jų įgyvendinimą.

[42] *ibidem*, p.24
[43] *ibidem*, p. 25
[44] *ibidem*, p. 24
[45] Pagal BDAR 9 str., 1 d.: „Draudžiama tvarkyti asmens duomenis, atskleidžiančius rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus ar narystę profesinėse sąjungose, taip pat tvarkyti genetinius duomenis, biometrinius duomenis, siekiant konkrečiai nustatyti fizinio asmens tapatybę, sveikatos duomenis arba duomenis apie fizinio asmens lytinį gyvenimą ir lytinę orientaciją.“
[46] Pagal BDAR 10 str.: „ Asmens duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas arba susijusias saugumo priemones remiantis 6 straipsnio 1 dalimi tvarkomi tik prižiūrint valdžios institucijai arba kai duomenų tvarkymas leidžiamas Sąjungos arba valstybės narės teise, kurioje nustatytos tinkamos duomenų subjektų teisių ir laisvių apsaugos priemonės. Bet kuris išsamus apkaltinamųjų nuosprendžių duomenų registras tvarkomas tik prižiūrint valdžios institucijai.

1.4. Kitos duomenų valdytojui taikomos pareigos

Be jau minėtų pareigų duomenų valdytojas, kaip pilnai atsakingas už atitiktį duomenų apsaugos teisei, turi pareigą atlikti visus veiksmus, kurie turi būti atlikti siekiant atitikties duomenų apaugos reglamentavimui yra duomenų valdytojo pareigos. Taip yra dėl to, jog būtent duomenų valdytojas atsakingas už bet kokios rizikos minimizavimą. Todėl jis turi pasirūpinti tinkamomis techninėmis ir organizacinėmis saugumo priemonėmis[47], kurios leis užtikrinti tiek techninį, tiek fizinį tvarkomų duomenų nepasiekiamumą ir apsaugą. Techninės ir organizacinės priemonės turi būti parenkamos įvertinus galimas rizikas ir pavojus duomenų subjektų teisėms ir laisvėms, atsižvelgiant į tvarkomų duomenų pobūdį, apimtis, tikslus ir būdus.

Duomenų valdytojas turi užtikrinti, kad organizacijoje atliekami duomenų tvarkymo procesai būtų aprašyti veiklos įrašuose[48]. Ši pareiga duomenų valdytojui kyla iš atskaitomybės principo, kuriuo remiantis, duomenų valdytojas turi būti pasiruošęs bet kuriuo metu pateikti įrodymus, kad duomenų valdytojas laikosi duomenų apsaugos teisės jam keliamų reikalavimų ir veiklos įrašai yra vienas pagrindinių įrodymų. Šie įrašai apima detalią informaciją apie organizacijoje vykdomus duomenų tvarkymo procesus, duomenų judėjimo srautus, saugojimo terminus, naikinimo būdu bei kitą reikšmingą informaciją.

Be jau išnagrinėtų pareigų, taip pat duomenų valdytojas turi užtikrinti duomenų subjekto teisių, kurias jam suteikia BDAR III skyrius, įgyvendinimą pilna apimtimi. Duomenų apsaugos taisyklės veiksmingos ir efektyvios tik tuomet, kai jos yra veikiančios. Duomenų apsaugos teisės normų tikslas leisti duomenų subjektui valdyti savo duomenis bei duomenų valdytojui pasirūpinti jam patikėtų duomenų apsauga. Todėl duomenų subjektui turi būti sudarytos galimybės tinkamai ir laiku gauti norimą informaciją ar kitaip įgyvendinti jo interesus.

Ne mažiau reikšmingas, BDAR prie duomenų valdytojo pareigų taip pat priskirtinas reikalavimą, kad rūpestingas duomenų valdytojas atliktų poveikio duomenų apsaugai vertinimą[49], atvejais, kai dėl duomenų tvarkymo rūšies, būdo ar aprėpties subjekto teisėms ir laisvėms gali kilti didelis pavojus. Šiuo atveju duomenų valdytojas turi objektyviai įvertinti visų duomenų tvarkymo aplinkybių visumą, siekiant nustatyti galimo pavojaus lygį.

Prie duomenų valdytojui priskirtinų pareigų, yra ne tik tęstinės pareigos, kurios vykdomos visą duomenų tvarkymo laikotarpį, tačiau atsiranda ir trumpalaikių pareigų.

[47] BDAR 32 straipsnis
[48] BDAR 30 straipsnis
[49] BDAR 35 straipsnis

Įprastai tai atvejai, kuomet atsiranda duomenų saugumo pažeidimai. Šie vienkartiniai atvejai, sukuria duomenų valdytojui pagrindą vykdyti kitą pareigą – pranešti apie nustatytą pažeidimą. Ši pareiga nustatyta ne tik BDAR 33-34 str., bet taip pat Reglamente (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje (eIDAS reglamentas)[50], Direktyvoje (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (TIS direktyva)[51] ir Direktyvoje 2009/136/EB (direktyva dėl piliečių teisių) ir Reglamentas (ES) Nr. 611/2013 (Reglamentas dėl pranešimo apie pažeidimus)[52]. Visuose šiuose teisės aktuose numatyta pareiga pranešti priežiūros institucijai apie įvykusius duomenų saugumo incidentus.

Duomenų valdytojas yra asmens duomenų teisės subjektas, kuriam krenta didžiausia našta – įgyvendinti visus asmens duomenų apsaugos teisės reikalavimus. Be to, kad privalu pilna apimtimi užtikrinti duomenų tvarkymui keliamų reikalavimų įgyvendinimą, reikšminga taip pat pateikti įrodymus, jog duomenų tvarkymo taisyklių iš tiesų laikomasi. Duomenų valdytojui skiriamos pareigos atlikti poveikio duomenų apsaugai vertinimą, vesti veiklos įrašus ar pranešti apie pažeidimą yra priemonės leisiančios užtikrinti atskaitomybės principo įgyvendinimą, kadangi leis įrodyti, jog duomenų valdytojas užtikrina tinkamų duomenų apsaugos standartų laikymąsi.

[50] ES 29 str. darbo grupės 2018 m. vasario 6 d. *Gairės dėl pranešimo apie asmens duomenų saugumo pažeidimą pagal Reglamentą* (ES) 2016/679 Nr.WP250, p. 30 [interaktyvus. Žiūrėta 2020 m. kovo 10 d.]. Prieiga per internetą: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052>.
[51] *ibidem.*
[52] *ibidem.*

2. DUOMENŲ APSAUGOS PAREIGŪNO ATSAKOMYBĖ UŽ ATITIKTĮ ASMENS DUOMENŲ APSAUGOS REGULIAVIMUI

2.1. Duomenų apsaugos pareigūno samprata

Kaip ir minėta, viena svarbiausių ir „mistiškiausių“ BDAR naujovių yra imperatyviai nustatyta pareigybė – duomenų apsaugos pareigūnas. Pati sąvoka nėra laikytina nauja, kadangi dar Direktyvos 95/46/EB galiojimo laiku kelios valstybės laikui bėgant išplėtojo duomenų apsaugos pareigūno skyrimo praktiką[53]. Tuo tarpu, pačioje Direktyvoje 95/46/EB apie tai užuominų nebuvo, taip pat tai nėra reguliuojama jokiame kitame akte. 29 straipsnio darbo grupės nuomone, būtent duomenų apsaugos pareigūnas laikytinas naujos teisinės sistemos pagrindu, kadangi tai pagrindinis asmuo padėsiantis organizacijoms laikytis BDAR įtvirtintų reikalavimų.

Duomenų apsaugos pareigūnas skirtas pagalbai laikantis reikalavimų, siekiant įgyvendinti atskaitomybės principą bei parinkti tinkamas atitikties priemones, o taip pat ne mažiau svarbu ir tai, jog duomenų apsaugos pareigūnas gali būti laikomas tam tikra prasme tarpininku, tarp skirtingų subjektų grupių, siekiančių komunikuoti bei ginti savo ar visuomenės interesus. Tikėtina, jog šios pareigybės įtaigumas yra nulemtas imperatyvios normos, nurodančios privalomus verslo segmentus ir jų požymius, kuomet duomenų apsaugos pareigūno skyrimas yra privalomas, be jokių išimčių. Sąlygas bei aplinkybes įtvirtina BDAR 37 straipsnis, reglamentuojantis tris konkrečius atvejus: „ a) duomenis tvarko valdžios institucija arba įstaiga; b) duomenų valdytojo arba duomenų tvarkytojo pagrindinė veikla yra duomenų tvarkymo operacijos, dėl kurių būtina reguliariai ir sistemingai dideliu mastu stebėti duomenų subjektus; arba c) duomenų valdytojo arba duomenų tvarkytojo pagrindinė veikla yra specialiųjų kategorijų duomenų tvarkymas dideliu mastu arba asmens duomenų apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas tvarkymas dideliu mastu“. Tai reiškia, jog esant bent vienam iš šių, reglamentu nustatomų pagrindų, duomenų valdytojas privalo savo įstaigoje ar bendrovėje paskirti duomenų apsaugos pareigūną.

29 straipsnio darbo grupė teigiamai vertina bei skatina taip pat ir tuos atvejus, kai duomenų apsaugos pareigūnas tam tikrų organizacijų, kurioms netaikomas imperatyvus kriterijus, paskiriamas savanoriškai. Svarbu įvertinti, jog net ir tuomet, kai nėra įstatymų reikalavimo paskirti tokį subjektą, kažkas turi padėti susigaudyti naujo reguliavimo

[53] ES 29 str. darbo grupės 2017 m. balandžio 5 d. *Duomenų apsaugos pareigūnų gairės* Nr. WP 243, p. 5 [interaktyvus. Žiūrėta kovo 12 d.]. Prieiga per internetą: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048>

apimtyje ir bent jau laikinas tokio subjekto paskyrimas būtų reikšminga pagalba. Tais atvejais, kai organizacija nusprendžia savanoriškai paskirti duomenų apsaugos pareigūną, pažymimą, jog jam taikomi tokie patys reikalavimai bei užduotys, remiantis BDAR 37-39 straipsniais, kaip ir privalomai paskirtam asmeniui. Iš dalies pasirenkant ir vertinant aptariamą pareigybę, atrodytų, jog reguliavimo abstraktumas leidžia interpretacijos laisvę paskiriant bet kurį asmenį. Nėra nustatyta konkretaus reikalavimo vertinant santykį su duomenų valdytoju, duomenų apsaugos pareigūnu gali būti paskirtas tiek organizacijos darbuotojas, įvertinant tai, jog jo pareigų vykdymas nesukels interesų konflikto, tiek išorinis partneris dirbantis pagal paslaugų teikimo sutartį.

Interesų konfliktas yra reikšminga aplinkybė, kuomet į šias pareigas skiriamas įmonės darbuotojas, kuris jau atlieka kitas jam pavestas funkcijas. Tai reiškia, jog kartu su duomenų apaugos pareigūno užduotimis negali būti einamos pareigos, kurios nustato duomenų procesų tikslus, apimtis, priemones ir kt. Duomenų apsaugos pareigūnu negalėtų būti direktorius, vadovai ar kt. subjektai laikomi vadovybės kategorija[54]. Kadangi tai tiesiogiai susiję su organizacijos pareiga užtikrinti duomenų apsaugos pareigūnui visišką autonomiją.

Konkretaus reikalavimo duomenų apsaugos pareigūno kvalifikacijai nenurodoma. Tačiau normos analizė rodo, jog išskiriami reikalavimai atitinkamoms savybėms, kurioms turi pasižymėti asmuo, paskirtas į šias pareigas ir tai panaikina abstraktumo viziją. BDAR 37 straipsnio 5 dalyje nurodoma, jog turi būti remiamasi pirmiausia asmens profesinėmis savybėmis, tai tiek teorinės žinios duomenų apsaugos apimtyje, duomenų valdytojo verslo apimtyje tiek praktinės žinios apie veiklos ypatybes bei kylančius pavojus siekiant atitikties.

Kitas griežtas reikalavimas – ekspertinių žinių lygis. Konkretus ekspertinių žinių lygis negali būti apibrėžiamas, tačiau remiantis 29 straipsnio darbo grupės išaiškinimu, duomenų apsaugos pareigūnas turi turėti pakankamai aukšto lygio ekspertines žinias, kurios leis išspręsti netgi labai keblias situacijas ir tinkamai padės duomenų valdytojui pasirūpinti itin komplikuotų duomenų valdymu.[55] Šioje vietoje taip pat atsiskleidžia duomenų apsaugos pareigūno, kaip itin reikšmingo subjekto duomenų apsaugos teisėje požymis, jis remiantis ekspertinėmis žiniomis bei patirtimi turi padėti duomenų valdytojui pritaikyti verslą prie duomenų apsaugos reikalavimų bei tinkamai parinkti reikalavimus konkretaus verslo subjekto specifikai. Be abejonės ekspertinės žinios pirmiausiai remiasi į teisines žinias,

[54] ES 29 str. darbo grupės 2017 m. balandžio 5 d. *Duomenų apsaugos pareigūnų gairės* Nr. WP 243, p. 19 [interaktyvus. Žiūrėta kovo 10 d.]. Prieiga per internetą: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048>.
[55] *ibidem*, p. 13

turint omenyje, jog pagrindiniai šaltiniai yra ne tik BDAR, bet ir kiti tiek nacionaliniai, tiek tarptautiniai teisės aktai. E. Lachaud, atkreipia dėmesį, kad, nepaisant to, kad reglamentu nustatomi pakankamai griežti reikalavimai duomenų apsaugos pareigūno įgūdžiams, nepateikiama jokių priemonių, kaip užtikrinti, jog duomenų apsaugos pareigūnas turi tinkamą kompetenciją[56]. Jo nuomone, turi būti išdirbtas sertifikavimo mechanizmas, leisiantis ne tik patikrinti asmens turimus įgūdžius, bet kartu užtikrinantis vienodą praktiką Europos lygiu.[57] Šiuo aspektu pažymėtina ir tai, jog pasirenkant asmenį, nereikėtų kliautis tik teisės išsilavinimo faktu, viena esminių sudedamųjų duomenų apsaugos dalių yra techninių priemonių tinkamas parinkimas – informacinių išteklių tinkamo lygio sauga, todėl, nors toks reikalavimas neįtvirtintas, būtų labai naudinga, jei duomenų apsaugos pareigūnas pasižymėtų platesniu spektru žinių, išeinant už teisinės kompetencijos ribų.

Trečioji savybė, kuria turėtų pasižymėti duomenų apsaugos pareigūnas yra gebėjimas atlikti užduotis. Kadangi duomenų apsaugos pareigūnas atlieka labai svarbų vaidmenį organizacijoje siekdamas asmens duomenų tvarkymo taisykles paversti neatsiejama kasdienio darbo dalimi, integruoti į kiekvieną organizacijos sektorių, kuriame atliekami bet kokio pobūdžio duomenų tvarkymo veiksmai, labai reikšminga vertinti asmens individualias savybes bei statusą organizacijoje.[58] Duomenų apsaugos pareigūnas turi pasižymėti sąžiningumu ir aukšta profesine etika, jis turi turėti pakankamą autoritetą, kad duomenų apsaugos reikalavimai būtų įgyvendinti, kaip viena iš organizacijos kultūros dalių. Tinkamo asmens parinkimas, kaip ir visa BDAR atitiktis, tenka duomenų valdytojui. Jis turi atidžiai įvertinti kandidatūras bei atlikti gilesnę analizę remiantis pareigybei aktualiais aspektais.

Duomenų apsaugos pareigūnas yra BDAR naujovė ir centrinė duomenų valdymo teisinio reglamentavimo modelio „figūra“, kurios paskirtis užtikrinti organizacijos atitiktį BDAR. Dėl šios subjekto svarbos, jam keliami reikšmingi profesinių, ekspertinių ir praktinių žinių reikalavimai bei disciplinuotos asmenybės požymiai, leisiantys atitikti keliamus lūkesčius. Šiai pareigybei skiriamas labai didelis dėmesys, kadangi bet kuriai

[56] Lachaud, Eric. Should the DPO be certified? International Data Privacy Law, 2014, Vol. 4, No. 3, p. 189-202 [interaktyvus. Žiūrėta balandžio 19 d.] Prieiga per internetą:<https://www.scribd.com/document/350068564/Should-the-DPO-Be-Certified>.
[57] *Ibidem*.
[58] ES 29 str. darbo grupės 2017 m. balandžio 5 d. *Duomenų apsaugos pareigūnų gairės* Nr. WP 243, p. 14 [interaktyvus. Žiūrėta balandžio 2 d.]. Prieiga per internetą: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048>.

organizacijai turės didelę reikšmę, kaip duomenų apsaugos pareigūnas sugebės panaudoti žmogiškuosius ir finansinius išteklius bei, kaip padės pertvarkyti organizacijos struktūrą[59].

2.2. Duomenų apsaugos pareigūno veiklos principai

Kiekviena organizacija ilgą laiką kuria savo taisykles bei vidinę kultūrą, todėl bet kokie pokyčiai ir naujovės yra labai bauginančios, ypač tuomet, kai seniai užleisto mechanizmo darbas turi būti peržiūrimas ir paleidžiamas iš naujo, bet jau naujų reikalavimų pagrindu.

Pirmiausia, tokiais atvejais ieškomas asmuo, galintis padėti susigaudyti naujo reglamentavimo voratinklyje ir apibrėžtį organizacijai artimiausius tikslu įgyvendinant naujoves. Vertinant duomenų apsaugos naujoves, tai jų centre yra būtent duomenų apsaugos pareigūnas – ekspertas duomenų apsaugos teisėje. Todėl jam suteikiamas ypatingas statusas bei jis veikia kitokiais pagrindais bei principais nei paprastas organizacijos darbuotojas. Duomenų apsaugos pareigūno statusą reglamentuoja BDAR 38 straipsnis. Straipsnio pavadinimui pasirinkta sąvoka *„statusas“* savaime suponuoja tai, jog ši pareigybė nėra lygiagreti bet kuriam panašios grandies darbuotojui, duomenų apsaugos pareigūnas organizacijoje yra privilegijuota pareigybė. Todėl BDAR 38 str., 1 d., nurodoma, kad turi būti užtikrinama galimybė duomenų apsaugos pareigūnui dalyvauti organizacijai sprendžiant visus klausimus susijusius su asmens duomenimis bei jų tvarkymu. Labai svarbu duomenų apsaugos pareigūną laiku įtraukti į naujai diegiamus duomenų tvarkymo procesus arba informuoti apie naujai pradedamus tvarkyti duomenis, tam, kad rekomendacijos būtų savalaikės ir būtų lengviau laikytis duomenų apsaugos teisės keliamų reikalavimų. Duomenų apsaugos pareigūnas turi tapti skirtingų darbo grupių dalimi, partneriu diskusijoms bei konsultantu priimant sprendimus asmens duomenų apsaugos apimtyje.

Kita šios normos dalis (BDAR 38 str., 2 d.) atkreipia dėmesį į tai, kad reikšmingas aspektas yra tai, jog duomenų apsaugos pareigūnui turi būti suteikiami būtiniausi ištekliai, skirti jam priskirtinų užduočių įgyvendinimui. Šiuos išteklius turi suteikti duomenų valdytojas, siekdamas suteikti duomenų apsaugos pareigūnui pagalbą.

Visų pirma, šias pareigas einantis asmuo turi jausti nuolatinę vyresniosios vadovybės paramą ir dalyvauti oficialiame paskyrime pristatant duomenų apsaugos pareigūną darbuotojams. Subjektas, kurio žodis nieko bendrovėje nelemia, nėra tinkamas kandidatas tapti duomenų apsaugos pareigūnų, kadangi šis asmuo turi turėti autoritetą ir vadovybės

[59]ZALESKIS, Julius. *Duomenų apsaugos pareigūno veiklos pagrindai pagal ES bendrąjį duomenų apsaugos reglamentą.* Teisė, t. 104, p.160. [interaktyvus. Žiūrėta balandžio 2 d.]. Prieiga per internetą: <https://www.zurnalai.vu.lt/teise/article/view/10851/8986>.

akyse, tam, kad jo rekomendacijos įgautų „svorį“ darbuotojų tarpe. Palaikymas taip pat turėtų pasireikšti suteikiant pakankamai laiko duomenų apsaugos pareigūnui atliekant savo pareigas. Vertinant šį aspektą svarbu grįžti prie duomenų apsaugos pareigūno skyrimo diskusijos vertinant tiek darbuotojo, tiek išorinio partnerio paskyrimo galimybę. Tiek darbuotojas, turintis kitų svarbių pareigų ar dirbantis ne pilną darbo dieną, tiek išorinis partneris, aptarnaujantis kelias įmones ar apribotas paslaugos valandų limitais, gali pristigti laiko ir dėl prioritetų priešpriešos apleisti duomenų apsaugos pareigūno pareigas. Todėl geriausia išeitis būtų turėti darbų planą, kuriuo remiantis galima bus vertinti likusius darbus ir jau išspręstus klausimus, nedarant neigiamo spaudimo.

Vertinant išteklius ne mažiau svarbu finansai, infrastruktūra ar net darbuotojai. Nuolat peržiūrint veiklos procesus, tvarkomus duomenis, tiriant teikiamas paslaugas ar informacinių sistemų saugumo ypatybes duomenų apsaugos pareigūnui gali prireikti pokalbių su darbuotojais ir informacinių sistemų specialistais, o nustačius trūkumus papildomų finansinių išteklių, siekiant įdiegti reikiamas priemones. Būtent duomenų apsaugos pareigūnas yra subjektas galintis pateikti rekomendacijas dėl techninių ar organizacinių priemonių tinkamo saugumo lygio užtikrinimui. Dėl šios priežasties reikšminga turėti žinių informacinių technologijų apimtyje. Iš šio aspekto kyla kitas itin svarbus poreikis, kuris turi būti patenkinamas – nuolatinis mokymasis. Duomenų apsaugos pareigūnas turi turėti galimybę gilinti žinias ir kelti ekspertinį lygį bei kvalifikaciją įvairiuose kursuose, seminaruose, forumuose ar kituose organizuojamuose renginiuose duomenų apsaugos temomis. Svarbu išteklių skyrimą vertinti pagal organizacijos veiklos specifiką, kuo sudėtingesni duomenų tvarkymo procesai ar jautresnis duomenų tvarkymas, tuo daugiau išteklių gali prireikti siekiant efektyvumo ir veiksmingumo[60].

Galiausiai skiriant išteklius reikšminga įvertinti organizacijos dydį, kadangi ne retai vieno asmens atliekančio duomenų apsaugos pareigūno funkcijas gali nepakakti, jei darbų apimtis itin didelė, todėl turi būti sudaryta reali galimybė sudaryti asmenų grupę, kurie padės duomenų apsaugos pareigūnui pilna apimtimi įgyvendinti jam atsirandančias užduotis.

Tinkamai įgyvendinat aptariamus išteklius, tiesiogiai užtikrinama kita duomenų apsaugos pareigūno specifika – autonomiškumas. BDAR 38 str., 3 d., tiesiogiai numato šia ypatybę – kuri yra pagrindinis duomenų apsaugos pareigūno veiklos principas, leidžiantis objektyviai vertinti organizacijos pasirengimo atitikčiai lygį. Duomenų apsaugos

[60] ES 29 str. darbo grupės 2017 m. balandžio 5 d. *Duomenų apsaugos pareigūnų gairės* Nr. WP 243, p. 17 [interaktyvus. Žiūrėta kovo 26 d.]. Prieiga per internetą: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048>.

pareigūnas negali gauti jokių nurodymų, nepaisant to, paskirtas asmuo yra organizacijos darbuotojas ar išorinis partneris, jis turi turėti galimybę vykdyti savo funkcijas nepriklausomai.[61] Šias pareigas einančiam asmeniui negali būti nurodoma, kuriuos klausimus ir kaip jis turi spręsti, kaip jis turi įgyvendinti abstrakčias įstatymų normas, kaip aiškinti vienas ar kitas teisės normas ir pan. O taip pat, tinkamam savarankiškumui užtikrinti turi laiku ir tinkamai būti aprūpintas visais jam būtinais ištekliais. Tačiau 29 str. darbo grupė atkreipia dėmesį į tai, jog: *„Duomenų apsaugos pareigūnų autonomija nereiškia, kad jie turi su 39 str., nurodytomis savo užduotimis nesusijusių įgaliojimų priimti sprendimus.“*[62]

Visų pirma, nors pavaldumo santykio nelieka, tačiau reikšminga pažymėti, jog atskaitomybė nagrinėjamoje normoje išlieka imperatyvi – duomenų apsaugos pareigūnas atsiskaito aukščiausio lygio vadovybei. Todėl negalima būtų vertinti duomenų apsaugos pareigūną, kaip subjektą turintį sprendimo teisę. Šiuo aspektu vis dėl to reikšminga nepamiršti, kad atsakomybė tenka organizacijai, todėl galutinį sprendimą priima valdymo organas. Ir esant įtarimams, jog sprendimai buvo netinkami ar dėl jų atsirado duomenų saugumo pažeidimas, turi išlikti galimybė įrodyti bei įgyvendinti BDAR reglamentuojamą atskaitomybės principą, kokiu pagrindu sprendimas buvo priimtas ir kokios aplinkybės lėmė būtent tokias išvadas.

Duomenų apsaugos pareigūno veikla turi būti skaidri – vadovybei turi būti aiškios jo konsultacijos ir rekomendacijos, be to 29 str., darbo grupės teigimu, vadovybei taip pat turėtų būti teikiama metinė duomenų apsaugos pareigūno veiklos ataskaita[63], todėl pareigūno veikla taip pat remiasi ir atskaitomybės principu. Tačiau, dėl to duomenų apsaugos pareigūno autonomija niekaip neapribojama ir išsaugoma pilna apimtimi, dėl BDAR 38 str., 3 d., nuostatos užtikrinančios tai, jog nepaisant to, kaip atliekamos pavestos užduotys, duomenų apsaugos pareigūnas negali būti baudžiamas ar atleidžiamas. Ši nuostata labai svarbi siekiant užtikrinti asmens apsaugą, tačiau tikslu būtu atkreipti dėmesį, jog draudimas taikyti nuobaudas apsiriboja tik duomenų apsaugos pareigūno pareigų atlikimu. 29 str., darbo grupė atkreipia dėmesį į tai, jog nuobaudos dėl kitų padarinių, nesusijusių su duomenų apsaugos pareigūno užduočių atlikimu taikomos gali būti įprasta tvarka ir gali atsirasti kitų priežasčių siekiant pakeisti vieną pareigūną kitu, todėl labai

[61] BDAR 97 preambulės punktas
[62] *ibidem*, p.17
[63] ES 29 str. darbo grupės 2017 m. balandžio 5 d. *Duomenų apsaugos pareigūnų gairės* Nr. WP 243, p. 17 [interaktyvus. Žiūrėta kovo 15 d.]. Prieiga per internetą: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048>.

pozityviai vertinamos tos sutartys su duomenų apsaugos pareigūnais, kurios yra griežtai apibrėžtos ir suteikia garantijų nuo neteisėto atleidimo.

Dr. J. Zaleskis prie duomenų apsaugos pareigūno veiklos principų priskiria ir prieinamumo principą[64]. Šis principas nulemiamas BDAR 38 str., 4 d., kuria užtikrinama duomenų subjektų teisė kreiptis bet kokiais klausimais, susijusiais su jų duomenų tvarkymu ar teisių įgyvendinimu. Konkrečių subjektų grupių norma nedetalizuoja, kas suponuoja, jog kalbama apie visus galimus fizinius asmenis, laikomus duomenų subjektais, tiek organizacijos darbuotojus, tiek klientus, tiek interesantus. Prie šių subjektų, autorius remdamasis BDAR 37 str., 7 d., taip pat priskiria priežiūros instituciją, kuriai organizacija pateikia savo duomenų apsaugos pareigūno kontaktus.

Duomenų apsaugos pareigūno pareigybė yra specifinė ir reikalauja kitokio požiūrio nei bet kokia kita organizacijos pozicija. Organizacijai kyla atsakomybė tinkamai užtikrinti visas būtinas priemones ir išteklius nuo darbuotojų iki finansinių resursų, leidžiant sukurti terpę duomenų apsaugos pareigūnui veikti autonomiškai, dėl ko įgyvendinama galimybė išlaikyti objektyvumą vertinat organizacijos pasirengimą bei teikiant rekomendacijas dėl reikiamų priemonių tinkamai atitikčiai užtikrinti.

2.3. Duomenų apsaugos pareigūno užduotys

Paviršutiniškai žvelgiant į duomenų apsaugos pareigūno veiklą reglamentuojančias normas gali susidaryti klaidingas įspūdis, jog pagrindinė šio subjekto užduotis – tik padėti organizacijai susigaudyti Reglamento reikalavimuose, tačiau taip nėra. BDAR 39 str., nurodo konkrečiai išskiriamas sritis, kuriose duomenų apsaugos pareigūnui suteikiama kompetencija veikti. Šios normos nėra griežtai nurodančios apibrėžtas funkcijas, kaip ir didžioji dalis Reglamento, normos yra abstrakčios ir tik nurodo kryptį, leidžiant pačiam pasirinkti interpretavimo apimtis bei įgyvendinimo priemones.

Visų pirma duomenų apsaugos pareigūnui iškeliama užduotis *informuoti ir konsultuoti* organizaciją ir jos darbuotojus apie jiems aktualias prievoles pagal duomenų apsaugą reglamentuojančius teisės aktus. Tai svarbi užduotis, kadangi teisės aktams yra būdinga kaita, kelis kart į metus atsiranda bent minimalūs pakeitimai nacionalinėje teisėje, kurie turi vienokios ar kitokios įtakos duomenų tvarkymo procesams skirtinguose sektoriuose. Ne mažiau svarbu ir tai, kad darbuotojams bet kokios naujai iškilusios situacijos bus neaiškios ir reikės nuolatinio asmenų konsultavimo siekiant įgyvendinti duomenų apsaugos normas

[64] ZALESKIS, Julius. *Duomenų apsaugos pareigūno veiklos pagrindai pagal ES bendrąjį duomenų apsaugos reglamentą.* Teisė, t. 104, p.167. [interaktyvus. Žiūrėta kovo 15 d.]. Prieiga per internetą: <https://www.zurnalai.vu.lt/teise/article/view/10851/8986>.

organizacijos viduje. Dėl to ši norma suponuoja nuolatinį duomenų apsaugos pareigūno aktyvumą, jis turi būti visuomet pasiruošęs pateikti atnaujintą informaciją, atlikti reikiamas korekcijas bei pateikti reikiamas rekomendacijas. Šios aplinkybės praktikoje parodo, kaip svarbu, tinkamai ir laiku įtraukti duomenų apsaugos pareigūną į bet kokius duomenų tvarkymo procesus, leisti nuodugniai susipažinti su nustatyta tvarka ir žinoti apie bet kokius vadovybės planuojamus pokyčius. Tačiau pastebėtina, tai, kad ši užduotis apsiriboja tik informacijos pateikimu, kaip toliau informacija bus apdorojama tai išskirtinai duomenų valdytojo klausimas.

Kita duomenų apsaugos pareigūno reglamentu įtvirtinta užduotis *stebėti*, kaip laikomasi duomenų apsaugos teisės aktų reikalavimų organizacijos viduje. Šią normą reglamentas patikslina nustatydamas, jog į stebėjimą įeina darbuotojų informuotumo palaikymas, darbuotojų mokymai ir auditai. Analizuojant šią užduotį reikšminga sugrįžti prie asmens duomenų tvarkymo pagrindų, reglamentuojamų BDAR 5 str., kadangi stebėti, kaip organizacijos viduje laikomasi duomenų tvarkymo taisyklių, tai reiškia, stebėti, kaip laikomasi asmens duomenų tvarkymosi principų, kuriais grįsta visa duomenų apsaugos prasmė. Vertinant tai, kaip organizacija laikosi teisėtumo principo, duomenis tvarkydama tik teisėtais pagrindais, kaip užtikrinamas skaidrumo principas, pateikiant informaciją apie duomenų tvarkymą subjektams renkant iš jų duomenis, ar duomenys renkami tik teisėtiems tikslams ir yra atitinkantys duomenų kiekio mažinimo principą, ar tvarkomi organizacijos duomenys yra tikslūs ir prireikus nuolat atnaujinami, ar užtikrinamas ribotas saugojimo terminas, ar įgyvendinamos tinkamos saugumo priemonės bei pateikiant reikiamas rekomendacijas proceso korekcijoms. Tačiau stebėjimo nereikėtų sieti su duomenų apsaugos pareigūno asmenine atsakomybe, remiantis BDAR 5 str., 2 d., tik pats duomenų valdytojas – organizacija yra atsakingas už tinkamų priemonių atitikčiai įgyvendinimą.

Sekanti duomenų apsaugos pareigūnui skiriama užduotis yra *konsultavimas dėl poveikio duomenų apsaugai vertinimo bei jo atlikimo stebėjimas*. Remiantis reglamentu duomenų apsaugos pareigūnas turėtų tik konsultuoti ir stebėti kaip atliekamas poveikio duomenų apsaugai vertinimo procesas, tačiau praktikoje tai dažnu atveju veikia išeinant už šia norma nubrėžtų ribų.

Poveikio duomenų apsaugai vertinimas – tai procesas, kurio metu įvertinamas galimas pavojus duomenų saugumui atsižvelgiant į duomenų mastą, tikslus ir pasirinktą duomenų tvarkymo būdą. Nepaisant to, kad būtent duomenų valdytojas – organizacija, pati turėtų atlikti šį vertinimą, o duomenų apsaugos pareigūnas tik suteikti konsultaciją, atsakingiems asmenims, tai paprastai sekasi komplikuotai ir konsultacijos sklandžiai perauga į

pilnavertiškai atliekamą darbą. 29 straipsnio darbo grupė atkreipia dėmesį[65], jog BDAR 39 str., pateikiamu užduočių sąrašu numato, jog duomenų apsaugos pareigūnas atlieka *bent šias užduotis,* todėl niekas neužkerta kelio organizacijai paprašyti duomenų apsaugos pareigūno atlikti šiame straipsnyje nepaminėtas užduotis ir poveikio duomenų apsaugai vertinimas galėtų būti kaip viena iš jų.

Bendruoju požiūriu 29 straipsnio darbo grupė labai rekomenduoja, tiek sutartyje, tiek darbuotojams ar kitiems subjektams aiškiai apibrėžti duomenų apsaugos pareigūno užduotis ir jų sritį[66], ypatingai reglamento nedetalizuojamais atvejais. Tačiau, reikšminga paminėti, jog šioje vietoje atsakomybė taip pat tenka tik duomenų valdytojui, kadangi tik jis priima galutinius sprendimus, atvejais, kai nesutinka su duomenų apsaugos pareigūno nuomone, jis gali pasielgti savaip, tačiau tokiu atveju, svarbu turėti pagrįstą dokumentaciją, kodėl buvo nuspręsta neklausyti duomenų apsaugos pareigūno nuomonės.

Kita labai svarbi užduotis tenkanti duomenų apsaugos pareigūnui yra *bendradarbiavimas su priežiūros institucija* ir *kontaktinio asmens funkciją.* Ši užduotis reiškia, jog duomenų apsaugos pareigūnas tampa tarpininku tarp organizacijos ir antrosios šalies, norinčios spręsti klausimus duomenų apsaugos apimtyje, nepaisant to, kas ta antroji šalis, duomenų subjektas ar priežiūros institucija. Jis veikia kaip kontaktinis asmuo, kuris padeda gauti reikiamą informaciją, pateikia atsakymus į klausimus, reikiamus dokumentus, patikslinimus, pranešimus apie organizacijoje įvykusius pažeidimus. Duomenų apsaugos pareigūnas pristatomas duomenų subjektams ir priežiūros institucijai, kaip už duomenų apsaugos klausimus organizacijoje atsakingas asmuo bei viešai pateikiami jo kontaktai, siekiant įgyvendinti tiek skaidrumo, tiek tinkamo informavimo principus. Be to, jog jis turėtų teikti informaciją priežiūros institucijai. Duomenų apsaugos pareigūnui taip pat sudaryta galimybė bet kuriuo klausimu konsultuotis su priežiūros institucija[67].

Priežiūros institucija yra pagrindinis organas, atsakantis už duomenų apsaugos apimtyje kylančius klausimus, skundus, tyrimus ir kt., todėl neretai, susiduriant su normų abstraktumu reikšminga žinoti, kaip atitinkamus atvejus interpretuoja būtent priežiūros organas, kuris kilus ginčui vykdys tolimesnį tyrimą[68].

---

[65] ES 29 str. darbo grupės 2017 m. balandžio 5 d. *Duomenų apsaugos pareigūnų gairės* Nr. WP 243, p. 20 [interaktyvus. Žiūrėta kovo 17 d.]. Prieiga per internetą: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048>.

[66] *Ibidem*.

[67] Priežiūros institucijos funkcijas Lietuvos Respublikos teritorijoje atlieka Valstybinė duomenų apsaugos inspekcija

[68] ES 29 str. darbo grupės 2017 m. balandžio 5 d. *Duomenų apsaugos pareigūnų gairės* Nr. WP 243, p. 21 [interaktyvus. Žiūrėta kovo 17 d.]. Prieiga per internetą: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048>.

Vertinant jau pateiktą 29 straipsnio darbo grupės nuomonę, dėl galimybės plėsti duomenų apsaugos pareigūnui priskiriamų užduočių sąrašą, verta taip pat paminėti *veiklos įrašų vedimą*. Veiklos įrašai yra duomenų valdytojui kylanti prievolė tvarkyti duomenų tvarkymo operacijos įrašus, todėl kad ir kas juos bepildytų, atsakomybė tenka duomenų valdytojui. Įrašuose pateikiama išsami informacija apie tvarkomus duomenis, duomenų tvarkymo tikslus, subjektų kategorijas, duomenų gavėjus, duomenų perdavimą ar ištrynimą.

Dėl informacijos apimties, kuri pateikiama minėtame dokumente, manytina, jog šis dokumentas geriausiai leidžia duomenų apsaugos pareigūnui vykdyti apibrėžtas savo užduotis – stebėti bet kokius pokyčius, reikalavimų įgyvendinimą bei informuoti ir konsultuoti organizaciją pastebėjus neatitikimus ar trūkumus. Todėl iš pirmo žvilgsnio papildomai nustatyta užduotis iš tiesų gali tapti labai reikšminga pagalbos priemone, pilna apimtimi įgyvendinat visas kitas reglamentu nustatytas funkcijas. Kadangi nepaisant to, kad atsakomybė tenka organizacijai, kaip duomenų valdytojui, remiantis BDAR 39 str., 2 d., būtent duomenų apsaugos pareigūnas turi įvertinti galimą pavojų, susijusį su duomenų tvarkymo operacijomis. Pagal aptariamą normą pavojus vertinamas atsižvelgiant į duomenų pobūdį, kontekstą, aprėptį ir tikslus, kuriais tvarkomi duomenys. Iš tokio detalizavimo kyla natūralus poreikis duomenų apsaugos pareigūnui pirmiausia identifikuoti aukščiausio pavojaus lygio klausimus ir skirti jiems didesnį dėmesį. Tai leidžia tinkamai nustatyti silpnąsias vietas ir spragas priemonėse, kurios pasirinktos siekiant užtikrinti tinkamą saugumo lygį, be to tai konkretizuoja sritį, kurioje ir darbuotojai turi būti daug plačiau informuoti ir prižiūrimi.

Duomenų apsaugos pareigūnui tenkančios užduotys reikalauja, visiško asmens įsitraukimo ir neapsibrėžia tik pateikiamu BDAR 39 str. užduočių sąrašu, kartu gali būti nustatomos papildomos užduotis, kurias turi atlikti duomenų apsaugos pareigūnas, tačiau visais atvejais, atsakomybė tenka tik pačiai organizacijai – duomenų valdytojui, kadangi duomenų apsaugos pareigūno užduočių turinys apsiriboja stebėjimu, informavimu, rekomendavimu, kaip bus įgyvendinti keliami reikalavimai ir priimti duomenų apsaugos nuomonę ar ne, pasirenka tik pats duomenų valdytojas ir atsakomybė taip pat tenka būtent jam.

3. DUOMENŲ VALDYTOJO IR DUOMENŲ APSAUGOS PAREIGŪNO ATSAKOMYBĖS SANTYKIS

3.1. Atsakomybės pasiskirstymas už asmens duomenų apsaugos atitikties užtikrinimą

3.1.1. Atsakomybės pasiskirstymas už principų įgyvendinimą

Pirmojoje šio darbo dalyje, vertinant duomenų valdytojui priskiriamas pareigas, vienomis iš pagrindinių ir pamatinių pareigų pažymimas duomenų tvarkymo principų įgyvendinimas. Tai BDAR 5 str. nurodyti principai, kuriais privalo vadovautis duomenų valdytojas vykdant asmens duomenų tvarkymo procesus. Kiekvienas principas sukuria naujas pareigas ir duomenų valdytojui, pasiskyrusiam duomenų apsaugos pareigūną tvarkytis su visų reikalavimų įgyvendinimais iš ties lengviau. Kaip matyti iš duomenų apsaugos pareigūno vertinimo antrojoje šio darbo dalyje, tai yra asmens duomenų apsaugos teisės ekspertas, atliekantis nuolatinę duomenų tvarkymo veiksmų priežiūrą ir teikiantis pastabas, dėl šių procesų gerinimo ir atitikties teisės aktų reikalavimams. Todėl, siekiant užtikrinti principų įgyvendinimą duomenų valdytojas ir duomenų apsaugos pareigūnas dirba kaip viena komanda.

Neišvengiamai siekiant įgyvendinti BDAR 5 str., turi būti užtikrinama atitiktis eilei kitų normų ir ties tuo duomenų valdytojas ir duomenų apsaugos pareigūnas dirba kaip viena komanda. Teisėtumo principas, reikalauja, kad duomenų tvarkymas būtų grindžiamas BDAR 6 ir 9 str., pateikiamais teisėto duomenų tvarkymo pagrindais. Jautriausi duomenų tvarkymo pagrindai yra sutikimas ir teisėtas interesas. Duomenų apsaugos pareigūnas visų duomenų tvarkymo pagrindų tinkamumo vertinimo metu skiria didesnį dėmesį tikrinimui ar duomenų tvarkymą grindžiantys duomenų subjektų sutikimai yra gauti teisėtai ir ar išsaugoti sutikimo gavimo įrodymai bei teisėto intereso pagrįstumo aplinkybėms. Nustačius teisėta interesą, kaip duomenų tvarkymo pagrindą, duomenų valdytojas turi atlikti pusiausvyros testą, nustatant ar duomenų subjekto teisės ir laisvės nėra viršesnės už jo teisėtą interesą. Atvejais, kai duomenų valdytojas siekia pradėti naujų duomenų tvarkymą, duomenų valdytojas konsultuojasi su duomenų apsaugos pareigūnu, siekiant gauti jo nuomonę, dėl tinkamo duomenų tvarkymo pagrindo nustatymo.

Vertinant skaidrumo principą, jis suponuoja, kad būtų įgyvendinti BDAR 12 – 14 str., numatantys tinkamo subjekto informavimo sąlygas. Šiame procese duomenų apsaugos pareigūnas gali pateikti duomenų valdytojui rekomendacijas, kaip įgyvendinti šį reikalavimą – nurodant kokiu momentu, atsižvelgiant į verslo specifiką, galėtų būti teikiama pirminė informacija ir kokio ji turi būti turinio. Savo ruoštu duomenų valdytojas

pasirenka jam tinkamą verslo valdymo strategiją ir priima galutinį sprendimą dėl subjekto informavimo aplinkybių.

Sekantis duomenų tvarkymo tikslo apribojimo principas, nukreipia į BDAR 6 ir 26 str., kurie numato, kuo turi pasižymėti duomenų tvarkymo tikslai ir kaip jie nustatomi tais atvejais, kai duomenų tvarkymas atliekamas bendrų duomenų valdytojų. Duomenų valdytojas pradedantis veiklą, kurios vykdymui reikalinga užtikrinti duomenų tvarkymo procesų vykdymą, nustato tikslus, kuriais vėliau bus tvarkomi jo kliento, interesanto, darbuotojo ar kito duomenų subjektų duomenys. Šiuo atveju duomenų apsaugos pareigūnas turėtų pateikti vertinimą, kiek pagrįsti yra duomenų tvarkymo tikslai, kaip aiškiai jie suformuluoti ir ar nustatytų tikslų negalima pasiekti kitais būdais[69]. Atvejais, kai duomenų tvarkymas yra būtinas siekiamiems tikslams, duomenų apsaugos pareigūnas įvertina ketinamų tvarkyti duomenų apimtis ir pateikia savo rekomendaciją.

Atitinkamai siekiant užtikrinti duomenų kiekio mažinimo principus, turi būti atsižvelgiama į BDAR 25 str., normas, nustatančias saugumo priemones, kurios turi būti įgyvendinamos saugant duomenų subjektų teises. Nors duomenų apsaugos pareigūnui keliamas pagrindinis reikalavimas ekspertinių žinių lygis asmens duomenų apsaugos teisės apimtyje, tačiau jis taip pat, turėtų turėti bent jau bazines žinias informacinių technologijų apimtyje. Šis reikalavimas taikomas dėl to, kad duomenų apsaugos pareigūnas galėtų padėti duomenų valdytojui parinkti tinkamas saugumo priemones, ne tik fizinėje aplinkoje, bet ir informacinėje erdvėje. Duomenų apsaugos pareigūnas pateikia informaciją, ko teisės normos reikalauja iš duomenų valdytojo, o šis jam priimtinais būdais, turėtų atsirinkti ir pritaikyti verslui tinkamas priemones.

Sąveikoje su BDAR 16 str. – duomenų subjekto teisę reikalauti ištaisyti neteisingus jo duomenis, įgyvendinamas tikslumo principas. Nors, kaip jau minėta, šio principo įgyvendinimo apimtis priklauso ne tik nuo duomenų valdytojo, bet ir tame tarpe nuo duomenų subjekto ar trečiųjų šalių įsitraukimo į jų duomenų tvarkymą, vis dėl to pirmas „smūgis“ atiteks būtent duomenų valdytojui. Dėl to duomenų apsaugos pareigūno užduotis šiuo atveju, iškilus klausimams, pateikti rekomendacijas, kaip tinkamai įgyvendinti tiek subjekto teisę, tiek patį principą.

Vientisumo ir konfidencialumo principas sąlygoja BDAR 32 str., nustatomas saugumo duomenų tvarkymo priemonių užtikrinimą. Šio principo apimtyje duomenų apsaugos pareigūnas gali būti naudingas duomenų valdytojui, kaip ir kiekio mažinimo principo užtikrinime, parenkant tinkamas saugumo priemones, atsižvelgiant į naudojamos technikos

[69] BDAR preambulės 39 punktas

išsivystymo lygį. Tačiau taip pat konfidencialumo užtikrinimui svarbu ne tik saugumo užtikrinimas, bet ir komandos pasirengimas. Duomenų valdytojo darbuotojai turi būti įsipareigoję saugoti paslaptis apie jiems darbo metu tapusius žinomais duomenis, turi būti supažindinti su komunikacinių priemonių naudojimo taisyklėmis, todėl duomenų valdytojas turi itin rūpestingai rūpintis darbuotojų parinkimu bei vidaus taisyklių laikymusi organizacijoje. Duomenų apsaugos pareigūnas gali pateikti pastebėjimus, atsiradusius stebint įvairius procesus bei darbuotojų elgesį.

Vertinant duomenų apsaugos pareigūno ir duomenų valdytojo įsitraukimą į visų principų įgyvendinimą ir jiems tenkančias pareigas, nėra sudėtinga padėti atskyrimą atsakomybės klausimui. Duomenų valdytojui yra taikomas atskaitomybės principas ir įgyvendinant duomenų tvarkymo principus, duomenų apsaugos pareigūno vaidmuo yra tik antraeilis, jis turi kompetencijos pateikti duomenų valdytojui rekomendacijas remiantis asmens duomenų apsaugos teisės aktų pagrindu ir stebėti, kaip įgyvendinami visi reikalavimai. Duomenų valdytojas pats pasirenka atsižvelgti į duomenų apsaugos pareigūno rekomendacijas ar ne, taip pat jis pats nusprendžia, kokia apimtimi įgyvendinti rekomendacijas bei kokiais būdais tai turėtų būti įgyvendinama, kadangi duomenų apsaugos pareigūnas pateikia teisinį vertinimą, o duomenų valdytojas, turi savo požiūrį į tai, kaip norėtų vykdyti verslą. Todėl duomenų apsaugos pareigūnas asmens duomenų tvarkymo principų įgyvendinimo tikslu, turėtų būti atsakingas tik už jo teikiamas rekomendacijas, už tai, kad jos yra atitinkančios teisės aktų normas.

3.1.2. Atsakomybės pasiskirstymas už poveikio duomenų apsaugai vertinimą

Viena iš duomenų valdytojui keliamų pareigų yra *poveikio duomenų apsaugai vertinimas*. Ši asmens duomenų apsaugos dalis įtvirtinta BDAR 35 str., ir kurį laiką buvo mažiausiai eskaluojama, kadangi normoje nurodytos sąlygos buvo per abstrakčios. Tačiau per metus nuo reglamento įsigaliojimo parengtas nacionalinis teisės aktas, numatantis išsamų ir nebaigtinį sąrašą atvejų, kuomet duomenų valdytojai privalo atlikti poveikio duomenų apsaugai vertinimus. Šio proceso tikslas – aprašyti vykdomą duomenų tvarkymą ir įvertinti bei valdyti galimą pavojų duomenų subjektų teisėms ir laisvėms, kylantį dėl pasirinkto duomenų tvarkymo būdo[70]. Pagrindinis reikalavimas dėl kurio kyla pareiga atlikti poveikio duomenų apsaugai vertinimą yra duomenų tvarkymo sukeliamas „didelis pavojus“,

[70] ES 29 str. darbo grupės 2017 m. spalio 4 d. *Poveikio duomenų apsaugai vertinimo (PDAV) gairės, kuriomis Reglamento 2016/679 taikymo tikslais nurodoma, kaip nustatyti, ar duomenų tvarkymo operacijos gali sukelti didelį pavojų* Nr. WP248, p. 4 [interaktyvus. Žiūrėta kovo 26 d.] Prieiga per internetą: < https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236>.

remiantis BDAR 35 str., 3 d., tai galėtų būti: „a) sistemingas ir išsamus su fiziniais asmenimis susijusių asmeninių aspektų vertinimas <...>, b) <...> specialiųjų kategorijų arba <...> asmens duomenų apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas tvarkymas dideliu mastu, c) sistemingas viešos vietos stebėjimas dideliu mastu“. Šis sąrašas nėra laikomas baigtiniu, tačiau gerai iliustruoja normos prasmę. Pareiga atlikti šį vertinimą kyla duomenų valdytojui, tačiau priešingai nei kitais atvejais, šis vertinimas yra įtrauktas į tiesiogines duomenų apsaugos pareigūno užduotis. BDAR 39 str., 1 d., c) p., nurodo, kad duomenų apsaugos pareigūnas: „paprašius konsultuoja dėl poveikio duomenų apsaugai vertinimo ir stebi jo atlikimą“. Pagal taisykles poveikio duomenų apsaugai vertinimas atliekamas prieš pradedant duomenų tvarkymą[71]. Vertinime pateikiami duomenų tvarkymo veiksmai, duomenų valdytojo teisėti interesai bei tikslai ir tvarkomų duomenų apimtys, nurodomi galimi pavojai duomenų subjektams. Atitinkamai turi būti nurodytos saugumo priemonės, kurių bus imtasi siekiant sumažinti galimo pavojaus riziką ir užtikrinti duomenų apsaugą. Atliekant vertinimą duomenų valdytojas turi stengtis konsultuotis su duomenų apsaugos pareigūnu ir visa konsultacija turėtų būti dokumentuota poveikio duomenų apsaugai vertinime[72]. 29 straipsnio darbo grupės nuomone duomenų valdytojas galėtų kreiptis į duomenų apsaugos pareigūną su šiais klausimais[73]: ar reikia atlikti poveikio duomenų apsaugai vertinimą, kokia metodika reikėtų vadovautis šiame procese, ar poveikio vertinimą atlikti organizacijoje, ar jį užsakyti, kokias apsaugos priemones reikėtų taikyti siekiant sumažinti riziką, ar tinkamai parengtas vertinimas ir ar jo išvados atitinka duomenų apsaugos teisės reikalavimus. Duomenų valdytojas gali nesutikti su duomenų apsaugos pareigūno nuomone.

Tais atvejais, kai vertinimo rezultatas rodo didelę riziką, duomenų valdytojas turi paklausti duomenų subjektų nuomonės dėl tolimesnio duomenų tvarkymo[74]. Remiantis Europos duomenų apsaugos valdybos nuomone poveikio duomenų apsaugai vertinimas yra tęstinis procesas ir jokiu būdu ne vienkartinis. Taip yra dėl to, kad duomenų tvarkymas yra dinamiškas ir turi savybę nuolat kisti[75].

---

[71] BDAR 35 straipsnio 1 dalis

[72] ES 29 str. darbo grupės 2017 m. spalio 4 d. *Poveikio duomenų apsaugai vertinimo (PDAV) gairės, kuriomis Reglamento 2016/679 taikymo tikslais nurodoma, kaip nustatyti, ar duomenų tvarkymo operacijos gali sukelti didelį pavojų* Nr. WP248, p. 17 [interaktyvus. Žiūrėta kovo 29 d.] Prieiga per internetą: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236>.

[73] ES 29 str. darbo grupės 2017 m. balandžio 5 d. *Duomenų apsaugos pareigūnų gairės* Nr. WP 243, p. 28 [interaktyvus. Žiūrėta kovo 29 d.]. Prieiga per internetą: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048>.

[74] BDAR 35 straipsnio 9 dalis

[75] ES 29 str. darbo grupės 2017 m. spalio 4 d. *Poveikio duomenų apsaugai vertinimo (PDAV) gairės, kuriomis Reglamento 2016/679 taikymo tikslais nurodoma, kaip nustatyti, ar duomenų tvarkymo operacijos gali sukelti didelį pavojų* Nr. WP248, p. 16 [interaktyvus. Žiūrėta kovo 29 d.] Prieiga per internetą: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236>.

Poveikio duomenų apsaugai vertinimas yra duomenų valdytojo pareiga, kurią jis turi įvykdyti, jei jo atliekamas duomenų tvarkymas kelia „didelį pavojų“ duomenų subjektų teisėms ar laisvėms. Duomenų apsaugos pareigūno įsitraukimas į šį procesą yra tiesiogiai numatytas jo užduotis reglamentuojančiose normose. Duomenų apsaugos pareigūnas turėtų konsultuoti duomenų valdytoją tiek dėl klausimų ar reikia atlikti poveikio duomenų apsaugai vertinimą, tiek padedant parinkti tinkamas papildomas priemones saugumui užtikrinti ir įvertinant gautas išvadas. Todėl, šiuo atveju, duomenų valdytojo atsakomybė apima proceso inicijavimą ir atlikimą, net, jeigu vertinimą už jį atliks kas nors kitas, atsakomybė vienareikšmiškai teks jam[76]. Tuo tarpu duomenų apsaugos pareigūno atsakomybės turinį sudaro jo teikiamos konsultacijos. Duomenų apsaugos pareigūnas yra atsakingas už tai, kokias rekomendacijas teikia duomenų valdytojui, šiam siekiant atlikti poveikio duomenų apsaugai vertinimą.

3.1.3. Atsakomybės pasiskirstymas už IT saugumą

Kiekvienai organizacijai, siekiant apsaugoti vidaus informaciją nuo galimo išorinio poveikio, visų pirma reikia pasirūpinti tinkamų saugumo priemonių nustatymu ir diegimu. Tinklų ir informacinėms sistemoms bei paslaugoms tenka itin svarbus vaidmuo, nes jų patikimumas ir saugumas yra labai svarbūs ekonominei ir visuomeninei veiklai, ypač vidaus rinkos veikimui[77] Užtikrinant asmens duomenų saugumą, ši užduotis tenka duomenų valdytojui. BDAR 24 str., įpareigoja duomenų valdytoją įgyvendinti tinkamas saugumo technines ir organizacines priemones. Tiek techninės, tiek organizacinės priemonės, turi būti parenkamos atsižvelgiant į tvarkomus duomenis, tvarkomų duomenų apimtis, nustatytus duomenų tvarkymui tikslus bei pavojų, galintį pakenkti duomenų subjektų teisėms ir laisvėms. Ypač svarbu, tinkamai užtikrinti duomenų saugumą, kai saugomi jautrūs duomenys, tokie kaip sveikatos, vaikų duomenys, genetiniai duomenys ar duomenys apie nusikaltimus ir nusikalstamas veikas, ir kt. Ne mažiau reikšminga ir tai, jog naudojamos priemonės bus vertinamos, kaip įrodymai, jog duomenų valdytojas atitinka

[76] ES 29 str. darbo grupės 2017 m. spalio 4 d. *Poveikio duomenų apsaugai vertinimo (PDAV) gairės, kuriomis Reglamento 2016/679 taikymo tikslais nurodoma, kaip nustatyti, ar duomenų tvarkymo operacijos gali sukelti didelį pavojų* Nr. WP248, p. 16 [interaktyvus. Žiūrėta kovo 30 d.] Prieiga per internetą: < https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236>.

[77] 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti. OL L 194, 2016 7 19. [interaktyvu. Žiūrėta 2020 m. kovo 30 d.] Prieiga per internetą: <https://eur-lex.europa.eu/legal-content/lt/TXT/?uri=CELEX%3A32016L1148>.

duomenų apsaugos reikalavimus. Nustatant priemones, turėtų būti atsižvelgiama į BDAR, tačiau, teisė akte pateikiamos tik abstraktaus pobūdžio normos, numatančios apibrėžtį reikalavimams, tačiau nekonkretinančios ir nenurodančios galimas saugumo priemones. Šiuo atveju, reikėtų remtis ISO saugumo standartais, Europos Sąjungos kibernetinio saugumo agentūros (ENISA) bei priežiūros institucijos rekomendacijomis. Organizacinėmis duomenų saugumo priemonėmis laikomi organizacinio pobūdžio sprendimai, nustatantys darbo tvarką, atitinkamas procedūras, paskirstantys atsakomybę ar suteikiantys teises. Organizacinėms priemonėmis priskirtina[78]: a) duomenų saugumo politikos parengimas – duomenų valdytojas turi parengti politiką, kurioje būtų nustatoma informacinės saugos tvarka, b) vaidmenų paskirstymas – duomenų valdytojo darbuotojams turi būti labai aiškiai apibrėžta atsakomybė, už jų kompetencijai priskirtų duomenų tvarkymą, c) prieigos valdymo politikos parengimas – duomenų valdytojo darbuotojams turi būti suteiktos prieigos tik pagrįstos „būtina žinoti“ principu, d) keitimų valdymas – turi būti galimybė duomenų valdytojui atsekti visus atliktus pakeitimus bei identifikuoti darbuotojus, atlikusius pakeitimus, e) duomenų tvarkytojų įsipareigojimų užtikrinimas – duomenų valdytojas turi pareigą pasitelkti tik patikimus duomenų tvarkytojus, kurių saugumo lygis atitinka duomenų valdytojo užtikrinamo saugumo lygį, todėl prieš pradedant bendradarbiauti turi būti pasirašomas susitarimas, kuriuo apibrėžiamos duomenų tvarkymo sąlygos bei atsakomybė, f) saugumo incidentų valdymas – duomenų valdytojas turi apibrėžti procedūras, kurios turi būti atliktos, nustačius galimą duomenų saugumo pažeidimą, g) personalo konfidencialumo įsipareigojimai ir apmokymai – pavaldumo ryšiais su duomenų valdytoju susiję asmenys, turi būti įpareigoti saugoti bet kokius duomenis, tapusius jiems žinomais darbo funkcijų atlikimo metu, o taip pat turi būti reguliariai apmokomi saugumo užtikrinimo bei darbo su duomenimis apimtyje. Tai nėra baigtinis sąrašas organizacinių priemonių, kurių galėtų imtis duomenų valdytojas, tačiau tai pagrindinės sritys, kurioms turi būti skirtas dėmesys.

Duomenų valdytojui tenka visa atsakomybė, įskaitant darbuotojų netinkamus veiksmus. Tam, kad duomenų valdytojas galėtų reikalauti darbuotojų prisiimti atsakomybę už savo veiksmus, jis turi būti pasirūpinęs tinkama atitiktimi teisės aktų reikalavimams. Dėl to reikšminga, kad duomenų valdytojas tinkamai paruoštu darbuotojus ir šiuo atveju, organizuojant mokymus ir plečiant darbuotojų informuotumą bendradarbiaujama su

[78] Valstybinė duomenų apsaugos inspekcija. *Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams*, 2019 – 12 – 18, p. 8-17 [interaktyvus. Žiūrėta kovo 30 d.]. Prieiga per internetą:<https://vdai.lrv.lt/uploads/vdai/documents/files/VDAI_saugumo_priemoniu_gaires-2019-12-18.pdf.>.

duomenų apsaugos pareigūnu. Duomenų apsaugos pareigūnui užduotis stebėti darbuotojų pasirengimą nustatoma BDAR 39 str., norma.

Techninės saugumo priemonės, kurių turi imtis duomenų valdytojas apima informacinio saugumo erdvę. Techninėms saugumo priemonėms priskiriama[79]: a) prieigų valdymas – užtikrinama prieigų kontrolė prie informacinių sistemų, kuriose saugomi asmens duomenys, b) techninių žurnalų įrašų vedimas – saugos reikalavimas, leidžiantis stebėti naudotojų veiksmus, c) ryšių saugumo užtikrinimas – tinklo ir komunikacijos saugos kontrolė, d) atsarginių kopijų sistema – tai svarbiausias įrankis leidžiantis užtikrinti saugų duomenų atkūrimą ir darbo atstatymą, įvykus incidentui duomenų valdytojo organizacijoje, e) darbo mobiliaisiais ir nešiojamais įrenginiais valdymas – duomenų valdytojas turi pasirūpinti, kad darbuotojui dirbant nutolusiose nuo darbo vietose, būtų užtikrinama asmens duomenų apsauga, f) duomenų naikinimo, šalinimo užtikrinimas – šalinant asmens duomenis, turi būti užtikrinama galimybė atlikti naikinimą negrįžtamai, negali likti jokios galimybės jų atkurti. Kartu su techniniais sprendimais ne mažiau reikšminga užtikrinti fizinę saugą – apribotos bet kokios prieigos pašaliniams, rakinamos durys ar kitaip apsunkinamas asmenų patekimas į patalpas. Duomenų valdytojui labai svarbu parinkti tas priemones, kurios realiai padės užtikrinti duomenų saugą. Pažymėtina, jog duomenų apsaugos pareigūnui techninių žinių reikalavimas nėra keliamas ir jis neprivalo būti informacinių technologijų specialistas. Tačiau *soft law* šaltiniuose pateikiama nuomonė, jog duomenų apsaugos pareigūnui būtų vertinga turėti bent bazines žinias informacinių sistemų veikimo procesuose ir saugumo priemonių įvairovėje. Todėl įprastai duomenų apsaugos pareigūnas bendradarbiauja su organizacijos informacinių technologijų specialistu, siekiant įdiegti tinkamo lygio saugumo priemones. Ne tinkamai parinktos priemonės, kurios neužtikrina saugumo lygio, gali sąlygoti duomenų atskleidimą, teisės susipažinti su duomenimis, neturintiems asmenims, duomenų praradimą, kas daro įtaka konfidencialumo užtikrinimui.

Atsitikus duomenų apsaugos incidentui, kurio metu pažeidžiamas asmens duomenų konfidencialumas, prieinamumas ar vientisumas, gali būti padarytas labai neigiamas poveikis duomenų subjektams, todėl duomenų valdytojui kyla pareiga pranešti apie galimą pažeidimą Valstybinei duomenų apsaugos inspekcijai per 72 valandas nuo momento, kai sužinota apie įvykusį pažeidimą[80] bei nedelsiant informuoti duomenų subjektus, kurių duomenų saugumas buvo pažeistas[81]. Šie reikalavimai turi savo išimtis – galima nepranešti

[79] *ibidem*. p. 18-31
[80] BDAR 33 straipsnio 1 dalis
[81] BDAR 34 straipsnio 1 dalis

priežiūros institucijai ir duomenų subjektams apie įvykusį duomenų saugumo pažeidimą, jeigu jis nekelia pavojaus ar neigiamų padarinių duomenų subjektų teisėms ir laisvėms. Papildomos sąlygos, kai duomenų valdytojas gali neinformuoti duomenų subjekto, remiantis BDAR 34 str., 3 d., kai imtasi tinkamų saugumo priemonių, kai imtasi priemonių, kurios užtikrina, jog pažeidimas nepasikartos, kai duomenų subjektų informavimas reikalauja neproporcingai daug pastangų ir informacija pateikiama viešai. Visais kitais atvejais tiek priežiūros institucijai, tiek subjektui informacija pateikiama nedelsiant. Todėl duomenų valdytojas sužinojęs apie galimai įvykusį pažeidimą nedelsiant turėtų atlikti vidinį tyrimą. Vidinio tyrimo metu nustatoma, kokio kiekio duomenų saugumas galėjo būti pažeistas, kiek duomenų subjektų galėjo nukentėti, kokie pavojai gali kilti duomenų subjektams, dėl įvykusios asmens duomenų saugumo pažeidimo bei kitas reikšmingas pažeidimo aplinkybes. Duomenų valdytojui atlikus vidinį tyrimą, gautomis išvadomis pasidalinama su duomenų apsaugos pareigūnu, kuris padeda atlikti bendrą situacijos vertinimą bei nuspręsti, ar reikia pateikti pranešimą Valstybinei duomenų apsaugos inspekcijai bei, ar reikia informuoti duomenų subjektą.

Reglamentu duomenų apsaugos pareigūnui priskirtina pareiga bendradarbiauti su priežiūros institucija, dėl ko, pateikiant pranešimą apie pažeidimą pateikiami duomenų apsaugos, kaip kontaktinio asmens duomenys, tačiau asmens duomenų apsaugos teisė nedraudžia suderinti papildomų funkcijų atlikimą ir pažeidimų valdymą priskirti duomenų apsaugos pareigūno kompetencijai[82]. Tokiu atveju, duomenų apsaugos pareigūnas būtų atsakingas už tinkamą incidentų valdymo procesą. Bendruoju atveju, pranešimą pasirašo duomenų valdytojas ir pateikia duomenų apsaugos pareigūnas. Tolesnio tyrimo metu Valstybinė duomenų apsaugos inspekcija bendradarbiauja su duomenų apsaugos pareigūnu.

Kaip ir visi kiti klausimai asmens duomenų apsaugos teisėje, techninio ir organizacinio saugumo priemonės parenkamos bendradarbiaujant duomenų valdytojui ir duomenų apsaugos pareigūnui, tačiau vertinant atsakomybės klausimą, įgyvendinant informacinių sistemų saugumo priemones, atsakymą pateikia BDAR 24 str. Šio straipsnio 1 dalyje nurodoma, jog pats duomenų valdytojas atsakingas už jo atliekamo duomenų tvarkymo saugumo priemonių įgyvendinimą bei pažeidimų valdymo proceso užtikrinimą ir teisinė atsakomybė už pranešimą apie pažeidimą tenka duomenų valdytojui, nepriklausomai nuo to, kas turi atlikti šiuos veiksmus organizacijoje[83]. Atitinkamai vertinant duomenų apsaugos

[82] ES 29 str. darbo grupės 2018 m. vasario 6 d. *Gairės dėl pranešimo apie asmens duomenų saugumo pažeidimą pagal Reglamentą* (ES) 2016/679 Nr.WP250, p. 29 [interaktyvus. Žiūrėta 2020 m. kovo 20 d.]. Prieiga per internetą: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052>.
[83] *ibidem*. p. 15

pareigūno atsakomybę šioje apimtyje, pastebėtina tai, jog duomenų apsaugos pareigūnui nesuteikiama kompetencija spręsti techninio pobūdžio klausimus, todėl saugumo priemones bendradarbiaudamas su duomenų apsaugos pareigūnu parenka duomenų valdytojo informacini išteklių darbuotojas. Šiuo aspektu duomenų apsaugos pareigūnas pirmiausiai atsako už tinkamą incidentų valdymą, komunikaciją su priežiūros institucija bei duomenų subjektu, kurie gali kreiptis papildomais klausimais, dėl to, kad būtent duomenų apsaugos pareigūnas yra tarpininkas.

3.1.4. Atsakomybės pasiskirstymas už duomenų subjektų teisių įgyvendinimą

Duomenų valdytojui siekiant užtikrinti atitiktį duomenų apsaugos teisės normoms, turi būti ne tik atliktas didelis darbas organizacijos viduje, užtikrinant teisėtus duomenų tvarkymo procesus, tačiau taip pat turi būti tinkamai komunikuojama su išore. Duomenų apsaugos teisės normos suteikia duomenų subjektui teises, kurias jis gali įgyvendinti kreipiantis į duomenų valdytoją. Atitinkamai duomenų valdytojui kyla pareiga, įgyvendinti duomenų subjektų teises bei valdyti gaunamus prašymus.

Duomenų subjektams suteikiamos teisės leidžia kontroliuoti duomenų valdytoją bei reikalauti tinkamo duomenų tvarkymo proceso įgyvendinimo. Pirmiausia, duomenų subjektas turi teisę būti informuotas apie duomenų tvarkymą. Duomenų valdytojas įgyvendindamas skaidrumo principą, duomenų rinkimo metu, privalo pateikti duomenų subjektui pilnos apimties informaciją apie planuojamą atlikti duomenų tvarkymą. Pagrindinis tikslas – sudaryti duomenų subjektui galimybę valdyti duomenų sklaidą. Todėl, asmuo turi būti informuojamas apie tai, kas atlieka duomenų tvarkymą, kokie tikslai, kokiais teisiniai pagrindais, kam bus perduoti pateikti duomenys, duomenų apsaugos pareigūno kontaktai, taip pat reikšminga informuoti ir tais atvejais, kai jo duomenys, gaunami iš kitų šaltinių ar trečiųjų asmenų[84], taip pat ir saugumo pažeidimo atvejais[85] ar kitais atvejais, kai pasikeičia anksčiau pateikta informacija. Duomenų valdytojas kartu su duomenų apsaugos pareigūnu parenka būdus, kuriais duomenų subjektas bus informuojamas ir aiškia vidutiniam vartotojui kalba suformuluoja pranešimo tekstą. Spręsdamas dėl duomenų subjektui teikiamos informacijos, duomenų valdytojas turi įvertinti atliekamų duomenų tvarkymo operacijų ypatumus[86]. Dėl šios priežasties duomenų valdytojui reikalinga duomenų apsaugos pareigūno pagalba, kuris remdamasis savo

[84] BDAR 14 straipsnis
[85] BDAR 34 straipsnis
[86] ZALESKIS, Julius. *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: Registrų centras, 2019, p. 167.

žiniomis gali padėti įvertinti duomenų tvarkymo operacijas. Teismų praktikoje jau žinomi atvejai, kuomet duomenų subjektų neinformavimas apie atliekamą duomenų tvarkymą, net jei duomenys tvarkomi siekiant nustatyti nusikalstamus veiksmus, nėra laikomas teisėtu[87], nes tai tiesiogiai sąlygoja asmens teisės į privatumą apsaugos ribas.

Duomenų subjektas turi teisę susipažinti su jo tvarkomais duomenimis pagal BDAR 15 str. Šiuo aspektu, duomenų valdytojui tenka ne tik pareiga patenkinti duomenų subjekto pateiktą prašymą, tačiau taip pat, įsitikinti asmens tapatybę, prieš teikiant jam bet kokią informaciją apie jo duomenis ar duomenų tvarkymą. BDAR preambulės 63 punkte atkreipiamas dėmesys į tai, kad įgyvendinant šią teisę, duomenų valdytojas turi užtikrinti, kad nebūtų pažeistos trečiųjų asmenų teisės. Pavyzdys galėtų būti vaizdo stebėjimo duomenys – pateikiant vaizdo įrašą susipažinimui, jame gali būti matomi ir kiti duomenų subjektai. Duomenų valdytojas yra atsakingas šiuo atveju, tiek už subjekto teisių įgyvendinimą, tiek už kitų duomenų subjektų duomenų saugumo užtikrinimą.

Kita duomenų subjekto teisė yra labai palanki ir pačiam duomenų valdytojui. Tai teisė reikalauti ištaisyti duomenis. Pats duomenų valdytojas turi pareigą vadovautis tikslumo principu, kurio prasmė yra tik teisingų ir tikslių duomenų tvarkymas. Todėl įgyvendinant šią duomenų subjekto teisę gaunama abipusė nauda.

Remdamasis subjektyviomis aplinkybėmis, duomenų subjektas gali nuspręsti nutraukti duomenų tvarkymo veiksmus ir pareikalauti duomenų valdytojo ištrinti visus su juo susijusius duomenis. Kitaip ši teisė vadinama „teise būti pamirštam“. Tačiau neteisinga būtų vertinti šios teisės kai absoliučios. Pasinaudoti šia teise duomenų subjektas gali apibrėžtais atvejais[88]: kai duomenys nebėra reikalingi, tikslams, kuriais buvo renkami, kai atšaukiamas duotas sutikimas, kuris yra vienintelis duomenų tvarkymo pagrindas, kai nesutinkama su duomenų tvarkymu, kai duomenys tvarkomi neteisėtai, kai duomenys turi būti ištrinti remiantis teisine prievole, kai duomenys surinkti vaiko sutikimo pagrindu. Dėl šių aplinkybių duomenų valdytojas turi atidžiai įvertinti gautą prašymą ir jo atitiktį nustatytoms aplinkybėms.

Atitinkamais atvejais, kai užginčijamas duomenų tikslumas ar, kai nustatoma, kad duomenų tvarkymas yra neteisėtas, bet duomenų subjektas nesutinka, kad duomenys būtų ištrinti, ar, kai duomenų tvarkymas nereikalingas duomenų valdytojui, tačiau reikalingas duomenų subjektui siekiant pareikšti teisinį reikalavimą, ar, kai duomenų subjektas

[87] Europos Žmogaus Teisių Teismas (Didžioji kolegija). 2019 m. spalio 17 d. sprendimas byloje *Lopez Ribalda ir kiti prieš Ispaniją* (paraiškos Nr. 1874/13 ir 8567/13) [interaktyvus. Žiūrėta 2020 m. kovo 25 d.]. Prieiga per internetą:<https://hudoc.echr.coe.int/fre#{%22fulltext%22:[%22lopez%20ribalda%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-197098%22]}>.
[88] BDAR 17 straipsnis

papriešTaravo duomenų tvarkymui, duomenų subjektas turi teisę apriboti duomenų tvarkymą. Šio proceso tikslas – sustabdyti duomenų tvarkymo veiksmus, kol bus priimti atitinkami sprendimai. Kokiu būdu duomenų valdytojas gali įgyvendinti šią subjekto teisę, remiantis teisinę praktika galėtų parekomenduoti duomenų apsaugos pareigūnas.

Nusprendęs pakeisti duomenų valdytoją, duomenų subjektas turi teisę į duomenų perkeliamumą. Ši teisė leidžia tiesiogiai persiųsti asmens duomenis iš vieno valdytojo kitam. Tačiau, reikšminga atkreipti dėmesį į sąlygas, kurioms esant galima pasinaudoti šia teise. Tam, kad asmens duomenys galėtu būti perkelti kitam duomenų valdytojui, jie turi būti tvarkomi sutikimo ar sutarties pagrindu ir privalo būti tvarkomi automatizuotomis priemonėmis. Tai reiškia, jog nesant šių aplinkybių visumos, šia teise negali būti naudojamasi. Duomenų valdytojas turi iškomunikuoti duomenų subjektui šias aplinkybes, siekiant išvengti keblumų. Duomenų subjektai įprastai mano, jog asmens duomenų apsaugos teisės, jiems suteikiamos teisės yra absoliučios ir ne retai ginčai kyla jau šiame lygyje.

Įgyvendinant duomenų subjekto teisę nesutikti, duomenų valdytojas turi nutraukti duomenų tvarkymą, kuris paremtas konkrečiais interesais (duomenų valdytojo, trečiosios šalies ar viešojo). Šiuo atveju, turėtų būti įvertinta tokių teisinių pagrindų pusiausvyra su duomenų subjekto turimomis teisėmis. Dr. J. Zaleskis atkreipia dėmesį, kad ši subjekto teisė gali būti vertinama trimis aspektais: kai duomenų tvarkymas grindžiamas viešosios valdžios funkcijų atlikimo pagrindu, kai duomenų tvarkymas grindžiamas teisėtu duomenų valdytojo ar trečiosios šalies interesu, kai duomenų subjektas nesutinka su profiliavimu, kai jis grindžiamas minėtais pagrindais[89]. Šios teisės nėra duomenų subjektams itin gerai suprantamos ar žinomos, todėl įprastai sulaukia mažiau dėmesio. Nepaisant to, duomenų valdytojo atsakomybės apimčiai tai jokios įtakos nedaro.

Duomenų subjektų teisių įgyvendinimo proceso valdymas yra duomenų valdytojo prerogatyva. Jis paskiria atsakingus asmenis, kurie administruoja gautus prašymus. Duomenų apsaugos pareigūnui nėra numatytos tiesioginės pareigos užtikrinti subjekto teisių įgyvenimą, tačiau jis turėtų stebėti procesą ir pateikti rekomendacijas, pagal aktualius teisės aktus, kas suponuoja jo dalyvavimą duomenų subjektų teisių įgyvendinimo procese. Pažymėtina ir tai, kaip jau minėta anksčiau, kad duomenų apsaugos pareigūnas yra kontaktinis asmuo tiek Priežiūros institucijai, tiek duomenų subjektams. Todėl, pateikiant jo kontaktus internetinėje organizacijos svetainėje, tikėtina, kad prašymai taip pat bus

[89] ZALESKIS, Julius. *Duomenų apsaugos pareigūno veiklos pagrindai pagal ES bendrąjį duomenų apsaugos reglamentą*. Teisė, t. 104, p.179-180. [interaktyvus. Žiūrėta balandžio 1 d.]. Prieiga per internetą: <https://www.zurnalai.vu.lt/teise/article/view/10851/8986>.

nukreipti nurodytais kontaktais. Taip pat, primintina ir tai, kad asmens duomenų apsaugos teisė nedraudžia susitarti dėl papildomų paslaugų, todėl duomenų valdytojas suderinęs šį klausimą su duomenų apsaugos pareigūnu gali paskirti jį atsakingu už duomenų subjektų prašymų administravimą. Šiuo aspektu svarbu tai, kad būtų susitarta, kadangi teikti nurodymus duomenų valdytojas negali, siekiant užtikrinti visišką duomenų apsaugos pareigūno autonomiją.

Nepaisant to, kas atlieka veiksmus, paskirtas darbuotojas ar duomenų apsaugos pareigūnas, reikšminga yra tai, jog atsakomybė išlieka duomenų valdytojui, kuriam ir suteikiamos pareigos įrodyti, jog organizacijoje laikomasi asmens duomenų apsaugos teisės reikalavimų. Jis atsakingas ne tik už prašymų įgyvendinimą ar įrodymus, jis taip pat atsakingas už tinkamą asmenų identifikavimą, siekiant išvengti neteisėto asmens duomenų atskleidimo.

Valstybinės duomenų apsaugos inspekcijos duomenimis[90] 7 proc. 2019 m. Valstybinei duomenų apsaugos inspekcijai pateiktų skundų susiję su teisių įgyvendinimu. Tai reiškia, kad dalis duomenų valdytojų nesiima visų resursų siekiant užtikrinti duomenų apsaugos teisės normų veikimą visais lygiais, tiek organizacijos viduje, tiek komunikacijoje su išorės subjektais.

Tiesioginė pareiga užtikrinti duomenų subjektų teisių įgyvendinimą tenka duomenų valdytojui, kuris privalo veikti pagal asmens duomenų tvarkymo principus. Duomenų apsaugos pareigūno indėlis šiuo klausimu yra toks, kaip ir bet kurioje kitoje duomenų apsaugos teisės srityje – stebėti, ar viskas vyksta pagal keliamus reikalavimus bei konsultuoti ir nukreipti reikiama linkme. Tačiau šiuo atveju, pažymėtina, jog duomenų apsaugos pareigūnas yra tiesioginis tarpininkas tarp duomenų subjektų ir duomenų valdytojo, todėl padeda įgyvendinti duomenų subjektų teises. Organizacijai nepaskyrus duomenų apsaugos pareigūno duomenų subjekto teisių įgyvendinimo procesas būtų labiau komplikuotas. Tačiau tik pareigos suponuoja atsakomybės atsiradimą ir šiuo atveju, būtent duomenų valdytojas yra atsakingas už subjektų teisių įgyvendinimą.

3.2. Atsakomybė už duomenų apsaugos teisės pažeidimus

Pagrindinis asmens duomenų apsaugos teisės tikslas yra užtikrinti duomenų subjektų teisių saugą ir leisti duomenų subjektams valdyt jų duomenų sklaidą. Todėl organizacijos, kuri

[90] Valstybinės duomenų apsaugos inspekcijos viešoji konsultacija*: Bendrasis duomenų apsaugos reglamentas. Ginama teisė susipažinti su savo asmens duomenimis*. [interaktyvu. Žiūrėta 2020 m. balandžio 3 d.]. Prieiga per internetą: <https://vdai.lrv.lt/lt/naujienos/bendrasis-duomenu-apsaugos-reglamentas-ginama-teise-susipazinti-su-savo-asmens-duomenimis>.

atlieka duomenų tvarkymą atitiktis teisės aktų reikalavimams yra reikšmingas aspektas, nepaisant to, kad daugeliui duomenų valdytojų iki šiol atrodo, jog tai nėra didelės svarbos tema. Šio aspekto reikšmingumas atsiskleidžia vertinant asmens duomenų apsaugos teisės koreliaciją su teise į privatumą. Šią nuomonę patvirtina I. Petraitytė teigdama, jog asmens duomenų apsauga ir teisė į privatų gyvenimą yra neatsiejamos[91]. Autorės teigimu tai sąlygoja du aspektai: pirma duomenų apsaugos teisinės nuostatos pagal turinį yra skirtos užtikrinti privatumo apsaugą, antra, duomenų apsauga užtikrinama ta apimtimi, kiek yra būtina asmens informacinio privatumo saugumo užtikrinimui. 29 straipsnio darbo grupės teigimui esminė duomenų apsaugos sistemos sąlyga yra nuoseklus duomenų apsaugos taisyklių laikymasis[92]. Duomenų valdytojas įpareigotas rūpestingai vykdyti jam priskirtas pareigas, kadangi duomenų saugumo pažeidimas turės labai didelės reikšmės ne tik duomenų saugumui bet ir duomenų subjekto privatumui.

Duomenų valdytojui įgyvendinti keliamus duomenų teisės reikalavimus padeda duomenų apsaugos pareigūnas. Vienais atvejais jis paskiriamas privalomai, kitais atvejais savanoriškai, tačiau ir vienu, ir kitu atveju, jam taikomos tos pačios sąlygos bei priskiriamos tos pačios užduotys. Pagrindinė užduotis nuolat stebėti ir konsultuoti duomenų valdytoją bet kokiais klausimais asmens duomenų apsaugos apimtyje. Taip pat jis padeda įgyvendinti darbuotojų apmokymo procesus bei konsultuoja dėl poveikio duomenų apsaugai vertinimo atlikimo. Reikšminga yra pažymėti, jog būtent duomenų apsaugos pareigūnas, pagal jam keliamus reikalavimus, turi ekspertines žinias, leisiančias jam interpretuoti ir aiškinti teises normas, ką užtikrinti duomenų valdytojui vienam yra tikrai sudėtinga.

Vertinant tai, jog duomenų valdytojas ties organizacijos atitiktimi dirba bendradarbiaudamas su duomenų apsaugos pareigūnu, ne retai, kyla daug neaiškumų dėl atsakomybės pasidalijimo. Itin reikšmingas šis klausimas, kai kalbama ne tik apie atitiktį duomenų apsaugos teisės normoms, tačiau, kai kalbama apie atsakomybę jau nustačius duomenų apsaugos teisės pažeidimą. Siekiant išspręsti šį klausimą reikėtų teisės normas vertinti pagal jų paskirtį.

Vertinant asmens duomenų teisinės apsaugos normas, pastebėtina, kad centrinis subjektas į kurį nukreiptos pareigos dėl duomenų apsaugos atitikties yra duomenų

[91] PETRAITYTĖ, Ilona. *Asmens duomenų apsauga ir teisė į privatų gyvenimą*. Teisė, 2011, 800, p. 166. [interaktyvu. Žiūrėta 2020 m. balandžio 3 d.]. Prieiga per internetą: <https://www.journals.vu.lt/teise/article/view/158/124>.

[92] ES 29 str. darbo grupės 2017 m. spalio 3 d. *Administracinių baudų taikymo ir nustatymo pagal Reglamentą 2016/679 gairės* Nr. WP253, p. 4 [interaktyvu. Žiūrėta balandžio 5 d.] Prieiga per internetą: < https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237>.

valdytojas. Pagrindine duomenų valdytojo statuso pasekme laikoma atsakomybė[93]. Jis turi vykdyti duomenų tvarkymą vadovaujantis nustatytų principų (BDAR 5 str.), jis turi užtikrinti, kad duomenys tvarkomi teisėtais pagrindais (BDAR 6 str.), jis užtikrina tinkamas saugumo priemones (BDAR 32 str.), jis užtikrina duomenų apsaugos pareigūno paskyrimą (BDAR 37 str.), jis atlieka vertinimą, dėl galimo pavojaus duomenų subjektų teisėms ir laisvėms (BDAR 35 str.), jis įgyvendina duomenų subjektų teises (BDAR 13 – 22 str.). Atitinkamai vykdant pareigas, sąlygojama ir atsakomybė, kuri taikoma duomenų valdytojui (BDAR 24 str.).

Visame šiame procese duomenų apsaugos pareigūnas yra pagalbininkas, kuris turi kompetenciją suprasti duomenų apsaugos teisės reikalavimus. Žinoma, jam BDAR 39 str., pagrindu priskiriamos užduotis, kurias jis turi vykdyti, tačiau jam nesuteikiama sprendimo teisė, kuri sąlygotų atsakomybės atsiradimą ir jo tiesioginės pareigos apribojamos pagalba aiškinant ir taikant duomenų teisės normas bei priežiūra normų atitikčiai. Tačiau vertinant duomenų apsaugos pareigūno atsakomybę reikšminga nepamiršti, jog duomenų apsaugos pareigūnas negali būti baudžiamas už netinkamą pareigų vykdymą. Dr. J. Zaleskis savo monografijoje[94] teigia: „*Atitikties priežiūra nereiškia, kad duomenų apsaugos pareigūnas yra asmeniškai atsakingas už reguliavimo pažeidimus*.“ Tokią nuomonę išsako ir 29 straipsnio darbo grupė[95], nurodydama, jog tiek reikalavimų užtikrinimas, tiek įrodymų pateikimas yra duomenų valdytojo pareiga ir atsakomybė.

Netinkamai įgyvendinami teisė aktų reikalavimai – duomenų tvarkymo principų ir teisėtų pagrindų nesilaikymas ar parinktos saugumo priemonės neatitinka galimo pavojaus lygio, ar neįgyvendinamos subjektų teisės ir kt., sąlygoja pažeidimų atsiradimą. Pažeidimai duomenų apsaugos teisėje gali turėti rimtas pasekmes duomenų subjektams, gali būti pavogta tapatybė, pakenkta reputacijai, atskleisti konfidencialūs duomenys ar net galėtų būti padarytas kūno sužalojimas. Dėl šių aplinkybių ir asmens teisių užtikrinimo svarbos BDAR 82 str., įtvirtina subjekto teisę į kompensaciją, kai yra nustatyta žala. Reglamentas nustato, kad bet kokia, duomenų subjekto patirta žala, turi būti atlyginama duomenų valdytojo. Vienintelė išimtis, kuomet duomenų valdytojas gali būti atleistas nuo atsakomybės, yra, kuomet pateikiami įrodymai, jog jis nėra atsakingas už atsiradusią žalą. Šios išimties apimtyje galima būtų vertinti galimą duomenų apsaugos pareigūno

[93] Europos duomenų apsaugos vadovas. 2014 m. p. 48 [interaktyvu. Žiūrėta 2020 m. balandžio 5 d.]. Prieiga per internetą: <https://www.echr.coe.int/Documents/Handbook_data_protection_LIT.pdf
[94] ZALESKIS, Julius. *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: Registrų centras, 2019, p.224
[95] ES 29 str. darbo grupės 2017 m. balandžio 5 d. *Duomenų apsaugos pareigūnų gairės* Nr. WP 243, p. 28 [interaktyvus. Žiūrėta balandžio 5 d.]. Prieiga per internetą: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048>.

atsakomybę už atsiradusią žalą. Viena dažniausių duomenų saugumo pažeidimo priežasčių yra žmogiškasis faktorius. Todėl neteisinga būtų vertinti, jog duomenų valdytojas atsakingas už neteisėtus darbuotojo ar partnerio veiksmus, tačiau vien pranešimas, kad duomenų valdytojas nėra kaltas, nėra pakankamas. Brendan Van Alsenoy teigia, jog turi būti įrodyta: pažeidimo atsiradimas, priežastinis ryšys su žala ir duomenų valdytojo kaltės nebuvimas[96].

Atsakomybės pagrindas kyla iš susiklosčiusio teisinio santykio tarp duomenų valdytojo ir duomenų apsaugos pareigūno. Atveju, kai duomenų valdytojas patiria žalą dėl neteisėtų duomenų apsaugos pareigūno veiksmų ar netinkamo sutarties vykdymo, jam gali būti taikoma atsakomybė už sukeltą žalą. Kaip jau minėta anksčiau, duomenų apsaugos pareigūnu gali būti paskirtas duomenų valdytojo darbuotojas. Tokiu atveju, atsakomybės pagrindu bus laikytinas Lietuvos Respublikos darbo kodeksas (toliau – DK), pvz.: DK 154 str., numato atvejus, kuomet darbuotojas privalo atlyginti visą žalą, įstatyme numatytais atvejais. Iliustruojant situaciją, galima būtų pateikti atvejį, kuomet nesilaikoma konfidencialumo įsipareigojimų, dėl ko atsiranda duomenų saugumo pažeidimas. Kitu atveju, jeigu duomenų apsaugos pareigūnu paskiriamas išorės partneris, tuomet bendradarbiavimo pagrindu laikoma paslaugų teikimo sutartis ir jo atsakomybė vertintina Lietuvos Respublikos civilinio kodekso (toliau – CK) apimtyje. Dėl netinkamo sutarties vykdymo patyrus žalą, duomenų valdytojas gali reikalauti nuostolių atlyginimo. Šiuo atveju, remiantis CK 6.295 str., duomenų valdytojas turės įrodyti, jog dėl netinkamai teikiamų paslaugų, jam atsirado nuostoliai.

Duomenų saugumo pažeidimo vertinimas duomenų valdytojo atžvilgiu tenka priežiūros institucijai. Skiriant baudą, 29 straipsnio darbo grupės nuomone[97], turi būti vertinamos visų aplinkybių visuma. Visų pirma vertinamas *pažeidimo pobūdis, sunkumas ir trukmė* (BDAR 83 str., 2 d.). Jeigu incidentą galimą klasifikuoti kaip „nedidelį pažeidimą“ arba (atvejais, kai duomenų valdytojas fizinis asmuo) duomenų valdytojas nėra pajėgus sumokėti baudą, vietoj šios priemonės, gali būti pareikštas papeikimas. Turi būti kompleksiškai įvertinamas tiek pažeidimo pobūdis, tiek laikotarpis, kurį tęsėsi pažeidimas, tiek priemonės, kurių buvo imtasi ir kt.

[96] VAN ALSENOY, Brendan. *Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation,* 7. 2016. JIPITEC 271 para 15, p. 276 [interaktyvu. Žiūrėta 2020 m. balandžio 18 d.]. Prieiga per internetą: < https://www.jipitec.eu/issues/jipitec-7-3-2016/4506/van_alsenoy_liability_under_eu_data_protection_law_jiptec_7_3_2016_271.pdf>.

[97] ES 29 str. darbo grupės 2017 m. spalio 3 d. *Administracinių baudų taikymo ir nustatymo pagal Reglamentą 2016/679 gairės* Nr. WP253, p. 10 [interaktyvu. Žiūrėta balandžio 5 d.] Prieiga per internetą:<https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237>.

Sekantis vertintinas aspektas yra *tyčia, ar aplaidumas*. Reikšminga nustatyti ar pažeidimas padaryta sąmoningai ar pažeidimas atsirado dėl neatsargumo, neturint intencijos sukelti incidentą. Duomenų valdytojo pasiteisinimai ribotais ištekliais nebus vertinami, kadangi tai duomenų valdytojo pareiga pasitelkti rizikos lygį atitinkančius išteklius. Atitinkamai tyčiniai pažeidimai vertinami, kaip sunkesni, kas sąlygoja didesnės baudos galimybę[98]. Sušvelninti savo padėti duomenų valdytojas gali, jeigu *ėmėsi bet kokių veiksmų, kurie leistų sumažinti duomenų subjektų patirtą žalą*. Nustačius pažeidimo faktą, turi būti imamasi bet kokių priemonių, kurios sudarytų galimybę sumažinti galimus padarinius. Tokį duomenų valdytojo elgesį turėtų įvertinti priežiūros institucija nustatant baudos dydį.

Tyrimo atveju, priežiūros institucijai siekiant pilna apimtimi įvertinti situaciją, bus peržiūrimas duomenų valdytojo *atsakomybės lygis, įgyvendinant technines ir organizacines priemones*. Vertinant šį aspektą remiamasi „gerosios patirties“ būdais, atsižvelgiant į sektorių, kuriame veikia duomenų valdytojas. Ne mažiau reikšmingos yra aplinkybės ar buvo *anksčiau nustatytų duomenų valdytojo pažeidimų* bei kaip pasireiškia *bendradarbiavimas su priežiūros institucija*. Šios aplinkybės charakterizuoja duomenų valdytoją bei parodo jo suinteresuotumą įtraukti korekcijas į savo vykdomą veiklą. Jeigu nustatoma, jog tai pakartotinis pažeidimas, vertinama *ar buvo laikytasi paskirtų priemonių.*

Vienas svarbiausių aspektų, *asmens duomenų kategorijos, kurioms atsirado poveikis, dėl įvykusio pažeidimo.* Jei tai jautri informaciją apie duomenų subjektą, pvz.: specialieji duomenys, tokiu atveju tai neigiamai turėtų paveikti duomenų valdytojo vertinimą, taip pat, kaip ir informacija *kokiu būdu priežiūros institucija sužinojo apie pažeidimą*, kadangi šis aspektas yra rodiklis, ar duomenų valdytojas vykdo jam duomenų apsaugos teisės priskirtas pareigas. Jeigu tyrimo metu nustatomos kitos švelninančios ar sunkinančios atsakomybę aplinkybes, jos taip pat atidžiai įvertinamos. Visų nurodytų aplinkybių visumos vertinimas leidžia parinkti duomenų valdytojo atsakomybei proporcingas sankcijas.

BDAR įtvirtintas baudų mechanizmas nustato baudas, kurių dydis gali siekti iki 20 000 000 EUR arba, jeigu pažeidimas skiriamas įmonei, gali būti nuspręsta paskirti iki 4 % ankstesnių finansinių metų bendros metinės pasaulinės apyvartos. Baudų skyrimo praktika pradėta taikyti jau per pirmąjį BDAR galiojimo pusmetį. Pirmoji Europoje žinoma bauda fiksuojama Portugalijoje. Priežiūros institucija paskyrė 400 000 EUR baudą ligoninei dėl trijų reglamento reikalavimų pažeidimų. Antroji bauda paskirta Vokietijoje ir baudos dydis 20 000 EUR. Lietuvoje pirmoji bauda priežiūros institucijos paskirta po metų nuo

[98] *ibidem*. p. 11

reglamento įsigaliojimo ir baudos dydis sudarė 61 500 EUR. Bauda skirta UAB „MisterTango“, dėl asmens duomenų saugumo pažeidimo mokėjimo iniciavimo paslaugų sistemoje bei dėl nepateikto pranešimo Valstybinei duomenų apsaugos inspekcijai, apie bendrovėje įvykusį saugumo incidentą.

Duomenų valdytojo statusas tiesiogiai sąlygoja teisinę atsakomybę laikytis duomenų apsaugos teisėje numatytų pareigų [99]. Duomenų valdytojas yra vienintelis subjektas, kuriam duomenų apsaugos teisė suteikia kompetenciją nustatyti duomenų tvarkymo tikslus ir būdus. Atitinkamai pradėjus duomenų tvarkymo procesus atsiranda pareigos ir atsakomybė. Visa atsakomybė už netinkamą pareigų vykdymą, kurio pasėkoje nustatytas duomenų apsaugos teisės pažeidimas tenka duomenų valdytojui. Net ir atvejais, kai paskirtas duomenų apsaugos pareigūnas, atsakomybe nėra dalijamasi, kadangi duomenų apsaugos pareigūnas negali būti baudžiamas už netinkamą užduočių įvykdymą. Atsakomybė taikoma duomenų apsaugos pareigūnui tik tuomet, kai nustatoma asmeninė kaltė, dėl kurios duomenų valdytojas patyrė žalą. Tokiu atveju duomenų apsaugos pareigūnas turi atlyginti duomenų valdytojo nuostolius.

[99] Europos duomenų apsaugos vadovas. 2014 m. p. 48 [interaktyvu. Žiūrėta 2020 m. balandžio 5 d.]. Prieiga per internetą: <https://www.echr.coe.int/Documents/Handbook_data_protection_LIT.pdf

IŠVADOS

1. Duomenų valdytoju laikomas fizinis ar juridinis asmuo, kuris turi galios nustatyti duomenų tvarkymo tikslus ir priemones, kuriomis tų tikslų bus siekiama. Duomenų valdytojas yra pagrindinė duomenų apsaugos teisės figūra, kadangi jis sudaro terpę duomenų apsaugos reguliavimui veikti, jam keliami reikalavimai duomenų apsaugos normų atitikties įgyvendinimui. Pagrindinė duomenų valdytojo pareiga yra užtikrinti tinkamą duomenų subjekto jam patikėtų asmens duomenų apsaugą ir jo, kaip duomenų subjekto, teisių įgyvendinimą.
2. Duomenų apsaugos pareigūnas yra BDAR ypatybė ir centrinė duomenų valdymo teisinio reglamentavimo modelio „figūra“, kurios paskirtis padėti užtikrinti organizacijos atitiktį BDAR. Jam keliami reikšmingi profesinių, ekspertinių ir praktinių žinių reikalavimai Tačiau duomenų apsaugos pareigūno funkcijos.
3. Duomenų apsaugos pareigūno pareigybė yra specifinė ir reikalauja kitokio požiūrio nei bet kokia kita organizacijos pozicija. Organizacijai kyla atsakomybė sudaryti galimybę duomenų apsaugos pareigūnui veikti autonomiškai, kas leidžia išlaikyti objektyvumą vertinat organizacijos pasirengimą bei teikiant rekomendacijas dėl reikiamų priemonių tinkamai atitikčiai užtikrinti. Autonomija, be kita ko, sąlygoja duomenų apsaugos pareigūno atsakomybę, už jo teikiamas rekomendacijas ir konsultacijas.
4. Duomenų valdytojas ir duomenų apsaugos pareigūnas bendradarbiauja užtikrinant organizacijos atitiktį asmens duomenų apsaugos teisės aktų reikalavimams. Duomenų apsaugos pareigūnas remiasi turimomis teorinėmis ir praktinėmis žiniomis teikiant duomenų valdytojui rekomendacijas ir stebi atliekamus duomenų tvarkymo procesus. Kompetencija priimti sprendimus, kaip bus įgyvendinamos teisės normos bei vadovautis ar ne duomenų apsaugos pareigūno rekomendacija priima duomenų valdytojas, dėl to jam taikomos atsakomybės už atitiktį asmens duomenų teisei sąlygos.
5. Asmens duomenų apsaugos teisės pažeidimų atsiradimą sąlygoja netinkamai įgyvendinami duomenų apsaugos reikalavimai. Atsakomybė už atitiktį teisės normoms taikoma duomenų valdytojui, todėl atsakomybė už nustatytus duomenų apsaugos pažeidimus pilna apimtimi taip pat tenka subjektui, priimančiam sprendimus dėl saugumo priemonių įgyvendinimo duomenų valdytojui, nebent duomenų valdytojas pateikia įrodymus, jog pažeidimas atsirado ne dėl jo kaltės.

6. BDAR neįtvirtina duomenų apsaugos pareigūno atsakomybės, priešingai, nustatoma, kad duomenų apsaugos pareigūnas negali būti baudžiamas už užduočių atlikimą, tačiau yra išimtinių atvejų. Nustačius, jog asmens duomenų apsaugos teisės pažeidimas įvyko ne dėl duomenų valdytojo kaltės bei įrodoma duomenų apsaugos pareigūno kaltė, pvz.: konfidencialumo pažeidimas, jam atsakomybė taikoma pagal nacionalinės teisės normas. Jeigu duomenų apsaugos pareigūno pareigas eina duomenų valdytojo darbuotojas, jo atsakomybė bus nagrinėjama DK ribose, kitu atveju, jeigu duomenų apsaugos pareigūnas yra išorinis partneris ir veikia sutarties pagrindu, jo atsakomybės ribas nustatys CK normos.

ŠALTINIŲ SĄRAŠAS

Norminiai teisės aktai:

1. 1950 m. lapkričio 4 d. Europos žmogaus pagrindinių teisių ir laisvių konvencija. Valstybės žinios, 1995, Nr. 40-987. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.19841.
2. 1981 m. Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (Konvencija Nr. 108). Valstybės žinios, 2001, nr. 32-1059. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.129872
3. Sutartis dėl Europos Sąjungos veikimo (suvestinė redakcija). OL C 202, 2016; Prieiga per internetą: https://eurlex.europa.eu/legalcontent/LT/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN.
4. Europos Sąjungos pagrindinių teisių chartija. OL C 326, 2012. Prieiga per internetą: https://eurlex.europa.eu/legalcontent/LT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR.
5. 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti. OL L 194, 2016 7 19. Prieiga per internetą: https://eur-lex.europa.eu/legal-content/lt/TXT/?uri=CELEX%3A32016L1148.
6. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OJ L 119, 4 5 2016. Prieiga per internetą: https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32016R0679.
7. 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmens duomenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. OJ L 281, 23 11 1995. Prieiga per internetą: https://eur-lex.europa.eu/legal-content/lt/TXT/?uri=CELEX%3A31995L0046.
8. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, TAR, 2018-07-11, Nr. I- 11733. Prieiga per internetą: https://eseimas.lrs.lt/portal/legalAct/lt/TAD/bc0837f27f9511e89188e16a6495e98c.
9. Lietuvos Respublikos elektroninių ryšių įstatymas, Valstybės žinios, 2004-04-30, Nr. 692382. Prieiga per internetą: https://www.etar.lt/portal/lt/legalAct/TAR.82D8168D3049/hlbWSfsMOw.

Specialioji literatūra:

10. ZALESKIS, Julius. Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Vilnius: Registrų centras, 2019.
11. ZALESKIS, Julius, ES bendrasis duomenų apsaugos reglamentas: reikšmė duomenų apsaugos teisei. Teisė, 2017, t. 103., p. 45-54. Prieiga per internetą: http://www.zurnalai.vu.lt/teise/article/view/10779/8959.
12. ZALESKIS, Julius, Duomenų apsaugos pareigūno veiklos pagrindai pagal ES bendrąjį duomenų apsaugos reglamentą. Teisė, 2017, t. 104. Prieiga per internetą: http://www.zurnalai.vu.lt/teise/article/view/10851/8986.
13. PETRAITYTĖ, Ilona, Asmens duomenų teisinės apsaugos principai: daktaro disertacija. Vilnius: Vilniaus universitetas, 2013. Prieiga per internetą: http://www.tf.vu.lt/wp-content/uploads/2016/08/Ilona-Petraityt%C4%97_Asmens-duomen%C5%B3-teisin%C4%97s-apsaugos-principai-.pdf.
14. PETRAITYTĖ, Ilona, Asmens duomenų apsauga ir teisė į privatų gyvenimą. Teisė, 2011, t. 80; Prieiga per internetą: http://www.journals.vu.lt/teise/article/view/158/124.
15. CIVILKA, M. IR ŠLAPIMAITĖ, L. Asmens duomenų samprata elektroninėje erdvėje. Teisė. 2015. t. 95; Prieiga per internetą: http://www.zurnalai.vu.lt/teise/article/view/8761/7647.
16. VAIŠVILA, Alfonsas. Teisės teorija: vadovėlis. Vilnius: Justitia, 2000.
17. VAN ALSENOY, Brendan. Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation, 7. 2016. JIPITEC 271 para 15, Prieiga per internetą: https://www.jipitec.eu/issues/jipitec-7-3-2016/4506/van_alsenoy_liability_under_eu_data_protection_law_jiptec_7_3_2016_271.pdf.
18. Lachaud, Eric. Should the DPO be certified? International Data Privacy Law, 2014, Vol. 4, No. 3, p. 189- 202. Prieiga per internetą:https://www.scribd.com/document/350068564/Should-the-DPO-Be-Certified.
19. KOKOTT, Juliane; SOBOTTA, Christoph. The distinction between privacy and data protection in the jurisprudence CJEU and the ECtHR. *International Data Privacy Law*, 2013, Vol. 3, No. 4 p. 222- 228, Prieiga per internetą: https://watermark.silverchair.com/ipt017.pdf.

20. JANUŠEVIČIENĖ, Justina. *Praktiniai asmens sveikatos duomenų tvarkymo aspektai pagal bendrąjį asmens duomenų apsaugos reglamentą*. Teisė. 2018. T. 107; Prieiga per internetą: <https://www.zurnalai.vu.lt/teise/article/view/11674/10258>

Teismų praktika:

21. Europos Žmogaus Teisių Teismas (Didžioji kolegija). 2019 m. spalio 17 d. sprendimas byloje *Lopez Ribalda ir kiti prieš Ispaniją* (paraiškos Nr. 1874/13 ir 8567/13). Prieiga per internetą: https://hudoc.echr.coe.int/fre#{%22fulltext%22:[%22lopez%20ribalda%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-197098%22]}.
22. Europos Sąjungos Teisingumo Teismo 2018 m. birželio 5 d. sprendimas byloje C-210/*16 Wirtschaftsakademie Schleswig-Holstein*, EU:C:2018:388, 43 par. Prieiga per internetą: http://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=4877022.
23. Europos Sąjungos Teisingumo Teismo 2018 m. liepos 10 d. sprendimas byloje C-25/17 *Jehovan todistajat*, EU:C:2018:551, 68 par. Prieiga per internetą: http://curia.europa.eu/juris/document/document.jsf?text=&docid=203822&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=4876877.
24. Europos Sąjungos Teisingumo Teismas. 2019 m. spalio 1 d. sprendimas *Planet49 GmbH* C- 673/17, EU:C:2019:801. Prieiga per internetą: http://curia.europa.eu/juris/document/document.jsf;jsessionid=B542D71188C4C1DA290A6EE2BAA843F3?text=&docid=218462&pageIndex=0&doclang=LT&mode=req&dir=&occ=first&part=1&cid=1821361.
25. Lietuvos vyriausiojo administracinio teismo 2011 m. balandžio 15 d., nutarimas byloje Nr. N62-939/2011. Prieiga per internetą: < https://eteismai.lt/byla/97187080245856/N-62-939-11>.
26. Lietuvos vyriausiojo administracinio teismo 2013 m. gegužės 23 d. nutartis byloje Nr. A822-1173-13 UAB „Init“ prieš Valstybinę duomenų apsaugos inspekciją. Prieiga per internetą: < https://eteismai.lt/byla/245492016270101/A-822-1173-13?word=init.

***Soft law* šaltiniai:**

27. ES 29 str. darbo grupės 2017 m. spalio 4 d. *Poveikio duomenų apsaugai vertinimo (PDAV) gairės, kuriomis Reglamento 2016/679 taikymo tikslais nurodoma, kaip*

nustatyti, ar duomenų tvarkymo operacijos gali sukelti didelį pavojų Nr. WP248, p. 16 Prieiga per internetą:https://ec.europa.eu/newsroom/article29/itemdetail.cfm?item_id=611236.

28. ES 29 str. darbo grupės 2010 m. vasario 16 d. *Nuomonė Nr. 1/2010 dėl sąvokų „duomenų valdytojas“ ir „duomenų tvarkytojas“* Nr. WP169, p. 9. Prieiga per internetą: <https://ec.europa.eu/justice/article29/documentation/opinionrecommendation/files/2010/wp169_lt.pdf
29. ES 29 str. darbo grupės 2017 m. balandžio 5 d. *Duomenų apsaugos pareigūnų gairės* Nr. WP 243, p. 23. Prieiga per internetą:https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048.
30. ES 29 str. darbo grupės 2017 m. spalio 3 d. *Administracinių baudų taikymo ir nustatymo pagal Reglamentą 2016/679 gairės* Nr. WP253, p. 4 .Prieiga per internetą: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237.
31. Europos Taryba: Europos duomenų apsaugos vadovas, Liuksemburgas: Europos Sąjungos leidinių biuras, 2014 m. p. 49. Prieiga per internetą: https://www.echr.coe.int/Documents/Handbook_data_protection_LIT.pdf.
32. Valstybinės duomenų apsaugos inspekcijos viešoji konsultacija*: Bendrasis duomenų apsaugos reglamentas. Ginama teisė susipažinti su savo asmens duomenimis*. Prieiga per internetą: https://vdai.lrv.lt/lt/naujienos/bendrasis-duomenu-apsaugos-reglamentas-ginama-teise-susipazinti-su-savo-asmens-duomenimis.
33. Valstybinė duomenų apsaugos inspekcija. *Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams*, 2019 – 12 – 18, p. 8- 17. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/VDAI_saugumo_priemoniu_gaires-2019-12-18.pdf..
34. ES 29 str. darbo grupės 2018 m. vasario 6 d. *Gairės dėl pranešimo apie asmens duomenų saugumo pažeidimą pagal Reglamentą* (ES) 2016/679 Nr.WP250, p. 29 Prieiga per internetą: https://ec.europa.eu/newsroom/article29/itemdetail.cfm?item_id=612052.
35. Valstybinė duomenų apsaugos inspekcija. *Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams*, 2019 – 12 – 18, p. 8- 17. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/VDAI_saugumo_priemoniu_gaires-2019-12-18.pdf.
36. Valstybinės duomenų apsaugos inspekcijos viešoji konsultacija*: Bendrasis duomenų apsaugos reglamentas. Ginama teisė susipažinti su savo asmens duomenimis*. Prieiga

per internetą: https://vdai.lrv.lt/lt/naujienos/bendrasis-duomenu-apsaugos-reglamentas-ginama-teise-susipazinti-su-savo-asmens-duomenimis.

SANTRAUKA

2018 m. gegužės 25 d. įsigaliojus BDAR, įgyvendinta ES asmens duomenų apsaugos teisės reforma. Ši reforma į duomenų apsaugos teisę įnešė ne tik teigiamų aspektų, kaip išplėstos duomenų subjektų teisės, padidintos duomenų valdytojo atsakomybės ribos, bet ir nemažai neaiškumų. Naujai įtvirtinta duomenų apsaugos pareigūno pareigybė nėra iki galo aiški, o pakankamai abstrakčios BDAR nuostatos, suteikia didelę terpę skirtingoms interpretacijoms. Iškyla klausimu vertinant duomenų valdytojo ir duomenų apsaugos pareigūno santykius. Sparčiai vystantis informacinėms technologijoms, didėjant galimų pavojų saugumui įvairovei iškyla labai svarbus atsakomybės pasidalinimo klausimas. Todėl šio darbo tikslas atskleisti kaip atribojama duomenų valdytojo ir duomenų apsaugos pareigūno atsakomybė remiantis asmens duomenų apsaugos teisės aktais.

Magistro darbe atskleidžiama duomenų valdytojo ir duomenų apsaugos pareigūno samprata, analizuojamos duomenų valdytojui priskiriamos pareigos bei duomenų apsaugos pareigūno veiklos principai. Vertinant duomenų apsaugos pareigūną, atskleidžiamas „kitoks“ jo statusas duomenų valdytojo organizacijoje, nepriklausomai ar tai, duomenų valdytojo darbuotojas ar išorės partneris.

Siekiant nustatyti atsakomybę atskiriančius aspektus vertinta tiek šių dviejų duomenų apsaugos teisės subjektų atsakomybės atskirtis siekiant duomenų apsaugos teisės normų atitikties, tiek atsakomybės atribojimą nustačius asmens duomenų apsaugos teisės pažeidimus.

Atlikta teisės normų ir *soft law* šaltinių analizė leido nustatyti, jog tiek atitikties teisės aktų reikalavimams atsakomybė, tiek atsakomybė dėl nustatytų pažeidimų tenka duomenų valdytojui. Šią atsakomybę nustato BDAR normos bei suponuoja jam suteiktos pareigos. Duomenų apsaugos pareigūnas neturi teisės priimti sprendimus, jis įpareigotas stebėti duomenų valdytojo vykdomą duomenų tvarkymo procesą bei teikti konsultacijas, dėl duomenų valdytojo veiklai taikytinų teisės aktų reikalavimų. Duomenų valdytojo turimos pareigos bei suteikta kompetencija savaimę sąlygoja pilnos apimties atsakomybės atsiradimą. Vienintelis atvejis, kuomet duomenų apsaugos pareigūnui tenka atsakomybė, kai duomenų valdytojas patiria žalą, dėl asmeninių duomenų apsaugos pareigūno neteisėtų veiksmų. Tokiu atveju taikytinos DK arba CK atsakomybę nustatančios normos.

SUMMARY

The Relation of the Responsibility of the Data Protection Officer and the Data Controller for Compliance with Data Protection Law

Since the entry into force of the GDPR, the reform of EU personal data protection law has been implemented. This reform has brought not only positive aspects to data protection law, such as the extension of data subject's rights, increased limits on the data controller's liability, but also many uncertainties. The newly established post of data protection officer is not entirely clear, but rather sufficiently abstract in the GDPR, providing ample scope for differing interpretations. The issue arises when it comes to needing to draw a line in the relationship between the controller and the data protection officer. With the rapid development of information technology and the increasing diversity of potential security threats, the issue of shared responsibility comes into the first place. Therefore, the purpose of this work is to reveal how the responsibilities of the data controller and the data protection officer under personal data protection legislation are delimited. The master 's thesis reveals the concept of data controller and data protection officer, analyzes the duties assigned to the data controller and the principles of activity of the data protection officer. The evaluation of the data protection officer reveals a "different" status in the controller's organization, whether it is an employee of the controller or an external partner. To determine the aspects separating liability, both the separation of liability of these two data protection law subjects to comply with the data protection law norms as well as the delimitation of liability in case of violations of personal data protection, law was assessed. The analysis of legal norms and soft law sources revealed that both the responsibility for compliance with legal requirements and liability for identified violations rests with the data controller. This responsibility is determined by the norms of the GDPR and presupposes the duties assigned to it. The Data Protection Officer is not entitled to take decisions, he is obliged to monitor the data processing process carried out by the data controller and to provide advice on the requirements of the legal acts applicable to the activities of the data controller. The duties held by the data controller and the competence granted automatically result in the occurrence of full liability. The only case in which the liability of the Data Protection Officer may be established is his own fault or improper performance of the contract governing the provision of the Data Protection Officer’s services.